



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 5 | 2026

Art. 14

Digital Arrest Scams: Need For a Separate Cybercrime Framework in India

Harsh Raj

*Law Student, BA.LL.B., 4th Year,
North-Eastern Hill University, Meghalaya*

Recommended Citation

Harsh Raj, *Digital Arrest Scams: Need for a Separate Cybercrime Framework in India*, 5
IJHRLR 148-158 (2026).

Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of
Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact submission.ijhrlr@gmail.com

Digital Arrest Scams: Need For a Separate Cybercrime Framework in India

ABSTRACT

Digital arrest scams have turned out to be one of the most damaging cyber-enabled economic offences in India. In this kind of scam, the fraudster pretends to be a police official, investigating agency, or even a judge over video call and threatens the victim to hand over money to protect them from arrest. Unlike typical cyber fraud cases, in these scams, impersonation, extortion, digital forgery, and psychological harassment of the victim run concurrently as methods to induce payment. Digital arrest scams mostly originate from fraud factories in Cambodia, Myanmar, and Laos, where scam artists are trafficked in. As per government data presented before Parliament and the Supreme Court, Indians have been defrauded of close to Rs 3,000 crore by 2025 in such scams. Moreover, it has been observed that the vulnerable senior citizens are the prime targets of such scams. Indian laws do not have any specific provisions criminalizing such scams; they are dealt with by randomly applying various provisions of the Bharatiya Nyaya Sanhita, 2023, and the Information Technology Act, 2000, which were not designed to tackle such multi-jurisdictional cybercrimes. This paper will examine the legal framework on digital arrest scams, its shortcomings in light of recent developments such as the Supreme Court suo motu cognizance of such scams and its subsequent directions to the Central Bureau of Investigation, and highlight the lacunae in the current framework by comparing relevant statutes such as the Protection from Scams Act, 2025 of Singapore and the Anti Telecommunications and Network Fraud Law of China. It will conclude by recommending certain legal and administrative measures to address such scams.

KEYWORDS

Cybercrime, Digital Arrest Scam, Financial Fraud, Information Technology Act, 2000, Victim Compensation.

INTRODUCTION

India's rapid digitalization of India's banking, administration, and communications has resulted in an increase in the number of technologically advanced frauds. One such type of scam has been termed as 'Digital Arrest', where fraudsters lure the victims to transfer funds to their account on the pretext of arresting them for alleged violations like money laundering, narcotics trafficking, and terror financing. Digital arrest scams have raised concerns in India, as recently Prime Minister

Modi himself addressed the country about the problem on his “Mann Ki Baat”¹ radio program on 27th October 2024. Reports and parliamentary questions have since raised concerns about this emerging cybercrime, and the National Cybercrime Reporting Portal has seen a steep rise and a subsequent fall in complaints about digital arrest scams. The research problem tackled by the paper is that Indian laws do not specifically address this multi-jurisdictional cybercrime, and hence it is dealt with by scattered provisions of the Indian Penal Code and Information Technology Act, 2000. The paper aims to first identify the legal framework dealing with digital arrest scams, and then analyze if and how effectively it addresses this crime, with the help of recent case trends and comparative readings. The paper will, finally, recommend legal and administrative measures for plugging the identified loopholes. To achieve the objectives, the paper will review recent literature on digital arrest scams, focusing on its legal aspects. The paper will then analyze relevant case law and look at the Union Government’s administrative response to the problem, before concluding with recommendations.

LITERATURE REVIEW

As the digital arrest scam is still a recent phenomenon, there is not much literature on the topic. The early literature deals with collating statistics, state-wise, for reporting purposes. An article published in the international journal of novel research and development focuses on the number of cases in different states and concludes that Karnataka and Bihar are the hotspots for such scams due to poor digital literacy and weak cybercrime response.² Another set of literature on digital arrest scam mainly comes in the form of editorials, where various experts discuss the relevant laws and analyze the scam. For example, many articles discuss how Indian laws respond to digital arrest scams by relying on scattered provisions of the Indian Penal Code, Information Technology Act 2000, and the Bharatiya Nyaya Sanhita, 2023. It has been observed that the problem of such scams has prompted legislatures in other countries like China, Singapore, and the UK to take measures like creating specialized courts and imposing stricter penalties on fraudsters. A live law article observes that the legal vacuum around digital arrest scam has created a “legal shadow”³ wherein the fraudsters exploit the

¹ “Mann Ki Baat: PM Modi Warns About ‘Digital Arrest’”, ANI, October 27, 2024, available at: <https://aninews.in/news/national/general-news/mann-ki-baat-pm-modi-warns-about-digital-arrest20241027154602/> (last visited on August 7, 2026).

² Pramila Kori et al., “The Rise of Digital Arrest Scams in India: State-Wise Analysis, Awareness Initiative, and Data Collection”, 10(3) International Journal of Novel Research and Development 324 (2025), available at: <https://ijnrd.org/papers/IJNRD2503043.pdf> (last visited on August 7, 2026).

³ “The Legal Shadow Of Digital Arrests: Analysing Procedural Loopholes In The BNS And IT Act”, Live Law, February 7, 2026, available at:

legal powers of police to detain and interrogate persons as per the Bharatiya Nagarik Suraksha Sanhita, 2023 to justify their extortion as legitimate detention. However, a concrete alternative legal framework for such scams is still awaited. A final set of literature deals with the response to the digital arrest scam by the judiciary, especially the Supreme Court, which has taken several measures, such as directing the CBI to investigate such scams and take suo motu cognizance of matters relating to such scams. Few literature reviews analyze India's legal framework for digital arrest scam in light of international standards. This paper seeks to fill this lacuna by analyzing the efficacy of the current legal framework for digital arrest scam with the help of recent developments, including the Supreme Court's suo motu cognizance of the issues relating to digital arrest scams and directions to the Central Bureau of Investigation and the state governments. The paper will also refer to recent literature analyzing the Protection from Scams Act 2025 of Singapore and the Anti Telecommunications and Network Fraud Law of China to highlight India's need for legal reform to combat digital arrest scams.

RESEARCH METHODOLOGY

The paper will use a doctrinal and comparative research methodology. Primary sources for the study will include statutes such as the Bharatiya Nyaya Sanhita 2023, Bharatiya Nagarik Suraksha Sanhita 2023, The Indian Penal Code, Information Technology Act 2000, and the orders passed by the Supreme Court on matters relating to digital arrest scams. Additionally, the paper will use reports submitted by the Ministry of Home Affairs in Parliament, and the National Cyber Crime Reporting Portal to get statistics on digital arrest scams. Secondary sources for this paper will include literature reviews, news articles, and commentaries analyzing the problem of digital arrest scams and the measures taken to mitigate it. The paper will use secondary sources to collate information on how India's cybercrime reporting mechanisms respond to digital arrest scams, especially since the National Crime Records Bureau does not have a specific category for such scams. The paper will use secondary sources to collate information on the number of cases, affected people, and the economic loss caused by such scams since official statistics on the same are scarce. Finally, the paper will use comparative secondary sources to analyze statutes in other countries, such as the Protection from Scams Act, 2025 of Singapore, Anti Telecommunications and Network Fraud Law of China, and similar laws in the UK and the European Union.

<https://www.livelaw.in/articles/digital-arrests-bns-it-act-522245> (last visited on August 7, 2026).

DISCUSSION AND ANALYSIS

Statutory Framework Presently Applied for Digital Arrest Scams

Indian laws do not have specific provisions for digital arrest scams. Consequently, the authorities charge such scams with various provisions of the Indian Penal Code, The Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023. For example, digital arrest scam provisions of Indian Penal Code, 1860 include sections 318 (cheating and dishonest misappropriation of property), 308 (criminal intimidation), 318 (forged documents with intent to cause harm) 336 and 351 (criminal intimidation).⁴ Further, the Information Technology Act, 2000 deals with digital frauds under section 66D (cheating by personation by means of computer resource), and 66C (identity theft).⁵ The Bharatiya Nagarik Suraksha Sanhita, 2023 provides for service of process by electronic mode by the police under section 63, which requires encryption of the process with a digital signature of the court.⁶ This implies that a person under digital arrest cannot be legally summoned through WhatsApp or any other instant messaging service since such a process does not meet the requirements specified under section 63 of the Bharatiya Nagarik Suraksha Sanhita, 2023. Due to the absence of a specific law, the police record digital arrest scam cases as different types of crimes depending on the state where the FIR is registered. This leads to confusion, inconsistent punishment and does not allow for accurate data collection at a national level.

JUDICIAL INTERVENTION

The judiciary is the main interpreter of the laws and so in the absence of a specific law dealing with digital arrest scams, the courts have had to fall back on different laws to deal with the offense. For instance, in October 2025 the Supreme Court took suo motu cognizance of a complaint received by the Chief Justice of India from a 73-year-old woman in Ambala, Haryana. The woman was defrauded of more than one crore rupees after fraudsters tricked her to believe that the Supreme Court had issued an arrest warrant against her bearing the signature of a former Chief Justice of India.⁷ The Supreme Court observed that such

⁴ The Bharatiya Nyaya Sanhita, 2023, ss. 308, 318, 336 and 351.

⁵ The Information Technology Act, 2000, ss. 66C and 66D.

⁶ The Bharatiya Nagarik Suraksha Sanhita, 2023, s. 63.

⁷ In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Crl.) No. 3 of 2025, order dated October 17, 2025 (SC); “‘Matter Of Grave Concern’: Supreme Court Takes Suo Motu Cognisance Of Digital Arrest Scams Using Forged Court Orders”, Free Press Journal, October 17, 2025, available at: <https://www.freepressjournal.in/india/matter-of-grave-concern-supreme-court-takes-suo-motu-cognisance-of-digital-arrest-scams-using-forged-court-orders> (last

scams not only harassed the victims but also questioned the integrity of the Court. The Supreme Court on 1.12.2025 has directed the Central Bureau of Investigation to lead the probe into digital arrest scams with directions to the states to facilitate the investigation.⁸ Notably, the court directed enhanced cooperation from states which previously did not give its consent to CBI investigations. As a result, the Union Government formed a committee to monitor digital arrest scams and submit monthly reports to the Chief Justice of India. The Reserve Bank Innovation Hub and the Indian Cyber Crime Coordination Center have signed a Memorandum of Understanding, while 69 banks with a network of more than 1.23 lakh branches have launched the Grievance Redressal Mechanism Portal and the States have launched the Money Restoration Mechanism. These are some of the steps taken to fight digital arrest scams. Thru this mechanism, till June 2026, over 18.05 crores were restored to 36,290 complainants.⁹ The Supreme Court also directed the Ministry of Electronics and Information Technology, the Department of Telecommunications, and the Indian Cyber Crime Coordination Center to consider the implementation of time-bound restrictions on incoming and outgoing calls by victims of digital arrest scams and directed the Committee to examine the possibility of lowering the Rs 10 cores threshold for CBI investigation. According to the National Cybercrime Reporting Portal, the complaints received by the portal decreased from 1,23,672 in 2024 to 58,239 in 2025 and further decreased to 16,377 in the first half of 2026.¹⁰ Thus, even though the judiciary has played a significant role in addressing digital arrest scams, such interventions are ad-hoc and remain dependent on the whims of the judiciary and executive, especially since no specific law addresses such scams. Hence, the measures taken so far may not be a long-term solution to combating digital arrest scams.

visited on August 7, 2026).

⁸ In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Crl.) No. 3 of 2025, order dated December 1, 2025 (SC); "Supreme Court Orders CBI Investigation Into Digital Arrest Scams", MediaNama, December 2, 2025, available at: <https://www.medianama.com/2025/12/223-supreme-court-cbi-probe-digital-arrest-scams/> (last visited on August 7, 2026).

⁹ "Supreme Court Issues Directions to Curb Digital Arrest Scams, Asks RBI To Frame SOP on Mule Accounts", Bar and Bench, August 4, 2026, available at: <https://www.barandbench.com/news/supreme-court-issues-directions-to-curb-digital-arrest-scams-asks-rbi-to-frame-sop-on-mule-accounts> (last visited on August 7, 2026).

¹⁰ "SC Asks RBI To Issue SOP, Review Compensation For Digital Arrests", MediaNama, August 4, 2026, available at: <https://www.medianama.com/2026/08/223-sc-rbi-sop-review-compensation-digital-arrests/> (last visited on August 7, 2026).

INSTITUTIONAL AND ENFORCEMENT ARCHITECTURE

When it comes to institutional and enforcement architecture, the Union Government plays the leading role combating digital arrest scams. It has created the Indian Cyber Crime Coordination Center, which manages the National Cybercrime Reporting Portal, including the 1930 helpline. Further, the Union Government established the Cyber Fraud Mitigation Center, which facilitates real-time coordination between banks, telecommunication companies, and police to take measures to block fraudulent transactions. According to data published in the Indian Express, till early 2025, the enforcement machinery managed to block more than 83,668 Whatsapp accounts, 3,962 Skype IDs, more than 7.8 lakh SIM cards, and more than 2 lakh IMEI numbers in connection with digital arrest scams and other cybercrimes.¹¹ Further, as per reports published from the Indian Cyber Crime Coordination Centre, the number of SIM cards de-activated reached 1.2 million and mule accounts frozen stood at 1.33 million in 2025 alone, helping recover an amount estimated at Rs 5,489 crores.¹² According to data published by the Indian Cyber Crime Coordination Centre and cited in the Indian Express, investment frauds constitute 77% of all cybercrime frauds in terms of value. Digital arrest scams account for 8% of all cybercrime frauds, which though lower in value pose a significant threat due to the vulnerability of the victims.¹³ The measures discussed above have certainly helped reduce digital arrest scams, as evidenced by the reduction in complaints on the National Cybercrime Reporting Portal. However, as explained above, there is no law specifically addressing digital arrest scams, and hence all measures are taken on an ad-hoc basis. Even the Cyber Fraud Mitigation Center, Grievance Redressal Mechanism Portal and Money Restoration Mechanism are based on executive coordination, MOUs, and Reserve Bank of India directives. Consequently, such measures can be withdrawn or modified at any time, and hence are not a reliable way to combat

¹¹ Ministry of Home Affairs, Government of India, Reply to Unstarred Question No. 2117, Rajya Sabha, March 11, 2025; reported in "Govt Blocked 3,962 Skype IDs And 83,668 WhatsApp Accounts Used For Digital Arrest: Centre", ETV Bharat, March 13, 2025, available at: <https://www.etvbharat.com/en/!bharat/government-india-skype-ids-whatsapp-accounts-digital-arrest-centre-enn25031204310> (last visited on August 7, 2026).

¹² "1.2M SIM Cards Deactivated, 1.33M Mule Accounts Frozen: MHA Dismantles Scam Networks, Recovers ₹5,489 Cr", NewsMeter, August 19, 2025, available at: <https://newsmeter.in/nation/12m-sim-cards-deactivated-133m-mule-accounts-frozen-mha-dismantles-scam-networks-recovers-5489-cr-753663> (last visited on August 7, 2026).

¹³ "The Data Behind India's Digital Fraud Surge", CyberPeace Foundation, March 11, 2026, citing The Indian Express, available at: <https://cyberpeace.org/resources/blogs/the-data-behind-indias-digital-fraud-surge> (last visited on August 7, 2026).

digital arrest scams.

COMPARATIVE INSIGHTS FROM OTHER JURISDICTIONS

Some jurisdictions around the world have adopted a similar approach to combating digital arrest scams. For instance, the Protection from Scams Act, 2025 of Singapore enables police authorities to impose a “Restriction Order” on the banks, compelling them to freeze accounts of suspected fraudsters. This law allows a wide range of preventive measures targeting the financial flows of fraudsters. The order stays in place for a maximum of six months before review by the court.¹⁴ The main difference between the Singapore model and India is that the former uses the law to target financial flows, whereas in India, freezes are imposed on a case-to-case basis. Further, the law gives the victim of a scam an option to apply to the court for a “Restriction Order” against the suspected fraudster. Thus, similar to India, the Singapore model also lacks a specific law that targets digital arrest scams. However, it does help in freezing the accounts of fraudsters by targeting financial institutions directly. Another country that India can learn from is China, which imposes stringent obligations on telecom companies, banks, and internet service providers in relation to fraud and cybercrimes. The Chinese law requires telecom companies to adopt real-identity registration systems that prevent fraudsters from using false identities to commit frauds via SMS, emails, or phone calls. The law also requires telecom companies, banks, and other financial institutions to preserve relevant data and share it with law enforcement agencies. Further, the law requires such institutions to notify the police of suspected frauds and crimes related to telecommunications networks and to take preventive measures, such as suspending transactions or services. Violations of these obligations lead to penalties, such as fines and deregistration.¹⁵ Unlike China, India does not have laws imposing similar limitations on telecom companies and banks in relation to digital frauds and cybercrimes. In short, while India has adopted a multi-pronged approach of combining preventative, punitive, and compensatory measures, such as directing banks to create the Grievance Redressal Mechanism Portal and the Money Restoration Mechanism, other countries take a more stringent approach by imposing obligations on banks, telecom companies, and internet service providers. Thus, India could benefit

¹⁴ The Protection from Scams Act 2025 (Singapore), No. 1 of 2025, ss. 2–3; Ministry of Home Affairs, Singapore, “Framework for Restriction Orders under Protection from Scams Act 2025”, June 30, 2025, available at: <https://www.mha.gov.sg/media-room/newsroom/restriction-orders-issued-under-protection-from-scams-act-2025/> (last visited on August 7, 2026).

¹⁵ The Anti-Telecom and Online Fraud Law of the People’s Republic of China, 2022, arts. 9–11, 15, 18 and 21, available at: https://en.moj.gov.cn/2023-12/15/c_948363.htm (last visited on August 7, 2026).

from adopting some of the preventive and compensatory measures utilized by other jurisdictions.

ASSESSMENT OF THE ADEQUACY OF THE EXISTING FRAMEWORK

After examining the relevant statutes, case law, and administrative measures, it becomes evident that India's current framework for combating digital arrest scams is inadequate for several reasons. First, India does not have specific provisions targeting digital arrest scams. As a result, these scams are treated as a collection of different offenses, depending on the manner in which they are reported. Hence, appropriate punishment for such scams is difficult to determine, as they are punished as a range of different offenses, with varying punishments for each. Further, due to the absence of specific provisions, the statistics relating to such scams are difficult to collate, as reflected in the discussion above. Second, although recent steps have been taken to improve reporting mechanisms for digital arrest scams, such measures are taken ad-hoc and hence, are not binding on the relevant authorities. For example, as discussed above, the Memorandum of Understanding between the Reserve Bank Innovation Hub and the Indian Cyber Crime Coordination Center, the Grievance Redressal Mechanism Portal by banks, and the Money Restoration Mechanism by the states are based on executive coordination and not on any specific law. Hence, such measures can be withdrawn at any time, nullifying their positive impact on combating digital arrest scams. Finally, the current framework provides limited compensation to victims of digital arrest scams. Although steps such as the Money Restoration Mechanism by the states have improved compensation, such avenues are still limited and available on a case-to-case basis. Thus, the existing framework fails to provide adequate restitution to victims of digital arrest scams, especially since such scams result in significant financial loss for the victims.

FINDINGS

India has no specific law criminalizing digital arrest scams, and hence such scams are dealt with by applying various laws targeting different aspects of the offense.

The National Crime Records Bureau does not have a specific category for digital arrest scams, since such scams are dealt with on a case-to-case basis. India's recent measures targeting digital arrest scam have resulted in a decrease in the number of such scams, as reflected in the decrease in the number of complaints on the National Cybercrime Reporting Portal. However, the measures are taken ad-hoc and hence, are not binding on

the relevant authorities. Further, although restitution mechanisms such as the Money Restoration Mechanism have been initiated, they provide limited compensation to the victims of digital arrest scams.

RECOMMENDATIONS

First, Parliament should consider bringing in a separate provision, either as an amendment to the Bharatiya Nyaya Sanhita, 2023, or as a Digital Fraud and Impersonation Act, to recognise “digital arrest scam” as an aggravated composite offence of impersonating a public servant, extortion and coercive confinement by digital means, with enhanced punishment for victims who are elderly. Second, the Reserve Bank of India’s guidelines to banks and other financial institutions on identifying suspicious transactions should be statutory, with mandatory “cooling-off” periods for such transactions, and a “kill-switch” for transfers that match fraud indicators, as is the case, for instance, in Singapore. Third, the National Crime Records Bureau must be directed to create a specific category for digital arrest scams and related cyber impersonation scams to allow for consolidated data collection at the national level. Fourth, the threshold of Rs 10 crore for CBI investigation should be reviewed, with the possibility of aggregating complaints that implicate a network of fraudsters, in line with the Supreme Court’s observation on the matter. Fifth, the Money Restoration Mechanism needs to be given the status of a victim compensation fund, with a formalised procedure for allocation from the proceeds of the “mule” accounts used by fraudsters, and time-bound payouts to victims. Sixth, given the cross-border nature of digital arrest scams, India should seek greater bilateral cooperation from Cambodia, Myanmar and Laos in investigating and prosecuting digital frauds, while also considering statutory mechanisms for public awareness on the ground rather than ad hoc measures by the government.

CONCLUSION

Digital arrest scams highlight a lacuna in India’s cybercrime legislation, where an offence with a distinct set of activities and consequences has so far been prosecuted through an interpretative framework better suited to unrelated offences. While the judiciary’s suo motu cognizance of the matter, culminating in the Supreme Court’s directions to the Central Bureau of Investigation in December 2025, has spurred executive coordination and a partial reduction in the number of complaints, it is still best placed as an administrative measure and reliant on courts’ continuing oversight. By contrast, countries such as Singapore and China have demonstrated that a more durable solution requires plugging the lacuna through a legislative framework that explicitly addresses digital arrest scams through a specific offence, victim compensation mechanism

and preventive measures such as cooling-off periods for financial transactions. India now needs to turn the ad hoc inter-ministerial coordination on cybercrimes into a formal statutory framework to protect its citizens from this novel offence.