



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

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBERCRIMES AND LEGAL REMEDIES IN INDIA: AN ANALYSIS OF THE LEGAL FRAMEWORK AND JUDICIAL APPROACH

~ Fizza Jafar

ABSTRACT

The rapid expansion of digital technology has transformed communication, commerce, education and public administration in India. Alongside these developments, cybercrimes have emerged as a significant legal and social concern. India has developed a legal framework to address cybercrimes but the changing nature of technology continues to expose gaps in investigation, enforcement and victim protection. This article examines the statutory framework and discusses judicial decisions that have shaped cyber law. It also considers the legal remedies available to victims and the challenges faced by enforcement agencies. The article argues that effective cybercrime control requires not only legislation but also timely investigation, digital awareness, institutional coordination and safeguards for fundamental rights.

KEYWORDS: Cybercrime, Information Technology Act, 2000, Digital Personal Data Protection Act, Cybersecurity, Electronic Evidence, Legal Remedies.

INTRODUCTION

In today's world, digital technology is a part of everyday life. Services have become more accessible and more efficient through online banking, digital payments, social media, e-commerce and electronic communication. But the increased reliance on digital platforms has also generated opportunities for criminal activities that can be carried out from afar, rapidly and in some cases across national borders. Cybercrime no longer just involves attacks on

computer systems but also includes offences where digital platforms are used to deceive, threaten, exploit or harm others.

In India, the Information Technology Act, 2000 (IT Act) was enacted to give legal recognition to electronic records and electronic transactions and to address offences relating to computer resources. Later, legal developments such as the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and the Digital Personal Data Protection Act, 2023 (DPDP Act) have also contributed to the legal framework for addressing digital offences. The challenge is to apply these laws effectively while protecting constitutional rights, including freedom of speech and the right to privacy. This article examines the meaning and forms of cybercrime, the legal framework in India, relevant judicial decisions, available remedies and the difficulties that continue to affect enforcement.

MEANING OF CYBERCRIMES

Cybercrime generally refers to unlawful activities in which a computer, computer system, computer network or digital platform is used as a tool, target or means of committing an offence. The IT Act does not provide one exhaustive definition covering every form of cybercrime. Instead, it identifies and penalises particular activities involving computer resources and electronic communication.

Broadly, cybercrimes can be divided into two categories:

Cyber-Dependent Crimes: These are crimes in which computer systems or networks are targets. Examples include hacking, unauthorized data manipulation, and shutting down networks through digital attacks.

Cyber-Enabled Crimes: These are traditional crimes where technology is just used as a means of making the crime easier, faster or broader in scope. These include activities such as digital cheating, online extortion, stalking, harassment and the digital distribution of illegal content, all of which remain punishable under traditional criminal laws.

MAJOR FORMS OF CYBERCRIMES IN INDIA

Cybercrimes in India involve diverse offences targeting systems, data and individuals through digital means:

HACKING AND UNAUTHORIZED ACCESS

Hacking refers to an unauthorized access to information technology systems, such as computers, computer accounts or networks. Hacking may involve obtaining information through theft; altering data; impacting services and gaining control over computers. Section 43 of the IT Act provides compensation for unauthorised acts; Section 66 criminalises such acts when done dishonestly, with imprisonment for a term of up to three years, or a fine of up to ₹5 lakh, or both.

IDENTITY THEFT AND ONLINE IMPERSONATION

Identity theft involves the fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. Section 66C of IT Act deals with identity theft and Section 66D deals with cheating by personation by using communication devices or computer resources. Such offenses may occur via fake social media accounts, fake websites, emails or other types of online communication.

PHISHING AND ONLINE FINANCIAL FRAUD

Phishing is a method of sending messages or communications with an intention of gathering sensitive information from the victims, such as passwords and the details of the bank accounts. With this information, the perpetrator may conduct unauthorised transactions, attracting Sections 66C and 66D of the IT Act and, depending on the facts, Sections 318 and 319 of the BNS.

CYBERSTALKING, BULLYING AND ONLINE HARASSMENT

Digital platforms may be used to threaten, intimidate, stalk or bully individuals. Online harassment and cyberstalking may involve repeated unwanted contact without consent, sending threatening messages, or attempting to intimidate or manipulate the victim. Based on the actions taken, different provisions of BNS and respective sections of IT Act may apply. Where the victim is a woman or a child, additional legal provisions may apply, depending on the circumstances.

DATA THEFT AND BREACH OF PRIVACY

Personal and corporate information may be accessed, obtained or misused without authorisation. Personal information of financial and identity-related nature can be retrieved as a result of data breach. Sections 43 and 66 of the IT Act may apply to certain unauthorised acts,

while the DPDP Act establishes a framework for the processing of digital personal data in accordance with its provisions.

MALWARE AND RANSOMWARE

Malware is a type of software used to impair, alter, monitor or obtain unauthorized access to computer systems. Ransomware can be defined as malicious software which can limit access to documents and ask for money for restoration of documents. Attacks can be made against particular companies, institutions, hospitals, educational organizations, and public organizations.

FRAMEWORK FOR CYBERCRIME IN INDIA

India's cybercrime framework comprises the following legislation:

INFORMATION TECHNOLOGY ACT, 2000

The IT Act is the principal Indian law dealing specifically with electronic records, electronic transactions and various computer-related offences. It recognises electronic records and provides a legal basis for addressing unlawful activities involving computer resources.

Important provisions include:

Section 43: Provides for compensation in respect of specified unauthorised acts involving computer systems or networks.

Section 65: Penalises tampering with computer source documents in the circumstances covered by the provision.

Section 66: Criminalises specified acts under Section 43 when committed dishonestly or fraudulently.

Section 66C: Addresses identity theft involving electronic signatures, passwords or other unique identification features.

Section 66D: Deals with cheating by personation using a communication device or computer resource.

Section 66E: Addresses violation of privacy through the capturing, publishing or transmitting of images of a person's private area without consent, in the circumstances specified.

Sections 67, 67A and 67B: Address the publication or transmission of obscene material, sexually explicit material and material depicting children in sexually explicit acts, respectively.

Section 69A: Provides a statutory framework for blocking public access to information in specified circumstances.

Section 70B: Provides for CERT-In and its functions relating to cybersecurity incident response.

BHARATIYA NYAYA SANHITA, 2023

The BNS, which came into force on 1 July 2024, replaced the Indian Penal Code, 1860. It is relevant where cyber-enabled conduct also constitutes a general criminal offence, including cheating, criminal intimidation, extortion, stalking, forgery or offences against women and children. The application of the BNS depends on the facts and ingredients of the particular offence. The IT Act and BNS may operate alongside one another where their respective legal requirements are met.

THE BHARATIYA SAKSHYA ADHINIYAM, 2023

The Bharatiya Sakshya Adhiniyam, 2023 replaced the Indian Evidence Act, 1872, with effect from 1 July 2024. It contains provisions regarding the admissibility and proof of electronic and digital records. The law is particularly important in cybercrime cases where messages, emails, call records, CCTV footage, device data and transaction records may all form part of the evidence. The statutory requirements for producing and proving electronic records must be followed to ensure their evidentiary reliability.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The DPDP Act serves as a regulating law for digital personal data processing. It defines the responsibilities of data fiduciaries and grants individuals, called data principals, certain rights over their personal data. The Act is helpful in the broader context of curbing and regulating misuse of the data. The Act and the DPDP Rules, 2025 provide the framework for implementation, with the applicable provisions operating according to the notified enforcement timeline.

JUDICIAL APPROACH TO CYBER CRIMES AND DIGITAL RIGHTS

Judicial decisions have clarified the relationship between cyber regulation, constitutional rights, electronic evidence and intermediary responsibility.

***Shreya Singhal v. Union of India*¹**

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

In this case, the Supreme Court declared Section 66A of the IT Act unconstitutional for violating the right to freedom of speech and expression under Article 19(1)(a) of the Constitution. This decision is important because it means restrictions on online speech must fall within the bounds of the Constitution. The decision also addressed aspects of intermediary liability and the statutory blocking framework.

Justice K.S. Puttaswamy (Retd.) v. Union of India²

In this case, a nine-judge bench of the Supreme Court recognised the right to privacy as a fundamental right protected by the Constitution. The judgment has important implications for digital privacy, personal data and state action involving information. It provides a constitutional foundation for evaluating laws and practices that affect personal information and individual autonomy.

Anvar P.V. v. P.K. Basheer³

The Supreme Court considered the admissibility of electronic records under the former Indian Evidence Act. In this case, the Court explained the importance of complying with Section 65B for the admissibility of secondary electronic evidence. Although the BSA now governs evidence in proceedings to which it applies, the judgment remains important for understanding the development of Indian electronic-evidence law.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal⁴

In this case, the Supreme Court reiterated and clarified the requirements relating to certificates for electronic records under the erstwhile Section 65B of the Evidence Act. The Court also considered the circumstances in which such a certificate could be obtained and clarified the role of the court in dealing with electronic evidence.

Sharat Babu Digumarti v. Government of NCT of Delhi⁵

The Supreme Court considered the application of the IT Act to alleged obscenity in electronic form. The judgment explained the role of the IT Act as a special legislation dealing with

²*K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

³*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).

⁴*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).

⁵*Sharat Babu Digumarti v. Gov't of NCT of Delhi*, (2017) 2 SCC 18 (India).

offences involving electronic records and the relationship between its provisions and general criminal law. It is relevant to the interpretation of cyber-specific offences.

***Internet and Mobile Association of India v. Reserve Bank of India*⁶**

In this case, the Supreme Court examined the RBI circular that prohibited regulated entities from providing services in relation to virtual currencies. The Court held the circular to be disproportionate and accordingly set aside the RBI circular. Although the case was not a direct prosecution for cybercrime, it is relevant to the regulation of digital financial activity and the relationship between technological innovation and regulatory action.

LEGAL REMEDIES AND REDRESSAL MECHANISMS AVAILABLE TO VICTIMS

Victims may avail the following legal remedies under Indian law:

POLICE COMPLAINT

A victim may report a cyber offence to the local police or a cybercrime police station. Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) provides the procedure for reporting information relating to a cognizable offence. This gives the victim a formal legal route to initiate criminal action against the offender. The victim should also preserve screenshots, URLs, transaction records, emails and messages, as these may be useful as electronic evidence during the investigation.

ONLINE CYBERCRIME REPORTING MECHANISM

A victim may also seek redressal by filing a complaint through the National Cyber Crime Reporting Portal at cybercrime.gov.in. The portal allows victims to report cyber offences online and track their complaints. It is particularly useful for reporting financial fraud and offences against women and children. However, filing a complaint only starts the reporting and investigation process and does not by itself guarantee recovery of money or a favourable outcome.

FINANCIAL FRAUD REPORTING AND BANKING REMEDIES

In cases of online financial fraud, the victim may report the fraud by calling 1930 and immediately informing the concerned bank. This allows the bank and the authorities to take

⁶*Internet & Mobile Ass'n of India v. Reserve Bank of India*, (2020) 10 SCC 274 (India).

timely steps to trace or freeze the transferred funds, where possible. The victim may also be protected from liability for unauthorised transactions under the RBI's customer-protection rules, depending on the circumstances and the time taken to report the fraud. Thus, prompt reporting provides an important remedy, although recovery of the lost money is not always possible.

COMPENSATION UNDER THE INFORMATION TECHNOLOGY ACT, 2000

A victim may seek compensation under Section 43 of the Information Technology Act, 2000 for certain unauthorised acts involving computer systems, data or computer resources. Section 46 provides for adjudication of such claims, while Section 47 sets out factors relevant to determining compensation, including the loss caused and the wrongful gain made by the person responsible. The remedy is intended to provide financial relief to a person who suffers loss or damage due to such unauthorised acts.

REMEDIES UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

A person whose digital personal data is misused may seek redressal under the Digital Personal Data Protection Act, 2023. The person can first raise a grievance with the concerned data fiduciary and, if the grievance is not resolved, approach the Data Protection Board in accordance with the Act.

REMOVAL OF UNLAWFUL CONTENT AND GRIEVANCE REDRESSAL

A victim whose unlawful or harmful content is shared online may approach the platform's grievance officer under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2026. The grievance mechanism provides a way for the victim to request removal or disabling of unlawful content within the prescribed time limits. For certain serious forms of content, such as material involving nudity, sexual acts, morphing or impersonation, the rules provide for quicker action. If the victim is not satisfied with the platform's response, the victim may use the available appellate mechanism or approach a court for appropriate relief, including removal of the content or an injunction. Government blocking of online content is separately dealt with under Section 69A of the Information Technology Act, 2000.

CHALLENGES IN CYBER LAW ENFORCEMENT

Statutory provisions exist, but it is difficult to enforce them effectively. There is a serious concern about the technical complexity of cyber offences. Investigators will need specialist knowledge of networks, digital devices, encryption, cloud services and electronic payment systems. A shortage of trained personnel and forensic facilities can delay investigations.

Another challenge is that cybercrime crosses borders. The data may be stored in a foreign country while the victim and offender are in different parts of India or outside India. Obtaining evidence from overseas service providers may require formal legal cooperation and may take considerable time.

The rapid development of technology also creates new forms of misuse. Artificial intelligence can be used to generate convincing impersonations, manipulated images, synthetic audio and fraudulent messages. Existing laws may apply to particular conduct, but the identification of the offender, preservation of evidence and determination of liability may remain difficult.

Victims may also be reluctant to report offences because they are embarrassed or fear harm to their reputation or are unsure about the reporting process. In cases of financial fraud, delayed reporting may reduce the opportunity for timely intervention. Furthermore, the delicate balance between cybersecurity and constitutional freedoms has to be taken into account. Overbroad restrictions or poorly implemented surveillance measures may affect privacy and freedom of expression.

RECOMMENDATIONS FOR STRENGTHENING THE LEGAL FRAMEWORK

The following measures are recommended to strengthen India's cybercrime framework:

First, police officers, prosecutors, judges and forensic personnel should be trained specifically to improve their handling of electronic evidence and technically complex offences. Cybercrime units should have adequate resources and access to reliable forensic facilities.

Second, awareness should be raised through educational institutions, banks, government agencies and digital platforms. People need to be educated on common fraud schemes, secure password habits, multi-factor authentication and the need to report suspicious activity promptly.

Third, coordination between law enforcement agencies, banks, intermediaries and cybersecurity institutions should be improved. Timely communication and legally compliant

evidence-preservation procedures can assist investigations, particularly in financial fraud and data-breach cases.

Fourth, data protection obligations should be clear and consistently enforced. Organisations that collect or process personal data should adopt appropriate security safeguards, restrict unnecessary access and respond to breaches in accordance with applicable law.

Finally, enforcement of cybercrime should be consistent with constitutional principles. Regulatory and investigatory powers should be exercised with appropriate safeguards, accountability and access to remedies under clear legal authority. The objective should be to address unlawful conduct without imposing unjustified restrictions on legitimate digital activity.

CONCLUSION

Cybercrime is a continuing challenge in India's increasingly digital society. The Information Technology Act, 2000, together with the BNS, the BSA, the DPDP Act and the applicable rules, provides a framework for addressing different aspects of cyber offences, digital evidence and personal data protection. Judicial decisions have also clarified important principles concerning online speech, privacy, electronic evidence and the interpretation of cyber-specific legislation.

However, the existence of laws alone cannot ensure effective protection. Timely reporting, technically competent investigation, reliable digital evidence, institutional cooperation and public awareness are equally important. The legal framework must also remain responsive to emerging technologies while respecting fundamental rights. A balanced approach—one that combines enforcement, prevention, accountability and constitutional safeguards—is necessary to strengthen trust and safety in India's digital environment.

REFERENCES

Statutes

1. Information Technology Act, 2000 (Act 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
2. Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
3. Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).
4. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
5. Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

Rules, notifications and circulars

6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), 25 February 2021.
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified by MeitY on 10 February 2026 (G.S.R. 120(E)), in force from 20 February 2026.
8. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025, Ministry of Electronics and Information Technology, Government of India.
9. Reserve Bank of India, Circular DBR.No.Leg.BC.78/09.07.005/2017-18, Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, 6 July 2017.

Official portals

10. National Cyber Crime Reporting Portal, Ministry of Home Affairs, <https://cybercrime.gov.in>
11. Indian Computer Emergency Response Team (CERT-In), <https://www.cert-in.org.in>
12. India Code (for official texts of the Acts), <https://www.indiacode.nic.in>
13. Ministry of Electronics and Information Technology, <https://www.meity.gov.in>
14. National Crime Records Bureau, Crime in India (annual report), <https://ncrb.gov.in>