International Journal of Social Science Research (IJSSR)
Volume- 3, Issue- 4 | July - August 2026 ISSN: 3048-9490

Digital Arrest Fraud in India: Examining the Legal and Investigative Challenges in Combating Emerging Cyber Scams

Harsh Gaur
Gitarattan International Business School, Guru Govind Singh Indraprastha University

ABSTRACT

Cybercrimes have seen a massive surge in the recent years due to an upsurge in financial transactions and digital communications in India. Digital Arrest Scams have become one of the costliest cybercrimes affecting the victims financially and causing psychological damage. In these types of scams, the perpetrators impersonate law enforcement officials, judges and government regulators and interact with victims over digital communication platforms. In the present paper, Digital Arrest Frauds have been analysed as a separate category of Cyber Crimes within the framework of Digital Payment Frauds, Mule Account Money Laundering and Organized Cyber Crimes. All sorts of psychological tactics and Forensic Tools that are used to track and to expose such scams have been analysed in detail. The study has also been made of various frameworks and of various institutions dealing with Cyber Crimes in India, such as Indian Cyber Crime Coordination Centre (I4C) established under Ministry of Electronics and Information Technology (MEIT), National Cyber Crime Reporting Portal established under Ministry of Home Affairs (MHA). The paper identifies various jurisdictional and intermediary liability gaps in Information Technology Act, 2000 and suggests amendments thereto. This paper is written from a socio-legal perspective. In the paper, technological, inter-institutional, public awareness and law-based measures to prevent, investigate and punish digital arrest scams are outlined and argued for.

KEYWORDS: digital arrest scams, cybercrime, cyber fraud, digital forensics, mule accounts, deepfake technology, cybercrime regulations.

1. INTRODUCTION

The demonetization, UPI, and COVID-19 pandemic have created a digital revolution in India, shifting the population from cash-based payments to digital and opening new ways for scammers to exploit the vulnerable. One such cybercrime is the ‘digital arrest,’ with the perpetrators impersonating police, CBI, customs officials, and regulators via social media or video calls. They accuse the victims of crimes, such as money laundering, terror financing, or drug trafficking, and take them on ‘custody,’ cutting their access to friends, family members, and legal assistance. Criminals also demand the target to send money to “verify” them or keep the illegally obtained proceeds in “safe custody,” and fake warrants increase the believability of the scam. However, digital doppelgängers using artificial intelligence and deepfake videos

Published: 27 August 2026
DOI: https://doi.org/10.70558/IJSSR.2026.v3.i4.301269

to threaten and extort money from unsuspecting marks have emerged as a more dangerous version of this scam.

India has witnessed a rise in scams this year, with a staggering figure of 297,270 digital arrest-related complaints in 2022– May 2026. Over 1.23 lakh (123000) complaints and ₹1,935 crore in losses were registered in 2024 alone, with thousands of crores of fraud reported so far. The deluge of complaints suggests that the scam has mutated and grown more sophisticated, with ordinary people, doctors, and even retired bureaucrats and police officials falling prey to it.

India's cybersecurity agencies have responded by cancelling fraud SIM cards, freezing the mule accounts, and considering using a transaction 'kill switch,' but they need to move faster to combat such crimes. India's current laws regulating digital payment systems, data security, user privacy, and cybercrimes of all forms are fragmented, with the IT Act, 2000, and the Bhartiya Nyaya Sanhita, 2023, providing insufficient and unclear guidelines on digital custody-related theft and fraud. This study will discuss digital arrest scam operations, psychological aspects and legal loopholes to offer recommendations and insight into combating such cybercrime in India.

2. Recent Reported Cases of Digital Arrest Scam

Case 1: CBI Action in the ₹2.07 Crore Digital Arrest Scam

The Central Bureau of Investigation (CBI) has arrested three persons following simultaneous searches at seven locations across Odisha and Rajasthan in connection with a digital arrest scam involving a retired public servant. The victim was intimidated by fraudsters impersonating law enforcement and regulatory officials with fake legal actions and compelled to transfer ₹2.07 crore. The CBI registered the case in March 2026 on the directions of the Punjab and Haryana High Court, and the searches in June resulted in the arrest of two accused from Balasore, Odisha, and one from Nagaur, Rajasthan. The accused were involved in layering the defrauded funds through multiple bank accounts, including one in the name of a trust to obscure the trail of money investigators said.

Case 2: New Town Resident Defrauded of ₹53 Lakh

In yet another case reported by The Times of India, a 77-year-old New Town resident was cheated of Rs.53 lakh after being browbeaten by cyber-criminals who posed as CBI and Supreme Court judges. The conmen had used the prestige of the CBI and the Supreme Court to intimidate the old man into believing that they were investigating him for anti-national money laundering activities.

Case 3: Retired Banker Defrauded of ₹2.3 Crore Over 47 Days

According to the latest report by The Newsblare, there has been a case of cybercrime where a man was defrauded almost ₹2.03crore. It has come to notice that the fraud was orchestrated by the cyber criminals and they used to threaten the victim regarding the terror financing. In a similar long-drawn scam, the con artistes had impersonated as government officials and threatened the 78-year-old retired banker, Naresh Malhotra, that his landline number and Aadhaar card details are tampered with and are involved in terror funding cases. Such scams

take a long time to unfold and the crooks manage to keep their victims under their control for several weeks. Mr. Malhotra was confined to his residence for a total of 47 days in a month.

The three cases involved different amounts of money, different groups of people, and different methods of approach. In all of the cases, the criminals were using the same approach: impersonating the authorized organizations such as CBI, Supreme Court, and Anti-Terrorism agencies. The first case included several steps of money laundering to transfer the money all over the country. All of the three cases also involved blackmailing and psychological torture. The only difference was that the first case involved the money laundering process where the second and the third cases did not involve it. The crime affected different groups of people: in the first case, the victim was a retired employee, in the second case, the victim was a 77-year-old defence official, and in the third case, the victim was a retired banker.

3. Statistics of Digital Arrest Scam

From 2022 till May 2026, 297727 fraud complaints of Digital arrest were registered in India, leading to a loss of ₹4057.7 crore. Thus, 297727 Indians suffered from fraud, 8% of which turned out to be arrested by fraudsters. The total damage from cyber-fraud in general in the last six years is more than 52976 crore rupees.

Top Affected States	**Losses**
Maharashtra	1,637.66crore
Karnataka	1,097.37 crore
Tamil Nadu	897.79 crore
Uttar Pradesh	734.19 crore
Gujarat	643.82 crore
Chandigarh	630.53 crore
Telangana	614.18 crore

Table 1: State-wise ranking of monetary losses due to digital arrest fraud (till July 2026), according to The Indian Express.

Top Affected States	**Complaint Registered**
Uttar Pradesh	1.85 lakh
Maharashtra	1.58 lakh
Karnataka	1.21 lakh
Gujarat	97,937
Bihar	93,137

Table 2: Top five states with the highest number of cybercrime complaints registered up to July 2026, according to The Indian Express.

4. Observed Pattern

4.1 Stage by Stage Pattern

Initial Trigger: A scam almost always begins with a caller using any pretext irrelevant to law enforcement: a call informing you that a courier or delivery parcel had contraband, a call from "TRAI" informing you that your connection is about to be disconnected, or a message about your KYC or Aadhaar details being misused. In one common scam, the caller pretends to be someone from the Telecom Regulatory Authority of India informing the victim that his mobile number is going to be disconnected as a criminal complaint has been filed against it.

Manufactured Escalation to "Law Enforcement": The caller then pretends to be from CBI, ED, Customs or Police. The scammer disguises as CBI, ED, Customs, Interpol, or Police personnel by making calls, sending emails or WhatsApp messages, or writing letters to the victim. The impersonation is usually explicit in most cases, with the scammer stating his or her name and staff ID as he admonishes the victim for being targeted in the scam. The victim is usually berated and threatened with police arrest for being involved in a crime.

Fabricated evidence of guilt: They show the victims fake FIRs, arrest warrants, or ID cards. They typically accuse them of crimes of a socially or legally significant nature: money laundering, drug trafficking, and so on - the kinds of offences that often serve as a basis for high-profile corporate scandals, or that are associated with serious crimes in real life.

Psychological confinement ("The Arrest" itself): This is the modus operandi of the conmen. The victims are made to keep on a video call, through apps such as Skype or WhatsApp, and are instructed not to end the call or seek help from anyone else as they would be under 'digital arrest'. CERT-In's advisory also observes that scammers induce panic and exploit the victims' desperation by threatening to involve law enforcement agencies if the victim does not comply with their demands. CERT-In has directed government agencies to stop using WhatsApp or Skype for any official communication as fraudsters were taking advantage of the belief that authorities may use such apps to lure people into fake video conferences. It may be noted that the Prime Minister himself has cautioned that agencies probing the case would not go in for such digital conferencing.

Coercion and payment extraction: Victims are tricked into depositing money in the bank accounts of UPI IDs as "clearance of their name", "assisting the investigation", or a "refundable security deposit/escrow account". The threat to their finances is minuscule to the social stigma and legal harassment that coercive tactics can force them into.

Layering and Disappearance: Funds are transferred through shell companies, crypto wallets, and mule accounts. After the money is transferred, the scammers disappear, and the victim is left to figure out what has happened on their own, which can take a while. The funds that scammers extort from their victims are divided into small amounts and transferred to different accounts before being transferred to offshore accounts.

4.2 Victims Profile and Targeting Pattern

The targeting has widened over the years. These schemes saw a surge in 2024 and have grown

to a level where they are becoming large-scale operations, almost in the Mold of the 'Jamtaara' model of organized fraud. Targets included high-ranking officials, journalists, security personnel and elderly individuals, who were earlier assumed to be the only victims, being naive or elderly. This is evident from case reporting. In the cases in Delhi and Bengaluru, the victims included senior citizens, journalists, and professionals. Fraudsters threatened victims using fake police IDs and fake FIRs.

4.3 Organizational/Structural Pattern

The Enforcement Directorate's probe into these cases has uncovered connections to international cybercrime rings, not just isolated dishonest actors. One of the high-profile scandals resulted in the CBI's nationwide investigation into the alleged Rs 3,000 crore fraud after the Supreme Court directed it to do so. It appears that the accused was utilizing video calls to coerce victims and laundering money through fabricated police authorities and corporations. Moreover, at the infrastructural level, 14C collaborated with Microsoft to delist over 1,000 Skype IDs linked to digital-arrest scam operations, indicating a pattern of organized cybercrime rather than ad-hoc frauds.

5. Government Initiative & Legal Framework for Combating Digital Arrest Scams in India

5.1 Institutional Architecture

Indian Cyber Crime Coordination Centre (14C): 14C was approved as a central sector scheme in October 2018 with an outlay of ₹415.86 crore. It was formally launched in January 2020. With effect from 1 July 2024, 14C was upgraded to an Attached Office of MHA. It is the national nodal agency for cybercrime, bringing together academia, industry and government for prevention, detection, investigation and prosecution.

The 14C structure consists of seven verticals/components:

- National Cybercrime Threat Analytic Unit (NCTAU) – identifies new trends and methods of cybercrime.
- National Cybercrime Reporting Portal (NCRP, cybercrime.gov.in) – citizen-facing complaint portal launched on 30 August 2019, with dedicated confidential channels for crimes against women and children.
- Platforms for Joint Cybercrime Investigation Team – facilitates inter-state investigation coordination; operationalized through 07 Joint Cyber Coordination Teams (JCTTS) in identified cybercrime hotspots.
- National Cybercrime Forensic Laboratory (NCFL) ecosystem, now NDISC - assists State/UT investigating officers at the early stages of investigation; the flagship facility at CyPAD, Dwarka, New Delhi, has a centre in Assam. By October 31 2025, 12,952 cybercrime cases had received forensic assistance and 2,118 LEA personnel had been trained on forensic tools.
- National Cybercrime Training Centre (CyTrain, cytrain.ncrb.gov.in) – a MOOC

platform hosted by NCRB for capacity building of police officers, prosecutors and judicial officers offering standardized, court-presentable certifications ("14C Certified Specialist" and "14C Certified Expert"). There are over 12,500 registered police officers and over 3,050 certificates have been issued.

- Cybercrime Ecosystem Management Unit – engages with private sector and academic stakeholders.
- National Cybercrime Research and Innovation Centre – collaborates with research institutions locally and overseas to carry out research and development (R&D) on new detection and forensic technology.

Cybercrime Prevention Against Women and Children (CCPWC) Scheme: The CCPWC, launched in 2018, funded the establishment of Cyber Forensic Labs in State/UTs and training of LEA personnel, public prosecutors, and judicial officers. Under the scheme, MHA has released approximately ₹131-133 crore, Cyber Forensic Labs have been established in 33 States/UTs, and training in cybercrime awareness, investigation, and forensics has been imparted to more than 19,900 personnel of LEA, prosecutors, and judicial officers under the scheme.

National Critical Information Infrastructure Protection Centre (NCIIPC): NCIIPC, which has been designated pursuant to Section 70A of the Information Technology Act, 2000, and which is based at the National Technical Research Organisation, serves as the country's principal agency for the protection of critical information infrastructure in fields including banking, telecommunications, power, and transportation. In relation to the issue of digital arrests, its role is mainly indirect, as instead of dealing with individual complaints from citizens, it strengthens the banking and telecommunications systems that are exploited by scammers for spoofed calls and the use of mule accounts.

CERT-In: The Indian Computer Emergency Response Team (CERT-In), is the national body responsible for handling cybersecurity incidents, designated under Section 70B of the IT Act. The team runs a Cyber Forensic Lab that has been recognized as an Examiner of Electronic Evidence pursuant to Section 79A of the IT Act and is therefore capable of examining digital evidence from both storage devices and mobile phones. It also organizes training workshops for law enforcement agencies and operators an automated cyber threat intelligence exchange platform via its National Cyber Coordination Centre (NCCC).

5.2 Telecom-Sector Measures (Department of Telecommunication)

- **Sanchar Saathi Portal and App** - A citizen-facing portal (sancharsaathi.gov.in) has been launched, with services available in Hindi and 21 other regional languages. It provides information about SIM cards issued in the name of the user and enables blocking of lost/stolen handsets, which is used for tracing and blocking 22.76 lakh stolen/lost handsets and 37.28 lakh devices blocked till date.
- **Chakshu Facility** – Launched on Sanchar Saathi, enabling citizens to proactively report suspected fraudulent communication (fake KYC update messages, scam calls,

and WhatsApp fraud). Crowd-sourced Chakshu reports (11.18 lakh) had led to 50.90 lakh mobile-connection disconnections as of July 15, 2026. SEBI.

- **Digital Intelligence Platform (DIP)** - A secure platform that enables two-way flow of information from more than 1200 organisations on-boarded on it, including central agencies, 36 State/UT police forces, I4C, around 1100 banks, UPI/payment-system operators, telecom companies and WhatsApp.
- **SIM and call-authentication measures** – Re-verification of "mule" SIMs, blocking of spoofed international calls (through the CIOR mechanism), and work on finalizing the Telecommunications (User Identification) Rules, 2025, in addition to a stock-take of shortcomings in bulk/corporate SIM allocations and the supply chain.

5.3 Financial Sector Measures (RBI and Banks)

- **MuleHunter.ai** – An AI-based tool, developed by the Reserve Bank Innovation Hub (RBIH) for detecting fraudulent "mule" bank accounts used for laundering proceeds from scams; it is now used by 26 banks, while others use their own proprietary AI/ML detection mechanisms.
- **PMLA Section 12AA** – The Ministry of Finance and the RBI are examining whether they can apply this provision of the Prevention of Money Laundering Act, enabling them to temporarily suspend suspicious transactions before the funds are dissipated.
- **Victim compensation framework** – As reported in its February 2026 status report, the Supreme Court has ordered the RBI to investigate bank staff accountability and establish a liability/compensation framework for scam victims in conjunction with other stakeholders. This appears to still be under examination, rather than finalised, at this point.
- **Transaction 'friction' proposals** — While the RBI was reportedly pondering extra hurdles for large and/or first-time transfers and even a transaction "kill switch", trading-off speed, what makes UPI globally distinct.

5.4 Legal Framework

"Digital arrest" has no legal recognition or definition under Indian law. In its absence, investigations and prosecutions currently proceed under general-purpose provisions:

- **Bharatiya Nyaya Sanhita (BNS), 2023** – provisions on cheating, criminal intimidation, impersonation, extortion, forgery and identity theft are applied to digital arrest conduct; commentators note the offence can also carry elements resembling extortion or robbery, which the Supreme Court itself observed during the July 2026 hearing. place.
- **Information Technology Act, 2000** – provisions dealing with electronic funds transfer fraud, identity theft and impersonation through computer resources, Section 70A deals with NCIIPC, 70B deals with CERT-In and 79A deals with notified examiner of electronic evidence.

- **Prevention of Money Laundering Act (PMLA)** – could be used to trace proceeds of crime and also, under section 12AA to temporarily freeze transactions and go after mule account networks.
- **Digital Personal Data Protection Act, 2023** – while not directly addressing scams, this act targets the issue of personal data being misused by 'Data Fiduciaries'. This act penalises 'data fiduciaries' for failure to secure personal data of citizens and notify the Data Protection Board on data breaches with penalties of up to ₹250 crores for such failure. With the requirement of personal information being a pre-requisite for most scams (since the scammer is contacting the victim), increased enforcement of this act would result in reduced availability of such information (phone numbers, names etc.) as part of impersonation scams. However, it does not create any offence specifically dealing with scams and also does not provide any compensation for being a victim of scam.

5.5 Judicial Intervention

The most consequential driver for the evolution of the Indian State's response to date has also been its ongoing Suo motu case before the Supreme Court (as of this writing) initiated in October 2025, which increasingly nudged the Union Government towards more centralized coordination, platform accountability, and in recent months, a dedicated criminal statute.

Date	Development
Sept 2025	In Ambala, Haryana, a 73-year-old woman and her husband were duped of ₹1.5 crore using forged Supreme Court orders and impersonation of CBI/IB/Judiciary officials.
17 Oct 2025	SC takes Suo Muto cognizance, issues notice to the Centre and CBI.
27 Oct 2025	SC seeks data from all States/UTs on the availability of resources to deal with all FIR cases across the country, and queries CBI.
Dec 2025	SC directs CBI probe, seeking joints action across India against digital arrest networks.
6 Jan 2026	MHA meets high-level officials of Google, Meta, and Microsoft to review preventive measures on platforms.
2 Feb 2026	Second IDC meeting, status report notes Microsoft's responsiveness, and WhatsApp's failure to take remedial action.
10 Feb 2026	MHA advises court about Standard Operating Procedure while RBI is requested to look into personnel responsibility and liabilities / compensation.
20 Feb 2026	IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 came into force. "Synthetically Generated Information" Rules with 3-hours take down window.

April 2026	WhatsApp reported that more than 9,400 accounts were banned for their role in digital arrest scams over a 12-week period.
28-29 July 2026	Centre reveals that a BILL is in the pipeline SC (CJI Surya Kant, Justices Bagchi and Mohan) proposes separate criminal offences with stringent punishments and asset freezing powers.

The Bench, which consisted of Chief Justice of India Surya Kant, justices Joymalya Bagchi, V. Mohan, and N.V. Anjaria at different stages of hearing, also repeatedly pointed out the international nature of these fraud networks. Responding to this, Attorney General R. Venkataramani said that CBI was currently probing about 20 such major cases where losses exceed rs.10 crore, others being investigated by state police. states were being directed to give consent for investigation by CBI as per section 6 of Delhi special police establishment act, 1946 and CBI would be coordinating with INTERPOL to track down cross-border networks.

6. Identified Gaps and Challenges

No Legal Definition – The term 'digital arrest' lacks a specific legal definition, leaving law enforcement to rely on generic sections addressing cheating/extortion/impersonation.

Federal Division of Responsibility – Given that policing is primarily under the state government's purview and although supplemented by the centre via initiatives like 14C and advisories along with funding, the need to coordinate pan-India enforcement, especially on higher value/high impact/cross-state cases has necessitated interventions at the Supreme Court level along with putting into place consent mechanisms involving the CBI.

Responsiveness from the Platform - As can be observed from the status reports by the MHA to SC, there appears to be a certain degree of inequality in the level of co-operation provided by intermediaries. This is evident in how certain platforms do not take the necessary remedial action to the same extent as more prominent counterparts such as Microsoft do.

Cross-Border Enforcement Limitations – While Indian agencies may be able to freeze a mule account within the country, there is no jurisdiction on the part of domestic law enforcers against those 'masterminds' who operate out of scam compounds overseas highlighting the need for INTERPOL-level co-operation.

Victim Compensation Mechanism – There currently exists no formal compensation/liability framework that addresses these victims, whether that includes potential accountability of banks involved or not, which is still being examined.

Data Availability – A cursory glance at data published by the National Crime Records Bureau suggests that digital arrest isn't specifically tracked in its official crime data.

7. The Way Forward: Preventing Digital Arrest Scams

7.1 Legal Clarity Campaign (mandatory disclaimer)

Awareness campaigns today are saying digital arrest does not exist, but in a fragmented manner through advertisements, metro ads, caller tunes etc. A more effective way would be to have

such a disclaimer appear in a mandated format in all communications from the agencies mentioned by the finance minister (Police, CBI, RBI, Income Tax, Courts) stating "No government agency will ever ask you to stay on a call, transfer money or share OTPs. Hang up and verify at cybercrime.gov.in", something similar to the standard terms and conditions that appear while logging into various government websites.

Such a disclaimer could be made mandatory:

- In all SMS communications from Banks/Govt Departments (already done for OTPs).
- On the official website/app for the particular department,
- As a recorded disclaimer read out over IVR systems of banks and telecom companies.

This would take away the onus from citizens to remember this information from some campaign, which would be reinforced in a standard format they will inevitably come across while dealing with a scam call or SMS.

7.2 Bank-Side Friction for High-Risk Transfer

Add automatic friction (not blocking, but introducing a delay) for transactions that fit a certain fraud pattern profile, e. g., large transfer right after an unusually long inbound call, or a transfer to a new payee above a certain limit. The friction could be implemented via

- Mandatory 30 mins-24 hrs cooldown period for first-time large transfers to new payees.
- Mandatory biometric re-verification (e. g., fingerprint/face match) for transfers above a threshold that would trigger the panic-induced confirmation step.
- A warning message asking if the transfer is being made as a result of the phone call/video chat.

7.3 Telecom-level AI Call Pattern Detection

Shift from static spoofed number blocking (India already does this; over 7.81 lakh SIM cards and 2,08,469 IMEIs blocked as of February 2025) to behavioural/pattern detection: flagging calls based on common scam call characteristics, international origin numbers spoofed to look domestic, abnormally long call durations to one number, calls immediately preceded by financial app usage, or matching voice patterns to known scam-script recordings.

Blocking now is reactive (numbers are blocked after they’re reported). AI pattern detection could flag a call as suspicious in real time, before or during the call with an on-screen warning such as “possible scam call in progress” rather than after the fact.

7.4 School and College Curriculum Module

Among the suggested preventive measures, the curriculum-based approach seems most preferable as it would create long-term resilience at the community/population level rather than addressing individual cases.

While students are unlikely to become scammed targets directly, they are in the best position

among their families to understand such threats and act accordingly. They are often the first-person elderly would reach out to in case of a scam call. This makes such a curriculum-based intervention even more valuable, as it would have a multiplier effect, benefiting the population beyond just the students.

The suggested curriculum should address the following three areas. (i) There is no such thing as digital arrest in India, with no investigative agencies having the authority to ask for payments/arrests during phone/video calls; (ii) Understanding the scammer's psychology, including their intent to isolate a victim and create a false sense of urgency via fabricated documents; and (iii) appropriate actions to take in case the scam call occurs anyway, including cutting communication, asking for help from trusted persons, and contacting 1930 helpline or cybercrime.gov.in to verify and report the scam. It could be helpful to plan a simulated scam call where students would practice what to do in case of such a call, thereby converting the above areas into an actionable guide. Such a simulation could be based on inoculation theory, a behaviourally-informed method used in social and behavioural sciences.

7.5 Mandatory Scam-Recognition Training in Banking

In addition to extending the "bank on boarding" procedure (which is currently mandatory for KYC and net banking setup), banks should be compelled to introduce a short compulsory module of scam recognition that users need to complete as part of the onboarding process. This could consist either of a brief 5-10 min long video or an interactive quiz to test basic knowledge about recognizing scams.

This should also happen every year for senior citizen's accounts specifically, to ensure that they keep themselves updated with emerging fraud tactics. As many banks already have dedicated desks/schemes for their senior citizens, this seems well within reach.

Senior citizen banking services could be expanded to offer: A physical pamphlet along with a verbal briefing on digital arrest scams when an account is opened – annual mandatory "customer care-ups" by the bank to all senior citizen account holders (in order to refresh knowledge).

Designated bank staff trained to recognise distress signs (e.g. a customer who seems panicked or on call while transacting, mention of "police" or "investigation") and intervene at the counter/flag transaction.

7.6 Public "verify-first" App/Portal

A unified tool that allows anyone to quickly verify their phone number/ID/badge number is connected to a genuine government entity during ongoing calls.

This could include integrating both:

i. A searchable database of legitimate department's contact numbers (Sanchar Saathi currently has partial support for telecom related checks.

ii. Real time cross referencing against 14C's list of blocked number from previous digital arrests.

We also propose that we make one step quicker by integrating 'Report & verify', into an easy to use 'quick report & verify button', as these two things are currently done separately verifying the legitimacy vs. reporting the fraud at cybercrime.gov.in.

Currently, if you want to verify, you need to know about the various portals/helplines available for this process. However, during times of high stress, such as when making calls from panicked states, people aren't able to recall all possible avenues on their own, especially those who haven't used them before. So having this functionality in one well-known application can bridge the time of decision making.

8. Conclusion

Unlike traditional cybercrimes, digital arrest fraud involves a unique convergence of financial, psychological, and technological dimensions, posing new challenges to India's legal and regulatory systems. With close to 3,000 complaints and a value of Rs 4,057.7 crore, digital arrest fraud has exploited three keys 'weak links' – trust (by masquerading as the CBI, courts, and regulators), technology (deepfakes, spoofed phone numbers, and video calling apps), and financial systems (mule accounts, round-tripping). The cases of a Rs 2.07-crore fraud on a Rajasthan–Odisha express and a 47-day 'custody' of Naresh Malhotra, as discussed in the article, demonstrate why India's current laws, which criminalize offences such as cheating, extortion, and criminal intimidation, are inadequate.

Although India's response to digital arrest fraud through central government coordination, the CBI's nationwide jurisdiction, judicial review by the Supreme Court on Suo motu basis, takedown notices to platforms by CBI, and enforcement of the new IT Rules, 2022 by the central government represents an improvement over the earlier fragmented approach, several critical loopholes and challenges remain. Digital arrest fraud is yet to be criminalized in India via a specific section in the BNSS and the IT Act, 2000, and victim compensation and liability of banks for fraudulent transfers continues to be contentious.

The recommendations made in this article – from disclaimer regimes and transaction friction to AI-enabled detection tools, targeted awareness, and a unified verification and reporting mechanism – address digital arrest fraud at the level of individual awareness, but also at the level of the phone call, the click, and the blockchain. To disrupt digital arrest fraud, India's policymakers must converge on three key areas: a stand-alone section in the relevant laws to clarify the legal ambiguity around digital arrest frauds, a binding framework on compensating victims, and liability and information-sharing mechanisms between banks, telecom providers, and countries, and technology-enabled 'protection by design' built into the financial and communication systems. India's digital economy and its citizens' trust in its legal and technological systems will remain at risk if it fails to protect its weakest link at the interface of technology and law – the phone call.

References:

Dr. Archana Singh Parmar, Dr. Monika Sharma (2025). A New Frontier in Cybercrime and Its Repercussions: Digital Arrest, *International Journal for Multidisciplinary Research,* 7, 1-5. https://www.ijfmr.com/papers/2025/1/33240.pdf

Anuprash Rajat, Upendra Grewal (2025), The Evolution of Digital Arrest Scams and Their Impact on Privacy Rights Guaranteed Under Constitution of India, *Journal of Neonatal Surgery,* 14 (22), 1329-1337. https://jneonatalsurg.com/index.php/jns/article/download/6106/5146/20785

E. Rutger Leukfeldt & Anita Lavorgna & Edward R. Kleemans (2016). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, *Springer Nature Links*, 23, 287–300. https://link.springer.com/content/pdf/10.1007%2Fs10610-016-9332-z.pdf

Manpreet Kaur, Munish Saini (2022), Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions, *Springer Nature Links,* 28, 581–615. https://doi.org/10.1007/s10639-022-11168-4

Kulshrestha, Prof. Dr. Pradeep, et al., editors. Cyber Crime, Regulation and Security: Contemporary Issues and Challenges. *Inkbound Publishers*, 2022. https://doi.org/10.55662/CCRSbook.2022.

Hannes Ebert (2020), Hacked IT superpower: how India secures its cyberspace as a rising digital democracy, *Taylor & Francis Online*, India Review, 19(4), 376–413. https://doi.org/10.1080/14736489.2020.1797317

Lekshmi Viswanath (2025), Digital Constitutionalism: Navigating Governance in The Technological Era, *Journal of Law and Legal Research Development*, 02 ,15-20. https://www.jllrd.com/index.php/journal/article/download/33/25

Dakshina Chandra (2025), Examining the Contours and Challenges of National Cybercrime Reporting Portal in Countering Digital Financial Frauds, *Journal of Victimology and Victim Justice*, 8(1), 65–83. https://doi.org/10.1177/25166069241306546

Anuj Wankhade (2026), Banking Frauds in India: A Road Map for Effective Regulation and Prevention, *International Journal for Multidisciplinary Research,* 8, 1-14. https://www.ijfmr.com/papers/2026/1/67038.pdf

Diya Charaya (2024), Digital Deception: An In-Depth Investigation of Identity Theft in the Indian Cyberspace. *International Journal of Research Publication and Reviews*, 5(4), 2235–2244. https://doi.org/10.55248/gengpi.5.0424.0961

Subhajit Saha, Surjashis Mukhopadhyay (2024), A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023, *International Journal of Law and Social Sciences*, 10, 2454-8553. https://www.journalsalliancepub.com/index.php/ijls/article/download/114/108

Shraddha Chaudhary, Shreedhar Kale (2024), Vijay Madanlal Choudhary v Union of India: A systematic breakdown of protections against testimonial compulsion during criminal investigations. *Jindal Global Law Review*, 15(1), 89–117. https://doi.org/10.1007/s41020-024-00220-8

Mark Button, Branislav Hock, Joon Bae Suh, Chol Soo Koh (2025), Policing cross-border

fraud 'Above and below the surface': mapping actions and developing a more effective global response. https://link.springer.com/content/pdf/10.1007/s10611-024-10186-2.pdf

Shashank Mittal (2024), Legal Challenges of Cyber Bullying & Online Harassments - A Comparative Analysis, International Journal for Multidisciplinary Research, *International Journal For Multidisciplinary Research*, 6(2). https://doi.org/10.36948/ijfmr.2024.v06i02.19295

Paolo Vanini, Sebastiano Rossi, Ermin Zvizdic, Thomas Domenig (2023), Online payment fraud: from anomaly detection to risk management Financial Innovation, 9(1). https://doi.org/10.1186/s40854-023-00470-w

Bhawna Vijay (2025), The evolution of digital arrest cyber-crimes in India: Trends and patterns preventive measures, *International Journal of Sociology and Humanities*, 7(1), 01-05. https://www.sociologyjournal.net/archives/2025/vol7issue1/PartA/6-2-5-518.pdf

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

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India)