DIGITAL ARREST IN INDIA: RETHINKING CRIMINAL LIABILITY & LEGAL REMEDIES FOR EMERGING CYBER FRAUD

Kritika Bhalla, Ideal Institute of Management and Technology (GGSIPU)

ABSTRACT

The phenomenon popularly termed 'digital arrest' a species of cyber-enabled extortion in which fraudsters impersonate law-enforcement or judicial authorities over video calls to coerce victims into transferring money under threat of confinement has emerged as one of the most significant criminal-justice challenges of India's digital decade. Though the expression has no statutory foundation, its architecture of coercion, surveillance and induced fear engages the constitutional guarantees of personal liberty, privacy and dignity under Article 21 as squarely as any physical detention. This paper undertakes a doctrinal and critical examination of digital arrest fraud through the Information Technology Act, 2000, and the recently enacted Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023. It critically analyses judgments of Indian constitutional courts. In particular, the paper rethinks the criminal-liability framework governing digital arrest fraud, addressing the graduated culpability of distributed syndicates, the mens rea threshold for mule-account holders, and the responsibility of banking, telecommunications and platform enablers, and it evaluates the adequacy of the victim's remedial and restitutionary options. It concludes with legislative, institutional and judicial recommendations aimed at reconciling technological governance with constitutional guarantees, drawing on comparative international cyber-governance principles.

Keywords: Digital Arrest; Right to Privacy; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023.

Introduction

India's rapid digitisation, accelerated by near-universal smartphone penetration and the proliferation of instant-payment infrastructure, has been accompanied by a corresponding surge in technologically mediated crime. Among the most alarming of these is the phenomenon of 'digital arrest', a coercive extortion technique in which perpetrators impersonate officers of the Central Bureau of Investigation, the Enforcement Directorate, the Narcotics Control Bureau or even courts themselves, and use sustained video-conferencing surveillance to place a victim under a fabricated condition of 'virtual custody'.[1] No such concept as 'digital arrest' exists anywhere in Indian criminal law; it is entirely a creature of criminal ingenuity exploiting citizens' unfamiliarity with due process safeguards. The scale of the problem has compelled judicial intervention at the highest level. In October 2025, the Supreme Court of India took suo motu cognisance of the rising incidence of digital arrest scams after a 73-year-old woman from Haryana was defrauded of over one crore rupees through a scheme employing forged Supreme Court orders.[2] The Court subsequently empowered the Central Bureau of Investigation with nationwide jurisdiction to investigate such scams, noting that victims had cumulatively lost approximately Rs 3,000 crore, and that the misuse of forged judicial orders struck at the very foundation of public trust in the justice system.[3]

Meaning and Evolution of Digital Arrests

'Digital arrest' is not a term of art recognised by the Code of Criminal Procedure, the Bharatiya Nagarik Suraksha Sanhita, 2023, or any other statute. It is, at its core, a confidence trick that borrows the vocabulary and visual grammar of law enforcement uniforms, forged warrants, simulated police stations rendered as video-call backgrounds to manufacture a coercive psychological environment.[4] Victims are typically informed that a parcel booked in their name contains contraband, that their bank account is linked to money laundering, or that a family

[1]Ministry of Home Affairs, Government of India, National Cyber Crime Reporting Portal, advisory on 'digital arrest' cyber fraud, available at: https://cybercrime.gov.in (last visited on August 26, 2026).
[2]'SC Takes Strong Note of Rising Digital Arrest Scams, Seeks Centre and CBI Response', All India Radio News, Oct. 17, 2025, available at: https://www.newsonair.gov.in/sc-takes-strong-note-of-rising-digital-arrest-scams-seeks-centre-and-cbi-response (last visited on August 26, 2026).
[3]'Supreme Court Empowers CBI to Investigate Digital Arrest Scams', Vision IAS, Dec. 2, 2025, available at: https://visionias.in/blog/current-affairs/supreme-court-empowers-cbi-to-investigate-digital-arrest-scams (last visited on August 26, 2026).
[4]ASV Legal LLP, "Digital Arrest Scams and the Supreme Court's Response: A Growing Cyber Threat in India', available at: https://www.asvlawoffices.com/news-insights/digital-arrest-scams-and-the-supreme-courts-response-a-growing-cyber-threat-in-india/ (last visited on August 26, 2026).

member is in custody, and are then compelled to remain on video call sometimes for days while transferring their savings to accounts controlled by the fraudsters.

Empirical data underscores the scale of the crisis. A study conducted by the non-governmental organisation PRAHAR, cited by the Central Reserve Police Force, estimated that Indians lost approximately Rs 120.3 crore to digital arrest scams in the first quarter of 2024 alone.[5] By late 2025, cumulative losses placed before the Supreme Court exceeded Rs 3,000 crore, with victims ranging from daily-wage earners to bankers, judges and retired police officers, dispelling any assumption that the crime targets only the digitally naive.[6] Investigative agencies have identified that a substantial share of these operations are run from call-centre compounds in Myanmar, Laos and Cambodia, often staffed through human trafficking networks, which has compounded jurisdictional difficulties for Indian law enforcement.[7]

Legally, the conduct constituting a digital arrest is prosecutable through a combination of general and special provisions: cheating by personation of a public servant is punishable under the Information Technology Act, 2000,[8] identity theft is separately penalised,[9] while the underlying acts of impersonation, criminal intimidation, cheating and extortion attract the Bharatiya Nyaya Sanhita, 2023. The absence, however, of a specific, named offence has meant that victims and even first-responder police officers frequently misclassify complaints, leading to fragmented FIR registration across multiple states for what is functionally a single, centrally coordinated criminal enterprise a deficiency the Supreme Court has itself flagged in directing all States and Union Territories to furnish consolidated data on registered FIRs.[10]

Emerging Modalities: AI-Enabled Impersonation and Deepfakes

A distinguishing feature of the most recent generation of digital arrest operations is their reliance on artificial intelligence to manufacture verisimilitude. Generative deepfake video

[5]Vishwa Mohan, 'The Digital Arrest Scam That Made India's Supreme Court Take Note', BOOM, Oct. 30, 2025, available at: https://www.boomlive.in/law/supreme-court-suo-motu-notice-of-digital-scams-in-india-29860 (last visited on August 26, 2026).
[6]Supra note 3.
[7]'Digital Arrests: SC's Alarm, a Call for Action', Deccan Herald, available at: https://www.deccanherald.com/opinion/editorial/digital-arrests-sc-s-alarm-a-call-for-action-3787974 (last visited on August 26, 2026).
[8]The Information Technology Act, 2000 (Act 21 of 2000), s. 66D.
[9]The Information Technology Act, 2000 (Act 21 of 2000), s. 66C.
[10]'SC Seeks Details from States, UTs on FIRs Registered in Digital Arrest Scam Cases', All India Radio News, Oct. 27, 2025, available at: https://www.newsonair.gov.in/sc-seeks-details-from-states-uts-on-firs-registered-in-digital-arrest-scam-cases (last visited on August 26, 2026).

now permits fraudsters to superimpose the likeness of identifiable senior police officers, judges or ministers onto the interrogating figure on screen, while real-time voice-cloning reproduces the cadence and vernacular of a genuine official from only seconds of sampled audio. These techniques defeat the very heuristics the official uniform, the recognisable face, the authentic-sounding voice on which citizens have traditionally relied to authenticate an interaction with the State, and they simultaneously complicate forensic attribution, since the synthetic artefact tendered in evidence may bear no biometric trace of its true author. The investigative response canvassed in Ritesh Sinha v. State of Uttar Pradesh, premised on the compelled production of an accused's own voice sample, is of limited utility where the incriminating voice is itself a machine-generated forgery. This emerging modality strengthens the case, developed below, for a distinct criminal-liability framework and for sustained investment in deepfake-detection forensics rather than continued reliance on statutory categories conceived for analogue impersonation.

Statutory Framework

Information Technology Act, 2000

The Information Technology Act, 2000 supplies the principal special-law architecture governing both phenomena. Section 66C penalises identity theft through fraudulent use of another person's identifying features,[11] directly applicable to the impersonation of investigating officers. Section 66D penalises cheating by personation using a computer resource, capturing the core conduct of digital arrest fraud.[12] Section 66E, protecting against violation of bodily privacy through capture or transmission of images, becomes relevant where scammers coerce victims into compromising video interactions.[13] Section 67 penalises publication of obscene material in electronic form, occasionally engaged where defamatory content carries sexual or obscene overtones.[14] Sections 69 and 69A empower the Government to intercept, monitor or block access to information in the interest of sovereignty, security or public order powers of obvious relevance to blocking fraudulent websites, fake court-order templates, and defamatory content once identified, subject to the procedural safeguards read into these provisions in Shreya Singhal.[15] Section 72 penalises breach of confidentiality and privacy by persons who,

[11]Supra note 8.
[12]Supra note 7.
[13]The Information Technology Act, 2000 (Act 21 of 2000), s. 66E.
[14]The Information Technology Act, 2000 (Act 21 of 2000), s. 67.
[15]The Information Technology Act, 2000 (Act 21 of 2000), ss. 69, 69A; Supra note 12 (Shreya Singhal v. Union

in pursuance of powers under the Act, disclose personal information without consent relevant to accountability for data leaks that fuel digital arrest scams.[16] These provisions operate alongside the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as subsequently amended, which impose due-diligence, grievance-redressal and traceability obligations on intermediaries and significant social media intermediaries.[17]

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, 1860 with effect from July 1, 2024, recodifies the substantive offences engaged by digital arrest and online defamation. Cheating by personation is penalised under Section 319,[18] criminal intimidation including intimidation by anonymous electronic communication under Section 351,[19] extortion under Sections 308 and 309, and defamation, together with its statutory exceptions of truth for public good and fair comment, under Section 356.[20] The consolidation of these offences under a single Sanhita has not, however, resolved the classificatory ambiguity that continues to attend digital arrest complaints, which frequently straddle extortion, cheating, impersonation and, where forged court orders are used, offences relating to the fabrication of judicial records.

Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023, successor to the Code of Criminal Procedure, 1973, governs arrest, investigation and the treatment of electronic evidence. Section 35 preserves and reinforces the requirement, drawn from "Arnesh Kumar v. State of Bihar and D.K. Basu, that arrest for offences punishable with imprisonment of less than seven years be preceded by a notice of appearance rather than automatic custodial arrest.[21] The Sanhita further permits search, seizure and production of electronic communication devices likely to contain digital evidence, and enables trials and depositions to be conducted through electronic mode provisions of direct relevance to prosecuting cross-border, technologically mediated crime

of India).
[16]The Information Technology Act, 2000 (Act 21 of 2000), s. 72.
[17]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, r. 3, r. 4.
[18]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 319.
[19]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 351.
[20]Supra note 10.
[21]The BNSS, 2023 (Act 46 of 2023), s. 35; see D.K. Basu v. State of West Bengal, supra note 19.

such as digital arrest fraud.[22]

Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023, replacing the Indian Evidence Act, 1872, governs the admissibility of electronic records. Section 63 is the direct successor to the erstwhile Section 65B, deeming a computer output admissible as a document without production of the original, subject to prescribed conditions and, significantly, a dual-certification requirement involving both the person in charge of the relevant device and an independent expert.[23] This dual-certification regime, discussed further in the analysis of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal in Part VIII below, is central to the successful prosecution of digital arrest and online defamation cases, both of which depend overwhelmingly on screen recordings, call logs, chat transcripts and social media data for proof.

Other Laws

The Digital Personal Data Protection Act, 2023 establishes, for the first time, a comprehensive statutory framework for the processing of personal data, imposing purpose-limitation, consent and data-security obligations on data fiduciaries whose failures frequently supply the raw material leaked phone numbers, purchase histories and financial profiles exploited in digital arrest scams.[24] The Telecommunications Act, 2023 empowers the Central Government to require biometric identification for SIM issuance and to disconnect telecommunication identifiers used for fraud, a power increasingly deployed by the Indian Cyber Crime Coordination Centre, which by late 2024 had blocked over 6.69 lakh SIM cards and 1.32 lakh IMEIs linked to cyber fraud.[25] The Indian Computer Emergency Response Team issues binding directions under Section 70B of the Information Technology Act requiring service providers to report cyber incidents and synchronise system clocks, facilitating cross-platform investigation.[26] The Reserve Bank of India has separately directed banks and payment intermediaries to strengthen transaction-monitoring and account-flagging mechanisms in response to the laundering of digital arrest proceeds through mule accounts, though

[22]The BNSS, 2023 (Act 46 of 2023), s. 176, s. 530.
[23]The BSA, 2023 (Act 47 of 2023), s. 63.
[24]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[25]The Telecommunications Act, 2023 (Act 44 of 2023); 'Supreme Court Empowers CBI to Investigate Digital Arrest Scams', supra note 6.
[26]Indian Computer Emergency Response Team, Directions under s. 70B(6) of the Information Technology Act, 2000, dated April 28, 2022, available at: https://www.cert-in.org.in (last visited on August 26, 2026).

commentators have observed that the Supreme Court's current framing treats banks primarily as sources of data rather than as institutions whose own omissions enable such laundering.[27] Finally, the National Cyber Crime Reporting Portal operates as the principal citizen-facing grievance mechanism, though its efficacy remains constrained by uneven state-level investigative capacity.[28]

Rethinking Criminal Liability

The statutory provisions surveyed above supply the raw material for prosecution, but they were not designed for a crime whose defining features are the diffusion of the criminal act across many hands, the concealment of the principal offenders behind foreign borders, and the indispensable, if often unwitting, participation of regulated domestic institutions. Three problems of criminal liability accordingly demand reconsideration.

Attribution and the Graduated Culpability of a Distributed Enterprise

A digital arrest is executed by a layered organisation: overseas scriptwriters and controllers, on-screen impersonators, domestic recruiters, and the holders of the 'mule' bank accounts through which proceeds are laundered. The offences under the Bharatiya Nyaya Sanhita, 2023 cheating, extortion, personation and criminal intimidation are framed around a principal offender and are ill-adapted to grading culpability across this hierarchy. The doctrines of common intention and criminal conspiracy permit the net to be cast widely, but risk sweeping in low-level, coerced or trafficked participants many themselves victims of the Southeast Asian 'scam compounds' on the same footing as the organisers who profit. A calibrated liability scheme, distinguishing organisers, knowing facilitators and coerced instruments, would better reflect both individual culpability and the transnational reality of the enterprise.

The Mule Account and the Threshold of Mens Rea

The mule-account holder occupies the most contested position on this spectrum. Prosecutions frequently founder on proof of mens rea, since the account may have been rented, sold, or opened under inducement without subjective knowledge of the specific fraud. Whether liability

[27]'Digital scams: The Supreme Court must direct banks to improve flagging mechanisms", Supreme Court Observer, Nov. 11, 2025, available at: https://www.scobserver.in/journal/digital-scams-the-supreme-court-must-direct-banks-to-improve-flagging-mechanisms/ (last visited on August 26, 2026).
[28]National Cyber Crime Reporting Portal, available at: https://cybercrime.gov.in (last visited on August 26, 2026).

should attach on the basis ‘f actual knowledge, wilful blindness, or a lower standard of recklessness as to the criminal use of the account is a question the present law leaves unresolved. A bespoke provision could legislate a rebuttable presumption, triggered by defined objective indicia such as the rapid pass-through of disproportionate sums, while preserving a genuine defence of innocent use so as not to criminalise the merely careless or the exploited.

Liability of Enablers: Banks, Payment Systems, Telecom and Platforms

The most significant gap concerns the institutions whose systems the fraud necessarily traverses. Banks and payment intermediaries onboard mule accounts and clear the impugned transfers; telecom operators issue the SIMs used to place the calls; and platforms host the impersonation profiles and forged court-order templates. As the Critical Analysis below observes, the Supreme Court's current framing treats banks primarily as custodians of data rather than as actors whose own compliance failures deficient know-your-customer verification, ignored transaction-monitoring alerts are a but-for condition of the loss. A rethinking of criminal liability must confront whether, and on what threshold of negligence or wilful default, such enablers should bear responsibility, whether criminal, quasi-criminal, or through statutory penalty, rather than being treated as mere conduits shielded by safe-harbour immunity or regulatory forbearance. The conditional intermediary immunity under Section 79 of the Information Technology Act, 2000, as construed in "Google India Pvt. Ltd. v. Visaka Industries, offers a template of graduated, due-diligence-contingent liability capable of extension, with appropriate modification, to financial and telecommunications enablers.

The Case for a Bespoke Offence

These difficulties converge on a single recommendation, elaborated in the Recommendations below: the enactment of a specific, named offence of impersonation-based extortion through electronic communication. A dedicated provision would end the classificatory drift by which functionally identical conduct is charged variously as cheating, extortion or personation across different States; would permit tailored sentencing, evidentiary presumptions and enabler-liability rules unavailable under the borrowed general offences; and would supply a clear statutory hook for the cross-border investigative and mutual-assistance measures that the transnational structure of the crime demands. The objection that existing offences already cover the conduct mistakes availability for adequacy: the fragmentation of FIR registration that the Supreme Court has itself had to address is the direct product of relying on a patchwork of provisions never designed to operate together.

Legal Remedies and Victim Recovery

A criminal conviction, even where achievable against a transnational syndicate, does little to restore the victim who has watched a lifetime's savings vanish within hours. The adequacy of the legal response to digital arrest fraud must therefore be judged as much by its remedial and restitutionary architecture as by its penal provisions.

The Golden Hour: Reporting and Fund-Freezing

The single most consequential remedy is speed. The Citizen Financial Cyber Fraud Reporting and Management System, accessible through the national cyber-fraud helpline 1930 and the National Cyber Crime Reporting Portal, is designed to interrupt the layering of stolen funds during the so-called 'golden hour' immediately following a transfer, enabling participating banks and payment intermediaries to place a hold before the money is withdrawn or dispersed across further accounts. Its efficacy, however, depends on the victim's prompt recognition of the fraud precisely what the coercive, isolating design of a digital arrest is engineered to delay and on the responsiveness of the receiving institution. Delay at either point ordinarily renders the funds unrecoverable, which is why victim awareness and mandatory, time-bound bank cooperation are properly understood as remedial rather than merely preventive measures.

Banking Remedies, Account-Freezing and Institutional Responsibility

Beyond the golden-hour mechanism, the Reserve Bank of India's directions on the monitoring, flagging and freezing of mule accounts furnish an administrative remedy that operates independently of criminal adjudication. Yet these remedies remain, in practice, discretionary and unevenly enforced, and the victim ordinarily has no enforceable right to compel a bank to freeze or reverse a fraudulent transfer. A rights-based remedial framework would convert these regulatory expectations into enforceable obligations, coupled with a presumption of institutional liability to compensate where a bank's demonstrable failure to act on a timely report enabled the loss aligning the remedial regime with the enabler-liability analysis developed above.

Restitution, Confiscation and Statutory Compensation

Where funds cannot be frozen in time, restitution must be pursued through the confiscation of criminal proceeds and their return to victims. The Bharatiya Nagarik Suraksha Sanhita, 2023 preserves and strengthens the court's power to order restoration of property and the payment of

compensation to victims, and a dedicated victim-compensation scheme funded in part from confiscated proceeds, as recommended below would mitigate the disproportionate devastation visited upon elderly and lower-income victims. Statutory compensation of this kind gives effect to the State's positive obligation, recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India, to protect against the very data-driven harms whose materialisation it has failed to prevent.

Civil and Constitutional Remedies

Finally, the victim's remedial repertoire is not exhausted by the criminal process. Civil suits in tort for deceit and conversion, though hampered by the anonymity and frequent insolvency of the perpetrators, may lie against identifiable enablers; and the constitutional remedy under Articles 32 and 226, for enforcement of the State's positive duty to protect life, liberty and privacy, offers a route foreshadowed by the horizontality reasoning in Kaushal Kishor v. State of U.P. to hold both State agencies and private institutions to account for systemic failures of protection. The Supreme Court's suo motu supervision of the digital arrest crisis is itself an exercise of this constitutional remedial jurisdiction.

Case Law Analysis

Five judgments of Indian constitutional courts, decided between 2015 and 2020, are analysed below for their direct bearing on the criminal-liability, evidentiary and remedial dimensions of digital arrest and cyber fraud.

1. Justice K.S. Puttaswamy (Retd.) v. Union of India

Decided by a nine-judge Bench of the Supreme Court in August 2017, this case arose from a challenge to the Aadhaar biometric identification scheme and required the Court to determine, as a threshold question, whether privacy is a fundamental right.[29] The nine-judge Bench unanimously recognised privacy as intrinsic to Article 21, testable only against legality, necessity and proportionality. It grounds the treatment of data leaks fuelling digital arrest as independent constitutional harms, though its call for a data-protection statute went unanswered until 2023, leaving a fraud-prone gap.

[29]Supra note 17 (Justice K.S. Puttaswamy (Retd.) v. Union of India).

2. Shreya Singhal v. Union of India

Decided in March 2015, this case concerned constitutional challenges to Section 66A of the Information Technology Act, 2000, which criminalised sending 'grossly offensive" or 'menacing' information through communication services.[30] The Court struck down Section 66A as unconstitutionally vague and overbroad, holding that online-speech restrictions must meet the same precision and proportionality standards as offline speech, while upholding Sections 69A and 79 with safeguards. It remains foundational, yet left no narrower substitute for genuinely harmful online communication.

3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

Decided by a three-judge Bench in July 2020, this case resolved conflicting precedent on the mandatory nature of the certificate requirement for electronic evidence under the then-applicable Section 65B of the Indian Evidence Act, 1872.[31] The Court held a Section 65B(4) certificate a mandatory precondition to admitting electronic evidence, subject to a narrow exception where it cannot be procured. Now carried into Section 63 of the Bharatiya Sakshya Adhiniyam, this governs the screen recordings and call logs central to digital arrest prosecutions, but disadvantages unrepresented elderly victims.

4. Ritesh Sinha v. State of Uttar Pradesh

Decided in August 2019, this case addressed whether a Magistrate could compel an accused to furnish a voice sample for investigative comparison in the absence of explicit statutory authorisation.[32] The Court held that a Magistrate may, under Article 142, compel a voice sample, which is non-testimonial and outside Article 20(3). It applies directly to the forensic voice and deepfake-audio analysis needed to unmask perpetrators, while its reliance on Article 142 illustrates courts improvising authority the legislature has been slow to supply.

5. Arnab Ranjan Goswami v. Union of India

Decided in May 2020, this case concerned multiple First Information Reports lodged across several States against a television journalist in respect of a single broadcast.[33] The Court

[30]Supra note 12.
[31]Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[32]Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1.
[33]Supra note 18.

quashed all but one of multiple FIRs as impermissible multiplicity arising from a common cause, protecting personal liberty under Article 32. This parallels the fragmentation of digital arrest cases, where one network spawns FIRs across States, but the readiness to grant high-profile petitioners relief raises equity concerns for ordinary victims.

Conclusion

Digital arrest fraud is best understood not as ordinary cheating but as a systemic assault on the individual's dignity, autonomy and due-process protections in an environment where technological mediation has outpaced the institutional capacity to safeguard them. The doctrinal architecture surveyed in this paper, from Puttaswamy's recognition of privacy as foundational to the evidentiary and voice-sample principles governing digital investigations, shows that Indian law possesses the conceptual resources to respond. What remains incomplete is the translation of that doctrine into operative, adequately resourced practice: a bespoke offence, calibrated liability for enablers, consolidated investigation, victim-centred evidentiary procedure and time-bound fund recovery. The Supreme Court's suo motu intervention in 2025 signals recognition that digital arrest fraud has crossed from ordinary criminality into a systemic concern. Whether that recognition yields durable protection will depend less on further doctrinal elaboration than on the legislative, institutional and remedial reforms outlined above, pursued with a seriousness commensurate with the scale of harm already done.