

EVOLUTION OF CYBER FRAUD COMPLAINT AND REDRESSAL MECHANISMS IN INDIA: A REVIEW OF LAWS, POLICIES, AND INSTITUTIONAL PRACTICE

Research Scholar: Chandra Deep Singh

Supervisor: Dr. Mithlesh malviya, Associate Professor

Career Point University, Kota, Rajasthan (India)

Abstract

Individuals, businesses, and government agencies in India are all feeling the effects of cybercrime, which has emerged as a major problem in the country's digital economy. Online financial services, e-commerce, digital payment systems, and the Internet have all grown rapidly in recent years, but so have cybercrimes including financial fraud, identity theft, phishing, ransomware, and online scams. In reaction, India has strengthened its system for receiving and processing complaints about cybercrime through new laws, revised policies, improved institutional procedures, and technological initiatives. This research article examines the legislative framework, including the IT Act, 2000, the BNS, 2023, and other relevant statutes, to critically examine the rise of cybercrime complaint and redressal systems in India.

Important judicial decisions, inter-agency collaboration mechanisms, and governmental actions to strengthen cybercrime investigation and victim compensation are also highlighted in the study. Major challenges such as cybercrime underreporting, jurisdictional complexities, hackers' exploitation of technological developments, investigative delays, inadequate digital forensic infrastructure, and public awareness are brought to light. The study finds that in order to create a redressal mechanism that is efficient, accessible, and victim-centric, there needs to be consistent legislative reforms, institutional capacity building, stakeholder coordination, and public awareness, even though India has made great strides in developing a comprehensive cybercrime complaint and redressal ecosystem. This evaluation provides a thorough understanding of how cybercrime governance in India has evolved over time and suggests ways to strengthen institutional and legal responses to growing cyber threats.

Keywords: Cybercrime, Cyber Crime Complaint Mechanism, Redressal Mechanism, Financial Frauds, IT Act, 2000, BNS, 2023,.

1.1 Introduction

Technology, the spread of the internet, and the rise of online banking have all had a significant impact on India's economy and governance. Internet banking, mobile wallets, e-commerce, Digital India, and the expansion of the Unified Payments Interface (UPI) are examples of government initiatives that have significantly enhanced digital accessibility and financial inclusion. People, companies, and financial institutions are more susceptible to cybercrimes, especially financial scams, as a result of these advancements, which have hastened economic growth and enhanced the delivery of public services. Many people have lost a lot of money and lost faith in digital financial systems because

cybercriminals are getting smarter and using new technologies to commit frauds like phishing, identity theft, malware attacks, SIM-swap, online investment, QR code, and illegal electronic fund transfers.¹

The number of reports of cybercrime in India has skyrocketed in the last decade, with financial crimes making up the bulk of these cases. Legislative changes, institutional cooperation, technical innovation, public awareness campaigns, and the growing sophistication of cyber offenses have all being pushed by the Indian government to bolster corrective and preventative measures. As a result, various regulatory directives issued by the RBI (RBI) and the “BNS, 2023, BNSS, 2023, Bharatiya Sakshya Adhiniyam, 2023”, the Payment and Settlement Systems Act, 2007, and the IT Act, 2000 have contributed to a more comprehensive regulatory framework that governs cyber crime.²

In response to the growing danger of cyber-enabled financial crimes, the government has set up various specialized agencies and channels for citizens to lodge complaints. National Cyber Crime Reporting Portal, “Citizen Financial Cyber Fraud Reporting and Management System, Indian Cyber Crime Coordination Centre (I4C)”, and the National Cyber Crime Helpline (1930) are among them. These efforts are made to make it easier to register complaints quickly, for law enforcement to work together better, for fraudulent transactions to be frozen in real-time, and for stolen cash to be recovered more easily. Simultaneously, the RBI has instituted regulatory steps to fortify the safety of online payments, safeguard consumers, and hold financial institutions to account when illegal electronic transactions occur.³

In India, the courts have been instrumental in developing the country's cyber jurisprudence through its interpretations of statutes pertaining to digital transactions, consumer protection, privacy rights, intermediary responsibility, electronic evidence, and intermediary liability. The constitutional concepts that govern digital governance have been reinforced by judicial rulings that have also defined the roles of government authorities, investigative agencies, intermediaries, and banks. The Supreme Court's recognition of the right to privacy as a basic right has had a further influence on India's cyber regulatory framework. This framework focuses on the protection of personal data and informational privacy in the digital era.⁴

There are still a number of obstacles that make cyber crime reporting and redressal systems less effective, even with these major institutional and legislative changes. Important issues that need to be addressed include investigative delays, poor reporting rates, insufficient cyber forensic infrastructure, a lack of qualified staff, complicated jurisdictional issues, cyber offenses that span international borders, public ignorance, and the difficulty in recovering monies that have been unlawfully moved. It is essential to constantly innovate policies and improve capacity since cyber dangers are changing at a faster rate than legislation and institutions can keep up with them.⁵

¹ References: (1) Digital India Programme, Ministry of Electronics and Information Technology, Government of India, 2015; (2) RBI Annual Report 2024-25 (2025).

² The following is a list of legislation passed in India: “the IT Act of 2000 (Act No. 21 of 2000), the BNSS Act of 2023 (Act No. 45 of 2023), the BNSS Act of 2023 (Act No. 46 of 2023), the BSAH Act of 2023 (Act No. 47 of 2023), and the PAS Act of 2007 (Act No. 51 of 2007);”.

³ (Updated for 2024) The Ministry of Home Affairs' Indian Cyber Crime Coordination Centre (I4C); the RBI's National Cyber Crime Reporting Portal

⁴ Cases decided by retired Justice K.S. Puttaswamy include Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473, Shreya Singhal (2015) 5 SCC 1, and UOI v. v. (2017) 10 SCC 1.

⁵ Sources: Ministry of Home Affairs Annual Report 2024-2025; NCRB Crime in India 2024; RBI Report on Banking Trends and Progress 2024-2025.

Within this context, this review article analyses the development of laws, policies, institutional frameworks, regulatory activities, and judicial reactions pertaining to cyber financial frauds in India, as well as the growth of procedures for filing complaints and seeking redress for cyber crimes. It draws on a review of the literature to assess the efficacy of the present administrative and legislative framework, finds ongoing problems with victim redressal and complaint registration, and draws attention to new changes that might improve India's cyber governance system. By outlining areas where research is lacking and offering suggestions on how to improve a cyber complaint and redressal system that is victim-centric, efficient, and technologically strong, this review hopes to add to the scholarly conversation.

1.2 Emerging Trends of Cyber Crimes in India

Both the economy and society in India have benefited greatly from the digital revolution that has recently swept the nation as a result of the extensive use of the internet. On the other hand, cybercrimes—which involve fraud, data theft, or system disruption—have flourished thanks to this shift. The frequency of cyberattacks in India, ranging from malware and phishing to more complex forms of cybercrime, has been steadily rising in recent years.

An alarming trend in India's cybercrime landscape is the exponential growth of online fraud and financial crimes. Statistics show that cybercrime in India has been a growing problem, with millions of complaints filed in 2023 and 2024 alone. The National Cybercrime Reporting Portal (NCRP) received over 17,000 complaints in 2024, up from 1,37,000 in 2021. The majority of these complaints were related to digital fraud and online financial crimes. In 2024, cyber fraud was expected to have cost more than ₹22,800cr.⁶

Assigned to the appropriate states or union territories (UTs) automatically, cybercrime complaints can be registered on the”, NCRP of the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs”,. It has been made clear that the power to lien, freeze, or unfreeze bank accounts does not reside with NCRP or I4C. According to the rules of BNSS/CrPC, the onus is on the LEAs of the individual states and union territories to ensure compliance. No administrative supervision over LEA operations within States/UTs is exerted by the Indian Cyber Crime Coordination Centre; it only provides a venue for complaints. As far as cybercrime prevention and detection activities are concerned, the only thing that I4C can do is work with LEAs and other interested parties.⁷

The "digital arrest" scam is a prevalent kind of financial fraud in which con artists pretend to be official government officials or law enforcement and coerce victims into sending money in order to evade capture or legal action. Cybercrimes of this kind cost various states thousands of crores of rupees annually, and they disproportionately affect the elderly and others without computer sophistication.

Cybercriminals continue to use phishing and social engineering as their primary methods of operation. These attacks utilize bogus messages, emails, or websites to deceive users into disclosing sensitive information such as login credentials, bank account information, or passwords. Scammers may now more readily propagate incredibly false texts and even audio or video recordings that appear like renowned individuals, owing to the growth of artificial intelligence (AI).

⁶ NCRB, 2023, Crime in India 2022: Statistics. Decision in Sabu Mathew George v. UOI, Ministry of Home Affairs, Government of India (2017) 5 SCC 360.

⁷ https://www.ijssr.com/wp-content/uploads/journal/published_paper/volume-3/issue-1/IJSSR30820.pdf

These days, AI-driven risks are more than just a fad; they're a real source of concern. Cybercriminals are becoming more cunning as they employ machine learning to create digital traps, malicious programs, and phishing emails that may bypass traditional security measures. This is about more than simply the increased frequency of these attacks. They are more lifelike, which is problematic for both average people and cyber security personnel. Infostealer, Lumma Stealer, and RedLine are just a few examples of the ransomware and malware that has infected tens of thousands of machines and stolen sensitive financial and login information. Additionally, ransomware assaults are on the rise. When hackers get control of a computer, they often demand payment before releasing it. Everywhere you look, essential services like schools and hospitals are taking a blow. Cybercriminals are also aiming their sights at mobile and identification systems. For instance, new frauds like SIM swaps and others that exploit Aadhaar-SIM linkages are cropping up everywhere. Criminals typically operate from across borders, making it difficult for authorities to detect when they exploit vulnerabilities in telecom and identification checks. As a result, they steal money or get access to accounts. International operations and organized criminal rings entangled with the Indian cybercrime scene operate frauds using global networks. Because of this, apprehending and punishing them becomes much more difficult.⁸

1.3 Laws, Provisions, and Legal Framework

This Sec. provides an overview of the main laws, regulations, and legal processes that India use to control and punish cybercrimes⁹.

a) *Primary Statutes*

- IT Act, 2000 and amendments: India is largely ruled by the IT. Electronic records and digital signatures are defined under Sec.s 66, 66A, 66B, 66C, 66D, 66E, 67, and 69 of the Act, which also lists certain offenses and associated penalties.
- It was revised in 2008 to incorporate new cybercrimes, intermediary liability requirements, and the idea of "reasonable security practices."
- The IT (Amendment) Act was changed to add sections 69A (authority to prohibit for public interest), 69B (monitoring), and 79 (safe harbor for intermediaries). According to the IT Act, the Indian Computer Emergency Response Team, or CERT-In, has the authority to require that cybersecurity incidents be reported, particularly through guidelines.

b) *BNS, 2023¹⁰*

Sec. 75: By "sexual harassment" we mean any form of unwanted sexual advances, including those made via technological means, and "sexually oriented remarks" refers to actions of exhibiting pornography against someone's will.

Sec. 77: Taking or sharing private photos (typically in cyber or digital settings) without permission is called voyeurism.

Sec. 78: This clause applies to cyberstalking, which involves monitoring and tracking someone's internet activity.

⁸ CyberCERT-In Indian Journal, Rules and Guidelines for Reporting Cybersecurity Incidents. Ministry of Communications and Technology, 2022.

⁹ R.Tripathy (2025). A thorough examination of cybercrimes committed in India during the last 10 years.

¹⁰ BNS 2023, No. 45 of 2023, Acts of Parliament, Government of India.

Sec. 79: Online harassment, "electronic form" insults, deepfakes, and other forms of outraging modesty through speech, body language, or display all fall under this category.

Sec. 111: Cybercrimes are specifically mentioned as one type of organized crime that falls within Sec. 111 of the BNS.

Other Sec.s: Defamation sent by email or other electronic transmission is allegedly punishable under BNS Sec. 356, for example.

Forgery / Reputation harm: It's possible that digitally altered papers or photos fall under BNS Sec. 336, which deals with forgery that damages reputation.

c) ***Bharatiya Sakshya Adhiniyam, 2023***

Sec. 61: "Just because something is in electronic form doesn't mean it is inadmissible," states the principle of admissibility of electronic / digital documents.¹¹

The potential of the possibility of the contents of the contents of the contents of the contents of the contents of the contents of the contents of the records of the records.

Sec. 63, "Admissibility of electronic records / computer output," specifies the circumstances in which digital evidence (such as outputs from computers or communication devices) can be used in court, as well as the necessary certifications.

The requirement for a "certificate" (which is similar to the previous Sec. 65B) is included in Sec. 63(4)(c), which deals with electronic evidence.

The procedure for providing evidence of a digital signature is addressed in Sec. 73.

d) ***Rules and subordinate legislation***

- "IT regulations" (Intermediaries Guidelines) Rules from 2011;
- The "IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)" Rules, 2011;
- "CERT-In Regulations for reporting, log preservation, and network security";
- Additional acts, such as blocking policy, etc.

e) ***Data protection and privacy laws***

Data principals have rights, obligations, and penalties under the Digital Personal Data Protection Act, 2023 (DPDP rules), notwithstanding the fact that India lacks comprehensive data protection law. The DPDP rules enhances current cyber legislation by defining rules for how personal information should be handled throughout its lifespan.

¹¹ BSA, 2023, No. 46 of 2023, Acts of Parliament, Government of India.

Fundamental Provisions, Liability, and Enforcement

- Safe Harbor (Sec. 79): If intermediaries (e.g., platforms or ISPs) remove disputed information after obtaining takedown warnings or a court order, they are not held accountable for third-party content.
- The government can ban or intercept content to defend sovereignty, integrity, public order, or avoid incitement (Sec.s 69 and 69A).
- The IT Act punishes offenses such as identity theft, hacking, misrepresentation, and distributing obscene information with financial and prison penalties (e.g., fines up to three years).
- CERT-In rules require designated entities to notify cybersecurity occurrences within specified timeframes. Their procedural instruments include interception orders, bank account freezes, search and seizure warrants, and the capacity to coordinate with foreign agencies.
- Those affected by blocking orders, takedowns, or interception can challenge these acts through judicial review and appeals. International collaboration and Mutual Legal Assistance Treaties (MLATs):” India is a signatory to MLATs and participates in treaties (such as the Budapest Convention)”; through bilateral cooperation, although not being a party to the Budapest Convention itself.

1.4 Judicial Perspective

The interpretation of cyber laws, preservation of constitutional rights, and appropriate administration of justice in the digital environment have all been significant contributions by the court to the development of India's cyber crime complaint and redressal machinery. Through their rulings, the courts have clarified the scope of cybercrimes, raised the weight of electronic documents as evidence, protected individuals' privacy, and made those responsible for investigating and prosecuting cybercrimes more accountable. To bring technological advancements in line with constitutional protections and ideas of natural justice, the judiciary has also been called upon to step in.

Shreya Singhal v. UOI; is a important cyber rule decision. In a historic ruling, India's top court declared that Sec. 66A of the ITA of 2000 infringed the right to free expression guaranteed by Art.19(1)(a) of the country's constitution. The Court emphasized the need to find a balance between cyber control and basic freedoms, stating that imprecise and overbroad prohibitions on online communication failed to withstand constitutional scrutiny.¹²

Another key choice was Justice *K.S. Puttaswamy (Retd.) v/s. UOI*, in which the SC unanimously concluded that Art. 21 secure a person's right to privacy. This case has far-reaching consequences for cyber law since it established the concept that data collection, surveillance, cybercrime investigations, and digital governance must comply to the norms of legality, need, and proportionality.¹³

The legal branch has also clarified the regulations for electronic confirmation. The Supreme Court's decision in *Anvar P.V. v/s. P.K. Basheer* stated that electronic documents must fulfill the certification standards established in Sec. 65B of the Indian Evidence Act of 1872, which is now substantially reflected in the Bharatiya Sakshya Adhiniyam of 2023. In order to ensure fair trials in cybercrime matters, the Court underlined the need of properly keeping and confirming digital evidence.¹⁴

In the case of *Arjun Panditrao Khotkar v/s.. Kailash Kushanrao Gorantyal*, the SC reaffirmed and expanded on the principles established in *Anvar P.V.*, holding that, with few exceptions permitted by law, the certificate under

¹² (2015) 5 SCC 1.

¹³ (2017) 10 SCC 1.

¹⁴ (2014) 10 SCC 473.

Sec. 65B is typically required for the admissibility of electronic evidence. When it comes to detecting and prosecuting cybercrime using digital evidence, the decision has become an important cornerstone.¹⁵

The Indian bench has played a major role in influential the lawful framework governing cyber fraud by interpreting the necessities of the IT Act, 2000 and related criminal laws. One of the earliest and most significant decisions is *NASSCOM v. Ajay Sood*,¹⁶ (Delhi High Court). In this case, the defendants sent fraudulent emails and created fake websites impersonating NASSCOM to obtain confidential information from unsuspecting individuals. The Delhi HC recognized phishing as a distinct form of cyber fraud involving misrepresentation, identity theft, and passing off. The Court granted a permanent injunction against the defendants and observed that phishing not only infringes intellectual property rights but also undermines public confidence in electronic communications. This judgment is regarded as the first Indian judicial recognition of phishing as a cybercrime and laid the foundation for future legal action against online financial fraud.

In *Sharat Babu Digumarti v. Government (NCT of Delhi)*¹⁷, the SC examined the relationship between the IT Act and the general criminal law. The Court held that where an offence is specifically covered by the IT Act, the provisions of the special legislation prevail over the general provisions of the criminal law. This decision reaffirmed the principle that cyber offences must primarily be prosecuted under the IT Act wherever applicable, thereby ensuring greater consistency in the prosecution of cyber fraud, identity theft, phishing, hacking, and other technology-enabled offences.

More recently, the *Rajasthan High Court*, in a cyber fraud case involving *IDBI Bank (2025)*, directed the bank to refund approximately ₹58.93 lakh lost by a customer through unauthorized online banking transactions. The Court noted that the consumer swiftly reported the fraud, and there was no proof of carelessness on the side of the account holder. Based on the RBI's rules on consumer accountability in unlawful electronic banking transactions, the Court ruled that banks have a duty to maintain strong security mechanisms and cannot reject reimbursement if the client performed conscientiously. This decision increases consumer protection in circumstances involving digital payment theft and underlines financial institutions' obligation for providing safe electronic banking services.

The need of effective cooperation among regulatory bodies, banks, digital payment intermediaries, internet service providers, and law enforcement in the fight against cyber financial frauds has been acknowledged by Indian courts. Early complaint registration, digital evidence preservation, victim rights protection, and swift investigation of cyber crimes have all benefited from judicial supervision. The public now has more faith in digital transactions, and the system for resolving cyber crimes has also improved thanks to these developments.

When it comes to investigating and adjudicating cyber crimes, court decisions have been crucial in interpreting statutory requirements, protecting constitutional freedoms, and ensuring procedural fairness. As a result, India's cyber crime complaint and redressal procedures have grown substantially. An all-encompassing, rights-based, and technologically responsive cyber justice system will require judicial interpretation to keep up with the ever-increasing volume of cybercrimes.

Conclusion

As the prevalence of digital technology and cyber-enabled wrongdoings continues to rise, India has taken a proactive stance by establishing procedures for reporting and resolving cyber crimes. By shifting its focus from

¹⁵ (2020) 7 SCC 1.

¹⁶ 119 (2005) DLT 596

¹⁷ (2017) 2 SCC 18

relying on conventional criminal justice systems to establishing cyber forensic laboratories, online complaint platforms, specialised cyber crime units, and coordinated national frameworks, India has greatly improved its institutional and legal capacity to tackle cybercrime. The convergence of financial fraud response systems and cyber crime reporting platforms, as well as legislative measures like the IT Act, 2000 and its revisions, have made it easier and faster to file complaints, investigate them, and help victims.

However, the increasing complexity, worldwide scope, and rapid development of cybercrime have proven to be insurmountable despite these advancements. Important obstacles persist, including public knowledge, underreporting of crimes, investigation delays, a shortage of trained personnel, problems with jurisdiction, and the difficulty of recovering damages caused by cyber financial fraud. Government agencies, financial institutions, technology service providers, and international organizations must work together more effectively to address these challenges, which also necessitate ongoing reforms to the law, new technologies, increased public digital literacy, and capacity building for law enforcement.

In order to protect cybersecurity, individual rights, and public confidence in the digital economy, a reliable system for reporting and resolving cybercrimes is crucial. To effectively address the increasing types of cybercrime and ensure that justice is swift, transparent, and victim-centric as India progresses towards a digitally empowered society, the legal, institutional, and technological frameworks must be continuously modernized.

References

1. Government of India. (2000). *The IT Act, 2000 (Act No. 21 of 2000)*. <https://www.meity.gov.in>
2. Government of India. (2008). *The Information Technology (Amendment) Act, 2008*. <https://www.meity.gov.in>
3. Indian Cyber Crime Coordination Centre. (2024). *National Cyber Crime Reporting Portal*. Ministry of Home Affairs. <https://cybercrime.gov.in>
4. Ministry of Electronics and Information Technology. (2023). *Digital India: Annual report 2022–2023*. Government of India. <https://www.meity.gov.in>
5. Ministry of Home Affairs. (2023). *Indian Cyber Crime Coordination Centre (I4C)*. Government of India. <https://www.mha.gov.in>
6. National Crime Records Bureau. (2023). *Crime in India 2023: Statistics*. Ministry of Home Affairs. <https://ncrb.gov.in>
7. RBI. (2023). *Master direction on digital payment security controls*. <https://www.rbi.org.in>
8. RBI. (2024). *Annual report 2023–24*. <https://www.rbi.org.in>
9. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.
10. Clough, J. (2021). *Principles of cybercrime* (3rd ed.). Cambridge University Press.
11. Furnell, S., & Dowland, P. (2020). *Cybercrime: Key issues and debates*. Palgrave Macmillan.
12. Grabosky, P. (2007). *Electronic crime*. Pearson Education.
13. Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring internet crimes and criminal behavior*. CRC Press.
14. Wall, D. S. (2017). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.
15. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.