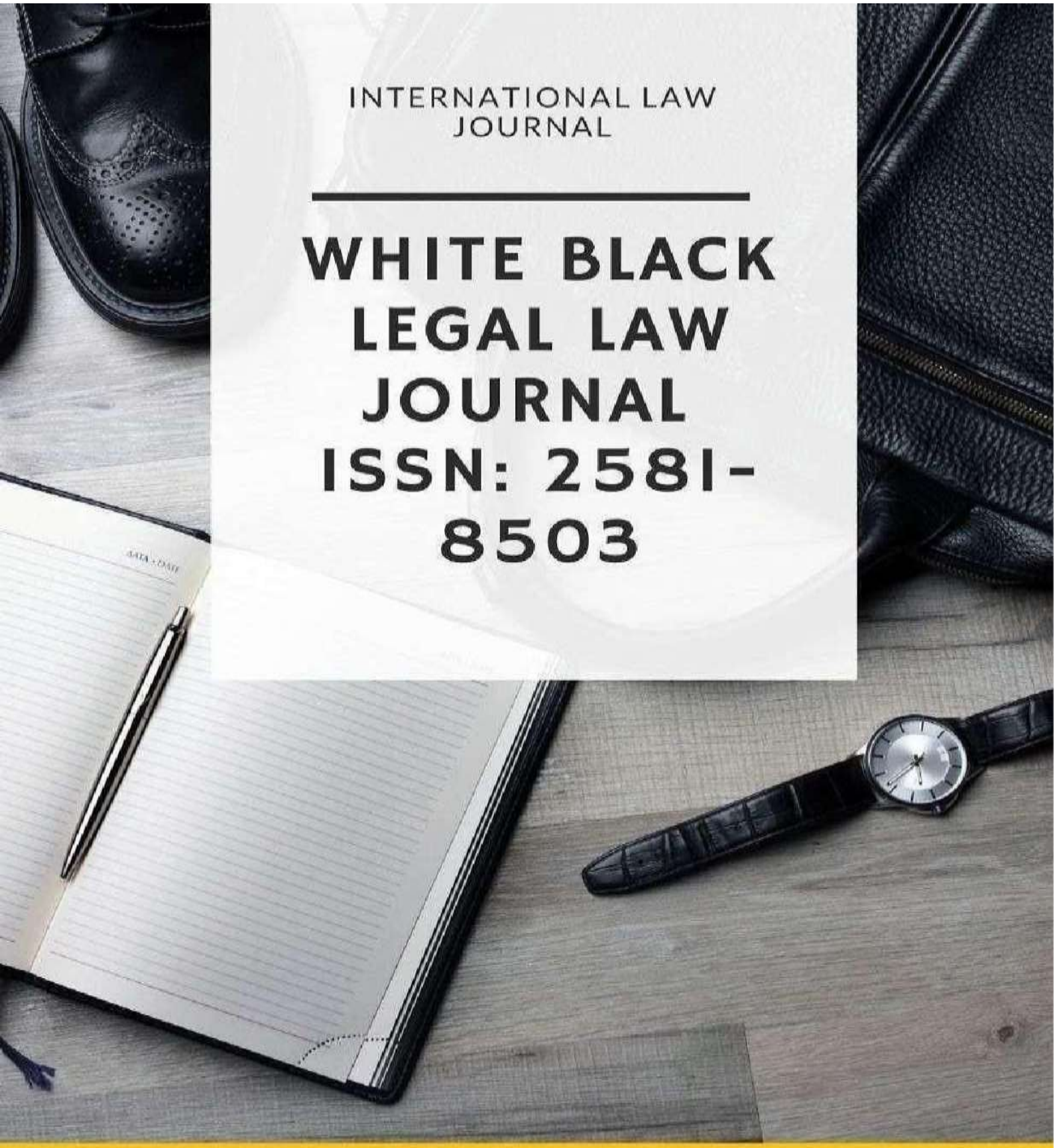

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 6 | April 2026 ISSN: 2581-8503

STANDARD OPERATING PROCEDURE OR STRUCTURAL REFORM? THE SUPREME COURT AND THE GOVERNANCE OF DIGITAL ARREST SCAMS IN INDIA

AUTHORED BY - ANISHA KAR
PhD Scholar, KIIT School of Law

Abstract

The recent involvement of the Supreme Court of India (SC) in cases about "digital arrest" scams has drawn new attention to the scale of impersonation-based cyber extortion in India. These scams rely on the fake representation of police and judicial authority through digital platforms. They have caused significant financial losses and serious emotional distress to victims. In response, the Supreme Court has instructed the Union Government to create a Standard Operating Procedure (SOP) to tackle this issue. This paper contends that establishing an SOP cannot adequately address what is fundamentally a failure in cyber governance. It argues that digital arrest scams are not just gaps in enforcement; they reflect the divided regulatory authority among banks, telecom companies, digital platforms, and law enforcement agencies. By placing the Supreme Court intervention in the larger context of debates about regulatory capacity and the judicial role in governance, the paper argues that relying on SOPs risks resulting in symbolic action rather than meaningful reform. Effective prevention, it claims, requires a fundamental change in how responsibility and accountability are structured within India's cybercrime regulatory framework.

Keywords: Cyber Governance, Digital Arrest Scams, Intermediary Liability, Judicial Intervention, Regulatory Fragmentation, Standard Operating Procedures (SOP)

Introduction

The issue known as "digital arrest" is a form of cyber fraud where criminals impersonate law enforcement or court officials to extract money from victims. Unlike standard online scams, these operations depend on prolonged psychological control, fake legal authority, and real-time digital monitoring, which often force victims into isolation and compliance for long periods[1].

[1] Siddharth Ugra, *Digital Arrests: Rhetoric vs. Remedy*, 61(5) *Econ. & Pol. Wkly.* 45 (2026).

The growing number and scale of these incidents have revealed weak points in India's digital and financial systems. Recent remarks from the Supreme Court reflected serious concern over these scams, describing them as organised robbery[2]. The Supreme Court has called on the Union Government to develop a SOP to confront this crisis. While this action indicates institutional urgency, it also raises important questions about how effective the response can be. While procedural coordination is necessary, it may fall short without clear accountability across the institutions involved in allowing or failing to prevent these crimes. This paper argues that digital arrest scams highlight deeper structural problems in India's cyber governance system. These include divided regulations, conflicting incentives within financial entities, and poor accountability for intermediaries. Therefore, the SC's intervention is not just a legal reaction to cybercrime; it is also a glimpse into the wider governance challenges posed by digital risk in India.

Research Questions

1. Does the Supreme Court's directive to create a SOP effectively tackle the root causes of digital arrest scams?
2. Do these scams indicate a failure in enforcement, or do they reflect deeper structural problems in India's cyber governance framework?
3. How does the divided regulation among banking, telecom, platform governance, and law enforcement help maintain the problem of digital arrest scams?
4. What are the limits of judicial action in dealing with complex failures in digital governance?

Research Objectives

1. To analyse digital arrest scams as a failure of governance and institutions rather than solely a criminal issue.
2. To critically evaluate the effectiveness and limitations of responses to cybercrime based on SOPs.
3. To investigate how institutional design and accountability impact the management of cyber fraud.
4. To look into how increased judicial involvement may affect cyber governance.

[2] Supreme Court of India, *Bail Proceedings on Impersonation* (Nov. 2025).

Research Methodology

This paper uses a qualitative, analytical approach based on doctrinal and policy analysis. It looks at the SC's remarks and proceedings related to digital arrest scams and examines the laws governing cybercrime, banking regulation, telecom oversight, and intermediary liability. It also analyses secondary sources like regulatory reports, policy documents, and publicly available data on trends in cyber fraud to understand institutional responses better. In particular, it relies on materials issued by the Reserve Bank of India (RBI)[3] and the Department of Telecommunications (DoT)[4]. The study takes a governance-focused approach to assess how suitable procedural reforms are and to pinpoint structural weaknesses in India's cyber regulatory system.

The Anatomy of Digital Arrest Scams: Beyond Opportunistic Crime

Digital arrest scams are sophisticated forms of cyber fraud, distinct from others, not only by the absence of any physical transfer of money, but also by the precise nature of the kind of psychological and emotional manipulation used to extract money from victims, and the sheer institutional exploitation behind the scam. These scams involve random calls through WhatsApp using police in the caller ID, Skype links reflecting the Central Bureau of Investigation (CBI) logo, Telegram links in the name of messages that appear to be from the Enforcement Directorate (ED). Victims of the digital arrest scam are told that they have been accused of committing offences under the laws dealing with the Prevention of Money Laundering Act (PMLA) or violations of the Narcotic Drugs and Psychotropic Substances Act (NDPS) or the hawala, and asked to pay fines in cryptocurrencies. Fraudsters circulate fake warrants, attachment orders under Section 83, seizure notices, sentencing letters, fake emails and forged Supreme Court orders[5].

The "digital arrest" usually lasts between 24 to 72 hours, during which the victim must keep video calls open, isolate themselves hermetically, give their phones to the extortionists, and send money to "safe custody" accounts. The money is then often routed through multiple mule wallets to obscure tracking. This is not random opportunism; it is structured impersonation enabled by gaps in digital infrastructure[6].

[3] Reserve Bank of India, *Cyber Fraud Policy Analysis* (2025).
[4] Dep't of Telecomms., *Annual Telecom Fraud Report* (2024).
[5] Indian Cybercrime Coordination Ctr., *Cyber Fraud Trends 2025* (2025).
[6] Reserve Bank of India, *Bank Fraud Monitoring Report* (2024).

The scammer will present as a "deputy superintendent" of police and also involve a "director general", in an attempt to make the scam seem more convincing. Most victims of the scam are aged between 45 and 70 and are professionals or retirees, worried about damage to their reputation or potential prosecution. Psychological pressure, like the immediate threat of arrest, seizure of goods, or criminal prosecution, leads to compliance. The emotional shock experienced by the victims often compounds the financial loss. In 2024, over 1.2 lakh complaints of vishing/voice phishing or phishing through phone calls were recorded with estimated losses of Rs.1,935 crore (I4C 2024). Projections for 2025 have pegged the figure at over Rs.20,000 crore (I4C 2025).

Victim Case Studies: Human Cost

High-net-worth individuals, business communities in smaller towns, and individuals from low-tech backgrounds are not the only victims. The elderly have also been targeted, for example, the 86-year-old Mumbai widow who lost Rs.20.1 crore over 45 days in March 2025[7].

Digital arrest scams are akin to psychological warfare. A 48-year-old neurologist was put through a 48-hour "video trial" by a fraudster posing as "Judge Dhananjay" (WhatsApp profile photo resembling CJI Chandrachud) before being coerced into transferring Rs.15 lakh for imaginary PMLA violations[8]. An 84-year-old textile magnate lost Rs.2 crore after getting similar "seizure orders" from an individual impersonating the same judge[9]. A retired brigadier was "sentenced" to 7 years, forced to isolate for 72 hours while transferring Rs, 8 lakh to 'safe custody' [10].

I4C data indicate 230 million portal accesses between January 2020 and November 2025, 184 thousand FIRs, more than 20 thousand arrests, 12 lakh suspicious SIMs cancelled, 3 lakh IMEIs blocked[11]. Yet only 2 percent of complaints were resolved within 24 hours[12]. The RBI's nationwide re-KYC drive from July to October 2025 highlighted mechanical rejections that left out rural users. This oversight unintentionally allowed mule networks to thrive, which managed 70% of suspicious transfers without being checked[13]. These instances show serious weaknesses

[7] *Mumbai Widow Loses Rs 20 Crore to Digital Arrest Scam*, Times of India, Mar. 17, 2025.
[8] *Neurologist Loses Rs 15 Lakh to Fake Judge Dhananjaya*, Times of India, Oct. 20, 2025.
[9] *Mumbai Widow Loses Rs 20 Crore to Digital Arrest Scam*, Times of India, Mar. 17, 2025.
[10] *Retired Brigadier Loses Rs 8 Lakh in Digital Arrest*, Hindustan Times, Dec. 12, 2025.
[11] Press Info. Bureau, *I4C Crosses 230 Million Portal Accesses* (Nov. 19, 2025).
[12] Indian Cybercrime Coordination Ctr., *Cyber Fraud Trends 2025* (2025)
[13] Reserve Bank of India, *Bank Fraud Monitoring Report* (2024)

in the system, including VoIP spoofing from Cambodia and Myanmar, AI-generated deepfakes, and failures in KYC that let trillions of rupees flagged by the RBI move freely[14].

Supreme Court Interventions: From Suo Motu to SOP Directive—A Timeline of Judicial Frustration

The Supreme Court intervention started in November 2025, during bail proceedings in a case involving impersonation-based extortion, where the Supreme Court described the fabrication of judicial orders as a direct assault on judicial authority, which is even more perilous than the crime[15].

A suo motu writ gives CBI pan-India powers on 1 December 2025, freezes 30 minutes of AI-transactions, issues red alerts from INTERPOL against foreign syndicate hubs in Cambodia and Myanmar and directs RBI-DoT to clean mule accounts. The Supreme Court, headed by Justice Surya Kant, expressed grave concern over the scale of digital fraud loss, which was stated to be over Rs.50,000 crores, and viewed such cybercrime at the systemic level as akin to robbery, and directed the Union government to formulate inter-agency SOPs in consultation with the RBI, banks, and telecom regulators[16].

By February 2026, the scale of reported losses had intensified institutional concern regarding systemic cyber governance failures. The Ministry of Home Affairs (MHA)'s status report on the daily theft-of-data led by phones, drones, and clone, prompted urgent inter-ministerial coordination efforts of the Ministry of Electronics and Information Technology (MeitY), the Department of Technology (DoT), and private platform operators. RBI's latest weapon, a 15-minute hold on all bank debits following a text alert of that ominous beep, and the DoTs' suspension of 100-million bulk SIMs made it into the new SOP alongside MeitY's weekly "deepsix" of 5 offending platforms, the Centre's decision to sanction a CBI probe into the last 10,000 gigabyte Gujarat/Delhi First Information Reports (FIRs) of cell & cybercrime are some of the steps taken recently. The Supreme Court urged compensation protocols with "pragmatic liberality": the fund would be moneyed by the thieves. Yet, the rhetoric far outstrips the remedy, as these revised SOPs largely replicate earlier 2024 procedural measures with minimal

[14] Id.
[15] Supreme Court of India, *Bail Proceedings on Impersonation* (Nov. 2025)
[16] Supreme Court of India, *Suo Motu Writ on Digital Arrests* (Dec. 1, 2025).

structural innovation[17]. Post such "resilient" policing between 2019-26, cell-fuelled crime cases shot up by 104 percent, the loot by 21 times[18]. These increasing directives indicate more than judicial activism; they are functional substitutes for deficient systems. The courts increasingly seem to be shouldering a dispute-regulating responsibility that the executive could not discharge. Legally, all this falls within the court's prerogative under Articles 32 and 142 of the Constitution. However, the clean-up also seems like an institutional statement of distrust in administrative coordination rather than one of the confidence reposed in regulatory architecture.

The Supreme Court hearing on 8th February of 2026 brought out the core of the crisis: CJI Surya Kant described the Rs.54,000 crore syphoned as "absolute robbery or dacoity"[19]. The bench ordered MHA-RBI-DoT stakeholder SOP in 4 weeks, sanctioned CBI investigations in Gujarat/Delhi's more than 20,000 cyber FIRs, and added AI-monitoring based interconnectivity led real-time account heists-prevention. RBI activated 15-minute debit locks after SMS notifications; DoT blocked 100 million bulk connections; MeitY assured 5 weekly repeat protocol ban of identified 5 spurious domains[20]. However, the Court noted that complicity among bank staff was entrenched and recommended cost recovery measures, timely freezing of bank accounts upon receiving a caution alert, as well as victim indemnification under a "pragmatic liberality" approach. INTERPOL Red Corner Notices covered the 15 Cambodia/Myanmar centres pinned down on December 1 suo motu PIL[21].

Why SOP-Based Governance Fails in Fragmented Regulatory Structures

SOPs are meant to streamline coordination within an existing administrative set-up by clarifying reporting channels, standardising response times and creating frameworks for inter-agency communication[22]. In fairly consolidated regulatory regimes, such instruments may lead to improved efficiency. However, digital arrest scams exist in what institutional theorists would call a fragmented regulatory architecture, where there are many centres of authority without a

[17] Id
[18] Nat'l Crime Recs. Bureau, *Crime in India 2025* (2026).

[19] Supreme Court of India, *Suo Motu Writ on Digital Arrests* (Dec. 2025); *SC Slams "Robbery" in Digital Arrest Case*, Indian Express, Feb. 9, 2026.
[20] *SC Directs SOP for Digital Arrests; CJI Calls it "Dacoity"*, NDTV, Feb. 8, 2026
[21] Id
[22] Girish Gulati & S. Sridhar, *Standard Operating Procedures in Indian Administration*, 80 *Pub. Admin. Rev.* 456 (2020).

clear hierarchy or locus of accountability[23].

In the Indian digital ecosystem, banks are regulated by the RBI (2025), telecom infrastructure is regulated by the DoT (2024), online intermediaries operate under Section 79 of the Information Technology Act, 2000 (IT Act), and criminal enforcement is carried out by multiple state police forces coordinated through the I4C[24]. Each of these actors are governed by different statutory mandates, budgetary lines and incentive structures.

While SOPs may be able to align their actions to a certain extent, they cannot realign structural incentives or reallocate blameworthiness[25]. This difference is important because while SOP-based reforms operate within existing structures of legal authority, structural reforms rightly place blame on these existing authority structures instead.

For example, a SOP may require banks to freeze suspect transactions within a certain time period, but does not change the underlying threshold for negligence for failure to do so[26]. It may mandate repeated telecom verification drives, but does not make telecom providers bear the costs of failed SIM card verification which results in fraud[27]. It may direct platforms to take down impersonation content when notice is issued, but safe harbour will continue to operate until an amendment is made to Section 79 of the IT Act to increase their duty of care[28].

Therefore, the failure of SOP-based responses is not merely in botched or imperfect implementation, SOP-based responses fundamentally assume that the failure of co-ordination is the problem. What we often see instead is that the disaggregated nature of responsibility and blameworthiness means that they tend to travel as liability is avoided by one actor after another—banks blame telecom failures, telecom blames platform misuse, platforms blame user conduct, and enforcement agencies blame lack of co-ordination and resources[29].

The central problem is not lack of information or delayed reporting. It is structural and until

[23] Eugene Bardach, *Getting Agencies to Work Together: The Practice and Theory of Interorganizational Management* (Brookings Inst. 1998).
[24] Id
[25] Id
[26] Id
[27] Id
[28] Information Technology Act, No. 21 of 2000, § 79 (India); Ministry of Elecs. & Info. Tech., *IT Rules 2025 Draft Notification* (2024).
[29] Id

liability is redistributed, hierarchy of reporting is made clear and authority is vested in a central authority for enforcement, SOPs are likely to continue being administrative responses to long-term regulatory weaknesses.

Intermediary Liability: The Section 79 Bottleneck

A central illustration of this structural diffusion of responsibility lies in the safe harbour regime under Section 79 of the IT Act, 2000. Section 79 provides "safe harbour" immunity to intermediaries (social media platforms, Internet Service Providers [ISPs], and e-commerce platforms) from liability for third-party content, data, or links hosted by them[30].

This statutory immunity operates at a higher threshold than the proactive due-diligence obligations imposed under the European Union's Digital Services Act[31]. *Shreya Singhal v. Union of India* (2015) made takedowns effective only on court/police orders, rendering the already overwhelmed, understaffed cyber cells virtually non-functional[32]. WhatsApp/Meta enable 70 percent of initial scam contact points; while Telegram harbours the largest instances of fake warrant distribution[33]. The proposed IT Rules 2025 amendment (to be tabled in Parliament) require the appointment of 24/7 Grievance Officers and for Level 1 takedowns to occur within 24hrs, however, these amendments are toothless as they do not prescribe graduated penalties or victim compensation levies[34]. The National Cyber Coordination Centre (NCCC), which deals with metadata flows, works in tandem with CERT-In's mandate on incident response operations. The similar domains of operations may cause friction in jurisdictional issues[35].

Internationally, results have been likewise mixed. The introduction of the 2023 Scam-watch SOPs in Australia was associated with a 13 percent increase in fraud[36]. Alerts issued by the US Federal Trade Commission (FTC) reduce low-skill phishing by 8% but are not effective against higher skilled attackers[37]. Indian statistics for January to March 2025 were 17,718 SOPs with

[30] Information Technology Act, No. 21 of 2000, § 79 (India).
[31] European Comm'n, *Digital Services Act Package* (2022).
[32] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).
[33] Id
[34] Ministry of Elecs. & Info. Tech., *IT Rules 2025 Draft Notification* (2024)
[35] Ministry of Home Affairs, *I4C Annual Report* (2025).
[36] Australian Competition & Consumer Commission, *Scamwatch Annual Report* (2024)
[37] Federal Trade Commission, *Consumer Fraud and Phishing Trends Report* (2025).

Rs.210 crore in losses[38]. But concerns persist that SOPs are performative not structural. Weak Know Your Customer (KYC) compliance allows mule networks to operate through different accounts, many of which are undetected. Telecom service providers continue issuing large quantities of SIM cards that are then used for illegal activities. Digital service providers often prioritize engagement metrics and lag behind in fraud detection. In this context, the MHA draft seems to consolidate existing measures without determining a clear supervisory authority.

Structural Failures Exposed: Regulatory Anarchy Fueling Digital Arrests

Fragmentation dominates as different sectors in India are regulated by separate authorities: banking under the RBI (Payment and Settlement Systems Act, 2007), telecom under the DoT (Telecom Regulatory Authority of India Act, 1997), and digital platforms under the intermediary liability framework of the IT Act. Policing powers are divided between the 36 states but are generally coordinated through the I4C for responding to cybercrime. Requests to identify the source of fraudulent digital transactions carried out via I4C take an average of just under six months, and many cross-border requisitions to the United States come "untraceable" after procedural timeframes have lapsed[39].

Fragmentation is further worsened by compliance failures within the financial and telecommunications industries. A large percent of mule transactions at banks involve collusion by insiders, and KYC rules are frequently flouted. Bank frauds worth trillions of rupees have been flagged by the RBI by late 2024[40]. In telecommunications, despite the mandatory re-verification exercise conducted in 2022 which reduced the number of fake connections, e-SIM mis-utilisation, routing through inappropriately monitored gateways and cross-border exploitation are inadequately monitored and used extensively for easing 'hawala' style transactions bypassing the Interconnect Clearing House (ICH)/International Clearing Centres (ICCs)/international gateways, posing a structural vulnerability[41].

Meta and WhatsApp reportedly account for a substantial majority of initial scam contact points. Unlike the obligations under the European Union's (EU) Digital Services Act, which are of an ex-ante, proactive take-down and reporting nature, India's immunity under Section 79 does not

[38] *Id*
[39] Indian Cybercrime Coordination Ctr., *Cyber Fraud Trends 2025* (2025).
[40] Reserve Bank of India, *Bank Fraud Monitoring Report* (2024).
[41] Dep't of Telecomms., *Annual Telecom Fraud Report* (2024).

carry such obligations unless actual knowledge is proven[42]. Other issues which weaken the immunity regime of India for internet intermediaries are: (i) cyber cells suffer from low human resources and (ii) inter-state data sharing is fragmented with national bodies.

Though banking and telecom reporting cycles and SIM verification thresholds are formal rules, they are inconsistently enforced as industries prioritize revenue over consumer protection measures. The Indian government estimates that approximately Rs.500 crore (USD 60 million) was invested in cyber and human intelligence infrastructure for I4C[43]. Additionally, from 2020 to the first quarter of 2025, reported losses from cyber frauds have increased. Further, India has one of the highest share in global banking cybercrimes and has few institutional mechanisms for liability partitioning [44].

It is not simply a matter of more resources and human power to absorb the machinery that is already in place, but also of rethinking responsibility in the Information and Communications Technology (ICT) ecosystem. This is not merely a question of execution or whining competitive benchmarking with global cyber powers, but also a question of institutional design. SOPs may improve coordination, but they cannot, by themselves, correct structural diffusion of accountability.

Global Lessons: Why Unified Regulators Trump Procedural Patches

Singapore's Cyber Security Agency (CSA) restructured its post-2023 scams response process, creating a single coordinating agency for banks and telcos, and increasing total response-related financial penalties[45]. The United Kingdom's National Cyber Security Centre (NCSC) improved inter-agency coordination by requiring businesses to disclose breaches, leading to a 47 percent drop-off in scams between 2022 and 2025[46]. In Australia, the eSafety Commissioner focuses on platform liability; and in the United States, the FTC received about 5.2 billion dollars from interagency actions against scam networks in 2024[47].

By contrast, India's National Cyber Resilience Agency (NCRA), which will address the issues

[42] European Comm'n, *Digital Services Act Package* (2022).
[43] Ministry of Home Affairs, *I4C Annual Report* (2025).
[44] Cyber Sec. Agency of Sing., *Post-Scam Restructuring Framework* (2024)
[45] Id
[46] Federal Trade Commission, *Consumer Fraud Report* (2024).
[47] Ministry of Elecs. & Info. Tech., *IT Rules 2025 Draft Notification* (2024).

of synergies and overlapping jurisdictions between bodies, is still not operationalised. Amending the IT Act is also under discussion, but pending. With some IT Act provisions merged into the 2024 Digital Personal Data Protection Act (DPDP Act), it also does not address scam liability architecture[48]. The Supreme Court can catalyse reform: through Public Interest Litigation (PIL), it can direct the government to establish an NCRA at the MHA with centralized account freezing capacity, artificial-intimacy tracing technology, and a designated intermediary levy for victim compensation. From experience in reforming Singapore's gaming industry, centralized oversight would prove effective[49]. Without this organisational change, crude estimates suggest liability exposure could double in India by 2027[50]. The comparative lesson is not that unified regulators eliminate fraud, but that consolidation clarifies accountability that something procedural harmonisation alone cannot achieve.

One such model that has been proposed is establishing a statutory National Cyber Regulatory Authority (NCRA), a new autonomous body that subsumes the RBI's existing fraud cell, incorporates vigilance departments of the DoTs, and has control over various digital platforms and their operations.

Additionally, the authority could secure powers to live-tracking (with a warrant), force banks to accept higher negligence damages (up to five times victim losses), impose pre-emptive compliance obligations on platforms (inspired by the European Union), and regulate AI systems and the SIM issuance process; it could raise revenue through a small levy on digital transactions. The body could be headed by a Chief Executive Officer (CEO) under the Prime Minister's Office and managed by a nine-member independent board, including judicial and state representatives. A proposed structure, based on the legislative model for the Securities and Exchange Board of India (SEBI) established in 1992, may provide a bipartisan model[51].

Judicial Limits and Opportunities in Cyber Governance

The Supreme Court of India has historically employed varying degrees of judicial intervention to address administrative failures. Under its powers under Articles 32 and 142, it has assigned the CBI to investigate the allocation of coal blocks, the Commonwealth Games scam and other

[48] Id
[49] PwC India, *India Cyber Liability Forecast* (2026).
[50] Securities and Exchange Board of India Act, 1992 (India).
[51] Supreme Court of India, *Coal Block Allocation Case Proceedings* (2014).

matters (Supreme Court of India 2014). Recently again, when faced with a flood of PILs, the Supreme Court has introduced interim procedural directives to stem the "waterfall of PILs" (e.g., "digital arrests" relating to complaints of cyber fraud)[52].While well-intentioned, these attempts may risk overstepping. Most of the systemic reforms mandated by the Constitution's Parts III (Fundamental Rights) and IV (Directive Principles of State Policy) are to be performed by the Union and state executives. While the investigation of cybercrime relies on the police powers of the States under List II, the regulation of telecommunications and digital infrastructure falls under the Union List. This creates overlapping constitutional responsibilities[53]. The 2G spectrum case (*Centre for Public Interest Litigation v. Union of India*, 2012) illustrates this[54]. The 2G spectrum judgment demonstrated that judicially imposed corrective mechanisms can generate immediate fiscal recovery but do not, by themselves, reconfigure regulatory design. It gave rise to expectations, and without reform of telecommunication policies, we only auctioned for more resources. The rot structurally remained. On India's new cyber-frontier, WhatsApp "digital arrests" scams targeting Unified Payments Interface (UPI) and Aadhaar-linked Digital India caused common losses of Rs 2000 crores in 2024[55]. PILs now flood the SC, demanding instant fixes. The judiciary's SOPs such as real-time police verification for high-value transactions offer quick relief but risk becoming crutches, absolving the executive of its duty under Article 21 (right to life and privacy) and the IT Act, 2000.

Federalism's Federal Headache in the Cyber Age

High federalism isn't just political rhetoric. Article 246 constitutionalises federalism. Cybercrimes are often interstate (interstate phishing rings, dark web syndicates), but only poorly resourced state police enforce cyber laws with little federal assistance. Nevertheless, India's progress remains slow, with only some provisions of the Digital Personal Data Protection Act, 2023 in force and the Digital India Act yet to come into force. Where there are elaborate standard operating procedures issued by the court, there may be an incursion by the judiciary into the policy domain of the executive, a phenomenon that the Supreme Court itself has been apprehensive about in the context of fiscal federalism (Supreme Court of India 2020). Environmental PILs (M.C. Mehta orders for Ganga pollution) and moral crusades (liquor

[52] Supreme Court of India, *Suo Motu Writ on Digital Arrests* (Dec. 2025).
[53] Nat'l Crime Recs. Bureau, *Crime in India 2025* (2026).
[54] *Centre for Pub. Interest Litig. v. Union of India*, (2012) 3 S.C.C. 1 (India).
[55] Indian Cybercrime Coordination Ctr., *National Cybercrime Report* (2024).

prohibition) are traceable to a PIL's competence to promote public interest. Cybercrimes need tech solutions: AI-based fraud detection, blockchain for UPI trails, a National Cyber Coordination Centre with teeth. Courts issuing ad-hoc SOPs may provide temporary disruption but cannot substitute for comprehensive legislative reform.

Conclusion: From Procedural Containment or Structural Reform

Digital arrest scams are not isolated episodes of cyber fraud, they reveal the incoherence of regulatory design when power is distributed with diffusion of responsibility. The Supreme Court's direction to develop a SOP is recognition of institutional urgency, and signals judicial cognizance of systemic risk. But, as this paper has demonstrated, process coordination is not a substitute for structural reform.

The problem is not whether a SOP can enhance efficiency, it is whether tools like SOPs can shift the balance of responsibility between banks, telcos, over-the-top service providers, and law enforcement agencies. Coordination in an uncoordinated regulatory environment functions at a horizontal level, while structural reform seeks to concentrate power vertically. Unless there is a reallocation of statutory duties with re-emphasis on intermediary liability, regression of regulatory fragmentation with re-centralisation of federal oversight, and establishment of a dedicated central agency with clear legislative authority to oversee and execute digital payment fraud investigation protocols, there will be no consolidation of responsibility.

Direction under Articles 32 and 142 of the Constitution of India is a useful starting point for judicially-mandated reforms, but courts are not best placed to set holistic techno-regulatory design right through continuing mandamus. What is required for effective long-term governance of cybercrime is unequivocal parliamentary legislation and robust executive enforcement, not ongoing monitoring by judges.

The answer to the problem of digital arrest scams is not a choice between inaction and new SOPs, it is a choice between procedural mitigation and structural rebuilding. This wave of cybercrime has exposed the "price" of coordination paradigms. The frequency, duration, and productivity of the Supreme Court's directions in the matter will reflect India's appetite for systemic change.

References

1. Australian Competition & Consumer Commission, *Scamwatch Annual Report* (2024).
2. Eugene Bardach, *Getting Agencies to Work Together: The Practice and Theory of Interorganizational Management* (Brookings Inst. 1998).
3. Cyber Sec. Agency of Sing., *Post-Scam Restructuring Framework* (2024).
4. Dep't of Telecomms., *Annual Telecom Fraud Report* (2024).
5. European Comm'n, *Digital Services Act Package* (2022).
6. Girish Gulati & S. Sridhar, *Standard Operating Procedures in Indian Administration*, 80 *Pub. Admin. Rev.* 456 (2020).
7. *Retired Brigadier Loses Rs 8 Lakh in Digital Arrest*, Hindustan Times, Dec. 12, 2025.
8. Indian Cybercrime Coordination Ctr., *National Cybercrime Report* (2024).
9. Indian Cybercrime Coordination Ctr., *Cyber Fraud Trends 2025* (2025).
10. *SC Slams "Robbery" in Digital Arrest Case*, Indian Express, Feb. 9, 2026.
11. Information Technology Act, No. 21 of 2000, India Code (2000).
12. Maharashtra Police, *Cybercrime Statistics Maharashtra* (2025).
13. Ministry of Elecs. & Info. Tech., *IT Rules 2025 Draft Notification* (2024).
14. Ministry of Home Affairs, *I4C Annual Report* (2025).
15. Nat'l Crime Recs. Bureau, *Crime in India 2025* (2026).
16. *SC Directs SOP for Digital Arrests; CJI Calls it "Dacoity"*, NDTV, Feb. 8, 2026.
17. Press Info. Bureau, *I4C Crosses 230 Million Portal Accesses* (Nov. 19, 2025).
18. PwC India, *India Cyber Liability Forecast* (2026).
19. Reserve Bank of India, *Bank Fraud Monitoring Report* (2024).
20. Reserve Bank of India, *Cyber Fraud Policy Analysis* (2025).
21. *Centre for Pub. Interest Litig. v. Union of India*, (2012) 3 S.C.C. 1 (India).
22. *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).
23. Supreme Court of India, *Bail Proceedings on Impersonation* (Nov. 2025).
24. Supreme Court of India, *Suo Motu Writ on Digital Arrests* (Dec. 2025).
25. *Mumbai Widow Loses Rs 20 Crore to Digital Arrest Scam*, Times of India, Mar. 17, 2025.
26. *Neurologist Loses Rs 15 Lakh to Fake Judge Dhananjaya*, Times of India, Oct. 20, 2025.
27. Siddharth Ugra, *Digital Arrests: Rhetoric vs. Remedy*, 61(5) *Econ. & Pol. Wkly.* 45 (2026).