The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 4 | Issue 5 | May 2026
ISSN: 2583-973X (Online), SJIF IF: 5.6
Website: www.theacademic.in

When the State Calls and Steals *Digital Arrest Frauds in India: Awareness, Legal Protection, and the Architecture of Reform*

Abhishek Rajan

[1] Assistant Professor at Lloyd Law College, Greater Noida, and is currently pursuing doctoral research as a Part-Time Research Scholar at Amity Law School, Amity University Uttar Pradesh, Noida.

DOI : https://doi.org/10.5281/zenodo.20682297

ARTICLE DETAILS

Research Paper

Accepted: 23-05-2026

Published: 10-06-2026

Keywords:

Bharatiya Nyaya Sanhita, Supreme Court, Digital Arrest

ABSTRACT

A certain kind of fraud has snuck into everyday Indian life, and the reason it works, above all else, is this: it speaks with the borrowed tongues of the State. A telephone rings. A figure in uniform materialises on a video call. An official letterhead is angled towards the camera. Within hours, sometimes within minutes, an ordinary citizen has handed over a lifetime of savings to people she will never identify. The Government has given this confidence trick a name, the "digital arrest" scam. Indians are reported to have lost close to ₹1,935.51 crore to it during 2024, against 1.23 lakh complaints lodged on the National Cyber Crime Reporting Portal. The doctrinal oddity at the centre of the phenomenon is that "digital arrest" enjoys no legal existence whatsoever, neither under the Bharatiya Nyaya Sanhita, 2023, nor under the Information Technology Act, 2000, nor under any procedural code in force. It is theatre that has grown to the dimensions of an industry. This article maps the legal architecture ranged against that industry: the statutes through which the conduct must be prosecuted, the gaps those statutes leave open, the Supreme Court's increasingly assertive interventions in the suo motu proceedings now pending as *In Re: Victims of Digital Arrest* (SMW (Crl.) 3/2025), the regulatory machinery assembled by the Reserve Bank of India and the Department of Telecommunications, and the comparative experience of jurisdictions

wrestling with the same trans-national problem. It concludes with a series of calibrated proposals: statutory recognition of digital impersonation extortion; a United Kingdom-style reimbursement regime for authorised push payment fraud; and the institutional scaffolding that any serious victim-protection scheme will need.

I. Introduction

India's digital transformation has mostly been narrated as a story of inclusion. The Jan Dhan, Aadhaar and Mobile trinity, the Unified Payments Interface, and the cheapest mobile data found anywhere on earth have together drawn hundreds of millions of citizens into a financial system that their parents and grandparents were shut out of. Yet an infrastructure built for inclusion is, of necessity, also an infrastructure of exposure. The very rails that deliver a welfare transfer to a tribal hamlet in Jharkhand will, with no greater resistance, carry a defrauded pensioner's savings into a mule account in Phnom Penh. The figures speak for themselves. The Indian Cyber Crime Coordination Centre logged roughly 4,52,414 cybercrime complaints in 2021; by 2023 that number had climbed to 15,56,176, and in 2024 it passed 22 lakh. Aggregate losses to cyber fraud in 2024 touched Rs. 22,845.73 crore, a rise of 206 per cent over the preceding year.

The digital arrest fraud has its own unique niche in that landscape. Where the phishing scam preys on greed, the investment scam on hope, and the matrimonial scam on affection, the digital arrest variant preys on something far less comfortable to acknowledge: the citizen's habit of deference to the State. It holds out no reward; it holds out a punishment. The very instinct that keeps a person law-abiding, the quiet voice that says one does not argue with the officer, becomes the lever by which she is robbed. Speaking on the 115th episode of Mann ki Baat on 27 October 2024, the Prime Minister was unusually direct. No such legal process exists, he said; the whole thing is fraud, deceit, a criminal enterprise got up in the colours of the law. This article takes that observation as its point of departure and asks what the law has so far made of it, and what it has yet to do.

II. What "Digital Arrest" Is, and What It Is Not

Taken at its word, the expression "digital arrest" is something close to a contradiction in terms. In Indian criminal procedure, arrest is a physical act, governed by Sections 35 to 62 of the Bharatiya Nagarik Suraksha Sanhita, 2023. Those provisions envisage a hand laid on a shoulder, a formal notice, production before a magistrate, a warrant of custody. Nowhere do they contemplate confining a person

inside a Skype call. On this the Supreme Court has left little room for doubt. In *Satender Kumar Antil v. Central Bureau of Investigation*, the Court reiterated that a notice contemplating arrest cannot be served by WhatsApp, electronic mail, or any comparable medium; service must follow the modes the BNSS prescribes, and anything outside those modes is not law at all but coercion got up to resemble it.

So what, exactly, is the "digital arrest" scam? It is a species of cyber-enabled cheating in which a fraudster, working over a voice or video link, passes himself off as an officer of the State, of the CBI, the Enforcement Directorate, the Narcotics Control Bureau, the Telecom Regulatory Authority of India, on occasion even a sitting judge, and charges the victim with involvement in some grave offence. The accusation tends to be both generic and theatrical: money laundering, narcotics trafficking, a parcel stopped at customs, a SIM card said to be linked to terrorism. The fraudster, using a combination of psychological pressure and constant audio-visual surveillance, often for hours and sometimes days, obtains a transfer of funds under threat of imminent arrest, frozen accounts, seizure of property, and family disgrace. The arrest never happens. The transfer always does.

In conceptual terms the offence is anything but new. It is a composite of three long-recognised wrongs: cheating by personation, criminal intimidation, and extortion. Its novelty lies elsewhere, in the medium through which it is carried out, in the cross-border architecture of its commission, and in the use of forged digital imitations of official authority, the fake police uniforms, the counterfeit court seals, and, in the most brazen recent episodes, doctored letterheads of the Supreme Court of India itself. The novelty, in short, is operational rather than doctrinal. The wrong is ancient; only the staging is new.

III. The Evolution of Cyber-Enabled Fraud in India

Cyber-fraud in India has moved through three reasonably distinct phases. The earliest, running from roughly 2000 to 2010, belonged to the relics of the early internet: the Nigerian advance-fee letter, the lottery email, the crude phishing page got up to look like a familiar bank. A second phase, from about 2011 to 2019, saw OTP-based UPI fraud, manipulation of KYC and the call-centre scam. The third phase, triggered by the COVID-19 pandemic and the swift normalisation of video communication, is the age of high-value, narrative-driven impersonation fraud. It is the signature specimen of the digital arrest scam.

Its growth curve is steep. The opening four months of 2024 alone generated 7.4 lakh cybercrime complaints, of which losses of around ₹120.30 crore were traceable to the digital arrest variant specifically. By the year's end that figure stood at ₹1,935.51 crore. The first two months of 2025 by

themselves produced 17,718 separate digital arrest incidents and associated losses of ₹210.21 crore. Over the same stretch the Government blocked upwards of 7.81 lakh SIM cards and 2.08 lakh IMEI numbers, and took down 83,668 WhatsApp accounts together with 3,962 Skype identities. By the close of the calendar year the consolidated numbers tabled by the Union Home Minister at the National Conference of February 2026 were larger still. More than 8.2 million cybercrime complaints had been registered on the I4C portal as on 30 November 2025, of which roughly 184,000 had been converted into FIRs; the Government had cancelled over 12 lakh suspicious SIM cards and blocked the IMEI numbers of more than 3 lakh devices; and 20,853 accused had been arrested. One is meant to read these tallies as evidence of an enforcement response, which is precisely how the Government intends them. The difficulty is that the fraud has, so far, grown faster than the apparatus built to suppress it.

Five conditions, working in concert, account for the surge. The first is the sheer ubiquity of cheap smartphones and cheap data, which has placed the necessary tools in every hand. A second is the porousness of telecom KYC, a structural weakness that for years fed a steady supply of mule SIM cards into the system. A third is the trans-national displacement of the perpetrators to weakly governed jurisdictions across Southeast Asia, where industrial-scale scam compounds operate with an operational discipline that a district-level cyber cell in India cannot readily match. A fourth, true until very recently, was the absence of any real-time inter-bank tracing protocol capable of intercepting defrauded money before it disappeared through layered accounts. The fifth condition is demographic. The main quarry has been the senior citizen, deferential to authority, often less adept at digital ways, with a bankroll worth taking.

IV. The Modus Operandi

The digital arrest fraud unfolds case by case in a stylised, almost choreographed sequence. It begins with reconnaissance. Personal data, the kind that allows the caller to sound knowledgeable and authoritative, is gathered from database leaks, dark-web marketplaces and previous phishing campaigns: an Aadhaar number, a PAN, a residential address, banking details, anything that makes it possible to start the conversation with a line such as, “Am I speaking to Mr X, residing at the following address, holding PAN number such and such?”

Then the trigger call comes. It will say it is from the Department of Telecommunications, or TRAI or a courier company such as FedEx or DHL or India Post. The caller informs that there is a problem: a SIM card in the name of the victim has been used to send obscene messages, or a parcel in the name of the victim has been intercepted at the airport with drugs inside, or an account opened in the name of the

victim has been used to launder money. Details differ from script to script; purpose never does. The call is there to give the first jolt of fright.

The third movement is the passing of the baton. The call is then – with some ceremony – referred to an alleged officer of the Mumbai Crime Branch, the CBI, the Enforcement Directorate or the Narcotics Control Bureau. The voice switches register. The wording gets tighter. His accent becomes clipped and official. "Case number supplied. A piece of law is heard.

Then we come to the "arrest" itself. The victim is called in to a video platform, traditionally Skype and more and more often WhatsApp, where a figure in uniform appears against a background arranged to look like a police station: a notice board, a tricolour, maybe a portrait of Gandhi or the President. A fake FIR comes under the lens. They show you a fake warrant. In the most audacious recent cases the fraudster has produced what purports to be a freeze order under the PMLA bearing the seal of the Enforcement Directorate, or, more brazenly again, a sealed order said to issue from the Supreme Court of India.

But the fifth and most psychologically devastating phase is digital imprisonment. The victim is told not to hang up, not to leave the room, not to tell family members, not to get a lawyer. The pretexts change: it is a matter of national security; the investigation is sub judice; any breach will be read as proof of complicity. The victim, under constant audio-visual observation, sometimes for as long as forty-eight hours, enters into what the clinical literature calls dissociative compliance. That part of the brain which would normally have paused to ask why a CBI officer would be making an arrest over Skype simply ceases to function.

The sequence closes with settlement. The victim is induced to transfer funds, to an “RBI escrow account,” a “Supreme Court verification deposit,” or an account said to be held in custody by the investigating agency, on the promise that everything will be returned once the inquiry concludes. The money, predictably, evaporates. It passes through dozens, sometimes hundreds, of mule accounts; it is more often than not converted into cryptocurrency; and it leaves the jurisdiction within hours.

A telling recent instance is the case of an 82-year-old Mumbai industrialist who lost Rs. 22.92 crore between the middle of 2024 and the early part of 2025, reportedly the largest single digital arrest fraud yet recorded in India. By an order of 30 January 2026 the Supreme Court issued notice to the Union of India, the Reserve Bank of India, the Central Bureau of Investigation, and seven private banks on his

petition under Article 32, in which he has asked the Court to lay down a uniform national policy on victim protection in such cases.

The Bengaluru Rs. 24 crore case of May 2026 is no less instructive. There the suspects, who had posed as senior officials of the CBI and the Enforcement Directorate, were found by the Karnataka Cyber Command to be tied to a separate Rs. 15 crore scam in Belagavi and to several further interstate offences; by the time of reporting more than Rs. 1.46 crore had been recovered. The pattern that surfaces across these investigations is a consistent one. The digital arrest variant is, by now, not an opportunistic one-off but a serial enterprise, run by interlocking groups whose operational reach extends across States and, frequently, across borders. In this sense, the Bengaluru case is a more representative specimen than its headline figure suggests, not for its scale, but for how deeply it is woven into a wider web of recidivism.

V. The Multi-Layered Harm

The harm these frauds inflict operates at three separate levels, and any response that engages only one of them is, predictably, bound to fail.

At the individual level the injury is financial loss but it seldom ends there. The case histories that have been recorded include suicide, severe depressive episodes, marriages that fall apart and families that break up. The target group is the senior citizens, and they often lose their entire retirement savings, but they lose much more than just money. A man who has worked for thirty years to build up a modest corpus to see him through his old age, and loses it overnight to a stranger masquerading as a CBI officer, does not get the corpus back. Nor the sense of security on which that old age was supposed to rest, for the rest of his life. Victims have encashed fixed deposits, sold gold and mortgaged property in the clutch of contrived emergencies that would have been dispelled by a moment's sober reflection. The whole point of the fraud is to preclude sober reflection.

At the institutional level the consequence is more diffuse, though hardly less grave. Each time a fraudster successfully impersonates the CBI, the ED, or the judiciary, public confidence in those institutions erodes a little further. The phrase "the CBI is calling," which ought to signal the seriousness of legitimate investigation, has come in the popular imagination to suggest something closer to a scam in progress. The Supreme Court itself, in the suo motu proceedings of October 2025, remarked that the use of fake court orders strikes at the very foundation of the public trust reposed in the judiciary and must be viewed with seriousness. That collateral damage to the State's investigative legitimacy is exactly what one would expect, and it is not recovered easily.

At the systemic level the aggregate numbers begin to do work that the individual cases cannot. The Rs. 22,845 crore lost to cyber fraud in 2024 amounts, in round terms, to about 0.07 per cent of GDP. For a four-trillion-dollar economy that is not, in itself, a catastrophic figure. It is, however, a regressive drag on household savings, falling disproportionately on the group least able to absorb it; it pushes laundered proceeds offshore, with the attendant balance-of-payments and anti-money-laundering implications; and, because so much of that money is now converted into cryptocurrency, it hastens the migration of value into a regulatory grey zone that Indian law has only begun to confront.

VI. The Marriage of Technology and Social Engineering

At bottom the digital arrest fraud is applied social engineering laid over cheaply available technology. Three vectors converge to produce it.

The first is the spoofing and VoIP infrastructure that lets a fraudster mask his real number and display, on the victim's screen, an Indian landline or even an officially issued government caller identity. Through its International Incoming Spoofed Call Prevention System, launched in October 2024, the Department of Telecommunications claims a 90 per cent fall in spoofed international calls within two months of deployment. The success is measurable, but it has been met with a swift adaptive countermove: the perpetrators have migrated to domestic numbers and to WhatsApp-based calling, which bypasses the carrier-level filter altogether.

The second vector is synthetic media, the deepfakes, the face-mapping software, the off-the-shelf voice cloning that has made the video-based execution of the fraud both cheaper and more persuasive. The Cambodian raids of late 2025 turned up scam compounds equipped with rows of terminals, scripted dialogue, fake Indian-police uniforms, and printed counterfeit tricolour insignia. These are, in a literal sense, fraud factories: industrial operations with a division of labour, quality control, and the metrics-driven performance management of any other industry. WhatsApp's own investigation, conducted at the Inter-Departmental Committee's instance and disclosed to the Supreme Court in April 2026, confirms that the bulk of such operations aimed at Indian users originate in Southeast Asia, particularly Cambodia, and run through clusters of accounts and groups marked by repeated patterns, common names, reused media, coordinated behaviour, that lend themselves to network-level enforcement once the seed signals have been identified.

The third vector, and the most important, is psychological. The fraudster trades on three well-mapped cognitive vulnerabilities: authority bias, which disposes the citizen to defer to a uniform; urgency

bias, which narrows attention under perceived time pressure; and what social psychologists call the isolation effect, the degradation of judgment in a person cut off from her support network. In the Mann ki Baat address that has since become a touchstone, the Prime Minister broke the methodology into three operational steps, the collection of personal information, the manufacture of fear, and the application of time pressure. His prescription, to stop, think, and then act, is at one level glib; at another it is the only counter-formula that actually works at the moment of attack.

VII. The Legal Framework in India

The Indian law has no provision under the title 'digital arrest fraud' and no provision that treats the conduct as a single, unitary offence. This constellation of instruments, namely the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and a body of subordinate regulation issued by the Reserve Bank of India and the Department of Telecommunications, principally, prosecute the wrong. They each capture some fragment of the behaviour. None gets the whole of it.

A. The Information Technology Act, 2000

The IT Act, particularly in its post-2008 form, supplies the primary technology-specific offences. Section 66 criminalises computer-related offences, carrying imprisonment of up to three years or a fine of up to ₹5 lakh. Section 66C punishes identity theft, the fraudulent or dishonest use of any electronic signature, password, or unique identification feature, again with imprisonment of up to three years and a fine of up to ₹1 lakh. Section 66D, which speaks more directly to the digital arrest variant, criminalises cheating by personation through any communication device or computer resource on the same scale of punishment. Section 43 affords a civil remedy in damages where a computer or system is accessed, damaged, or used without consent. Sections 67 and 67A, which regulate the publication of obscene and sexually explicit material, are sometimes pressed into service where a fraudster subjects the victim to a bogus "strip-search" humiliation, a peculiarly degrading variant that has been recorded with troubling frequency over the past twelve months.

B. The Bharatiya Nyaya Sanhita, 2023

The BNS, in force since 1 July 2024, replaces the Indian Penal Code, 1860. It carries no discrete chapter on cyber-crime, but it has redrawn the traditional offences in technology-neutral language. Section 316 defines cheating; Section 318 punishes it with imprisonment of up to seven years and a fine. Section 319, successor to the old Section 416 of the IPC, addresses cheating by personation, the very

heart of the digital arrest variant, and applies squarely where a fraudster pretends through electronic means to be a public officer. Sections 204 and 205, corresponding to former Sections 170 and 171 of the IPC, criminalise impersonating a public servant and wearing the garb or carrying the tokens of one with fraudulent intent. Section 351(4), successor to Section 507, punishes criminal intimidation by anonymous communication, a feature invariably present in digital arrest.

The most significant doctrinal advance is Section 111. For the first time in Indian statutory law it introduces the offence of "organised crime," and, critically, it draws cyber-crime committed by syndicates operating across borders within the definition. Punishment scales up to death or life imprisonment where the conduct causes death, and otherwise carries a minimum of five years. What Section 111 makes possible, and earlier law did not, is the prosecution of the syndicate as a syndicate, rather than of individual operatives whose conduct, viewed in isolation, can look like garden-variety cheating. Whether the provision is used to its full doctrinal potential will turn on whether prosecutors and investigators develop the institutional muscle to assemble the kind of evidence it demands.

An Ahmedabad case registered in May 2025, in which a senior citizen was defrauded of ₹55.50 lakh through forged judicial documents, illustrates the prosecutorial template that has since emerged in practice. The FIR invokes Sections 318(4), 319(2), 338, 336(3), 340(2), 341(1), 204, 205 and 3(5) of the BNS together with Sections 66C and 66D of the IT Act. But one notes that there is not a single charge in that bouquet which captures the essential character of the offence as a co-ordinated syndicate-driven extortion. The aggregation does what the individual provisions, on their own, cannot do.

C. Reserve Bank of India Guidelines and NPCI Consumer Protection

The most consequential regulatory intervention in the field remains the Reserve Bank of India's circular of 6 July 2017 on Customer Protection and the limiting of customer liability in unauthorised electronic banking transactions. The circular sets up a tiered liability regime. Whenever she reports it, the customer has no liability at all where the unauthorised transaction is attributable to the bank. Nil if neither bank nor customer is at fault and the customer reports within three working days. 2. In case of delays of four to seven working days, the liability is capped at Rs 5,000 to Rs 25,000 depending upon the type of account. If the customer's own negligence is proved the customer takes the loss up to the time that she reports.

Importantly, the responsibility of demonstrating customer negligence is on the bank, a view reiterated by Allahabad High Court in Suresh Chandra Negi v. Bank of Baroda . The bank will also have to credit the disputed amount within 10 working days and settle the complaint within 90 days. But in the case of the

digital arrest, there is a thorny conceptual question. The bank's record shows the victim is the one who started the transfer. The bank can point to a transaction that satisfied every authentication requirement, OTP entered, biometric matched, two-factor authentication cleared, and assert, with technical accuracy, that this was customer-initiated. The reality, of course, is that the customer was acting under sustained psychological duress. Whether a transaction of that kind is "authorised" in any meaningful sense, or whether the very concept of authorisation as drafted in 2017 even contemplates the species of deception now in play, is the doctrinal nub of the pending Article 32 proceedings. The honest answer, on the present text of the circular, is that the question remains open; and for as long as it stays open, the bank will, predictably, maintain that the loss lies where it falls.

Alongside the RBI regime sits the National Payments Corporation of India's consumer-facing fraud-awareness portal, which, ever since the rapid expansion of UPI, has tried to fill the user-protection gap that the RBI circular leaves on the demand side. The portal documents the principal modalities of UPI, IMPS, and digital-payment fraud, names the impersonation and digital arrest variants expressly, and prescribes safe-payment conduct for end-users of the NPCI rails. Its analytical reach is limited, since it neither does nor could override the liability allocation under the RBI circular, but it has in practice become a primary channel through which the rails operator communicates risk to the ordinary user. The deeper point is structural. In a payment ecosystem where the rails operator carries no statutory liability for fraud committed over the rails, awareness is what the operator can offer the consumer in place of indemnity.

D. The Cybercrime-Specific Regulatory Architecture

The Indian Cyber Crime Coordination Centre (I4C), set up under the Ministry of Home Affairs in 2020, runs the National Cyber Crime Reporting Portal (cybercrime.gov.in) and the round-the-clock toll-free helpline 1930. Its Citizen Financial Cyber Fraud Reporting and Management System enables the real-time freezing of fraudulent transactions within what has come to be called the "golden hour," the one to two hours after the fraud during which the money is likely still recoverable. The Cyber Fraud Mitigation Centre, also housed at the I4C, co-locates representatives of major banks, payment aggregators, telecom service providers, and law-enforcement so that the response can be coordinated. As on 30 November 2025 the I4C reporting portal had been accessed more than 230 million times, with over 8.2 million complaints registered, a figure that measures not only the scale of cyber-fraud but the platform's arrival as the country's default channel for reporting digital harm.

The Sanchar Saathi portal, operated by the Department of Telecommunications, hosts the Chakshu facility for reporting suspect fraud communications; the Telecom Analytics for Fraud Management and Consumer Protection (TAFCOP) module for checking the SIM connections issued in one's name; and the Central Equipment Identity Register (CEIR) for blocking lost or stolen handsets. The Digital Personal Data Protection Act, 2023, still in its phased rollout, will in time add a meaningful protective layer by regulating the processing of personal data, the very data whose leakage supplies the raw material on which every digital arrest fraud is built.

VIII. Cyber Cells and the Architecture of Enforcement

The investigation of cybercrime in India is, on paper, a shared responsibility, and in practice a fragmented one. State police forces run Cyber Crime Police Stations in all major districts, backed by State Cyber Crime Coordination Cells. The Central Bureau of Investigation maintains a dedicated Cyber Crime Cell. The National Investigation Agency assumes jurisdiction in cross-border and terrorism-linked cyber offences. The Enforcement Directorate, in several digital arrest cases, has invoked the Prevention of Money-Laundering Act, 2002, treating the laundered proceeds as a predicate offence.

Over the past year the institutional architecture has been substantially enlarged. On 10 February 2026, in a single ceremony in New Delhi, the Union Home Minister inaugurated a new Cybercrime Branch of the CBI and launched the State Cyber Crime Coordination Centre (S4C) dashboard of the I4C, two measures designed between them to furnish a national investigative locus for cybercrime and to give the State police a real-time platform for sharing data. The headline figures the Home Minister placed on record at the same conference offer the clearest snapshot yet of what the existing architecture has achieved and where its limits lie. Roughly 361,000 cyber-fraud complaints have together allowed the Government to safeguard Rs. 8,189 crore out of an estimated ₹20,000 crore in cyber fraud, a recovery rate of about 40 per cent. That is creditable as a first-order metric, yet it still leaves a great deal of money in the perpetrators' hands. Sixty-two banks and financial institutions had been onboarded to the I4C mechanism by the end of 2025, with the declared aim of bringing all financial institutions, cooperative banks included, into the system by December 2026; 795 institutions in all, spanning banks, fintechs, NBFCs, and e-commerce platforms, are presently connected. The Mule Account Hunter software, developed jointly by the Government of India and the Reserve Bank, is to be taken up across the banking sector. None of this is, on its own, a complete answer. It is, however, the first time the Indian State has assembled in a single architectural picture the inter-agency components the offence requires.

Sitting above this matrix, the Indian Cyber Crime Coordination Centre functions as the apex coordinating body. As on February 2025 the I4C had frozen over 24 lakh mule accounts and disabled millions of suspect identifiers through coordinated data-sharing with banks and telecom operators. Even so, the conviction rate stays stubbornly low: NCRB data put cybercrime convictions somewhere between 30 and 35 per cent, well beneath the all-India average for traditional offences. The reasons are not obscure. The perpetrators are, in the main, physically beyond the reach of Indian process. The evidentiary demands of the Bharatiya Sakshya Adhiniyam, 2023, and in particular its certification requirements for electronic records, raise obstacles that even the most diligent investigating officer struggles to clear when the relevant data sits on a server in Phnom Penh. And cyber-forensic capacity at the district level remains, in many States, embarrassingly thin.

A notable interim step came on 1 December 2025, when the Supreme Court, in *In Re: Victims of Digital Arrest*, empowered the CBI and the State police to freeze any bank account *prima facie* traceable to digital arrest fraud, with or without an FIR, on the strength of complaints made to the State police or the National Cyber Crime Reporting Portal. This represents a major departure from the orthodox FIR-first approach to coercive action. It is also a frank judicial acknowledgement that in cyber fraud, the FIR requirement, reasonable enough in physical-crime investigation, has become an evidentiary bottleneck that does little more than give the fraudster the extra hours she needs to move the money offshore.

IX. The Supreme Court and the High Courts: An Emerging Jurisprudence

Though the jurisprudence on digital arrest is still nascent, a handful of decisions, and one ongoing suo motu proceeding, have started to lay down the doctrinal scaffolding on which a coherent body of law might still be built.

The first reference point is *Satender Kumar Antil v. Central Bureau of Investigation*, supplemented by the supervisory orders of 21 January 2025 and 16 July 2025, and most recently by the order of 15 January 2026. On the face of it, the directions, which bar the serving of notices of intent to arrest by WhatsApp, email or other electronic means, and require service strictly under Section 41-A of the CrPC or Section 35 of the BNSS, read like procedural housekeeping. They're doing something more important, if you look more closely. They give the citizen a standard. Any “notice” or “warrant” served through WhatsApp is, ipso facto, not law. The rulings provide the ordinarily timorous citizenry a neat litmus test to spot the fraud at the precise moment it is being attempted.

Behind Satender Kumar Antil stands the older but doctrinally foundational decision in Arnesh Kumar v. State of Bihar, which predates the phenomenon of digital arrest but provides the principle from which the entire modern jurisprudence proceeds: that arrest is never automatic, that the officer must record his satisfaction against a checklist of objective considerations, and that custody is not the default position of the criminal process.

Read with the BNSS framework, *Arnesh Kumar* forecloses exactly the kind of summary, off-the-cuff "arrest" that the digital fraudster claims to be effecting. The fraudster's implicit theory of arrest is so wildly at odds with the constitutional law of India that, properly understood, no informed citizen could ever fall for it. The trouble, of course, is that the relevant constitutional law forms no part of the curriculum of an ordinary citizen's anxiety.

The most significant case directly on point is the Supreme Court's suo motu proceeding, *In Re: Victims of Digital Arrest Related to Forged Documents*, registered as SMW (Crl.) 3/2025. The Court took cognisance on 17 October 2025 after a 73-year-old resident of Ambala reported being defrauded of ₹1.05 crore through forged orders bearing the seal of the Supreme Court and a fabricated ED freeze order under the PMLA. A Bench of Justices Surya Kant and Joymalya Bagchi observed that a pan-India action with coordinated effort between the Central and State police was, at least *prima facie*, called for. The successive orders of 17 October, 27 October, and 1 December 2025 have, between them, begun to construct what may in time grow into a structured national framework: pan-India coordination, freezing without a prior FIR, mandatory inter-agency liaison. For now it is a framework drawn in outline rather than in detail. Whether it acquires that detail will depend on whether the Court keeps engaging with the issue, and on whether Parliament, in the meantime, picks up the legislative pen.

The most consequential procedural development in the proceeding has come in the months since. By orders of 9 February 2026 the Court constituted an Inter-Departmental Committee chaired by the Special Secretary (Internal Security) to oversee the inter-agency response, and directed the various stakeholders, telecom operators, digital platforms, financial regulators, to file status reports detailing the steps they had begun to take. The status report filed by the Attorney-General for India on behalf of the I4C in April 2026 is, in its own right, the most substantial single document yet placed on the record of any Indian court on this phenomenon. It records, among much else, that WhatsApp, acting on inputs from the I4C, the Ministry of Electronics and Information Technology, and the Department of Telecommunications, launched a structured multi-week investigation in January 2026 directed specifically at digital arrest scams targeting Indian users; that, on a methodology of seed signals leading to network mapping and

then to network-level enforcement, the platform mapped entire networks from a small set of flagged accounts and banned 9,400 accounts engaged in law-enforcement impersonation; that it has deployed logo-detection systems matching profile photos against databases of law-enforcement insignia, language-model-based impersonation-pattern detection, account-age disclosure, and profile-photo suppression for unknown contacts; and that it has begun work on SIM-binding in compliance with the DoT circular of 28 November 2025, with full rollout expected within four to six months. The report further records that the Department of Telecommunications has notified that the proposed Telecommunications (User Identification) Rules and the related framework for a Biometric Identity Verification System (BIVS) will need roughly three months for notification and a further six for full implementation, with deployment expected before December 2026; and that the Inter-Departmental Committee has under examination the feasibility of cutting the time taken to block a suspicious SIM card to two or three hours, in recognition of how often frauds occur within the first few hours of activation. Were one drafting a typology of Indian public-interest jurisdiction, *In Re: Victims of Digital Arrest* would already qualify as a textbook instance of structural-injunction litigation, the Court not adjudicating a discrete dispute so much as supervising the assembly of an institutional response from a position of continuing oversight. The doctrinal question is whether supervision of that kind is well suited to the architectural reform the field needs, or whether it is better understood, more modestly, as a placeholder for legislative action.

At the level of the High Courts, the Allahabad decision in *Suresh Chandra Negi v. Bank of Baroda* remains the principal authority on the allocation of liability in unauthorised electronic banking transactions, and the doctrinal principle it lays down, that the burden of proving customer negligence rests squarely on the bank, applies directly in the digital arrest context. The Rajasthan High Court, in *In Re: In the Matter of Tackling the Issue of Digital Arrest Scams* (2025), and the Telangana High Court, in pending proceedings concerning a Hyderabad victim defrauded of Rs.1.92 crore, have each entertained public-interest litigation seeking structured State responses. The shift in judicial posture, away from the case-by-case remediation of individual victims and toward the construction of systemic interventions, is the most consequential development in this area of law in the present decade.

Mention should also be made of *Shreya Singhal v. Union of India*, which, though chiefly concerned with the constitutionality of the now-repealed Section 66A of the IT Act, supplies the foundational reading of the IT Act in conformity with Article 19(1)(a) of the Constitution. Its principles continue to operate in defining the contours of the surviving offences under Section 66 and its companions.

X. The Comparative Perspective

The digital arrest variant is a distinctively Indian articulation of a global phenomenon, and a brief comparative survey rewards attention both for what it reveals about the universal vulnerabilities of digitised societies and for what it suggests about the institutional designs that are working elsewhere.

In the United States the Federal Trade Commission records annual losses of about USD 2.7 billion to imposter scams, in which fraudsters pose as IRS officials, Social Security Administration officers, or Border Patrol agents. The American response pairs aggressive criminal prosecution under the Wire Fraud statute (18 U.S.C. § 1343) with public-awareness work by the FTC and the FBI's Internet Crime Complaint Center (IC3). The arrest in February 2025 of one Zhipeng Lin, in connection with a USD 496,000 scam targeting a 74-year-old woman in which the fraudsters posed as McAfee security personnel, illustrates the prosecutorial strategy well enough: vigorous enforcement against the operative within reach, even as the syndicate behind him keeps working from beyond the jurisdiction.

China occupies an uncomfortable dual position. It is at once a source of trans-national fraud, through the Chinese-operated scam compounds in Myanmar, Cambodia, and Laos, and a victim of it, with hundreds of thousands of Chinese citizens defrauded each year. Since 2023 Chinese and Myanmar authorities have cooperated in the arrest of more than 57,000 individuals involved in cybercrime, alongside several mass-extradition operations. In October 2025 the United States Treasury and the United Kingdom Foreign Office imposed sanctions on Chen Zhi, chairman of Cambodia's Prince Holding Group, accusing him of running scam compounds that have defrauded victims around the world; United States prosecutors seized USD 14 billion in bitcoin in what they described as the largest cryptocurrency forfeiture on record.

The United Kingdom's response is, for present purposes, the most instructive of all. The Fraud Act 2006 criminalises fraud by false representation under Section 2, with a maximum penalty of ten years' imprisonment. More to the point, the Contingent Reimbursement Model Code, voluntary among major United Kingdom banks since 2019, mandates refunds in cases of authorised push payment (APP) fraud, a category that maps closely onto the Indian digital arrest variant. By a mandate effective October 2024 the Payment Systems Regulator has converted that voluntary code into a binding regime, requiring mandatory reimbursement of up to GBP 415,000 in qualifying APP fraud cases. India has at present no equivalent statutory framework, and the consequence of that absence is that the cost of the fraud falls, almost in its entirety, on the victim.

Singapore's Shared Responsibility Framework, effective from 2024, takes a different tack again, allocating the loss between banks, telecom operators, and consumers according to each party's adherence to specified anti-fraud measures. Hong Kong's Anti-Scam Consumer Protection Charter sets industry-wide standards for fraud detection. Both models repay close study by Indian policy-makers, not least for their explicit allocation of liability to telecom intermediaries, a step India has so far been unwilling to take.

On the supply side, finally, Cambodia, Myanmar, and Laos host the trans-national scam compounds that form the operational base of much of the global impersonation-fraud industry. In raids during late 2025 and early 2026 the Cambodian authorities dismantled compounds set up specifically to target Indian victims with fabricated Indian-police paraphernalia. More than 2,418 individuals were arrested in Cambodia in the first half of 2025, with 2,322 foreigners deported. The Amnesty International investigation of November 2025 documented widespread human trafficking and forced labour inside these compounds, a reminder, too often missed, that the operatives executing the fraud are themselves frequently the coerced victims of a deeper criminal enterprise. At its outer edges the story of digital arrest is, in part, a story about the trafficked.

XI. The Difficulties of Investigation and Enforcement

The investigation of digital arrest fraud is hampered by a particular cluster of structural, evidentiary, and jurisdictional difficulties. None of them is mysterious; all are, in principle, addressable; and at present not one is being addressed at the scale the problem demands.

The first difficulty is cross-border execution. The overwhelming majority of digital arrest operations are physically located in Cambodia, Myanmar, and Laos. Extradition under the Mutual Legal Assistance Treaty framework is slow and politically contingent. India has bilateral MLATs with more than forty countries, but enforcement in the part of Southeast Asia where the perpetrators actually sit remains uneven. "Thousands of Indian nationals were trafficked into such compounds with false promises of employment. They have now become perpetrators of the fraud on their own countrymen under conditions of physical confinement and threat," the Ministry of External Affairs reported in 2024.

The second is the proliferation of mule accounts. Money defrauded from a single victim passes through dozens, sometimes hundreds, of accounts before being converted into cryptocurrency or routed offshore. Tracing it calls for real-time cooperation among banks, the I4C, and law-enforcement, the very cooperation the Cyber Fraud Mitigation Centre is meant to provide, though the capacity remains patchy.

The I4C reports having frozen over 24 lakh mule accounts as on early 2025; yet new mule networks spring up as quickly as old ones are dismantled, in a pattern that recalls nothing so much as the futility of fighting the proverbial Hydra. The Mule Account Hunter software now being rolled out across the banking sector is, in that sense, the single most consequential technical intervention of the past year. As the Home Minister has himself acknowledged, though, until every bank has cleansed its accounts through the software, no customer can be regarded as fully protected.

The third difficulty is evidentiary. Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, successor to the former Section 65B of the Evidence Act, electronic records require a certificate to be admissible. Obtaining that certification, particularly where the data resides on a foreign server or in encrypted form, is frequently impossible as a practical matter. In *Anvar P.V. v. P.K. Basheer* and the rulings that followed, the Supreme Court has insisted on strict compliance with the certification requirement. As a matter of doctrine that is the correct position. As a matter of cyber-investigative practice it creates a structural problem that no quantity of investigative diligence can resolve. There may be a case, in due course, for a calibrated relaxation of the certification standard in cyber-prosecution, not the abolition of the safeguard but a procedural recalibration that takes account of the realities of trans-national digital evidence.

The fourth is capacity. A 2024 study by the Centre for Internet and Society estimated that India has roughly one cyber-forensic specialist for every 200,000 citizens, against a recommended ratio of one per 50,000. Many State cyber-crime cells lack even the basic facilities, the Faraday-shielded examination rooms, the licensed forensic software, the trained personnel to run it, that ought to form the minimum infrastructural floor for credible cyber-investigation.

The fifth, and culturally the hardest, is the reluctance to report. Senior citizens, the demographic most at risk, are often loath to report digital arrest victimisation, sometimes from embarrassment, sometimes from fear of family disapproval, sometimes from a deeper distrust of police institutions. Several documented cases involve victims who took their own lives before reporting the fraud at all. Cultural stigma thus suppresses the true incidence of the offence, and the official figures, daunting as they already are, almost certainly understate the scale of the problem.

XII. Awareness and Prevention

In this domain, more than most, awareness is the first and most cost-effective line of defence. The preventive architecture works at three levels.

At the level of personal vigilance, the citizen needs to absorb three propositions and, if it helps, keep them on a card beside the telephone. First, no Indian investigative agency communicates an arrest, a summons, or a freeze order by phone or video call; written process under the BNSS is the only lawful mode. Second, no agency asks for funds to be transferred to a "verification account," an "RBI escrow," or any private bank account. Third, a demand to stay on a continuous video call, to refrain from contacting family, or to "self-arrest at home" is categorically extra-legal. Taken together, these three propositions are enough to immunise the citizen against the digital arrest variant entirely. The whole trick lies in holding on to them at the very moment when fear is doing its work.

At the institutional level, banks are required under RBI guidelines to maintain round-the-clock channels for reporting unauthorised transactions and to register customers for SMS and email alerts. In its Master Direction on Digital Payment Security Controls of February 2021 the Reserve Bank requires regulated entities to deploy real-time fraud monitoring, two-factor authentication, and adaptive risk-based authentication. Payment aggregators, under the 2020 Guidelines, must escrow funds and observe strict KYC norms. NPCI's fraud-awareness portal, built for the consumer side of the same equation, supplies a single user-facing resource on the principal modalities of UPI and IMPS fraud and ranks among the most accessible authoritative sources of preventive guidance currently available. These are sound prescriptions. Implementation, as so often in this field, is uneven.

At the technological level, the Department of Telecommunications has deployed its International Incoming Spoofed Call Prevention System, the AI-based Stentor and Sahyog platforms for detecting fraudulent calls, and is integrating TRAI's caller-name presentation pilots. The Sanchar Saathi mobile application lets a citizen verify the connections issued in her name, report fraudulent communications through Chakshu, and block lost handsets through CEIR. These are useful tools, all of them. None substitutes for the basic point: the citizen who has internalised the three propositions above will not, in the first place, find herself needing them.

XIII. Government Initiatives and Public-Awareness Campaigns

Over the past three years the Government of India has layered a set of initiatives into something approaching a coordinated public-awareness response. The Indian Cyber Crime Coordination Centre, the National Cyber Crime Reporting Portal, the 1930 helpline, and the Citizen Financial Cyber Fraud Reporting and Management System together form the institutional spine. The Cyber Fraud Mitigation Centre at the I4C, formally inaugurated in 2024, gathers banks, payment aggregators, telecom operators, IT intermediaries, and law-enforcement under one roof, a single physical location for the coordinated

response the offence demands. The two-day National Conference on "Tackling Cyber-Enabled Frauds and Dismantling the Ecosystem," held in New Delhi on 10 and 11 February 2026, was the largest single convening on the subject the Government has yet attempted: 362 delegates attended in person, drawn from State police units, the I4C, telecom service providers, central law-enforcement agencies, public-sector and private banks, cooperative banks, fintechs and payment aggregators, cryptocurrency exchanges, IT intermediaries, academia, and the intelligence agencies, and the proceedings were telecast live to 2,356 locations covering every State Police unit and every CBI branch in the country. On the awareness side, the Prime Minister's Mann ki Baat address of 27 October 2024 marked a watershed: it brought the term "digital arrest" into mainstream public discourse and produced the now-familiar formula, "Stop, Think, Take Action."

Cyber Jaagrookta Diwas, observed on the first Wednesday of every month since 2022, is a Ministry of Home Affairs initiative requiring Central and State departments to conduct cyber-awareness sessions for their employees and outreach within their respective jurisdictions. The Indian Computer Emergency Response Team (CERT-In) issues regular advisories; its advisory of October 2024 set out twelve modalities of online scam and instructed government agencies not to use WhatsApp or Skype for official communication.

At the State level several units have mounted dedicated campaigns. Maharashtra's "Cyber Safe Maharashtra" programme, Karnataka's upgraded 1930 helpline with its multilingual IVR launched in April 2025, Haryana's integrated Central Cyber Reporting Portal, and Tamil Nadu's Cyber Crime Wing have all added to the public outreach. Through its Cyber Awareness modules the National Legal Services Authority supplies legal-literacy content for distribution through District Legal Services Authorities. Viewed in aggregate, the picture is one of considerable activity. Whether that activity translates into reduced victimisation is a measurement question remains the subject of debate.

XIV. Towards a Reform Agenda

Drawing on the analysis in the previous parts, this article sets out nine calibrated proposals for legislative, regulatory and institutional reform. Each is defended briefly. They are offered as a coherent package, not a menu.

First, statutory recognition of digital impersonation extortion. A dedicated provision should be inserted into either the Information Technology Act or the Bharatiya Nyaya Sanhita, defining and punishing the impersonation of public officials through electronic means for wrongful gain. It should

attract enhanced punishment, a minimum of seven years' imprisonment extending to life, where the impersonation involves the judiciary, the CBI, the ED, the police, or the armed forces. The aim is not to increase offences for the sake of it. The digital arrest is qualitatively different from ordinary cheating in that it turns the State's own authority against the citizen. It is to record this, in the criminal law itself.

Second, a statutory APP-fraud reimbursement program. India should consider the United Kingdom's Payment Systems Regulator model, and establish a framework that makes banks reimburse the victim of authorised push payment fraud, up to a certain limit such as ₹50 lakh, with the cost being borne by the remitting bank and the beneficiary bank. The RBI's 2017 circular should be amended to specifically cover transactions effected under coercion or deception, placing the burden of proof of "informed consent" on the bank. This one intervention would re-set the incentive structures of the whole system. As long as the bank knows that if there is fraud, the loss will be the customer's, it has no commercial incentive to spend serious money on fraud-prevention infrastructure. If the bank eats a meaningful slice of the loss, the investment will follow.

Third, a real-time inter-bank tracing protocol anchored in the Mule Account Hunter framework. A statutory obligation should be laid on banks, payment aggregators, UPI payment service providers, and the NPCI to follow a uniform real-time tracing protocol on receipt of a 1930 complaint, with prescribed turnaround times for freezing and reverse-tracing funds. Universal adoption of the Mule Account Hunter software, already developed jointly by the Government and the Reserve Bank, should be made a regulatory condition rather than an exhortation, on timelines that bind cooperative and urban co-operative banks alongside the larger institutions.

Fourth, mandatory caller-name presentation, biometric SIM verification, and rapid SIM blocking. TRAI's caller-name presentation pilot should be made mandatory for all telecom operators, so that the recipient of every call sees the verified name of the caller before answering. The Department of Telecommunications' proposed Telecommunications (User Identification) Rules and the related Biometric Identity Verification System should be notified at the earliest practicable date, and the Inter-Departmental Committee's proposal to cut the SIM-blocking window to two or three hours should be adopted as a binding service-level commitment. On the face of it they are narrow technical reforms. But their implications for impersonation fraud would be considerable. The fraudster who is forced to act under a verified name, on a biometrically attested SIM that can be blocked in hours of the first complaint, loses the principal levers of authority and persistence on which the digital arrest variant depends.

Fifth, platform-level enforcement of impersonation patterns. The WhatsApp investigation undertaken at the Inter-Departmental Committee's instance offers a template that should be generalised across all major messaging platforms operating in India. A regulatory framework, ideally under the IT Rules, 2021, with defined safe-harbour conditions, should require platforms to deploy logo-detection systems, language-model-based impersonation-pattern detection, network-level enforcement, and a minimum retention period for deleted-account data for law-enforcement purposes. SIM-binding, presently the subject of a DoT circular of 28 November 2025, should be made a uniform requirement across platforms.

Sixth, cyber-forensic capacity building. A National Cyber Forensic Mission, on the model of the BharatNet programme, should be established with the goal of ensuring at least one Tier-3 cyber-forensic laboratory per State and at least one Tier-2 facility per district by 2028. Personnel training should be conducted in partnership with the National Forensic Sciences University. Without this infrastructural floor the doctrinal advances of Section 111 of the BNS will stay merely doctrinal, since the syndicate cannot be prosecuted if the evidence to prosecute it cannot be assembled.

Seventh, trans-national cooperation. India should fast-track MLAT negotiations with Cambodia, Myanmar, and Laos, and should accede to the Budapest Convention on Cybercrime, which it has so far declined to sign, in order to ease evidence-sharing. A dedicated India-ASEAN Cyber Cooperation Mechanism would complement the existing bilateral arrangements. The cyber fraud problem is, in truth, a foreign-policy problem in domestic dress; treating it as anything less will go on yielding sub-optimal results.

Eighth, a senior-citizen cyber-protection programme. Given how disproportionately senior citizens are targeted, a dedicated outreach programme delivered through pension banks, residents' welfare associations, and senior-citizen forums should be institutionalised. It should include mock-call demonstrations and a single-point grievance liaison. The intervention has to meet the demographic where it actually lives.

Ninth, mandatory bank-side fraud-detection thresholds. The Reserve Bank should require banks to deploy adaptive, AI-based fraud-detection that flags large outward transfers from senior-citizen accounts, unusually rapid sequential transfers, and, most important of all, transfers made immediately after an inbound call. Where such a flag is raised, a mandatory thirty-minute cooling-off period should apply, during which the bank must reach the customer through an independent channel. This single point

of procedural friction would prevent a substantial share of completed frauds without imposing any serious burden on legitimate transactions.

XV. Conclusion

The digital arrest fraud is a hybrid animal. Its psychological technique is ancient, for the abuse of authority predates written law; its technological execution is modern; and its operational geography is trans-national. India's legal response has not been insignificant but rather reactive rather than architectural. Section 111 of the Bharatiya Nyaya Sanhita; the Supreme Court's suo motu intervention in *In Re: Victims of Digital Arrest*, now operating through an Inter-Departmental Committee under the Court's continuing supervision; the procedural safeguards consolidated in *Satender Kumar Antil*; the WhatsApp account-bans and platform-level enforcement now under way; the institutional scaffolding built around the I4C, the Sanchar Saathi platform, and the new CBI Cybercrime Branch, all of these, taken together, supply the rudiments of a protective regime. What they do not yet supply is the regime itself. The figures from 2024 alone, ₹1,935 crore lost to a single fraud variant, and ₹8,189 crore recovered out of an estimated ₹20,000 crore by early 2026, which is to say roughly two-fifths, are the measure of the gap between what we have and what we need.

What the situation needs is a paradigm shift. We need to move from a regime where the victim has to prove negligence on the part of the bank, to one where the State and the regulated intermediary share the responsibility to prevent the harm in the first place. The United Kingdom's mandatory APP-fraud reimbursement model, Singapore's Shared Responsibility Framework and the European Union's emerging Payment Services Directive 3 all provide a template. Given the scale of digital adoption and the corresponding scale of digital exposure, there is a need and an institutional capacity for India to build a world-class victim-protection regime. Until that happens, the digital arrest will continue to reveal something uncomfortable: that in cyberspace, as in physical space, the most consequential arrest is not the one effected by the State but the one in which the State's very authority has been hijacked against the citizen it was meant to protect.

The way ahead is not, in the main, technological. The technology is already there, and is being deployed in the deployments now visible on the record in SMW (Crl.) 3/2025. What has to be built is the legal scaffolding that links liability with capacity to prevent; the institutional machinery that enables real time inter-agency action; and the public consciousness that immunises the citizen at the point of attack. The challenge for legal scholarship in the next few years is to translate the moral clarity already expressed by

the Supreme Court and the Prime Minister into a calibrated, enforceable, victim-centric statutory framework. That, after all, is the measure for determining whether the constitutional guarantee of life and personal liberty under Article 21 has a meaningful reach into the digital domain. The answer on this record is that it doesn't yet. The work of the coming decade is the work of making it so.

References

Legal authorities (statutes and cases) are cited in standard legal form, consistent with the convention adopted by the Publication Manual of the American Psychological Association (7th ed.), which follows established legal-citation practice for such materials. All other sources are presented in APA 7th edition style.

A. Statutes and Legislation

Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (India).

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (India).

Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (India).

Information Technology Act, No. 21 of 2000, India Code (India).

Information Technology (Amendment) Act, No. 10 of 2009, India Code (India).

Digital Personal Data Protection Act, No. 22 of 2023, India Code (India).

Prevention of Money-Laundering Act, No. 15 of 2003, India Code (India).

Indian Penal Code, No. 45 of 1860, India Code (India) [repealed].

Code of Criminal Procedure, No. 2 of 1974, India Code (India) [repealed].

Fraud Act 2006, c. 35 (U.K.).

Wire Fraud, 18 U.S.C. § 1343 (U.S.).

B. Cases

In Re: Victims of Digital Arrest Related to Forged Documents v. Avishkar Singhvi, SMW (Crl.) 3/2025, orders dated Oct. 17, 2025; Oct. 27, 2025; Dec. 1, 2025; Feb. 9, 2026 (Supreme Court of India).

Satender Kumar Antil v. Central Bureau of Investigation, (2022) 10 SCC 51 (India).

Satender Kumar Antil v. Central Bureau of Investigation, M.A. No. 2034/2022, order dated Jan. 21, 2025 (Supreme Court of India).

State of Haryana v. Satender Kumar Antil, 2025 INSC 909, order dated Jul. 16, 2025 (Supreme Court of India).

Satender Kumar Antil v. Central Bureau of Investigation, 2026 INSC 115, order dated Jan. 15, 2026 (Supreme Court of India).

Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273 (India).

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

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

Suresh Chandra Negi v. Bank of Baroda, Writ (C) No. 24192 of 2022 (Allahabad H.C.) (India).

Joginder Kumar v. State of U.P., (1994) 4 SCC 260 (India).

C. Government and Regulatory Sources

Department of Telecommunications. (2024, December 24). *Press release on the International Spoofed Call Prevention System.* Government of India.

Department of Telecommunications. (2025, November 28). *Circular dated 28 November 2025: Proposed Telecommunications (User Identification) Rules and Biometric Identity Verification System.* Government of India.

Department of Telecommunications. (n.d.). *Sanchar Saathi portal.* Government of India. https://sancharsaathi.gov.in/

Indian Computer Emergency Response Team. (2024, October 27). *Advisory on digital arrest scams.* Ministry of Electronics and Information Technology, Government of India.

Indian Cyber Crime Coordination Centre. (2024). *Annual report 2023-24.* Ministry of Home Affairs, Government of India.

Ministry of Home Affairs. (2025, March 11). *Reply to Rajya Sabha Unstarred Question No. 1442* (Statement of B. Sanjay Kumar, Minister of State for Home Affairs). Parliament of India.

Ministry of Home Affairs. (2026, February 10). *Union Home Minister Amit Shah delivers keynote address at the National Conference on "Tackling Cyber-Enabled Frauds and Dismantling the Ecosystem"* [Press release, ID 2226082]. Press Information Bureau, Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226082

National Crime Records Bureau. (2023). *Crime in India 2022.* Ministry of Home Affairs, Government of India.

National Payments Corporation of India. (n.d.). *Fraud awareness portal.* https://www.npci.org.in/fraud-awareness

Press Information Bureau. (2024, December 10). *Digital arrest scam.* Government of India.

Prime Minister's Office. (2024, October 27). *Mann ki Baat, 115th episode* [Address to the nation]. Government of India.

Reserve Bank of India. (2017, July 6). *Customer protection: Limiting liability of customers in unauthorised electronic banking transactions* (Circular DBR.No.Leg.BC.78/09.07.005/2017-18).

Reserve Bank of India. (2021, February 18). *Master direction on digital payment security controls.*

D. Secondary Sources and News Reports

Amnesty International. (2025, November). *Trafficking and forced labour in Southeast Asian scam compounds.*

Bar and Bench. (2025, January 29). *How recent Supreme Court directions provide a meaningful way to tackle growing digital arrest crimes.*

Bharati, R. K. (2025, August 5). *Identity theft and impersonation in cyberspace (Sections 66C and 66D of the IT Act, 2000).* SSRN.

Bhagwat, V. (2024). *Bharatiya Nyaya Sanhita and cyber crimes.*

Cyril Amarchand Mangaldas. (2025, February 13). *From clicks to cuffs: Understanding digital arrest in the Indian legal landscape.* Dispute Resolution Blog.

CyberPeace Foundation. (2025, April 4). *The Government crackdown on digital arrest.*

CyberPeace Foundation. (2025, July 25). *Zero liability principle in cyber frauds: Recent verdicts and banking practices.*

Deccan Herald. (2026, May 25). *Bengaluru Rs 24 cr digital arrest case: Suspects found involved in another fraud.* https://www.deccanherald.com/india/karnataka/bengaluru/bengaluru-rs-24-cr-digital-arrest-case-suspects-found-involved-in-another-fraud-4015843

Inc42. (2025, March 14). *Indians lost ₹1,935 cr to digital arrest scams in 2024: Govt.*

ISACA. (2025, June 20). *Trapped virtually: Understanding digital arrest scams.* Industry News.

Oneindia News. (2026, February 12). *Inside Cambodia's digital arrest scam network that targeted Indians.*

Shrivastava, A. (2026, April 28). *WhatsApp banned 9400 accounts linked to digital arrest scams: MHA tells Supreme Court.* LiveLaw. https://www.livelaw.in/top-stories/whatsapp-banned-9400-accounts-linked-to-digital-arrest-scams-mha-tells-supreme-court-532063

The420.in. (2025, December 27). *Top 10 most highlighted cyber crime cases and trends in India in 2025.*

1. [1]Ministry of Home Affairs, Reply to Rajya Sabha Unstarred Question No. 1442 (Mar. 11, 2025) (statement of B. Sanjay Kumar, Minister of State for Home Affairs); see also Inc42, Indians Lost ₹1,935 Cr to Digital Arrest Scams in 2024: Govt (Mar. 14, 2025).
2. [1]Ministry of Home Affairs, Cybercrime Statistics [Press release] (Feb. 28, 2025); The420.in, Top 10 Most Highlighted Cyber Crime Cases and Trends in India in 2025 (Dec. 27, 2025).
3. [1]The420.in (2025), supra note 2.
4. [1]Prime Minister's Office, Address to the Nation, Mann ki Baat, 115th episode (Oct. 27, 2024).
5. [1]Satender Kumar Antil v. Central Bureau of Investigation, (2022) 10 SCC 51 (India); see also M.A. No. 2034/2022, order dated Jan. 21, 2025.
6. [1]In Re: Victims of Digital Arrest Related to Forged Documents v. Avishkar Singhvi, SMW (Crl.) 3/2025, order dated Oct. 17, 2025 (Sup. Ct. India).

7. [1]R. Kumar, Chief Executive Officer, Indian Cyber Crime Coordination Centre, public statement (Apr. 2024).
8. [1]Rajya Sabha Unstarred Question No. 1442 (Mar. 11, 2025), supra note 1.
9. [1]Ministry of Home Affairs, Cyber Fraud Mitigation Centre Briefing (Mar. 2025).
10. [1]Ministry of Home Affairs, Union Home Minister Amit Shah Delivers Keynote Address at the National Conference on "Tackling Cyber-Enabled Frauds and Dismantling the Ecosystem" [Press release, ID 2226082] (Feb. 10, 2026). The release records that the I4C reporting portal had been accessed more than 230 million times between January 2020 and 30 November 2025; that over 8.2 million cybercrime complaints had been registered, of which roughly 184,000 had matured into FIRs; that the Government had cancelled more than 12 lakh suspicious SIM cards and blocked the IMEI numbers of over 3 lakh devices by December 2025; and that 20,853 accused had been arrested in cybercrime cases.
11. [1]In Re: Victims of Digital Arrest, supra note 6 (recording loss of ₹1.05 crore through forged judicial orders purporting to issue under the Prevention of Money-Laundering Act, 2002).
12. [1]Writ Petition (Crl.) under Article 32 of the Constitution, notice issued Jan. 30, 2026 (Surya Kant, C.J.I., and Joymalya Bagchi, J.).
13. [1]Deccan Herald, Bengaluru Rs 24 Cr Digital Arrest Case: Suspects Found Involved in Another Fraud (May 25, 2026), https://www.deccanherald.com/india/karnataka/bengaluru/bengaluru-rs-24-cr-digital-arrest-case-suspects-found-involved-in-another-fraud-4015843 (the suspects, who posed as senior officers of the CBI and the Enforcement Directorate, were linked by the Karnataka Cyber Command to a separate ₹15 crore scam in Belagavi and to several further interstate offences; roughly ₹1.46 crore had been recovered by the date of reporting).
14. [1]In Re: Victims of Digital Arrest, order dated Oct. 17, 2025 (Sup. Ct. India).
15. [1]Department of Telecommunications, Press Release on the International Spoofed Call Prevention System (Dec. 24, 2024); Sanchar Saathi Portal, https://sancharsaathi.gov.in/.
16. [1]Oneindia News, Inside Cambodia's Digital Arrest Scam Network That Targeted Indians (Feb. 12, 2026); A. Shrivastava, WhatsApp Banned 9400 Accounts Linked to Digital Arrest Scams: MHA Tells Supreme Court, LiveLaw (Apr. 28, 2026) (recording WhatsApp's representation to the Inter-Departmental Committee that the bulk of such operations targeting Indian users originate from Southeast Asia, particularly Cambodia, and run through clusters of accounts and groups exhibiting repeated, machine-detectable patterns).
17. [1]Prime Minister's Office, Mann ki Baat (Oct. 27, 2024), supra note 4.

18. [1] Information Technology Act, No. 21 of 2000, Sec. 66C (India), inserted by the Information Technology (Amendment) Act, 2008.
19. [1]Information Technology Act, Sec. 66D.
20. [1]Bharatiya Nyaya Sanhita, No. 45 of 2023, Sec. 316, 318 (India).
21. [1]Bharatiya Nyaya Sanhita, Sec. 319.
22. [1]Bharatiya Nyaya Sanhita, Sec. 111.
23. [1]Ahmedabad Cyber Crime Branch, First Information Report (May 2025), as reported in The Hawk (May 12, 2025).
24. [1] Reserve Bank of India, Customer Protection: Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, Circular DBR.No.Leg.BC.78/09.07.005/2017-18 (Jul. 6, 2017).
25. [1]National Payments Corporation of India, Fraud Awareness Portal, https://www.npci.org.in/fraud-awareness (consumer-facing information on common UPI, IMPS and digital-payment frauds, including the impersonation and "digital arrest" variants, with prescribed safe-payment practices for end-users of the NPCI rails).
26. [1] Indian Cyber Crime Coordination Centre, Annual Report 2023-24 (Ministry of Home Affairs, Government of India); Ministry of Home Affairs, Press Release ID 2226082 (Feb. 10, 2026), supra note 10.
27. [1]Department of Telecommunications, Sanchar Saathi Portal, https://sancharsaathi.gov.in/.
28. [1]Ministry of Home Affairs, Press Release ID 2226082 (Feb. 10, 2026), supra note 10 (recording the inauguration of the CBI Cybercrime Branch and the launch of the State Cyber Crime Coordination Centre (S4C) dashboard of the I4C on 10 February 2026).
29. [1]Ministry of Home Affairs, Press Release ID 2226082 (Feb. 10, 2026), supra note 10 (recording that the Government had safeguarded ₹8,189 crore out of an estimated Rs. 20,000 crore in cyber fraud through roughly 361,000 complaints; that 62 banks and financial institutions had been onboarded to the I4C mechanism by 31 December 2025, with the target of onboarding all financial institutions, including cooperative banks, by December 2026; that 795 institutions across banks, fintechs, NBFCs and e-commerce platforms were connected to the I4C; and that the Mule Account Hunter software, developed jointly by the Government of India and the Reserve Bank, was to be adopted by all banks).
30. [1]The420.in (2025), supra note 2.
31. [1]In Re: Victims of Digital Arrest Related to Forged Documents v. Avishkar Singhvi, order dated Dec. 1, 2025 (Sup. Ct. India).

32. [1]Satender Kumar Antil v. CBI, (2022) 10 SCC 51; M.A. No. 2034/2022, order dated Jan. 21, 2025; State of Haryana v. Satender Kumar Antil, 2025 INSC 909 (Jul. 16, 2025); Satender Kumar Antil v. CBI, 2026 INSC 115 (Jan. 15, 2026).
33. [1]In Re: Victims of Digital Arrest, orders dated Oct. 17, 2025, Oct. 27, 2025 and Dec. 1, 2025 (Sup. Ct. India).
34. [1]A. Shrivastava, WhatsApp Banned 9400 Accounts Linked to Digital Arrest Scams: MHA Tells Supreme Court, LiveLaw (Apr. 28, 2026), https://www.livelaw.in/top-stories/whatsapp-banned-9400-accounts-linked-to-digital-arrest-scams-mha-tells-supreme-court-532063 (recording the status report filed by the Attorney-General for India on behalf of the I4C in SMW (Crl.) 3/2025 pursuant to the Court's directions of 9 February 2026; that WhatsApp, responding to inputs from the I4C, MeitY and the DoT, launched a structured multi-week investigation in January 2026 focused on digital arrest scams targeting Indian users and, on a methodology of seed signals, network mapping and network-level enforcement, banned 9,400 accounts engaged in law-enforcement impersonation; that the platform deployed logo-detection systems matching profile photos against databases of police insignia, language-model-based impersonation detection, and account-age and profile-photo suppression for unknown contacts; that SIM-binding was being rolled out under the DoT circular of 28 November 2025; and that the Inter-Departmental Committee was examining a reduction in the SIM-blocking window to two or three hours).
35. [1]U.S. Department of Justice [Press release] (Feb. 2025); ISACA, Trapped Virtually: Understanding Digital Arrest Scams (Jun. 20, 2025).
36. [1]Reports on the trafficking of Chinese nationals to overseas scam centres (2025); CNN, Cambodia Extradites Chen Zhi to China (Nov. 2025).
37. [1]Associated Press, Cambodia Raids on Scam Centres (2025); Amnesty International, Trafficking and Forced Labour in Southeast Asian Scam Compounds (Nov. 2025).
38. [1]Ministry of Home Affairs, Press Release ID 2226082 (Feb. 10, 2026), supra note 10 (recording that the National Conference convened on 10 February 2026 with 362 delegates present and proceedings telecast to 2,356 locations covering all State Police units and CBI branches, and that the sessions addressed (i) fraud-ecosystem trends, (ii) mule accounts and financial laundering, and (iii) SIM, eSIM and telecom-infrastructure misuse).
39. [1]Prime Minister's Office, Mann ki Baat (Oct. 27, 2024), supra note 4.
40. [1]Indian Computer Emergency Response Team (CERT-In), Advisory on Digital Arrest Scams (Oct. 27, 2024).