WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Arrest Scams in the Digital Era: Legal Loopholes and Regulatory Challenges

Diksha[1], Dr. Neetu Singh[2]

[1]LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[2]Assistant Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

ABSTRACT

Digital "arrest" scams in India are a coercive, technology-mediated form of extortion in which offenders impersonate police or central agencies over voice or video, manufacture fear of grave accusations, and drive instant transfers through UPI, wallets, or IMPS. This paper maps the offence end-to-end and evaluates whether India's post-2023 legal architecture already contains sufficient doctrinal tools and institutional levers to suppress it. Using a doctrinal method, the analysis reads the Bharatiya Nyaya Sanhita (BNS) on aggravated extortion and cheating, the Bharatiya Nagarik Suraksha Sanhita (BNSS on arrest safeguards, the Information Technology Act (IT Act) with the 2022 CERT-In Directions, the Telecommunications Act, 2023, the Digital Personal Data Protection (DPDP) Act, 2023, and RBI's consumer-protection framework alongside operational initiatives such as the National Cybercrime Reporting Portal/1930 helpline, CFCFRMS, and DoT's Sanchar Saathi/Chakshu. Findings show that the *substantive* law is largely adequate: aggravated extortion and personation provisions capture the core wrong; telecom and intermediary rules enable identifier controls, takedown, and log retention; and banking redress schemes create a parallel civil-recovery track. The *operational* gap lies in latency-slow attribution across telecom and platforms, non-uniform charging (personation without aggravated extortion), inconsistent freeze routing across banks, and uneven evidence certification for large volumes of electronic records. The paper argues for a single, time-bound operational sequence that is triggered the moment "digital arrest" is alleged: simultaneous BNS charges, CERT-In-aligned log preservation, telecom traceback on identifiers, and bank-centric freezing with ombudsman backstops. Aligning these corridors on shared clocks and templates reduces the scam's payoff window and restores public confidence in authentic state communications while preserving constitutional constraints on speech and arrest.

Keywords: digital arrest; impersonation; aggravated extortion; intermediary due diligence; BNSS 2023; BNS 2023; IT Act 2000; CERT-In Directions 2022; Telecommunications Act 2023; DPDP Act 2023; RBI 2017 limited liability; RBI Integrated Ombudsman; Sanchar Saathi; Chakshu; CFCFRMS.

Introduction

Digital arrest scams have gained visibility in Indian cities and tier-two towns because they combine strong psychological pressure with believable administrative detail and deliver both over communication tools that people have normalised for work and family contact. The call or video link arrives with an official-looking identifier, a stern voice explains that a parcel in the recipient's name was seized with drugs or that the phone number surfaced in a money-laundering chain, and the listener is told not to involve anyone else until the "verification" is over.[1] This conversation is then shifted to an extended video session in which a second person joins, posing as senior police, ED, or DoT staff. The victim is kept online for hours, sometimes being made to write down sections of law, sometimes being shown forged warrants, and at the end of the script is told to transfer money to a government account to "clear" the name. Because India's payment ecosystem allows instant, high-value, round-the-clock transfers, the deception converts into a loss inside the same call. The entire structure assumes that the recipient does not know that lawful arrest under "BNSS 2023" cannot be carried out in this fashion, that government officers do not use random video apps for financial instructions, and that official payments go through notified channels only.

A legal research study on this subject needs to start from the fact that Indian law already criminalises every key step of the scam but still sees repeat incidents in multiple states. State cyber police units in 2024 and 2025 have described arrest-scam call centres that run from rented premises, operate on foreign VoIP trunks, and keep renewing their identities faster than Indian telecom filters can act. This shows that the operative gap is not merely in the text of "BNS 2023", "BNSS 2023", or the "Information Technology Act, 2000", but in the speed and coordination across criminal investigation, telecom blocking, CERT-In log access, and banking freeze orders. The research gap lies in the absence of doctrinal writing that places digital arrest scams next to other coercive digital crimes such as sextortion or loan-app extortion and asks whether aggravated extortion under "Section 308(6)-(7) BNS 2023" can be the lead charge in such cases. Policy stakes are high because every such call weakens public confidence in real police communications, because it

[1] Talat Fatima, *Cyber Crimes* 112 (Eastern Book Company, Lucknow, 1st edn., 2016).

pulls private telecom and platform actors into urgent law-enforcement workflows, and because it pushes banks to act on complaints that arrived before the victim even came to the police station.[2]

Research Questions

The research questions for the study are as follows:-[3]

1. whether the current combination of "Section 308 of the BNS, 2023", "Section 66D of the Information Technology Act, 2000", and telecom offences under "Section 42 of the Telecommunications Act, 2023" adequately criminalises digital arrest scams without further statutory amendment?
2. whether the existing grievance and ombudsman pathways, including the "1930" cyber helpline and the "RBI Integrated Ombudsman Scheme, 2021", offer a recovery track that is fast and coordinated enough to make such scams economically unattractive to offenders?

Problem Statement

Digital arrest scams survive because no single authority in India today is able to see the entire fraud in real time. The criminal law authority sees a complaint of extortion or cheating but may not have instant access to telecom logs that prove spoofing. The telecom authority can see a burst of suspect calls from an international gateway but may not know that money was forced out of a citizen. The bank can see an unusual transfer but may not have the detail that it was induced by fear of a non-existent arrest. Offenders thrive on this fragmentation, on cross-border VoIP routes, on SIM cards acquired with falsified KYC, and on payment intermediaries that do not yet screen for coercive transactions. Any legal study that ignores these frictions would misdiagnose the cause of persistence of such scams.[4]

Objectives of the Study

The objectives of the study are as follows:-[5]

- To identify the substantive and procedural provisions across "BNS 2023", "BNSS 2023", the "Information Technology Act, 2000", the "Telecommunications Act, 2023", and the "Digital Personal Data Protection Act, 2023" that can be converged for tackling digital arrest scams.
- To propose a sequenced regulatory and investigative response that closes current timing, attribution, and recovery gaps in cases involving telecom-based impersonation and coerced digital payments.

Research Methodology

The research proceeds on a doctrinal footing that reads together the text of the "Bharatiya Nyaya Sanhita, 2023", the "Bharatiya Nagarik Suraksha Sanhita, 2023", the "Information Technology Act, 2000" with its rules, the "Telecommunications Act, 2023", and the "Digital Personal Data Protection Act, 2023" as carried on official and authenticated government sources, along with binding directions such as the CERT-In Order of 28 April 2022 and financial-sector circulars of the Reserve Bank of India on customer liability and ombudsman redress. These texts are interpreted in light of public advisories and enforcement notes released by the Department of Telecommunications on Sanchar Saathi and Chakshu that show the practical worry behind the legislative choices. Since the subject is emerging, the method also takes note of figures placed in Parliament or in press briefings on disconnections of fraudulent SIMs and blocking of spoofed calls, although such figures are treated as contextual material and not as primary authority.[6]

Anatomy of "Digital Arrest" Scams

A digital arrest fraud normally starts with a call that looks domestic and official even when it is not, followed by a staged conversation where the target is told that his or her number, Aadhaar, courier booking, or bank account is under watch in connection with a serious offence such as narcotics or anti-state activity. Once the initial fear is planted, the caller tells the target to move to a video app so that the call can be "recorded for court", and from that point the target is not allowed to disconnect or consult family, which is why the practice is widely described as a form of arrest conducted through a device. During the video call, forged documents, fake seals, or websites made to resemble government portals are shown, and the target is compelled to

[2] Indranath Gupta, Lakshmi Srinivasan, "Evolving Scope of Intermediary Liability in India", 1 *International Review of Law, Computers & Technology* 58 (2023).
[3] Karnika Seth, Computers, *Internet and New Technology Laws* 174 (LexisNexis, Gurgaon, 1st edn., 2016).
[4] Ananth Padmanabhan, "Give Me My Space and Take Down His: A Closer Look at Intermediary Liability", 9 *Indian Journal of Law and Technology* 64 (2013).
[5] Prashant Mali, *Cyber Law & Cyber Crimes* 150 (Snow White Publications, Mumbai, 1st edn., 2015).
[6] Nandan Kamath, "Should the Law Beat a Retweet? – Intermediary Liability in India", 9 *Indian Journal of Law and Technology* 58 (2013).

transfer money to accounts described as government audit accounts. Every one of these steps can be matched with an Indian offence and with an Indian regulator, which is why presenting the stages in a single layout clarifies the legal response.[7]

Stage	**Conduct**	**Primary offence/provision**	**Regulator/agency primarily engaged**	**Typical evidence required**
Initial spoofed/SIM-boxed contact	Fake police/agency call placed over OTT or VoIP with masked ID	"Section 66D IT Act 2000"; "Section 42 Telecommunications Act 2023"	Department of Telecommunications, telecom service provider	CDRs, IP logs, masked caller details, SIM KYC
Identity harvesting and intimidation	Victim asked for Aadhaar/PAN/selfie; threat of arrest, FIR or public disclosure	"Section 308(1)-(2) BNS 2023"; "Section 66C IT Act 2000"	State cyber police/city cyber cell	Video recording, screenshots, device metadata
Prolonged digital custody	Victim forced to stay on camera, told not to consult any person, warned of custodial action	"Section 308(6)-(7) BNS 2023"	State police/cybercrime police station	Full call record, IP of caller, identifiers of impersonated officer
Coerced UPI/wallet/bank transfer	Victim moves funds to "safe" or "escrow" accounts, funds split among mules	"Section 308 BNS 2023" read with cheating provisions; RBI 6 July 2017 circular for recovery	Banks, payment system operators, RBI, police	UPI/IMPS logs, time stamps, beneficiary accounts
Post-fraud reporting and traceback	Complaint on 1930/cybercrime.gov.in, request to freeze, CERT-In informed	CERT-In Directions 2022 (6-hour reporting, 180-day logs)	CERT-In, banks' fraud cells, state cyber nodes	Complaint IDs, log preservation, freeze acknowledgements

Table 1: Modus operandi stages vs applicable Indian offences and regulators

The value of this table lies in the way it reveals that the scam is not only a crime of speech but a crime of telecom misuse and of forced financial transfer, so prosecution must proceed on all tracks at once. The first two rows call for immediate DoT attention on spoofed numbers and SIM-boxes, the middle rows direct police to apply aggravated extortion under "Section 308(6)-(7) BNS 2023", and the last rows involve CERT-In and RBI-led recovery. Without this staged view, each agency might believe the matter belongs elsewhere, creating the space that organised fraud groups are exploiting.

Statutory Framework in India

The legal structure that responds to digital arrest scams can be seen as four coordinated corridors. Criminal law through the "BNS 2023" gives the power to register the FIR, to describe the conduct as extortion by threat of accusation, to add cheating by personation, and to seek custodial interrogation of the organisers. Procedural law through the "BNSS 2023" states the only conditions under which arrest is lawful and transparent, so that citizens and platforms can call out scams that claim to act outside those conditions. Cyber law through the "Information Technology Act, 2000" introduces identity-theft and personation offences and the blocking power under "Section 69A", which is vital when a specific app, link, or domain is used to stage fake video rooms. Telecom law, now recast in the "Telecommunications Act, 2023", supplies the authority to bar spoofed international incoming calls, to disconnect numbers taken on forged KYC, and to penalise misuse of telecom identifiers. Parallel to these corridors run the RBI rules on unauthorised electronic banking transactions and the "RBI Integrated Ombudsman Scheme, 2021", which create an immediate civil redress track for victims. The "Digital Personal Data Protection Act, 2023" adds a preventive layer by insisting on security safeguards and breach intimation so that identity material pilfered from a service provider cannot be silently recycled into arrest scams.[8]

Substantive Offences under BNS 2023

The centrepiece of a criminal case in a digital arrest scenario is "Section 308 of the BNS, 2023". The clause defines extortion as intentionally putting any person in fear of injury and dishonestly inducing that person to deliver property. Sub-clauses "Section 308(6)" and "Section 308(7)" address a sharper situation, namely where the fear created is of an accusation of an offence punishable with death, life imprisonment, or imprisonment for ten years. Arrest

[7] Pavan Duggal, *Textbook on Cyber Law* 139 (LexisNexis, New Delhi, 1st edn., 2016).
[8] Chinmayi Arun, "Gatekeeper Liability and Article 19(1)(a): Shreya Singhal v. Union of India", 7 *NUJS Law Review* 73 (2014).

scammers do exactly this when they claim that a narcotics parcel has been intercepted in the victim's name or that a terror funding channel used the victim's number. The call is often accompanied by forged e-mail or PDF material carrying insignia of central agencies, so forgery provisions under the same statute can be joined. Cheating by personation carried over from the IPC framework punishes pretending to be any other person, which is the essence of the video-call officer act. Together these provisions give the police a high-sentence, multi-count charge sheet that justifies requests for cross-border data, for platform logs, and for transit warrants.[9]

Old IPC provision	**Description under IPC**	**Corresponding BNS 2023 provision**	**Relevance to digital arrest scams**
IPC 384	Extortion	"Section 308(1) BNS 2023"	Basic threat to make victim deliver money
IPC 385	Putting person in fear of injury for extortion	"Section 308(2) BNS 2023"	Covers early threat stage on voice/video
IPC 386	Extortion by fear of death/grievous hurt	"Section 308(4) BNS 2023"	Fits where caller threatens custodial harm
IPC 387	Fear of death/grievous hurt to commit extortion	"Section 308(5) BNS 2023"	Fits where fake encounter or media leak is cited
IPC 388	Extortion by threat of accusation of serious offence	"Section 308(6) BNS 2023"	Core tool for digital arrest cases
IPC 389	Putting person in fear of accusation to extort	"Section 308(7) BNS 2023"	Used when threat is to publicise false FIR
IPC 419	Cheating by personation	BNS cheating/personation provision	Used when caller pretends to be police or CBI
IPC 420	Cheating and dishonestly inducing delivery of property	BNS cheating inducing delivery provision	Added when actual UPI/bank/wallet transfer is extracted

Table 2: IPC to BNS mapping for cheating, personation, extortion

This conversion table matters because it removes any doubt that the conduct once prosecuted under IPC 384-389, 419, and 420 is now to be booked under the specific BNS numbers listed, so that requests for telecom and platform cooperation carry the correct statutory references. It also shows that aggravated extortion under "Section 308(6)-(7)" is not a new concept invented for digital crimes but a restated device for punishing the exact kind of accusation-based pressure that these scammers deploy. Once the FIR names these sections, allied cyber and telecom offences can be added to support data seizure and blocking.

Procedural Guardrails under BNSS 2023

The procedural limb is supplied by "Section 35 of the Bharatiya Nagarik Suraksha Sanhita, 2023" which restates that arrest without warrant is justified only when definite conditions are met and that in many situations the correct course is to issue a notice of appearance. A real police officer is therefore expected to identify the offence, record reasons, issue written intimation, and provide an opportunity to appear. A scammer on a video call does the exact opposite by withholding identity, fabricating offences, demanding secrecy, and insisting on instant payment to avoid arrest. Public awareness of "Section 35" weakens the plausibility of such demands and gives platforms a standard against which they can flag or suspend accounts pretending to exercise arrest powers. It also gives courts a reference when they are asked to confirm or extend custody of those actually arrested for running such call centres.[10]

Information Technology Act 2000

The "Information Technology Act, 2000" contains two offences that recur in digital arrest FIRs. "Section 66C" punishes fraudulent or dishonest use of another person's electronic signature, password, or unique identification feature, and this is attracted whenever the scammer extracts Aadhaar images, selfies, or banking credentials during the call and reuses them. "Section 66D" punishes cheating by personation using a computer resource, which squarely covers the act of posing as a police or agency officer over an OTT app, VoIP call, or fake government website. Where the scam uses a fixed URL or app, the government can resort to "Section 69A" to block access, and intermediaries are required to comply. Safe harbour under "Section 79" remains for intermediaries that show due diligence, act on takedown requests, and preserve logs for investigation. These provisions, read with BNS charges, create a cyber-crime case that is not limited to the state where the victim lives, since servers, platforms, and telecom routes may lie in several jurisdictions.[11]

[9] Rohas Nagpal, *Introduction to Indian Cyber Law* 168 (Asian School of Cyber Laws, Pune, 1st edn., 2008).
[10] Bhavyakirti Singh, Aditya Bamb, "The Dichotomy of the 65B Certificate: Analysing Trends with Regard to the Authentication of Electronic Evidence in India", 10 *Christ University Law Journal* 85 (2021).
[11] Vakul Sharma, *Information Technology: Law and Practice* 120 (Universal Law Publishing, New Delhi, 1st edn., 2011).

Intermediary Due Diligence and Takedowns

The "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", along with later amendments, impose on intermediaries a duty to inform users that impersonation of another person or of a government department is not permitted, to put in place grievance redress, and to remove or disable access to such material within twenty-four hours once a complaint is received. This is immediately relevant where scammers operate WhatsApp or Telegram profiles carrying police photographs, or where they post video clips that instruct recruits on how to run arrest calls. During active scam waves, intermediaries are expected to apply "reasonable efforts" to identify and remove such content, while also preserving data for law enforcement for at least 180 days in line with the CERT-In Directions. Appeal to the Grievance Appellate Committee offers victims and agencies a further forum when takedowns are not processed fast. In this manner, intermediary rules function as the bridge between individual criminal process and systemic prevention on platforms.[12]

CERT-In Directions 2022

The CERT-In Directions of 28 April 2022, issued under "Section 70B(6) of the IT Act 2000", created a uniform six-hour reporting duty for specified cyber incidents and a 180-day log retention duty inside India for intermediaries, data centres, and VPN providers. Digital arrest scams often ride on remote desktop access, unauthorised wallet sessions, or cloud-hosted video rooms that leave forensic traces only for a limited time. Early reporting by platforms or payment intermediaries under these Directions allows CERT-In to circulate indicators of compromise, block malicious infrastructure, and supply logs to police so that they can connect separate FIRs to a single call centre. The Directions also require all such entities to designate a point of contact, which cuts through the earlier problem of police not knowing whom to approach in a foreign or private service. Non-compliance can attract action, so intermediaries have an added incentive to respond quickly to arrest-scam misuse.[13]

Telecommunications Act 2023 and Anti-Spoofing Regime

The "Telecommunications Act, 2023" furnishes the state with powers to secure telecom identifiers, to detect and punish their misuse, and to direct licensees to block or trace suspicious calls. "Section 42" targets tampering or unauthorised acquisition of identifiers and fits the SIM-box, forged-KYC SIM, and spoofed-caller-ID patterns that power digital arrest campaigns. The Department of Telecommunications has rolled out the Sanchar Saathi portal and the Chakshu feature to let citizens report suspected fraud calls, and has publicised the International Incoming Spoofed Calls Prevention System that filters calls entering India with Indian numbers. Periodic DoT releases show disconnection of lakhs of SIMs obtained on falsified documents and blacklisting of devices involved in such activity. When this telecom action is pressed into the same timeline as criminal and cyber action, the pool of numbers available to the fraudster narrows and repeated calling with the same identity becomes harder. This statutory backing is essential for service providers, because it allows them to act against customers misusing services without fear of contractual dispute.[14]

Data Governance under DPDP Act 2023

The "Digital Personal Data Protection Act, 2023" supplies a preventive frame that is often missing in cyber-fraud discussions. Many arrest scams begin with correct personal details of the victim, including mobile number, address, or recent transaction data, which gives the caller credibility. Under the Act, data fiduciaries are required to adopt reasonable security safeguards, to notify the Data Protection Board and affected data principals when a breach occurs, and to erase data once the purpose is over. If a telecom operator, courier service, or bank suffers a breach and keeps silent, those leaked datasets can be silently channelled to fraudsters who then run high-success arrest scams. Early breach notice enables potential targets to reject sudden arrest calls. The Act also allows the central government to classify certain entities as significant data fiduciaries, which can be used to bring large platforms and major payment players under tighter audit for exactly this kind of misuse. Over time, enforcement under this Act can cut into the supply of identity material that makes digital arrest scams believable.

Consumer Redress and Banking Liability

Once a victim has followed the scammer's instructions and sent money through UPI, IMPS, or a wallet, criminal investigation alone rarely recovers the amount because mules and money mules shift funds very fast. The Reserve Bank of India anticipated this difficulty in its circular on "Customer protection–Limiting liability of customers in unauthorised electronic banking transactions" dated 6 July 2017, which states that if a customer reports within three working days of such a transaction and the loss was due to contributory fraud by a third party, the customer's liability is zero and the bank must credit the account. The "RBI Integrated Ombudsman Scheme, 2021" then offers a channel to complain when banks do not act or when disputes arise about the nature of the transaction. In digital arrest scenarios, the consent of the customer is vitiated by fear and false personation, so it should be treated like an unauthorised transaction for the purpose of customer protection. Field practice has shown that early calls to 1930 and cybercrime.gov.in tickets help banks to freeze or recall amounts before further layering.

---

[12] Farasat Ahmed, "Recasting the Intermediary: Online Gatekeeping and Safe Harbour in India", 1 *Indian Law Review* 92 (2017).

[13] Sarthak Chaturvedi, "India's 2022 CERT-In Directions—A Case of 'Unconstitutional Delegated Legislation'?", 13 *International Data Privacy Law* 58 (2023).

[14] Debanshu Mukherjee, Karan Gulati, "Evaluating the Need for Sectoral Insolvency Frameworks in India: The Telecom Sector as a Case Study", 9 *NLS Business Law Review* 73 (2023).

Step	Action by victim/complainant	Legal or regulatory basis	Deadline/time window	Expected outcome
1	Contact "1930" or file on cybercrime.gov.in with transaction details	National cybercrime reporting framework; CERT-In Directions 2022	Immediate/same day	Alert to concerned bank/PSP for freeze/hold
2	Intimate own bank/PSP about coerced transfer	RBI circular 6 July 2017 on limiting customer liability	Within 3 working days for zero liability; within 7 days for limited liability	Provisional credit or investigation by bank
3	Lodge FIR citing "Section 308 BNS 2023", "Section 66D IT Act 2000", "Section 42 Telecommunications Act 2023" where applicable	BNS 2023 and BNSS 2023 framework	As soon as practicable	Formal criminal process, data requests to telecom/platforms
4	Approach RBI CMS under "RBI Integrated Ombudsman Scheme, 2021" if bank reply is unsatisfactory	RBI-IOS 2021	After 30 days or on unsatisfactory reply	Direction to bank to refund or improve handling
5	Raise data-security complaint if identity leak is suspected	"Digital Personal Data Protection Act, 2023"	As soon as breach is known	Record of breach, possible penalties on fiduciary

Table 3: Post-fraud pathways and deadlines

This closing table shows that recovery is a race against time and that the legal order has already set out clear windows within which the aggrieved person and the bank must act. Criminal law steps, telecom traceback, CERT-In reporting, and ombudsman escalation need to run in parallel, not one after another. When that parallelism is honoured, digital arrest scams lose the predictability on which they thrive, and the fragmented response that currently enables these crimes gives way to a single, repeatable playbook for Indian authorities and service providers.

Enforcement Architecture and Current Initiatives

The contemporary Indian response to arrest scams that originate on calls, encrypted chats or video interfaces is built around a national funnel that captures complaints fast, a financial freezing backbone that talks to banks and wallets, and a policing tier that works under "Bharatiya Nyaya Sanhita, 2023" and "Bharatiya Nagarik Suraksha Sanhita, 2023" to convert each complaint into a workable criminal case. The public-facing end of this chain is the Indian Cyber Crime Coordination Centre's "National Cyber Crime Reporting Portal" and the helpline "1930", both of which are meant to absorb the complaint within minutes of the transfer, tag it by fraud type and jurisdiction, and push it to the concerned State or UT so that money can be stopped before it leaves the banking system. The funnel works best when callers are able to give full identifiers in the first hour, because the next stage, the "Citizen Financial Cyber Fraud Reporting and Management System" (CFCFRMS), can freeze only what is correctly described in the complaint and can notify only those financial entities whose details are complete in the record. This explains why arrest scams that keep the victim on hold for long video calls to prevent reporting still score high on loss, since every delayed entry weakens the golden-hour advantage of the system and exposes routing gaps across States.

The practice box that this segment presupposes would tell a complainant, an NGO volunteer or even a first responder at a district cyber cell that within sixty minutes the report should contain the phone number or app ID used by the pretended officer, the exact time stamp of each transfer, the name of the bank, wallet or UPI handle used, the beneficiary account number or VPA, the screenshots of any fake warrant, and the link to the meeting or video call. Once this material sits inside NCRP, the CFCFRMS node can send freeze requests to banks, the local police can open an FIR under "Section 308(6) or 308(7) of the Bharatiya Nyaya Sanhita, 2023" together with "Section 66C" or "Section 66D of the Information Technology Act, 2000", and telecom service providers can be approached for call detail records. The bottleneck in real cases has been that helpline agents sometimes misclassify the complaint or route it to a State that is not hosting the mule account, which forces a second routing cycle and eats into the time that the receiving bank is willing to keep the transaction in a frozen state. The architecture is therefore impressive on paper but still dependent on human accuracy, and arrest scam operators exploit precisely that dependence.

Case Law and Precedents

Judicial decisions in India have already drawn a wide perimeter around personal liberty, electronic speech, intermediary conduct and evidentiary reliability, and that perimeter is exactly what digital arrest scams try to breach by persuading a citizen that arrest is instantaneous, that online platforms have no duties, or that electronic material can never be proved. The move from colonial-era codes to "Bharatiya Nyaya Sanhita, 2023", "Bharatiya Nagarik Suraksha Sanhita, 2023" and "Bharatiya Sakshya Adhiniyam, 2023" did not unsettle that judicial perimeter but in certain places codified it. "Section 35 of the BNSS" gathers the arrest standards that courts had insisted on over the years, "Section 63 of the BSA" follows the logic of earlier rulings on the need for certificates for digital records, and the continuing validity of safe-harbour logic under the IT Act after the striking down of "Section

66A" shows that courts wanted both protection of speech and traceability in criminal cases. Each of the following authorities therefore becomes a lens for reading how arrest threats on WhatsApp, Instagram, Telegram or VoIP should be treated.

Shreya Singhal v. Union of India

In the case of "*Shreya Singhal v. Union of India*[15], the Supreme Court examined a series of writ petitions that challenged the constitutionality of "Section 66A of the Information Technology Act, 2000" along with the blocking power in "Section 69A" and the intermediary immunity under "Section 79". The factual background placed before the Court showed that people had been arrested for tweets and Facebook posts, that expressions such as grossly offensive or menacing had been applied without a public-order context, and that online speech was being chilled on a large scale. The petitioners argued that Article 19(1)(a) protects political comment, satire and criticism, while Article 19(2) lists exhaustively the grounds on which such speech can be curtailed, and the impugned section, by using vague and subjective language, travelled far beyond those grounds. The Union defended the provision as a tool to curb spam, online harassment and defamation, and invited the Court to read it narrowly. The Court declined, holding that criminal law must present a clear line between conduct that attracts penal consequences and conduct that is protected, and that "Section 66A" was so wide and undefined that it would inevitably catch protected speech. The section was therefore struck down in its entirety. The Court upheld "Section 69A" and the blocking rules because they contained procedural safeguards such as reasons, hearing and review, and it read "Section 79" to mean that intermediaries would lose safe harbour only when they received an order from a court or a lawfully authorised government agency and failed to act. This fine balance is directly relevant for arrest scams, because it permits police cyber cell to send a lawfully authenticated notice to an intermediary for real-time takedown of a fake enforcement handle or forged summons without resurrecting the unconstitutional vagueness that "Section 66A" had created.

The judgment's reasoning also clarifies for present purposes that coercive content which is itself part of an offence, such as a forged FIR draft, a fake LOC threat or a demand for payment under the cover of arrest, never received protection under Article 19(1)(a) in the first place, so intermediaries that remove such content on receipt of a proper notice are not censoring speech but preventing the continuation of a criminal act. This makes it easier to argue that live impersonation scams should lead to immediate deactivation of the relevant account or link, because the Court had already recognised that safe harbour is conditional and not absolute. It becomes unnecessary to design fresh legislative language for every new scam variant, since the constitutional map already permits targeted executive action so long as it is reasoned and traceable. Arrest scams that rely on sending repeated menacing messages will therefore find it harder to remain on mainstream platforms once this reading of "Shreya Singhal" is applied by platform compliance teams and State cyber cells in tandem.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

In the case of "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[16], the Supreme Court had to decide whether an election petitioner could rely on video recordings to prove time of filing nomination papers without furnishing the certificate that "Section 65B(4) of the Indian Evidence Act, 1872" required. The Court surveyed its own earlier rulings and found that "*Anvar P.V. v. P.K. Basheer*[17] had laid down a clear rule that electronic records produced as secondary evidence are admissible only when they are accompanied by such a certificate setting out the source, the manner of production and the integrity of the device, while a later two-judge decision in "Shafhi Mohammad v. State of Himachal Pradesh" had created an impression that the requirement was procedural and could be relaxed. A larger Bench was therefore called on to reconcile these rulings. The Court chose the stricter path, affirming that the certificate requirement is mandatory because electronic material is especially vulnerable to editing, and courts cannot rely on material of uncertain provenance in deciding rights. This approach is decisive for arrest scams, because scam call recordings, screen captures of fake police dashboards and app-based chat logs are all electronic material produced on devices that are often not with the complainant, and yet they are central to proving the extortionate nature of the communication.

The Court did not ignore practical difficulties. It accepted that a victim or a litigant may not have access to the server or system that created the electronic record, and it therefore permitted such a party to seek an order from the court to summon the certificate from the person or entity in possession of the device. It also clarified that when the original device is produced in court and is examined in terms of primary evidence, the certificate is not necessary. What the Court effectively created was a two-lane road to electronic proof: one for cases where the party controls the device and must bring the certificate along with the copy, and another for cases where the device is outside its control, in which the court will compel the device-holder to supply the certificate. When this logic is read with "Section 63 of the Bharatiya Sakshya Adhiniyam, 2023", which preserves the insistence on technical certification, a cyber cell that receives an arrest scam complaint can seize the victim's device, mirror it, issue notices to the telecom operator, the over-the-top platform and the bank, and obtain a complete set of certified records that will stand at trial. That removes the familiar defence argument that because the call was on an internet application or because the money moved across several wallets, the evidence trail is too weak to support conviction.

Anvar P.V. v. P.K. Basheer

In the case of "*Anvar P.V. v. P.K. Basheer*[18], the Supreme Court was dealing with allegations of corrupt practices in an election dispute where CDs and other electronic records had been tendered without following the exact directions of "Section 65B of the Indian Evidence Act, 1872". The Court reviewed the statutory scheme and held that electronic records are a special species of document and Parliament had chosen to craft a complete rule for their admissibility. That rule, set out in sub-sections (2) to (5) of "Section 65B", demanded a certificate that identifies the electronic record, describes how it

[15] (2015) 5 SCC 1.
[16] 2020 SCC Online SC 571.
[17] (2014) 10 SCC 473.
[18] *Supra* note 17.

was produced, states that the device was in regular use, and is signed by a person occupying a responsible official position. The Court expressly disapproved of the earlier approach in "Navjot Sandhu" which had permitted parties to prove electronic records through oral evidence or other secondary material, and it held that such a route would defeat the very object of the special provision. For digital arrest scams this meant that a victim could no longer walk into court with only a CD or a pen drive of a threatening call and expect it to be admitted without certification, and that investigative agencies had to start planning for electronic proof at the time of registration itself.

The Court also drew a useful distinction between admissibility and proof, noting that unless the record is first admitted in accordance with statutory conditions, the question of the court attaching weight to it does not even arise. This distinction has been carried forward conceptually in the "Bharatiya Sakshya Adhiniyam, 2023", whose "Section 62" treats electronic records as documents and whose "Section 63" provides for the conditions of admissibility similar to the old "Section 65B". When read with "Arjun Panditrao", the decision ensures that unverified screenshots, doctored video calls allegedly showing a police officer, or edited chats in which the scammer pretends to be from a central agency will not form the sole basis of conviction, pushing police to secure original logs from platforms, telecom networks and payment companies. It makes the criminal process more reliable and prevents wrongful conviction on the basis of unreliable digital material, while still allowing genuinely captured threat calls to be proved when proper certificates are obtained. Arrest scams are therefore confronted with a stronger evidentiary gate, and investigators are supplied with a clear roadmap for satisfying it.

Arnesh Kumar v. State of Bihar

In the case of "*Arnesh Kumar v. State of Bihar*[19], the Supreme Court noticed that arrests were being made in a routine fashion for offences punishable up to seven years, particularly in matrimonial disputes under "Section 498A" and related provisions, and that such arrests were often unnecessary and oppressive. The Court pointed out that "Section 41(1)(b) of the Code of Criminal Procedure, 1973" required the police officer to be satisfied that arrest was necessary for one of the listed purposes, such as preventing further offence or ensuring proper investigation, and that "Section 41A" required issuance of notice of appearance in place of arrest in appropriate cases. The Court directed State governments to instruct their police forces to strictly follow these provisions, to prepare a checklist that records the reasons for arrest, and to forward those reasons to the Magistrate. Magistrates in turn were reminded that they should not authorise detention casually and must examine the reasons produced by the police. The Court even warned of departmental and contempt proceedings for non-compliance.

This ruling is of direct use in the digital arrest context because scam callers tell victims that arrest is automatic, that the crime is cognisable and non-bailable, and that once the video call is cut, the police team arrives. "Arnesh Kumar" demonstrates that for a large class of offences, including cheating and even some categories of extortion, arrest is not automatic, reasons must be recorded, and courts supervise the process. "Section 35 of the Bharatiya Nagarik Suraksha Sanhita, 2023" now folds these principles into a single provision, making it even clearer that the power to arrest must be exercised sparingly and with written justification. Therefore, when a scammer invokes the name of a police station or a central agency and threatens immediate custody, that threat is already in tension with both the judicially declared law and the statutory arrest code. This mismatch can be explained to victims, used in awareness material, and pleaded in prosecutions to show that the accused intended to put the victim in fear of accusation for the purpose of extracting money, which corresponds neatly to "Section 308(6) and (7) of the BNS".

D.K. Basu v. State of West Bengal

In the case of "*D.K. Basu v. State of West Bengal*[20], the Supreme Court took suo motu notice of custodial deaths and ill treatment in police stations and prisons and decided to lay down binding guidelines to prevent such abuse. The Court started from Article 21 and from the recognition that personal liberty cannot be curtailed except by a fair, just and reasonable procedure. It then listed a set of requirements to be followed in every arrest and detention: officers must bear clear identification, an arrest memo must be prepared and attested, a friend or relative must be informed, the arrestee must be examined medically at entry and every 48 hours, and all such details must be entered in a register. The Court further directed that the arrested person must be produced before the nearest Magistrate within 24 hours, and it held that failure to comply would attract not only departmental action but also contempt of court. These safeguards were adopted across India and later found reflection in legislation.

Digital arrest scams replicate the language of lawful custody but ignore each of these mandatory conditions. The caller dissuades the victim from speaking to relatives, prevents recording of the call, often uses a foreign number or spoofed local number without identification, and threatens immediate detention without medical examination or production before a Magistrate. When law enforcement and prosecutors frame such conduct as criminal, they can legitimately argue that it is not just cheating by personation under "Section 66D IT Act" but an aggravated form of extortion that trades on fear of accusation under "Section 308(7) BNS". The doctrinal structure from "D.K. Basu" also gives courts a reference point to judge the credibility of the scammer's narrative, since any account of arrest that does not include memo, intimation and production is prima facie not a genuine exercise of police power. This link between custody safeguards and cyber extortion has become stronger after the BNSS restated arrest, search and production rules in one code, and it can now be activated alongside telecom and IT rules to demand quick traceability from platforms whose services were misused.

Loopholes and Friction Points

Despite the scale of national reporting infrastructure, arrest scams succeed because they intersect four regimes that do not always move at the same speed, namely criminal law in the BNS and BNSS, cyber and intermediary regulation under the IT Act and IT Rules 2021, telecom controls under the "Telecommunications Act, 2023", and financial sector anti-fraud systems linked to CFCFRMS and RBI directions. The scammer exploits latency at every

[19] (2014) 8 SCC 273.
[20] (1997) 1 SCC 416.

junction. The call is routed through a spoofed or illegally obtained number so that telecom verification takes time, the payment is split across wallets and banks so that freeze requests must go to more than one entity, and the complainant is made to stay on call so that the golden hour for reporting is lost. Where States have fast 1930 pickup and well-staffed cyber cells, these tricks fail more often, which shows that the law on books is not the chief weakness. The weakness lies in uneven operationalisation and in non-uniform charging, which allows some cases to be booked as simple personation under the IT Act and others to be escalated as aggravated extortion. Arrest scams, being highly scripted and centrally managed, are tailored to those seams.

Personation-plus-extortion Splits

A recurring friction point is the over-reliance on "Section 66D of the Information Technology Act, 2000" for cheating by personation using a computer resource, without simultaneously framing the complaint under "Section 308(6) or 308(7) of the Bharatiya Nyaya Sanhita, 2023" which deals with extortion by putting a person in fear of accusation of a serious offence. Arrest scams do not aim merely to impersonate law enforcement. Their core act is to induce payment by threatening to register an FIR for offences that carry heavy penalties such as narcotics, pornography, money laundering or terrorism. That is precisely the mischief that sub-sections (6) and (7) of "Section 308 BNS" identify and punish more severely than ordinary cheating. When the FIR is drafted only under the IT Act, the maximum punishment is lower, inter-State investigation support may be slower, and bail may be easier, which in turn reduces deterrence. A harmonised charging practice that treats the digital impersonation as the means and the extortion as the object would close this particular window that scammers are exploiting.

Cross-border Telecom Vectors

Telecom controls have become smarter, and obvious VoIP spoofing is now harder to sustain at the gateway, so gangs have shifted to SIM boxes, domestic mule SIMs and identities that were acquired with poor KYC. The "Telecommunications Act, 2023" now criminalises unauthorised telecom equipment, telecom identifier tampering and false identification, which gives police and DoT field units clearer hooks for prosecution. Yet arrest scams often operate from outside India or work with foreign-hosted applications, which means the originating endpoint is not directly subject to Indian telecom controls. The mules and SIM boxes located in India therefore become crucial evidence, and they must be linked fast to the call in question. That link is often delayed because State police need to approach telecom service providers through formal channels, and not every circle responds with the same speed. A scammer who knows this can push the victim through the payment process before the SIM box is spotted. Cross-border cooperation under MLAT channels is still too slow to match the pace of these scams.

Recovery and Redress Gaps

The success of the CFCFRMS model depends heavily on correct and immediate routing. Arrest scams, however, frequently involve a victim in one State, a mule account in another, an e-wallet headquartered elsewhere, and sometimes an international off-ramp. If the NCRP record does not capture the exact bank identifier that matches the mule account, the system may route the complaint back to the State of the victim, which then has to re-route it, losing precious minutes. Bank cooperation is also non-uniform. Large scheduled banks have 24x7 nodal desks familiar with CFCFRMS freezes, but smaller or cooperative banks may not act fast, despite RBI directions. When the freeze does not happen within the golden hour the money is layered into vouchers, prepaid instruments or crypto rails, and criminal procedure under the BNSS becomes slower because it must now follow the money across companies and jurisdictions. This is a classic friction point that keeps arrest scams profitable.

Evidence at Scale

Arrest scams are often mass operations, and investigators need to obtain, certify and present large volumes of electronic evidence across multiple platforms, banks and telecom service providers. The legal framework is present in the "Bharatiya Sakshya Adhiniyam, 2023" and CERT-In directions that demand six-hour reporting for specified incidents, yet compliance across all layers of the private sector is still uneven. Smaller platforms may not store detailed logs for long, or may not have a ready format for issuing "Section 63 BSA" certificates. Telecom operators sometimes need reminders before they furnish call detail records. State police units do not always have automated tools to merge these records into a single timeline for trial. Every such delay can be exploited by the defence to claim that the chain of custody was broken or that the data was not obtained from the original source. Arrest scams thrive on such technical breaks in proof, so evidence-at-scale remains a real pressure point.

Platform Duty of Care

Arrest scams use mainstream messaging apps, social media platforms and video-conferencing tools to project credibility by sending forged IDs or deepfaked videos of officers. The "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" already speak of reasonable efforts to prevent impersonation and to act on complaints, and the "Digital Personal Data Protection Act, 2023" expects data fiduciaries to maintain security safeguards and prevent misuse. Yet live takedowns during an ongoing coercion call are still rare, because platforms prefer to act on court orders or emails from nodal officers, and not every State cyber cell is equipped to send such authenticated notices instantly. A clearer duty of care would make it explicit that a verified law-enforcement notice about an ongoing arrest scam is enough to trigger immediate suspension or warning, after which the platform may seek confirmation. That would remove the few hours of visibility that scammers currently enjoy.

Comparative Snapshots

The switch from IPC and CrPC to "Bharatiya Nyaya Sanhita, 2023" and "Bharatiya Nagarik Suraksha Sanhita, 2023" matters for arrest scams because it closes interpretative gaps on extortion, collects arrest powers in one place and updates illustrations to cover electronic communications. Where earlier provisions had to be stretched to cover video calls or app chats, the new provisions speak directly of electronic messages. Where arrest rules were spread

across several sections, they now sit in "Section 35 BNSS". This makes it simpler for a police officer handling a 1930 complaint to draft an FIR and to justify or defer arrest. It also allows national-level SOPs to quote a single provision for arrest control, improving uniformity.

IPC/CrPC vs BNS/BNSS

The earlier regime treated extortion by fear of accusation as a distinct but somewhat rarely used offence under old "Section 389 IPC", kept cheating and personation elsewhere, and distributed arrest standards across "Sections 41, 41A, 56, 57 and 167 of the CrPC". The new regime centres arrest-related discretion in "Section 35 BNSS", expands extortion in "Section 308 BNS" to cover threats made through electronic communications, and speaks in an idiom closer to current cybercrime practice. This does two things for arrest scams. It foregrounds the real wrong, which is not the use of a fake identity card or a fake email from a central agency, but the attempt to force payment by invoking the terror of a non-bailable offence. And it supplies a single statutory checkpoint to tell the public that genuine arrests will be recorded, justified and reviewed.

Aspect	IPC/CrPC position	BNS/BNSS position	Specific impact on digital arrest scams
Extortion through fear of accusation	"Section 389 IPC" covered threats to accuse of serious offences but did not mention electronic delivery	"Section 308(6)-(7) BNS" expressly covers threats made through electronic messages and video calls to accuse of offences punishable with death or life imprisonment	Arrest-scam scripts that use WhatsApp or video to threaten NDPS, PMLA or sexual crime can now be charged squarely as aggravated extortion
Arrest without warrant for offences up to 7 years	"Section 41(1)(b) CrPC" with "Section 41A CrPC" required reasons and notice of appearance	"Section 35 BNSS" consolidates grounds, mandates written reasons and, in some cases, prior approval	Scam callers claiming instant arrest stand contradicted by a single consolidated statutory rule that citizens can be educated about
Production and oversight	"Sections 56, 57, 167 CrPC" widely spread	BNSS Chapter on arrest and custody groups production, detention and remand	Any claim that police can keep a person in online custody without memo or production is more easily proved false in awareness and prosecution material

Table 4: Key transitions from IPC/CrPC to BNS/BNSS impacting cyber-extortion and arrests

The table makes visible that the change is not cosmetic. By importing electronic delivery into the aggravated extortion offence, the BNS adjusted for the exact technological vector that arrest scammers use. By gathering arrest and production rules, the BNSS made it easier for police, helpline operators and citizens to know what a lawful arrest looks like. This alignment between criminal code and operational architecture is what allows I4C, banks and telecom providers to write concordant SOPs. It also supplies a firmer ground for asking platforms to honour takedown requests that quote BNS and BNSS provisions, which are clearer than their predecessors.

Sectoral Levers

Telecom and digital sector levers have moved from advisory and licence-condition territory to clear statutory footing after the "Telecommunications Act, 2023". Earlier, DoT and TRAI could issue directions about spoofing, KYC and headers, but scammers could shift to OTT apps and foreign VoIP. Now identity, caller ID integrity, unauthorised network equipment and fraudulent acquisition of telecom resources are statutory offences, which means a cyber police station can pair a BNS extortion charge with a telecom offence when the same number is used for repeated arrest threats. This pairing gives prosecuting agencies leverage over SIM-box operators and retail SIM sellers who allowed their outlets to become a supply line for scammers. It also complements public tools such as Sanchar Saathi and Chakshu, because user reports can now lead not only to disconnection but to criminal prosecution.

Regulatory and Policy Proposals

A mature response to arrest scams in the digital era would blend doctrinal clarity, telecom enforcement, platform accountability, CERT-In aligned data flows, sharper redress and targeted public messaging. The building blocks are available across sectors, but they must be synchronised in time. BNS and BNSS give the offence and procedure, IT Act and IT Rules 2021 give intermediary obligations, the "Telecommunications Act, 2023" gives number-level control, the DPDP Act, 2023 gives a data-protection framing to platform behaviour, CERT-In directions give a six-hour reporting spine, and I4C's NCRP with CFCFRMS gives the financial freezing engine. The proposals below seek to push these elements into a single, time-bound workflow so that when a person reports an arrest threat and a transfer to 1930, the system does not depend on any single officer's memory or discretion to trigger the right legal consequences.

Charging Guidance and Sops

Charging guidance at national level should say clearly that digital impersonation of a police or central agency officer for the purpose of extracting money is presumed to be an attempt at extortion by putting a person in fear of accusation of a serious offence and therefore must be registered under "Section 308(6) or 308(7) of the BNS", with "Section 66C" and "Section 66D of the IT Act" added for identity misuse and personation through computer resources, and with "Section 63 of the BSA" formats attached for all electronic material. This single template will produce uniformity in FIRs across States, make

it easier for NCRP tickets to be understood by distant police stations, and give prosecutors a stronger basis to seek custody or oppose bail in large coordinated scams. It will also encourage banks and platforms to prioritise such cases, since the attached sections will signal gravity.

Telecom Enforcement Upgrades

Telecom upgrades should scale the Chakshu reporting channel into a law-enforcement grade triage line that can mark numbers connected to arrest scams as high priority, trigger immediate re-verification of their KYC, and require service providers to preserve detailed call and signalling data for at least 180 days for those numbers. Persistent SIM-box detection using pattern analytics and linking of suspicious IMEIs or CPEs to case numbers would further narrow the window that organised gangs currently enjoy. Retail SIM sales must also be tightened by demanding real-time Aadhaar or equivalent authentication and by penalising outlets that activate large batches which later show up in scam calls. A licence condition or regulation could oblige all access service providers to honour 1930 or CFCFRMS flagged numbers inside fifteen minutes.

Platform Accountability

Platform accountability must be stated in time metrics, not just in broad due-diligence language. A rule under the IT Act or a binding advisory under the IT Rules 2021 can require that when a verified cybercrime unit or I4C sends a digitally signed notice that an ongoing session is being used to threaten arrest or circulate forged police documents, the platform must within a short window suspend the session, warn the recipient, or put a visible risk label on the account. This action would later be subject to review so that free speech is not chilled, but the initial action would save victims from continuing coercion. Platforms should also participate in a secure bad-actor sharing arrangement so that identifiers used in one arrest scam cannot be used on another service. The DPDP Act's requirement of reasonable security safeguards offers the normative base for such an arrangement.

CERT-In Alignment

CERT-In already requires reporting of specified cyber incidents inside six hours and requires entities to maintain logs for at least 180 days. This can be extended by executive direction or sectoral circular to say that whenever a 1930 or NCRP complaint relates to digital arrest extortion, banks, telecom service providers and major platforms must open a joint traceback case on a secure portal within the same six-hour window and upload their respective logs, call records, IP details, KYC and transaction data. Once all entities work on the same ticket, State police will receive complete, certified electronic evidence, which will then comfortably satisfy "Section 63 BSA" and the standards in "Anvar" and "Arjun Panditrao". This will remove the present need for multiple, uncoordinated letters and will shorten investigations.

Redress Optimisations

Redress should move from State-by-State routing to bank-centric routing. Since digital arrest scams often use mule accounts in a different State, the 1930 interface should identify the bank and branch first, create a CFCFRMS ticket mapped to that bank's nodal officer, and only then inform the State where the victim resides. National dashboards should be published, perhaps monthly, showing for each major bank how many freeze requests were received, how many were actioned within sixty minutes, what quantum of money was saved, and how many cases were converted into FIRs under BNS. Public visibility of these numbers will incentivise faster cooperation and will help MHA and RBI to spot lagging entities. It will also be a data source for researchers tracking the effectiveness of the anti-scam architecture.

Public-facing Safeguards

Public-facing safeguards must stress that police, ED, CBI, NCB and courts do not collect money over video or chat, that "Section 35 BNSS" makes arrest a recorded, reviewable act, and that any claim of instant custodial pick-up is inconsistent with the law. Sanchar Saathi can be advertised as the first line for checking suspicious numbers and reporting them. Apps that are widely used by senior citizens or by people in high-risk income brackets can be nudged to display caller ID warnings for self-described government or police calls. Regional-language campaigns can describe in plain terms how to call 1930, what to tell the operator, and how to preserve screenshots. A better-informed public will report faster, help the CFCFRMS to freeze more accounts, and push the economics of arrest scams in the wrong direction for offenders.

Conclusion

The consolidated statutory framework enacted since late-2023 materially strengthens India's ability to counter "digital arrest" rackets, provided the system treats personation as the *means* and aggravated extortion as the *end*. BNS Section 308 supplies a graded palette for extortion, including threats of accusation of serious offences that these scams weaponize; read with BNS cheating/personation and forged-document counts, it gives police a high-sentence, multi-count charge that justifies urgent data requests and custodial interrogation of organised actors.[21] Equally decisive are BNSS arrest guardrails-now consolidated in Section 35-which codify the duty to record reasons, prefer notices of appearance in many cases, and subject custody to judicial oversight; these rules undercut the scammers' core lie that arrest can be done on a video call or avoided by paying money.[22] On the cyber side, the IT Act's personation offence (Section 66D) and identity-misuse (Section 66C), together with the CERT-In Directions of 28 April 2022 (six-hour

[21] The Bharatiya Nyaya Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/20062/1/a2023-45.pdf (last visited on November 2, 2025).

[22] The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on November 1, 2025).

reporting; 180-day domestic logs), create a legal basis for rapid platform takedown and forensics that can stitch together multi-platform evidence.[23] The Telecommunications Act, 2023 adds teeth: Section 42's prohibitions on tampering and fraudulent acquisition of identifiers support SIM-box seizures, KYC clean-ups, and action against spoofing, while DoT's International Incoming Spoofed Calls Prevention System and the Sanchar Saathi/Chakshu reporting rail have already cut volumes of spoofed international calls, forcing adversaries into narrower vectors.[24] Banking redress is no longer an afterthought: RBI's July 6, 2017 circular on limiting customer liability and the RBI Integrated Ombudsman Scheme, 2021 together make coerced digital transfers contestable and refundable if reported promptly, with 1930/NCRP and CFCFRMS providing the "golden-hour" freeze machinery.[25]

Yet strengths in doctrine reveal weaknesses in choreography. First, charging practice is uneven: FIRs often stop at IT Act Section 66D, under-using BNS Section 308(6)–(7), which better expresses the scam's coercive core and enhances deterrence. Second, latency persists at telecom and platform layers; while Section 42 and Chakshu enable identifier action, inter-circle responses and cross-border app liaison can still outlast the victim's payment window, and gangs have shifted to SIM-boxes and domestic mules when international spoofed calls are filtered.[26] Third, redress routing remains state-centric at moments when bank-centric routing would be faster; reporting errors or misclassification at 1930 can squander the first 60 minutes that CFCFRMS needs to freeze funds effectively.[27] Fourth, evidentiary scale is a grind: without disciplined CERT-In-timed preservation and Bharatiya Sakshya Adhiniyam (BSA) Section 63 certification, call/video/chat logs risk exclusion under the Supreme Court's *Anvar* and *Arjun Panditrao* line, even when facts are compelling.[28] Finally, prevention depends on upstream data hygiene: DPDP Act obligations to notify breaches to the Board and affected data principals must be operationalised so that credible personal details stop seeding scam scripts; otherwise, awareness alone cannot counter realism in the social-engineering pretext.[29] The net assessment, therefore, is balanced: India's codes, rules and sectoral rails are fit for purpose, but their power is realised only when criminal law, CERT-In, telecom controls, platform due diligence, and bank freezes run on a single, time-boxed playbook.

Suggestions

Framed in continuity with the study's analysis of arrest scams in the digital era, the following proposals translate doctrine into operations.

1. Adopt a national "charging template" that presumes aggravated extortion. Police stations and cyber cells should default to BNS Section 308(6)/(7) with cheating/personation counts, adding IT Act Sections 66C and 66D where devices and apps were instrumental. Station-house software (CCTNS) should embed a pre-filled template that auto-lists these sections and prompts attachment of BSA Section 63 certificate requests. State DGPs may issue standing orders to avoid "66D-only" FIRs, with periodic audits of charge mix.

2. Put all actors on the CERT-In clock. Mandate that upon a 1930/NCRP tag "digital arrest", banks, TSPs, and major platforms open a joint case within 6 hours on a secure portal and upload CDRs, IP logs, KYC, and transaction trails (retained for 180 days). CERT-In can host this "fusion ticket" and time-stamp each upload to preserve chain of custody. Non-compliance should be escalated to sectoral regulators (RBI/DoT/MeitY) for penalties.[30]

3. Switch to bank-centric freezing by default. Reconfigure CFCFRMS so the first router is the beneficiary bank/PSP, not the caller's location; build auto-directory lookups of nodal officers and require 60-minute acknowledgments. Publish monthly dashboards: freeze requests received, acted within 60 minutes, rupees saved, BNS-charged FIRs per bank. This transparency will surface laggards and tighten cooperation.[31]

4. Telecom "high-risk identifier" regime. Scale Chakshu into a LEA-grade triage: upon three or more verified "digital arrest" flags, trigger immediate KYC re-verification, SIM-box sweeps, and 180-day expanded signalling retention against the number/IMEI. Couple this with Section 42 prosecutions for tampering and fraudulent acquisition of identifiers to deter retail KYC abuse.[32]

5. Platform duty-of-care with timed interventions. Under IT Rules, require platforms to act within short windows on digitally-signed notices from verified cyber nodes when a *live* session is coercing payment under the guise of arrest-minimum actions: suspend session, display risk

[23] Section 66D Punishment for Cheating by Personation by Using Computer Resource, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=80 (last visited on October 31, 2025).
[24] The Telecommunications Act, 2023, *available at:* https://egazette.gov.in/WriteReadData/2023/250880.pdf (last visited on October 30, 2025).
[25] Prakash Baliarsingh, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions", *available at:* https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited on October 29, 2025).
[26] Mahesh Buddi, "Amid DoT Crackdown on Int'l Calls, Foreign Cyber Crime Gangs Turn to SIM Boxes to Dupe Indians", *available at:* https://timesofindia.indiatimes.com/city/hyderabad/amid-dot-crackdown-on-intl-calls-foreign-cyber-crime-gangs-turn-to-sim-boxes-to-dupe-indians/articleshow/123954842.cms (last visited on October 28, 2025).
[27] Madhu Rasala, "National Helpline, Local Roadblock: How 1930 Cyber Fraud Hotline Misses the Mark During 'Golden Hour'", *available at:* https://timesofindia.indiatimes.com/city/vijayawada/national-helpline-local-roadblock-how-1930-cyber-fraud-hotline-misses-the-mark-during-golden-hour/articleshow/121383875.cms (last visited on October 27, 2025).
[28] The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on October 26, 2025).
[29] The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 25, 2025).
[30] Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe and Trusted Internet, *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 24, 2025).
[31] National Cybercrime Reporting Portal (NCRP), *available at:* https://i4c.mha.gov.in/ncrp.aspx (last visited on November 2, 2025).
[32] Chakshu – Report Suspected Fraud and Unsolicited Commercial Communication, *available at:* https://www.sancharsaathi.gov.in/sfc (last visited on November 1, 2025).

label, warn recipient, preserve data. Follow-up review can restore accounts if mis-flagged, preserving speech while halting ongoing extortion. Maintain 180-day log preservation to support BSA-compliant proof.

6. Golden-hour evidence kit and BSA compliance. Issue a national kit: how to mirror victim devices, secure full-fidelity call/video/chat artefacts, and obtain Section 63 certificates from platforms, TSPs, and banks; generate a single timeline file per case. Training should reference *Anvar* and *Arjun Panditrao* to explain why uncertified screenshots fail at trial. Integrate auto-reminders in case software for missing certificates.

7. DPDP breach-to-fraud pipeline. Compel data fiduciaries (telecom, courier, banking, e-commerce) to push breach notifications not only to the Board and affected users but also-through a privacy-preserving alert-to CERT-In/I4C so that likely targets receive contextual warnings in-app/SMS about arrest-style pretexts. Prioritise designating large communication and payment platforms as Significant Data Fiduciaries to ensure DPO accountability and DPIAs that include impersonation-misuse scenarios. This reduces the supply of "true facts" that scammers exploit.

8. Exploit the anti-spoofing gains-then chase displacement. DoT's international spoofed-call filters have cut volumes sharply; now target displacement into SIM-boxes by mandating automated pattern analytics, IMEI/device blacklists, and rapid, templated LEA requests across circles. Require TSPs to label *all* foreign-origin calls clearly at the device level and to auto-throttle numbers linked to verified arrest-extortion reports pending KYC re-check. Publicise busts to deter retail SIM abuse.[33]

9. Victim-first, multi-track redress SOP. At the first contact: file 1930/NCRP with full identifiers; notify own bank for provisional credit under RBI's 2017 circular; lodge an FIR citing BNS 308(6)/(7), IT Act 66D, and Telecom Act Section 42; and, if bank response is deficient after 30 days, escalate to RBI-IOS. Police help desks should be trained to walk victims through all tracks simultaneously. Provide standard templates in 10 Indian languages.

10. Targeted public messaging anchored in the arrest code. Mass campaigns should drill three points: lawful arrest follows BNSS Section 35 safeguards; no government agency collects money over chat/video; and suspected fraud calls/SMS/WhatsApp must be reported via Sanchar Saathi/Chakshu and 1930 immediately. Use app banners and telco flash-SMS in regional languages during scam spikes, linking to a one-page "what to tell 1930" checklist.

Bibliography

Books:

- Karnika Seth, Computers, *Internet and New Technology Laws* (LexisNexis, Gurgaon, 1st edn., 2016).
- Pavan Duggal, *Textbook on Cyber Law* (LexisNexis, New Delhi, 1st edn., 2016).
- Prashant Mali, *Cyber Law & Cyber Crimes* (Snow White Publications, Mumbai, 1st edn., 2015).
- Rohas Nagpal, *Introduction to Indian Cyber Law* (Asian School of Cyber Laws, Pune, 1st edn., 2008).
- Talat Fatima, *Cyber Crimes* (Eastern Book Company, Lucknow, 1st edn., 2016).
- Vakul Sharma, *Information Technology: Law and Practice* (Universal Law Publishing, New Delhi, 1st edn., 2011).

Statutes:

- The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023)
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
- The Information Technology Act, 2000 (Act No. 21 of 2000)
- The Reserve Bank of India (Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions) Circular, 2017
- The Reserve Bank of India Integrated Ombudsman Scheme, 2021
- The Telecommunications Act, 2023 (Act No. 44 of 2023)

Articles:

[33] Department of Telecom (DoT) Acts Pro-Actively to Protect Citizens from Cyber Frauds through Spoofed Calls, *available at:* https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2087644 (last visited on October 31, 2025).

- Ananth Padmanabhan, "Give Me My Space and Take Down His: A Closer Look at Intermediary Liability", 9 *Indian Journal of Law and Technology* 64 (2013).
- Bhavyakirti Singh, Aditya Bamb, "The Dichotomy of the 65B Certificate: Analysing Trends with Regard to the Authentication of Electronic Evidence in India", 10 *Christ University Law Journal* 85 (2021).
- Chinmayi Arun, "Gatekeeper Liability and Article 19(1)(a): Shreya Singhal v. Union of India", 7 *NUJS Law Review* 73 (2014).
- Debanshu Mukherjee, Karan Gulati, "Evaluating the Need for Sectoral Insolvency Frameworks in India: The Telecom Sector as a Case Study", 9 *NLS Business Law Review* 73 (2023).
- Farasat Ahmed, "Recasting the Intermediary: Online Gatekeeping and Safe Harbour in India", 1 *Indian Law Review* 92 (2017).
- Indranath Gupta, Lakshmi Srinivasan, "Evolving Scope of Intermediary Liability in India", 1 *International Review of Law, Computers & Technology* 58 (2023).
- Nandan Kamath, "Should the Law Beat a Retweet? - Intermediary Liability in India", 9 *Indian Journal of Law and Technology* 58 (2013).
- Sarthak Chaturvedi, "India's 2022 CERT-In Directions-A Case of 'Unconstitutional Delegated Legislation'?", 13 *International Data Privacy Law* 58 (2023).

Websites:

- Chakshu - Report Suspected Fraud and Unsolicited Commercial Communication, *available at:* https://www.sancharsaathi.gov.in/sfc (last visited on November 1, 2025).
- Department of Telecom (DoT) Acts Pro-Actively to Protect Citizens from Cyber Frauds through Spoofed Calls, *available at:* https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2087644 (last visited on October 31, 2025).
- Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe and Trusted Internet, *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 24, 2025).
- Madhu Rasala, "National Helpline, Local Roadblock: How 1930 Cyber Fraud Hotline Misses the Mark During 'Golden Hour'", *available at:* https://timesofindia.indiatimes.com/city/vijayawada/national-helpline-local-roadblock-how-1930-cyber-fraud-hotline-misses-the-mark-during-golden-hour/articleshow/121383875.cms (last visited on October 27, 2025).
- Mahesh Buddi, "Amid DoT Crackdown on Int' l Calls, Foreign Cyber Crime Gangs Turn to SIM Boxes to Dupe Indians", *available at:* https://timesofindia.indiatimes.com/city/hyderabad/amid-dot-crackdown-on-intl-calls-foreign-cyber-crime-gangs-turn-to-sim-boxes-to-dupe-indians/articleshow/123954842.cms (last visited on October 28, 2025).
- National Cybercrime Reporting Portal (NCRP), *available at:* https://i4c.mha.gov.in/ncrp.aspx (last visited on November 2, 2025).
- Prakash Baliarsingh, "Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions", *available at:* https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited on October 29, 2025).
- Section 66D Punishment for Cheating by Personation by Using Computer Resource, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=80 (last visited on October 31, 2025).
- The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on November 1, 2025).
- The Bharatiya Nyaya Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/20062/1/a2023-45.pdf (last visited on November 2, 2025).
- The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on October 26, 2025).
- The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 25, 2025).
- The Telecommunications Act, 2023, *available at:* https://egazette.gov.in/WriteReadData/2023/250880.pdf (last visited on October 30, 2025).