DIGITAL ARREST IN INDIA: SIMULATED STATE COERCION, CYBER FRAUD AND THE REGULATORY LIMITS OF CRIMINAL LAW

Adv. Sonia Saini, Managing Partner, SS Global Law Firm, New Delhi

ABSTRACT

'Digital arrest' has emerged as one of the most disturbing forms of cyber-enabled financial fraud in India. Fraudsters impersonate police officers, officers of the Central Bureau of Investigation (CBI), the Enforcement Directorate, customs officials, regulators and even judicial authorities; display fabricated warrants and official-looking communications; accuse victims of offences such as money laundering, narcotics trafficking or misuse of identity; and thereafter use prolonged video surveillance and threats of arrest to obtain money. Yet the expression 'digital arrest' describes no legally recognised procedure. The CBI has expressly reiterated that there is no legal concept of digital arrest in Indian law. This paper argues that the phenomenon should not be understood merely as online cheating. Its distinguishing feature is the deliberate simulation of State coercion: private actors appropriate the identity, procedures, symbols and coercive legitimacy of public institutions so that a victim submits to demands that would otherwise be rejected. Deception establishes credibility, but fear of arrest, prosecution, asset seizure or imprisonment produces compliance. The conduct consequently sits at the intersection of cheating, extortion, public-servant personation, forgery, criminal intimidation, cyber-personation and, in qualifying cases, organised crime. The paper examines the Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), Information Technology Act, 2000, Telecommunications Act, 2023 and India's evolving cyber-fraud response. It further analyses the Supreme Court's continuing suo motu proceedings in In Re: Victims of Digital Arrest Related to Forged Documents, the January 2026 NCRP-CFCFRMS Standard Operating Procedure, CBI's ABHAY notice-authentication system, mule-account controls and emerging victim-restoration mechanisms. The paper concludes that India does not suffer from a complete criminalisation gap. The more serious weakness is a fragmented prevention, authentication, financial-interdiction and restitution architecture. It proposes a five-pillar model based on verifiable governmental communications, real-time financial intervention, telecom traceability, intermediary cooperation and victim restoration. In the digital State, the identity and authority of the State itself

must be treated as a cybersecurity asset.[12]

Keywords: Digital Arrest; Cybercrime; Simulated State Coercion; Cyber Fraud; Bharatiya Nyaya Sanhita; Artificial Intelligence; Mule Accounts; Cyber-Personation; Victim Restitution; State Impersonation.

I. INTRODUCTION

The most effective feature of a digital-arrest scam is not technological sophistication. It is authority. A victim receives a telephone or video call. The caller claims to represent the police, CBI, Enforcement Directorate, customs authorities, a telecommunications company or another public institution. Personal information may be recited to establish credibility. The victim is told that an Aadhaar number, mobile connection, bank account, passport or other identifying information has allegedly surfaced in a criminal investigation. The allegation is usually grave: money laundering, narcotics trafficking, terrorism financing, receipt of criminal proceeds or misuse of identity. A purported police officer may appear on video. A fabricated FIR, attachment order, warrant or judicial document may be displayed. The victim is instructed not to disconnect the call and, in some cases, not to communicate with family members. What begins as impersonation is gradually transformed into a sham investigation.[3]

The decisive representation then follows: the victim is under ‘digital arrest’. There is no such process in Indian criminal procedure. In May 2026, while launching ABHAY, the CBI stated that fraudsters initiate sham legal processes and keep victims under surveillance for days under the guise of a digital arrest, a concept that has no legal existence in Indian law. The absence of legal validity, however, does not prevent the victim from experiencing the command as real. A person who genuinely believes that a senior police officer or judge has ordered continued video presence may comply for hours. A person convinced that refusal to transfer money will result in immediate arrest may transfer retirement savings or family funds to an account supposedly designated for verification or safe custody.[4]

---

[1] Central Bureau of Investigation, ‘CBI Launches ABHAY - AI-Powered Notice Verification System’ (15 May 2026), Press Information Bureau, Release ID 2261539, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2261539&lang=2&reg=48.

[2] Ministry of Home Affairs, ‘CFCFRMS 2.0 Platform’ (28 July 2026), Press Information Bureau, Release ID 2290377, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2290377&lang=2&reg=48; Ministry of Home Affairs, NCRP-CFCFRMS SOP issued 2 January 2026, PIB Release ID 2241336.

[3] Ministry of Home Affairs / Indian Cyber Crime Coordination Centre (I4C), 'Alert against incidents of Blackmail and Digital Arrest by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies' (2024), PIB Release ID 2020570.

[4] Central Bureau of Investigation, ‘CBI Launches ABHAY - AI-Powered Notice Verification System’ (15 May

The scale of the wider cyber-fraud ecosystem explains why the problem cannot be dismissed as occasional impersonation. By 30 June 2026, the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) had recorded more than 32.80 lakh complaints in which more than Rs 11,158 crore had been saved from dissipation. The National Human Rights Commission (NHRC), at an Open House Discussion on digital-arrest scams on 9 June 2026, referred to reported losses of approximately Rs 52,976 crore from cyber-enabled fraud over six years and noted that nearly eight per cent of those losses were attributed to digital-arrest scams. The figures are not a direct measure of convictions or proven cases, but they demonstrate the economic and institutional stakes of cyber-enabled coercive fraud.[56]

The Supreme Court has also treated the issue as a distinct national problem. Suo Motu Writ Petition (Criminal) No. 3 of 2025, In Re: Victims of Digital Arrest Related to Forged Documents, remained pending in 2026, with an order recorded on 28 July 2026. A July 2026 CBI case illustrates the Court-linked enforcement architecture: the CBI reported that a case involving a senior citizen coerced into transferring Rs 25.65 lakh had been transferred for re-registration in compliance with the Supreme Court's order dated 1 December 2025.[78]

This paper argues that 'cyber fraud' is an accurate but incomplete description. In an investment scam, the offender fabricates an economic opportunity. In phishing, the offender often imitates a trusted institution to obtain credentials. Digital arrest adds a qualitatively different element: coercive submission to fabricated sovereign authority. The victim does not merely believe a false fact. The victim believes that the State has acquired lawful coercive power over him or her.

The paper therefore proposes the concept of simulated State coercion. The term denotes criminal conduct in which private actors use technology to imitate the identity, process and coercive authority of the State in order to obtain property, information, access, an act or an omission. Three appropriations commonly operate together. First, the offender appropriates State identity by claiming to be a police officer, investigator, regulator, prosecutor or judicial

2026), PIB Release ID 2261539.
[5] Ministry of Home Affairs, 'CFCFRMS 2.0 Platform' (28 July 2026), PIB Release ID 2290377.
[6] National Human Rights Commission / Press Information Bureau, 'Safeguarding human rights against digital arrest scams' (9 June 2026), PIB Release ID 2270875, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2270875&lang=1&reg=48.
[7] Supreme Court of India, In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Criminal) No 3 of 2025, order recorded 28 July 2026, Supreme Court Latest Orders page.
[8] Central Bureau of Investigation, 'CBI Arrests Accused in Digital Arrest Cyber Fraud Case' (2 July 2026), PIB Release ID 2280197, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2280197&lang=2&reg=48.

authority. Secondly, the offender appropriates State process by reproducing warrants, summonses, uniforms, police-station settings, legal terminology and hierarchies. Thirdly, the offender appropriates State coercion by threatening arrest, prosecution, imprisonment, asset restraint or consequences for relatives.

This framework produces a more precise legal inquiry. The question is not simply whether digital arrest is separately named in a penal statute. The question is whether existing criminal provisions capture the constituent wrongs, whether the regulatory ecosystem can interrupt them quickly enough, and whether citizens possess a reliable means to authenticate purported exercises of public power.

II. RESEARCH QUESTION, HYPOTHESIS AND METHODOLOGY

The principal research question is whether India's current legal framework adequately captures the distinctive wrong involved in digital-arrest scams and, if not, whether the principal deficiency lies in substantive criminal law or in the institutional architecture governing prevention, investigation, financial interdiction and restitution.

The paper proceeds on the hypothesis that India substantially criminalises the constituent acts involved in digital arrest but does not yet possess a sufficiently integrated framework for preventing and interrupting the offence as a coordinated misuse of State identity, telecommunications infrastructure, digital platforms and financial systems. A crime can be comprehensively punishable after it occurs and nevertheless remain inadequately regulated while it is occurring.

The methodology is primarily doctrinal and regulatory. The doctrinal component examines relevant provisions of the BNS, BNSS, Information Technology Act, 2000 and Telecommunications Act, 2023. The regulatory component examines official measures involving I4C, NCRP, CFCFRMS, the Cyber Fraud Mitigation Centre, telecom controls, suspect registries, mule-account detection, notice authentication, CBI investigation and victim restoration. The analysis relies predominantly upon statutes, Supreme Court material and official Government, CBI, NHRC and regulatory publications. The concept of simulated State coercion is an analytical contribution of this paper rather than an existing statutory category.[9]

[9] Bharatiya Nyaya Sanhita 2023; Bharatiya Nagarik Suraksha Sanhita 2023; Information Technology Act 2000;

The paper does not argue that every factual scenario popularly called a digital arrest must attract every offence discussed below. Criminal liability remains ingredient-specific and evidence-specific. Its purpose is instead to identify the doctrinal tools available and to show why the phenomenon is structurally wider than a single offence of cheating.

III. THE ANATOMY OF A DIGITAL ARREST

A. Acquisition of Credibility

A digital-arrest operation normally begins by constructing credibility. Fraudsters may possess real information about the victim, whether obtained from data leaks, publicly available sources, compromised databases, previous fraud activity or social engineering. Correct personal details weaken initial scepticism because they create an inference that the caller has institutional access.[10]

Visual and auditory cues deepen that inference. Uniforms, official logos, realistic office backgrounds, identification cards and authoritative legal vocabulary reproduce the social appearance of criminal investigation. The Ministry of Home Affairs had already warned in 2024 that offenders used studios modelled on police stations and government offices and remained visually connected to victims through video-conferencing platforms until their demands were met. Artificial intelligence now compounds the problem. Synthetic voice, manipulated video and automatically generated documents can make a false official communication far more persuasive than the crude impersonation scams of an earlier era.[11]

B. Manufacture of Criminal Jeopardy

Credibility alone does not produce compliance. The victim must next be placed in perceived legal jeopardy. A mobile number may allegedly have been used for illegal activity; a courier may supposedly contain narcotics; a bank account may be linked to money laundering; an

Telecommunications Act 2023.

[10] See Ministry of Home Affairs / I4C, 'Alert against incidents of Blackmail and Digital Arrest by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies' (2024), PIB Release ID 2020570; Central Bureau of Investigation, ABHAY notice-verification advisory (15 May 2026), PIB Release ID 2261539.

[11] Ministry of Home Affairs / I4C, 'Alert against incidents of Blackmail and Digital Arrest by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies' (2024), PIB Release ID 2020570.

Aadhaar number may have been used to open accounts connected with crime. The allegation is selected to induce panic before the victim has time to seek independent advice.[12]

The accusation changes the decision-making environment. A demand that would ordinarily appear absurd can begin to look like a condition of avoiding immediate arrest. This is why a legal analysis confined to deception is incomplete. The falsehood creates the stage on which coercion subsequently operates.

C. Simulation of Procedure

The third stage reproduces legal process. The victim may be transferred between supposed departments, questioned by multiple purported officials, shown fabricated records or told that a senior officer or judge is supervising the matter. The sequence imitates institutional hierarchy. One false official validates another, creating a closed system in which every source of apparent verification is controlled by the offenders.[13]

Procedural detail performs a legitimating function. A criminal who simply asks for money appears to be a criminal. A network that supplies a complaint number, displays a warrant, uses legal terminology, conducts an interview and purports to escalate the matter to a superior can make the same demand resemble official procedure.

D. Isolation and Coercive Control

The victim may then be instructed not to tell family members because the investigation is supposedly confidential. The video connection may remain active for long periods. The offender thereby removes the most obvious source of corrective information: another person who is not emotionally trapped inside the fabricated investigation.[14]

At this stage, the scam becomes what this paper calls coercion without custody. There may be no physical barrier and no offender present in the victim's home. Yet the victim's autonomy is

[12] Ministry of Home Affairs / I4C, 'Alert against incidents of Blackmail and Digital Arrest by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies' (2024), PIB Release ID 2020570; Central Bureau of Investigation, 'CBI Arrests Accused in Digital Arrest Cyber Fraud Case' (2 July 2026), PIB Release ID 2280197.

[13] In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 1 December 2025 (SC), recording the use of forged documents and sham official processes in digital-arrest scams; Central Bureau of Investigation, ABHAY notice-verification advisory (15 May 2026), PIB Release ID 2261539.

[14] Central Bureau of Investigation, ABHAY notice-verification advisory (15 May 2026), PIB Release ID 2261539 (describing sham legal processes capable of keeping victims under surveillance for prolonged periods).

constrained by the belief that a lawful authority has ordered continued presence and that disobedience will lead to arrest. Technology allows visual supervision to be simulated remotely and continuously.

E. Extraction and Laundering

The process culminates in extraction. Money may be described as a security deposit, verification transfer, refundable amount, tax, penalty or temporary movement of funds to a safe or government-supervised account. Once transferred, it may pass through multiple mule accounts, be converted into other assets or be moved outside the immediate reach of the victim's bank.[15]

The architecture therefore extends far beyond the caller. The offence depends upon communications infrastructure, digital accounts, payment rails, recipient accounts, rapid layering and often cross-jurisdictional coordination. The relevant regulatory problem is thus not only individual culpability but the availability of an ecosystem capable of absorbing and dissipating criminal proceeds.[16]

IV. THERE IS NO LEGAL PROCESS CALLED "DIGITAL ARREST"

The phrase derives much of its power from uncertainty about what lawful arrest entails. The BNSS regulates arrest through formal powers, safeguards and procedural requirements. Section 43 addresses the manner in which arrest is made; section 47 requires communication of the particulars of the offence or other grounds of arrest in cases of arrest without warrant; and the broader scheme of the BNSS subjects deprivation of liberty to lawfully conferred authority and procedure. Nothing in that framework recognises a free-standing process by which an unknown official can order a person to remain continuously visible on a private video call and transfer money as a condition of avoiding arrest.[17]

The CBI's 2026 statement that no legal concept of digital arrest exists is therefore more than a public-awareness slogan. It identifies the precise fraud at the centre of the scam: the invented

[15] Central Bureau of Investigation, 'CBI Arrests Accused in Digital Arrest Cyber Fraud Case' (2 July 2026), PIB Release ID 2280197; Ministry of Home Affairs / I4C, digital-arrest alert (2024), PIB Release ID 2020570.
[16] Reserve Bank of India, Master Direction - Know Your Customer (KYC) Direction, 2016, provisions concerning operation of bank accounts and money mules, as updated; In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 1 December 2025 (SC), paras 7-14.
[17] Bharatiya Nagarik Suraksha Sanhita 2023, ss 43 and 47; see also the statutory scheme governing lawful arrest and safeguards.

legal procedure itself.[18]

This gap is not a gap in arrest law. It is a gap between law as enacted and law as understood by the citizen. Digital-arrest fraud converts procedural ignorance into a cybersecurity vulnerability. A person may know never to share an OTP and still be deceived by a convincing but legally impossible investigative command.

Cyber-literacy policy should therefore include procedural legal literacy. Citizens need to know not only how to recognise suspicious links but how genuine coercive governmental processes work. Public awareness should repeatedly communicate that investigating agencies do not conduct arrests through video calls, do not demand a transfer to a safe account to prove innocence and do not make continued private video surveillance a substitute for lawful custody.

The deeper institutional response, however, should not place the entire burden on citizens to remember warnings. Where a purported governmental notice or communication is capable of objective verification, the State should build the mechanisms that permit such verification quickly. This principle later becomes central to the paper's argument for verifiable State authority.

V. THE EXISTING CRIMINAL-LAW FRAMEWORK

A. Personating a Public Servant: Section 204 BNS

Section 204 BNS addresses the assumption of a public office that the offender does not hold, including acting or attempting to act under colour of that office. The provision is directly relevant where a fraudster claims to be a police officer, CBI officer or other public servant and then issues purported commands in that false capacity. It captures the appropriation of State identity, which is one of the defining characteristics of digital arrest.[19]

Its limitation is equally important. Personation alone does not capture the complete economic and coercive harm. A digital-arrest operation may use the assumed office to extort large sums, forge documents and intimidate the victim. Section 204 should therefore be viewed as one

[18] Central Bureau of Investigation, ABHAY notice-verification advisory (15 May 2026), PIB Release ID 2261539.
[19] Bharatiya Nyaya Sanhita 2023, s 204 (personating a public servant).

component of a cumulative charging framework rather than a complete doctrinal characterisation.

B. Cheating: Section 318 BNS

Section 318 BNS criminalises cheating and includes deception that fraudulently or dishonestly induces a person to deliver property. A typical digital-arrest scam contains numerous deceptions: the caller's identity is false, the criminal case may be fictitious, the document may be forged and the supposed legal need to transfer funds does not exist.[20]

Where those deceptions induce transfer of money, cheating is plainly relevant. But describing the transaction exclusively as cheating risks understating why the victim pays. A victim of digital arrest may not believe that a beneficial transaction exists; the victim may believe that refusal will produce immediate arrest or prosecution. The law of extortion therefore deserves equal, and sometimes greater, attention.

C. Cheating by Personation: Section 319 BNS

Section 319 addresses cheating by personation. Digital-arrest schemes commonly involve layered personation: the offender may pretend to be a named officer, a generic officer of a particular agency or a representative of a government institution. The provision complements section 204 and section 318 by addressing the fraudulent assumption of identity through which the deception is delivered.[21]

D. Extortion: Section 308 BNS

Section 308 provides the most revealing doctrinal lens for the coercive core of digital arrest. Extortion is built around intentionally putting a person in fear of injury and thereby dishonestly inducing delivery of property or valuable security. The provision also specifically addresses fear generated through accusations of serious criminal conduct.[22]

This structure closely resembles the central mechanism of many digital-arrest operations. The

[20] Bharatiya Nyaya Sanhita 2023, s 318; Hridaya Ranjan Prasad Verma v State of Bihar (2000) 4 SCC 168 (on the ingredients of cheating and dishonest or fraudulent intention).
[21] Bharatiya Nyaya Sanhita 2023, s 319 (cheating by personation).
[22] Bharatiya Nyaya Sanhita 2023, s 308 (extortion), including provisions concerning fear generated by accusations of serious offences.

victim is told that he or she is implicated in a grave offence. The accusation generates fear of arrest, prosecution, imprisonment, asset seizure or stigma. That fear is then linked to a monetary demand. The Supreme Court-linked 2026 CBI case involving a Rs 25.65 lakh transfer is illustrative: according to the CBI, the victim was threatened with arrest and seizure of property after callers falsely claimed that her bank account had been used in terrorism-related activities, and the fraudsters shared a fabricated attachment order.[23]

Digital arrest therefore occupies the intersection of deception and coercion. Deception answers why the victim believes the caller has authority; extortion explains why the victim complies with the demand. Treating the entire phenomenon as 'online cheating' obscures this division of legal functions.

E. Criminal Intimidation: Section 351 BNS

Criminal intimidation may also be relevant where threats are used to cause alarm or compel conduct that the victim is not legally bound to perform. Digital-arrest scams frequently include threats directed not only at the victim but at family members, property or reputation. Whether the provision is attracted in a particular prosecution will depend upon the precise words and evidence, but its conceptual relevance reinforces the fact that many digital-arrest interactions are sustained coercive encounters rather than one-off misrepresentations.[24]

F. Forgery and Use of Forged Electronic Records

Fabricated warrants, FIRs, summonses, attachment orders and agency notices are often central to the offence. The BNS provisions governing forgery and the use of forged documents or electronic records are therefore highly relevant. The fact that a fraudulent warrant exists only as a PDF or image transmitted through a messaging application does not remove it from the concept of a false electronic record.[25]

Forgery in the digital-arrest context produces an institutional harm beyond immediate financial

[23] Central Bureau of Investigation, 'CBI Arrests Accused in Digital Arrest Cyber Fraud Case' (2 July 2026), PIB Release ID 2280197.
[24] Bharatiya Nyaya Sanhita 2023, s 351; Manik Taneja v State of Karnataka (2015) 7 SCC 423 (interpreting the corresponding offence of criminal intimidation under s 503 IPC and emphasising a threat intended to cause alarm or compel conduct).
[25] Bharatiya Nyaya Sanhita 2023, ss 335-340; see generally Sheila Sebastian v R Jawaharaj (2018) 7 SCC 581 (on the requirement that the accused be the maker of the false document for the offence of forgery under the predecessor IPC provisions).

loss. Judicial and investigative symbols become instruments of private crime. The State consequently has an interest not merely in compensating the victim but in protecting the authenticity of official process itself.

G. Organised Crime: Section 111 BNS

Section 111 BNS is potentially relevant to qualifying organised criminal networks. The statutory definition encompasses continuing unlawful activity and expressly refers to cyber-crimes, extortion and economic offences within the organised-crime framework. The provision, however, contains specific requirements concerning continuing unlawful activity and an organised crime syndicate. It should therefore not be mechanically invoked simply because more than one person participated in a single scam.[26]

Where those requirements are satisfied, section 111 offers an important shift in investigative focus: from the individual caller to the continuing criminal enterprise, its facilitators, proceeds and infrastructure.

H. Information Technology Act, 2000

Sections 66C and 66D of the Information Technology Act provide the cyber-specific identity and personation layer. Section 66C addresses fraudulent or dishonest use of specified identity features, while section 66D criminalises cheating by personation using a communication device or computer resource. These provisions are naturally relevant when electronic communication and misuse of digital identity are integral to the fraud.[27]

They should nevertheless be viewed as complementary to the BNS. The technological medium explains how the conduct is executed; it does not fully describe the false assumption of sovereign authority, coercive threats or laundering of proceeds.

I. Telecommunications Act, 2023 and Telecom Identity

The Telecommunications Act, 2023 creates an additional layer where telecommunications

[26] Bharatiya Nyaya Sanhita 2023, s 111 (organised crime), including cyber-crimes, extortion and economic offences within the statutory framework, subject to the requirements of continuing unlawful activity and an organised crime syndicate.
[27] Information Technology Act 2000, ss 66C and 66D (identity theft and cheating by personation by using a communication device or computer resource).

identifiers or services are obtained or used through fraud, cheating or personation. The relevance of telecom identity has increased as organised cyber-fraud networks exploit SIMs, spoofed calls, app-based communication accounts and remote account control.[28]

In December 2025, the Department of Telecommunications issued directions on SIM binding for app-based communication services specifically identifying phishing, digital arrest, impersonation and investment scams among the misuse patterns the measure was designed to address. The regulatory significance is clear: the communications layer is no longer viewed as a neutral background to the offence but as part of the prevention architecture.[29]

VI. WHY "CHEATING" ALONE IS AN INADEQUATE DESCRIPTION

Legal classification matters because it shapes investigative practice, public understanding, data collection and legislative design. Consider two transfers. In the first, A falsely promises B extraordinary investment returns, and B transfers Rs 10 lakh. In the second, A falsely claims to be a senior investigating officer, tells B that B is implicated in money laundering, displays a forged arrest warrant, prohibits communication with others and states that immediate arrest will follow unless Rs 10 lakh is moved to a purported government account.

Both transactions contain deception. But the social and legal wrong is not identical. The first corrupts economic decision-making through a fictitious benefit. The second corrupts the victim's relationship with public authority. Its effectiveness depends on a background fact the offender did not create: the State genuinely possesses authority to investigate offences and, under law, to deprive liberty. The fraudster parasitically appropriates that genuine authority.

This is the core of simulated State coercion. The private threat is disguised as public law. Procedures designed to legitimise and constrain State coercion—warrants, summonses, investigations, judicial orders and official identity—are counterfeited to produce unlawful private compliance.

The distinction has practical consequences. First, seriousness cannot be measured only by the amount ultimately transferred. A failed attempt may still involve hours of isolation,

[28] Telecommunications Act 2023, s 42(3)(e) (fraudulent acquisition of subscriber identity modules or other telecommunication identifiers through fraud, cheating or personation).
[29] Department of Telecommunications, 'Directions for SIM binding for prevention of misuse of telecommunication identifiers for ensuring telecom cyber security' (1 December 2025), PIB Release ID 2197146, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2197146&lang=2&reg=3.

surveillance, intimidation and psychological harm. Secondly, the State has an institutional interest in preventing its own symbols and processes from becoming reliable criminal tools. Thirdly, authentication becomes part of prevention: the citizen must be able to distinguish actual authority from fabricated authority without relying solely on visual appearance.

VII. "COERCION WITHOUT CUSTODY" AND THE LIBERTY PROBLEM

The popular expression 'digital arrest' can create doctrinal confusion because it suggests that an actual legal arrest occurs remotely. That is not the paper's claim. Whether an offence such as wrongful confinement is made out in any particular case depends on the statutory ingredients and facts, and should not be assumed from popular terminology.[30]

The phenomenon nevertheless creates a real liberty interest. A victim may remain in a room for hours because the offender has convincingly threatened that leaving, disconnecting or contacting another person will lead to lawful arrest. The restraint is mediated through belief rather than a locked door. This paper therefore uses the phrase coercion without custody to describe the factual phenomenon without collapsing it into a pre-existing offence of physical confinement.[31]

Technology changes the cost structure of coercion. A criminal no longer needs physical presence to exercise sustained supervision. Video calling allows continuous visual observation; instant messaging allows repeated commands; electronic documents provide apparent legal authority; and online banking permits the demand to be executed immediately. The victim's own home can become the physical setting of a fictitious custodial process.[32]

Any future specialised offence should recognise this feature. It should not depend on proof of technical physical confinement. The aggravating wrong is the fraudulent assertion of public authority combined with threats concerning arrest, prosecution, compulsory investigation or other exercises of State power.

[30] Bharatiya Nyaya Sanhita 2023, s 127 (wrongful confinement). Whether a digital-arrest fact pattern satisfies the provision depends upon proof that the victim was wrongfully restrained so as to be prevented from proceeding beyond circumscribing limits; the popular label is not determinative.
[31] Constitution of India, art 21; Maneka Gandhi v Union of India (1978) 1 SCC 248; Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (personal liberty, dignity, privacy and autonomy within the constitutional protection of life and liberty).
[32] Central Bureau of Investigation, ABHAY notice-verification advisory (15 May 2026), PIB Release ID 2261539; Ministry of Home Affairs / I4C, digital-arrest alert (2024), PIB Release ID 2020570.

VIII. THE CONSTITUTIONAL AND HUMAN-RIGHTS DIMENSION

Digital arrest is ordinarily committed by private criminals, and it would be doctrinally imprecise to label every such scam a direct violation of Article 21 by the State. The constitutional dimension arises through the State's positive regulatory role and the integrity of institutions that legitimately exercise coercive authority.[33]

The NHRC has already treated the subject as a human-rights concern. Its June 2026 Open House Discussion identified threats to rights, dignity and security, privacy concerns, psychological trauma, the need for victim redressal and the possibility of recognising digital-arrest scams as a distinct offence. The discussion also highlighted the role of mule accounts, telecom infrastructure, social-media intermediaries and even human trafficking in sustaining large-scale cyber-scam compounds.[34][35]

This rights-oriented perspective is important because a policy centred exclusively on 'consumer vigilance' can inadvertently transfer excessive responsibility to the victim. Personal caution remains essential, but increasingly sophisticated impersonation operates within a technological and institutional environment that individual citizens do not control. If a government notice can be convincingly forged, the strongest preventive intervention may be to make genuine notices independently verifiable rather than repeatedly instructing citizens to become better forensic examiners.[36]

The paper therefore proposes a principle of verifiable State authority: where governmental powers are capable of being communicated or represented digitally, citizens should have a simple and authoritative means of verifying that the communication genuinely originates from the State. As administration becomes increasingly electronic, authentication of significant governmental communications should become part of digital due process.[37]

---

[33] See Constitution of India, art 21; Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1. The argument in this paper concerns the regulatory implications of private impersonation of coercive State power and does not treat every private scam as direct State action.

[34] National Human Rights Commission, Open House Discussion on 'Safeguarding Human Rights against Digital Arrest Scams' (9 June 2026), official NHRC proceedings and press release.

[35] Ibid; see also PIB Release ID 2270875, recording stakeholder discussion on mule accounts, telecom infrastructure, social-media intermediaries and human trafficking.

[36] National Human Rights Commission, Open House Discussion on 'Safeguarding Human Rights against Digital Arrest Scams' (9 June 2026), official proceedings; PIB Release ID 2270875.

[37] See Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (privacy, dignity and individual autonomy). The formulation 'verifiable State authority' is proposed by this paper as a regulatory principle.

IX. FROM OFFENDER LIABILITY TO INFRASTRUCTURE RESPONSIBILITY

A. Mule Accounts and the Banking Layer

The proceeds of digital arrest must enter the financial system. Mule accounts provide the bridge between the victim and the criminal network. Some are knowingly rented or sold; others may be opened through deception, weak due diligence or compromised identities. Funds can then be rapidly layered across accounts or converted into other assets.[38]

The scale of the mule-account problem has produced increasingly systemic countermeasures. In February 2026, the Government reported that more than 21.65 lakh suspect identifiers and 26.48 lakh Layer-1 mule accounts had been shared with participating entities of the I4C Suspect Registry as at 31 December 2025, and transactions worth more than Rs 9,055 crore had been declined. By June 2026, official figures reported more than 30.48 lakh suspect identifiers and 32.08 lakh Layer-1 mule accounts shared with participating entities, with declined transactions worth Rs 25,698 crore. These figures concern the broader cyber-fraud ecosystem rather than digital arrest alone, but they show the centrality of financial infrastructure to cybercrime prevention.[39][40]

Bank liability should not be automatic merely because an account was misused. The appropriate inquiry concerns customer due diligence, account-opening practices, transaction patterns, response to alerts, suspicious-transaction reporting and compliance with applicable regulatory duties. The purpose of an ecosystem approach is not to convert every facilitator into an offender but to identify where institutional controls can prevent recurrent misuse.[41]

B. Telecommunications and App-Based Communications

Telecommunications infrastructure supplies reach, anonymity and persistence. Fraudulent or mass-issued SIMs, international spoofing and remotely controlled app-based accounts can

[38] Reserve Bank of India, 'Operation of Bank Accounts and Money Mules', RBI/2009-10/508, DBOD.AML.BC.No.102/14.01.001/2009-10 (24 May 2010); Reserve Bank of India, Master Direction - Know Your Customer (KYC) Direction, 2016, provisions on money-mule accounts, as updated.
[39] Ministry of Home Affairs, cybercrime measures and I4C Suspect Registry figures as at 31 December 2025, PIB Release ID 2223095.
[40] Ministry of Home Affairs, cybercrime measures and I4C Suspect Registry figures as at 30 June 2026, PIB Release ID 2290366.
[41] Reserve Bank of India, Master Direction - Know Your Customer (KYC) Direction, 2016, provisions concerning money-mule accounts, requiring diligence, meticulous monitoring and appropriate reporting action, as updated.

make the same network appear under changing identities. In response, the Government has increasingly linked cybercrime reporting to telecom enforcement. Official 2026 reporting records API integration between Sanchar Saathi and NCRP so suspect identifiers can be shared for real-time action by telecom service providers.[42]

The objective must be proportionate traceability rather than indiscriminate surveillance. Effective cyber-fraud regulation should make repeated criminal use of telecom identifiers expensive and detectable while preserving lawful privacy and communication rights.

C. Digital Intermediaries and Evidence Preservation

Messaging and communication services may possess account records, traffic information, device identifiers and other evidence relevant to investigation. Because cybercriminal infrastructure can be abandoned within hours, delay in preservation can be fatal to attribution.[43]

The appropriate regulatory concept is procedural cooperation rather than automatic substantive liability. An intermediary should not be treated as the perpetrator simply because its service was misused. At the same time, serious cross-border cyber-fraud investigations require lawful preservation and disclosure mechanisms that operate at a speed proportionate to the volatility of digital evidence.[44]

D. Cross-Border Networks

Digital arrest dissolves conventional territorial assumptions. The victim may be in one State, the receiving account in another, the SIM registered elsewhere and the principal operators abroad. The NHRC's 2026 discussion recorded a CBI view that large-scale digital-arrest scams were linked to cyber-scam compounds in Southeast Asia and sustained by mule accounts, telecom infrastructure, social-media intermediaries and human trafficking.[45]

[42] Ministry of Home Affairs, cybercrime prevention measures including API integration between Sanchar Saathi and NCRP, PIB Release ID 2238253.
[43] Information Technology Act 2000, s 67C (preservation and retention of information by intermediaries); In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 1 December 2025 (SC), directions concerning intermediary cooperation and preservation of relevant data.
[44] Information Technology Act 2000, s 79; Shreya Singhal v Union of India (2015) 5 SCC 1 (reading down the 'actual knowledge' requirement in s 79(3)(b) and distinguishing intermediary responsibility from independent adjudication of illegality).
[45] NHRC Open House Discussion on 'Safeguarding Human Rights against Digital Arrest Scams' (9 June 2026), PIB Release ID 2270875.

This structure makes fragmented complaint-by-complaint investigation inefficient. The appropriate investigative unit is often the criminal infrastructure: common devices, accounts, identifiers, payment routes, facilitators and command structures across many victims.[46]

X. THE SUPREME COURT'S SUO MOTU PROCEEDINGS

The Supreme Court's suo motu proceedings in In Re: Victims of Digital Arrest Related to Forged Documents are the most significant judicial development in India's current response. The case remained active in 2026 and the Supreme Court's official orders listing records an order dated 28 July 2026.[47]

The practical effect of the proceedings is visible in enforcement. In July 2026, the CBI stated that a digital-arrest case from Madhya Pradesh had been transferred for re-registration in compliance with the Supreme Court's 1 December 2025 order. The CBI re-registered the case in April 2026, arrested an accused in June 2026 and reported that Rs 2.65 lakh had been facilitated for refund to the victim after court orders.[48]

This development matters for two reasons. First, it confirms the national and multi-jurisdictional character of the problem. Secondly, it links investigation with restitution. A cyber-fraud regime that records an arrest but cannot recover traceable funds addresses only part of the victim's injury.

The continuing proceedings also signal a broader transition in judicial thinking. Digital arrest is not being treated as a problem for one police station or one statutory provision. It has drawn attention to central investigation, mule accounts, financial freezing, telecom controls, platform cooperation and restoration mechanisms. That is the architecture of cybercrime governance rather than merely prosecution.[49]

---

[46] Bharatiya Nagarik Suraksha Sanhita 2023, s 202 (jurisdiction for offences committed by electronic communications and certain cheating offences); In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 1 December 2025 (SC), directions facilitating pan-India investigation and interstate coordination.

[47] Supreme Court of India, Latest Orders, entry for In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Criminal) No 3 of 2025, 28 July 2026.

[48] Central Bureau of Investigation, 'CBI Arrests Accused in Digital Arrest Cyber Fraud Case' (2 July 2026), PIB Release ID 2280197.

[49] In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, orders dated 1 December 2025 and 9 February 2026 (SC) (addressing the CBI, RBI, banks, intermediaries, telecom providers, State authorities, mule accounts, data preservation and victim restoration).

XI. NCRP, CFCFRMS AND THE EMERGING RESTITUTION ARCHITECTURE

Cyber-fraud policy involves a race between reporting and dissipation. Money can move across multiple accounts in minutes. A perfectly lawful freeze order obtained only after the funds have been layered beyond reach may offer little practical benefit. Speed is therefore not merely operational; it is a legal design issue.[50]

The CFCFRMS was established for immediate reporting of financial cyber fraud and intervention against the siphoning of funds. The Government reported that by 30 June 2026 more than Rs 11,158 crore had been saved in more than 32.80 lakh complaints, and the 1930 helpline remained operational for rapid reporting.[51]

A comprehensive NCRP-CFCFRMS Standard Operating Procedure was issued on 2 January 2026. Official descriptions state that the SOP establishes a uniform, victim-centric framework for complaint processing, bank coordination, grievance redressal, removal of lien markings and restoration of defrauded funds to rightful claimants. Money Restoration and Grievance Redressal modules were subsequently made functional in 2026.[52][53]

These developments point towards an important reorientation. The quality of a cybercrime system should not be measured only by FIRs, arrests, chargesheets and convictions. It should also be evaluated through the proportion of reported funds intercepted, the time taken to impose a lien or hold, the speed of restoration, the accuracy of mule-account detection and the protection of innocent account holders from unnecessary freezes.

Restitution also has distributive consequences. A single downstream account may contain funds derived from multiple victims together with legitimate money. Rapid restoration therefore requires fair procedures for tracing, priority and competing claims. The objective must be speed without arbitrariness.[54]

---

[50] Ministry of Home Affairs, CFCFRMS 2.0 Platform (28 July 2026), PIB Release ID 2290377; In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 9 February 2026 (SC), addressing temporary debit holds, the NCRP-CFCFRMS SOP and timely restoration.
[51] Ministry of Home Affairs, 'CFCFRMS 2.0 Platform' (28 July 2026), PIB Release ID 2290377.
[52] Ministry of Home Affairs, comprehensive SOP for NCRP-CFCFRMS issued 2 January 2026, PIB Release ID 2241336, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241336&lang=1&reg=1.
[53] Ministry of Home Affairs, official statement on Money Restoration Module and Grievance Redressal Module under CFCFRMS, PIB Release ID 2287039 (21 July 2026).
[54] In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 9 February 2026 (SC), including directions concerning nationwide implementation of the NCRP-CFCFRMS SOP

XII. AUTHENTICATING THE STATE: ABHAY AND THE PRINCIPLE OF VERIFIABLE AUTHORITY

One of the most conceptually important developments occurred in May 2026 when the CBI launched ABHAY, an AI-based helpbot for authentication of CBI notices. The system allows a recipient of a purported CBI notice to upload it through the CBI's official mechanism and receive an indication whether the notice is genuine or potentially fraudulent.[55]

ABHAY matters because it reverses the ordinary verification burden. Without authentication infrastructure, a citizen receiving a convincing document must independently decide whether the document is fake. With official verification, authenticity becomes a question capable of authoritative resolution.[56]

The model should be extended cautiously but substantially. Investigative and regulatory authorities whose identities are frequently abused should provide simple verification mechanisms for significant notices, summonses and coercive communications. Secure reference numbers, QR-based verification, digitally signed records or interoperable government verification portals could perform that function.

The legal principle is more important than the specific technology: a citizen should not be required to trust the appearance of digital governmental authority where the State is capable of making that authority independently verifiable. Awareness asks the citizen to be suspicious. Authentication allows the citizen to know.

XIII. ARTIFICIAL INTELLIGENCE AS BOTH WEAPON AND DEFENCE

Artificial intelligence plays a dual role. On the offensive side, synthetic voices, generated documents and manipulated video reduce the cost of producing convincing impersonation. The CBI's ABHAY announcement expressly identified AI and deepfakes as technologies making it increasingly difficult for ordinary citizens to distinguish genuine material from fabricated

and consideration of a framework for victim compensation; Ministry of Home Affairs, NCRP-CFCFRMS SOP issued 2 January 2026, PIB Release ID 2241336.

[55] Central Bureau of Investigation, 'CBI Launches ABHAY - AI-Powered Notice Verification System' (15 May 2026), PIB Release ID 2261539.

[56] Central Bureau of Investigation, 'CBI Launches ABHAY - AI-Powered Notice Verification System' (15 May 2026), PIB Release ID 2261539.

communications.[57]

On the defensive side, AI can improve notice verification, fraud pattern detection, mule-account identification and prioritisation of suspicious transactions. The relevant regulatory question is therefore not whether AI should be characterised as inherently dangerous or protective. It is whether trustworthy institutions can deploy verification and detection tools quickly enough to offset the declining cost of high-quality impersonation.[58]

This creates a verification arms race. If generative systems lower the cost of counterfeiting official communications, law and regulation must lower the cost of authenticating genuine communications. The institutions that possess legal authority should also possess the strongest public mechanisms for proving that authority.

XIV. DOES INDIA NEED A SEPARATE OFFENCE OF DIGITAL ARREST?

The case for a specialised offence is substantial but should be stated carefully. The NHRC's June 2026 discussion included a proposal that digital-arrest scams be recognised as a distinct offence to facilitate investigation, prosecution and victim redressal. The continuing Supreme Court proceedings have also kept legislative attention focused on the phenomenon.[59]

A separate offence could improve conceptual clarity and statistical visibility. It could identify as an aggravating feature the fraudulent invocation of State coercion, rather than treating impersonation of a public servant as only one offence among many. It could also permit enhanced punishment where the conduct includes prolonged coercive surveillance, forged judicial material, substantial loss or targeting of vulnerable persons.

The argument against a new offence is equally important. Existing law already criminalises public-servant personation, cheating, extortion, criminal intimidation, forgery, cyber-personation and organised crime in qualifying cases. Creating another label will not itself

[57] Ibid (noting the role of artificial intelligence and deepfakes in making fabricated communications more difficult to distinguish from genuine ones).
[58] Reserve Bank of India, 'MuleHunter.AI: AI solutions to identify mule bank accounts', RBI Bulletin (December 2024); Reserve Bank of India, Annual Report 2024-25 (discussion of MuleHunter.ai); Central Bureau of Investigation, ABHAY notice-verification advisory (15 May 2026), PIB Release ID 2261539.
[59] National Human Rights Commission, Open House Discussion on 'Safeguarding Human Rights against Digital Arrest Scams' (9 June 2026), official press release; PIB Release ID 2270875.

disable a mule account, trace an app-based communication, preserve disappearing evidence or restore money that has already been layered across accounts.[60]

The correct legislative question is therefore not whether digital arrest is already illegal. It plainly is capable of attracting serious criminal liability. The question is whether a narrowly drafted specialised offence would capture an aggravated wrong or improve investigation in a manner existing provisions do not.

On balance, this paper supports a narrowly drafted aggravated offence focused on fraudulent invocation of coercive State authority rather than the popular phrase alone. The prohibited conduct should be defined through elements: knowingly and falsely representing oneself as a judicial, police, investigative, prosecutorial or regulatory authority, or as acting under such authority; invoking or threatening purported criminal process, arrest, detention, prosecution, asset restraint or compulsory investigation; and doing so to obtain property, information, access, an act, omission or other advantage.

Aggravated forms could address vulnerable victims, organised criminal activity, substantial loss, forged judicial documents, prolonged remote supervision, or artificial manipulation of the identity of a public official. Such a provision would recognise the distinctive wrong while preserving cumulative application of other offences where their ingredients are independently satisfied.

XV. A FIVE-PILLAR REGULATORY MODEL FOR INDIA

1. Authentication of Governmental Authority

The first pillar is authentication. India should move towards interoperable verification mechanisms for significant investigative and regulatory communications. ABHAY provides a prototype, but verification should not depend on citizens knowing the internal process of each agency. A common or interoperable architecture could permit rapid confirmation of whether a notice, summons or reference number exists.[61]

[60] Bharatiya Nyaya Sanhita 2023, ss 111, 204, 308, 318, 319, 336-340 and 351; Information Technology Act 2000, ss 66C and 66D; Telecommunications Act 2023, s 42.
[61] Central Bureau of Investigation, 'CBI Launches ABHAY - AI-Powered Notice Verification System' (15 May 2026), PIB Release ID 2261539 (an existing agency-specific model of independent notice authentication).

Authentication design should minimise the risk that criminals can imitate the verification system itself. Citizens should be directed to independently access official government domains or applications rather than click verification links supplied by the purported officer.

2. Real-Time Financial Interdiction

The second pillar is financial interdiction. Bank-CFCFRMS integration, suspect registries, mule-account analytics and lien marking already represent important steps. The policy objective should be to increase the probability that a suspicious transfer can be paused or traced before funds leave the regulated system.[62]

Possible safeguards include risk-based temporary holds for exceptional transaction patterns, enhanced confirmation for vulnerable customers in defined high-risk scenarios and rapid bank-to-law-enforcement escalation. Such measures must be carefully designed to avoid paternalistic blocking of legitimate transfers or discriminatory treatment of elderly customers.

3. Telecommunications Traceability

The third pillar is proportionate telecom traceability. Fraudulent SIM acquisition, spoofing, remote use of app-based accounts and frequent identifier changes undermine investigation. Regulatory systems should therefore improve subscriber verification, detect abnormal SIM patterns, act rapidly on verified scam identifiers and enable lawful cross-platform threat intelligence.[63]

The objective is not universal surveillance. It is to prevent the communications layer from becoming cheaply disposable criminal infrastructure.

4. Intermediary Cooperation and Evidence Preservation

The fourth pillar is a clear emergency preservation protocol for serious cyber-fraud investigations. Digital evidence is volatile. Account identifiers, device information, logs and

[62] Ministry of Home Affairs, CFCFRMS 2.0 Platform (28 July 2026), PIB Release ID 2290377; Reserve Bank of India, 'MuleHunter.AI: AI solutions to identify mule bank accounts', RBI Bulletin (December 2024); In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 9 February 2026 (SC).

[63] Telecommunications Act 2023, s 42; Department of Telecommunications, 'Directions for SIM binding for prevention of misuse of telecommunication identifiers for ensuring telecom cyber security' (1 December 2025), PIB Release ID 2197146.

other records may disappear or become inaccessible if preservation requests are delayed.[64]

The protocol should be grounded in law, necessity and proportionality. Fast preservation is compatible with privacy where disclosure remains subject to lawful process and the preservation obligation is narrowly targeted.[65]

5. Victim Restoration

The fifth pillar is victim restoration. India's 2026 NCRP-CFCFRMS architecture is an important step because it treats restoration and grievance redressal as explicit system functions rather than accidental by-products of prosecution.[66]

Future reforms should prioritise rapid return of undisputed traceable funds, transparent processes for competing claims, clear timelines, safeguards for innocent downstream account holders and accessible review where bank accounts are unnecessarily frozen. Where demonstrable institutional non-compliance materially facilitated fraud, the development of compensation or contribution rules may also warrant further study.

XVI. FROM CYBERCRIME ENFORCEMENT TO CYBERCRIME GOVERNANCE

Traditional criminal law imagines a relatively linear event: offender, prohibited act, victim, investigation and prosecution. Digital arrest is better represented as a network: offender network, communications infrastructure, impersonated institution, digital platform, victim, payment system, mule accounts, secondary accounts and potentially cross-border transfer.

The criminal code remains indispensable, but it regulates only part of this chain. Prevention requires coordination among institutions whose principal purposes are not criminal prosecution at all: banks, payment systems, telecom providers, digital intermediaries, identity-verification systems and government agencies responsible for authentic communications.[67]

---

[64] Information Technology Act 2000, s 67C; In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, order dated 1 December 2025 (SC), directions requiring relevant intermediaries to cooperate and preserve specified data.

[65] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; Shreya Singhal v Union of India (2015) 5 SCC 1. Any accelerated preservation or disclosure regime must remain tied to lawful authority and proportionate safeguards.

[66] Ministry of Home Affairs, 'CFCFRMS 2.0 Platform' (28 July 2026), PIB Release ID 2290377; Ministry of Home Affairs, NCRP-CFCFRMS SOP, 2 January 2026.

[67] In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, orders dated 1

This broader model can be described as cybercrime governance. Its objectives are prevention, authentication, detection, interruption, preservation, attribution, financial recovery and institutional learning. A mature system should measure success not only by punishment after the crime but by the degree to which the environment makes the crime difficult to execute successfully.

Digital arrest is especially suited to this governance approach because every successful case exposes several system-level questions. Could the purported notice have been authenticated? Could the communication identifier have been blocked or traced? Could a suspicious receiving account have been detected? Could the transfer have been paused? Could funds have been restored quickly? Could evidence have been preserved across jurisdictions? Each question identifies a point at which regulation can reduce expected criminal returns.

XVII. CONCLUSION

Digital arrest exposes a peculiar vulnerability of the digital State. The fraudster possesses no warrant, no lawful power to investigate, no authority to arrest and no power to order a citizen to remain on a video call or transfer money. Yet the victim may comply because the criminal has successfully replicated the appearance of institutions that genuinely possess coercive authority.

That is what distinguishes digital arrest from ordinary deception. The offender does not merely counterfeit another individual. The offender counterfeits the State.

Indian law already provides a substantial prosecutorial foundation. Public-servant personation, cheating, extortion, criminal intimidation, forgery, cyber-personation and organised-crime provisions can collectively reach the constituent conduct where their ingredients are established. The problem is therefore not one of complete criminal-law silence.[68]

The more serious weakness is institutional fragmentation. Digital arrest succeeds when false governmental authority, communications infrastructure, digital platforms and financial infrastructure can be combined faster than the State can authenticate, detect and interrupt them.

December 2025 and 9 February 2026 (SC), illustrating a coordinated model involving criminal investigation, banking supervision, telecommunications controls, intermediary cooperation and restitution.

[68] Bharatiya Nyaya Sanhita 2023, ss 111, 204, 308, 318, 319, 336-340 and 351; Information Technology Act 2000, ss 66C and 66D; Telecommunications Act 2023, s 42.

The current trajectory of Indian policy—CBI investigation, the Supreme Court's continuing proceedings, CFCFRMS, the 1930 reporting system, suspect registries, telecom controls, the January 2026 SOP and ABHAY—shows movement towards an ecosystem response rather than isolated prosecution.[69]

A narrowly drafted aggravated offence may form part of that framework, particularly if Parliament chooses to recognise fraudulent invocation of coercive public authority as a distinct wrong. But legislation cannot stop at nomenclature and enhanced punishment. A successful legal response must make fraudulent State authority difficult to authenticate falsely, easy to verify independently, financially interruptible, technically traceable and capable of rapid restitution.[70]

The deeper lesson concerns the architecture of digital governance. As courts, police agencies, regulators and public authorities communicate increasingly through electronic records and remote channels, institutional legitimacy will depend on citizens being able to distinguish authentic commands from sophisticated imitations. The rule of law in a digital society therefore requires more than limits on the State's exercise of coercive power. It also requires protection against the counterfeiting of that power by private actors.

Digital arrest is consequently not merely a story about cyber fraud. It is a warning that in an era of artificial intelligence, instant payments, electronic documents and remote communication, the identity and authority of the State itself have become cybersecurity assets that law must protect.

[69] In Re: Victims of Digital Arrest Related to Forged Documents, SMW(Crl) No 3 of 2025, orders dated 1 December 2025 and 9 February 2026 (SC); Ministry of Home Affairs, NCRP-CFCFRMS SOP issued 2 January 2026, PIB Release ID 2241336.

[70] National Human Rights Commission, Open House Discussion on 'Safeguarding Human Rights against Digital Arrest Scams' (9 June 2026), official proceedings and PIB Release ID 2270875 (recording the proposal to recognise digital-arrest scams as a distinct offence).

SELECTED PRIMARY AUTHORITIES AND OFFICIAL MATERIAL

- Bharatiya Nyaya Sanhita, 2023.
- Bharatiya Nagarik Suraksha Sanhita, 2023.
- Information Technology Act, 2000.
- Telecommunications Act, 2023.
- Supreme Court of India, In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Criminal) No. 3 of 2025, continuing proceedings (including order recorded 28 July 2026).
- Ministry of Home Affairs / Press Information Bureau, CBI Launches 'ABHAY' - AI-Powered Notice Verification System, 15 May 2026.
- Ministry of Home Affairs / Press Information Bureau, CFCFRMS 2.0 Platform, 28 July 2026.
- Ministry of Home Affairs / Press Information Bureau, Government measures on NCRP-CFCFRMS and SOP dated 2 January 2026.
- National Human Rights Commission, Open House Discussion on 'Safeguarding Human Rights against Digital Arrest Scams', 9 June 2026.
- Ministry of Communications / Press Information Bureau, DoT Directions for SIM Binding for Prevention of Misuse of Telecommunication Identifiers, 1 December 2025.