INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL ARREST SCAMS AND THE LEGAL VACUUM CHALLENGES FOR CRIMINAL JUSTICE IN THE DIGITAL AGE

AUTHORED BY - VENKATESAN. D

B. S. Abdur Rahman Crescent Institute Of Science And Technology, Vandalur, Tamil Nadu

Abstract:

Digital arrest scams impersonating police, CBI, ED and RBI officials extorting money from victims threatening to arrest them is increasingly becoming a challenge for criminal justice system in India. This study analyzes response to a survey of 55 respondents comprising advocates, law students and the public to assess their knowledge, perceived sufficiency of the law, challenges in its enforcement and preventive measures. The results show that there is high levels of awareness and almost universal recognition of the seriousness of the scams, but a striking lack of consistency as to whether existing criminal laws are sufficient. A significant number of respondents, including legal professionals, were either unaware of or uncertain about any specific legal provision dealing directly with digital arrest scams, highlighting a perceived legal void. The key challenges to enforcement identified included the cross-border nature of cybercrime, lack of technical resources and expertise, difficulty in identifying offenders and tracking digital and financial transactions. Stronger cybercrime laws, public awareness programs and faster freezing and retrieval of fraudulent funds were among the preferred measures. Victims were mainly considered vulnerable because of impersonation of government officials, fear of legal action and low awareness of cybercrime. And the scams seem to be widespread with a lot of respondents saying they either received suspicious calls themselves from fake government agencies or know someone who did. The study found high public awareness but a perceived fragmented and insufficient legal and institutional response. It recommends dedicated legislation on digital arrest fraud, enhanced inter-agency and international cooperation, capacity building for law enforcement and sustained awareness campaigns.

Keywords: digital arrest scams, cybercrime, legal vacuum, criminal justice, impersonation fraud, law enforcement, India.

ISSN: 2582-6433

Introduction:

The “digital arrest” scam is one of the scariest scams of the digital age. Crime isn’t what it used to be. In these scams, con artists pose as police, Central Bureau of Investigation (CBI), Enforcement Directorate (ED), Reserve Bank of India (RBI) or other government agencies. They call, video call or message the victims. They accuse the victim of serious crimes such as terrorism, drug trafficking or money laundering and then put them under “digital arrest”, a sort of forced psychological detention that can only be carried out online. Large sums of money must be remitted immediately or those who have been wronged will be threatened with arrest, prosecution and public shame[1]. This is generally in the name of verification, fines or settlement of legal proceedings. The issue with these scams is that the scammers use images of state power (uniforms, backgrounds that look like they are from the government, fake documents, legalese) to scare people and make them act without thinking.

In the past few years, there has been an alarming rise in digital arrest scams in India. The Indian Cyber Crime Coordination Center (I4C) and different state police forces have received thousands of complaints and lost hundreds of crores of rupees. The people who fall for these sophisticated scams are not just uneducated or elderly; they include professionals, retired officials, doctors, teachers, and even people who have studied law. Scammers use fake phone numbers, VPNs, and cryptocurrency channels to avoid being caught. Most of the time, the scammers are based in Southeast Asian countries. This international aspect makes it harder to investigate and bring charges because Indian police have to deal with tricky issues of jurisdiction, treaties for mutual legal assistance, and the slow workings of international cooperation[2].

From a legal point of view, the digital arrest scam makes me very worried about how well India's current criminal law system works. The Indian Penal Code (now Bharatiya Nyaya Sanhita), the Information Technology Act, 2000, and the new Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam are the main laws that are used in these situations. Although cheating, impersonation, forgery, and some other cybercrimes are against the law, there isn't a law that specifically and fully addresses the issue of digital arrest. To build a case, prosecutors have to put together different parts, like cheating by personation, criminal intimidation, forgery, and identity theft[3]. This often leads to legal ambiguity, inconsistent charging practices, and convictions that aren't as strong. There is what is called a "legal

[1] (S. James Robert, 2026)
[2] (E. Singhal, 2026)

ISSN: 2582-6433

vacuum" between the changing nature of crime and the fixed categories of the law when there isn't a specific law that covers it.

There are big problems with criminal justice because of this lack of laws. It changes how FIRs are filed, how charges are made, whether digital evidence is allowed, whether bail is granted, and how sentences are handed down[4]. It also makes it harder for police to do their jobs because they have to deal with issues of jurisdiction, finding criminals who are operating from other countries, and following digital and financial transactions that happen on many platforms and across borders. Also, not having a clear set of laws makes it harder to stop people from doing bad things and makes it hard for courts, prosecutors, and investigating officers to know what to do[5].

As a result, this study looks at how the public and professionals think about digital arrest scams and whether the current legal and institutional response is enough. In particular, it wants to find out: (i) how aware different groups of people are of digital arrest scams; (ii) how serious people think they are; and (iii) whether people think current criminal laws are enough to punish offenders. (iv) find out if India has a law specifically against digital arrest scams; (v) find out what the biggest problems are for law enforcement when they try to investigate these cases; (vi) figure out the best ways to stop these scams from happening; and (vii) figure out why people are likely to believe digital arrest scammers. The study gives a wide range of viewpoints on a current and important legal issue by collecting the opinions of lawyers, law students, and regular people[6].

The study's results should add to the ongoing conversation about legal reform in the digital age by giving real-world examples that can help shape policy suggestions, changes to the law, and strategies for law enforcement. This study shows how important it is to fill in the gaps in India's laws and give the criminal justice system the tools it needs to deal with digital arrest scams, a crime that takes advantage of people's trust in the government and their fear of the law. To stop this, we need strong laws, good technology, coordinated efforts between law enforcement agencies, and ongoing public education.

Literature Review

Indian legal scholars, judicial institutions, and policymakers are paying more and more attention to digital arrest scams. However, the literature is still fragmented between doctrinal

[4] (B.B. Meshram, 2025)
[5] (Shree, 2026)
[6] (K. L. Karikalan, 2026)

ISSN: 2582-6433

analysis, institutional reports, and empirical studies. This review brings together what we already know about four main topics: the lack of laws and inadequate doctrines; the vulnerability of victims[7]; the difficulties faced by law enforcement; and the responses from institutions, focusing on the Indian situation. One important finding from the Indian literature is that there isn't a specific law for digital arrest scams. The National Institute of Communication Finance (NICF) says that neither the Bharatiya Nyaya Sanhita, 2023, nor the Information Technology Act, 2000, specifically define "digital arrest" as a crime. This lack of specific laws makes it harder to get convictions. Instead, prosecutions have to rely on a patchwork of laws, including Section 66D of the IT Act for cheating by personation and the BNS's cheating, forgery, and extortion laws, which don't fully cover how the scam works to force people to do things.

A study of Section 66D's legal meaning says that it is "doctrinally adequate yet institutionally and punitively inadequate" for advanced digital arrest networks. The harshest punishment, three years in prison and a one lakh rupee fine, doesn't differentiate between simple online impersonation and complex, multi-victim operations that cause a lot of financial loss and mental trauma. The study suggests a graduated legal framework that takes into account things that make crimes worse, like pretending to be a public official, using fake media, going after weak victims, and being part of organized crime networks. This fits with the idea that digital arrest scams usually involve "a constellation of interconnected offenses rather than a single statutory violation[8]."

The most important response from an institution has been the Supreme Court's "suo motu" proceedings in Victims of Digital Arrest Related to Forged Documents. The Court is looking into more than just one person's case. It is also looking into systemic problems like mule accounts, temporary debit holds, grievance-redressal pathways, and getting back funds that were stolen. The Court also wants to make banks responsible for compensating victims of fraud that happens because they didn't do their homework. The CJI said, "We are proposing to direct that wherever such fraud occurs, bank will compensate victim and suffer prosecution[9]."

In Indian literature, authority bias is always mentioned as the main psychological trick that scammers use. The NICF report talks about how scammers "almost always appeal to authority: police and security forces; the judicial system and international organizations," taking advantage of people's "natural respect for authority." The report also says that socioeconomic

[7] (Upadhyay, 2025)
[8] (Yalala Rakesh, 2026)
[9] (S. K. Pandey, 2025)

ISSN: 2582-6433

factors affect vulnerability. For example, people from low-income backgrounds can't get cybersecurity training, and older people who aren't very good with technology are more likely to trust online interactions even though they don't know much about it[10].

The Chief Justice of India's comments during the 2026 proceedings showed how frustrated the courts were with this problem. He asked, "What kind of person are you in a democratic country if you think you are getting arrested on mobile?" to which many educated citizens replied in the affirmative. "Hit the cell phone against the wall, and the arrest goes away." The amicus curiae said that victims often do what they are told because they are afraid of being arrested. Psychologists call this a form of hypnosis.

Lokniti-CSDS study of Delhi residents in 2025 found that only 61% were aware of digital arrest as a specific scam. This was much lower than the over 90% who knew about traditional scams like OTP sharing and fake reward calls. This ignorance matters because digital arrest tactics are very sophisticated, and can be very hard to resist. During the Open House Discussion of the NHRC, it was emphasized that most of the victims of the scam are old persons, including retired professionals and government employees. The scams also cost financial resources and affect people's pride, mental health and self-worth[11].

The literature suggests there are a number of structural obstacles to effective investigation. The cross-border nature of the crime is repeatedly emphasized: syndicates operate from "scam compounds" in Southeast Asia, often with some degree of official patronage, and exploit trafficked individuals to commit fraud. The NICF report notes that stolen funds are divided into smaller amounts, funneled through numerous mule accounts, and ultimately transferred offshore, creating "a method of easy layering" that evades law enforcement. The research shows that there is a big capacity gap at the domestic level. Authorities in big cities may have the right tech tools, but "small district-level enforcement agencies are mostly poorly equipped." The prosecution process is slowed down by complicated steps that need to be taken, such as synchronizing between states, forensic screening, and verifying digital evidence[12].

Responses from institutions have been strong but not uniform. Real-time scrubbing technology has been put in place by the Department of Telecommunications at international gateways. This is said to have cut down on traditional network telecom spoofing by 99%. But scammers have changed their strategies by moving 80–85% of their business to unregulated OTT media because traditional telecom channels are now limited. The Indian Cyber Crime Coordination

[10] (Mangoli, 2025)
[11] (Ghodake, 2025)
[12] (Gaur, 2026)

ISSN: 2582-6433

Center has blocked thousands of Skype IDs and WhatsApp accounts that were being used to make digital arrests. However, research shows that these steps only fix the symptoms and not the underlying lack of laws[13].

There are some things that both scholarly and institutional proposals have in common. First, many people think that aggravated digital personation should have its own laws with graduated punishments. Second, a restorative justice framework focused on victims has been pushed for. This framework should use global Authorized Push Payment models and shared-liability frameworks to help get back 90–95% of the money that was lost by holding intermediaries, telecom providers, and banks financially responsible. Third, technological solutions to stop these problems have been suggested. These include automatic "kill-switches" for long unnatural audio and video streams on OTT platforms and AI-powered prediction models trained on digital arrest datasets. Fourth, public awareness campaigns need to be re-evaluated. In the Lokniti study, 72% of people knew that the government was sending calls and messages to raise awareness, but only 16% said that government efforts were "very effective."

Research Gap

The Indian literature that is already out there is mostly made up of institutional perspectives, such as judicial orders, regulatory reports, policy analyzes, and doctrinal legal commentary. There aren't many empirical studies that show how lawyers and regular people feel about the legal framework, the kinds of problems that come up with enforcement, and how well preventative measures work. This study fills in that gap by polling lawyers, law students, and regular people. This gives a multi-stakeholder empirical view of the perceived legal vacuum and the institutional response to digital arrest scams in India. In this way, it adds to the body of legal and policy literature by basing the analysis on the opinions of people who either have to deal with the current legal system or could be hurt by its flaws.

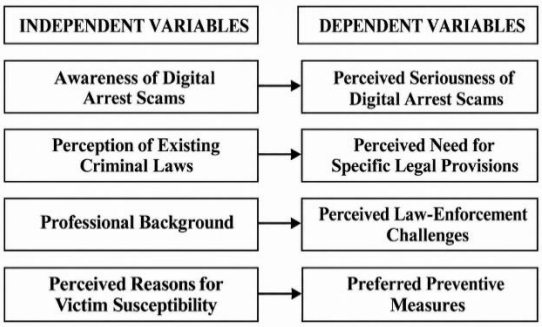
Hypothesis

1. There is a significant relationship between awareness of digital arrest scams and the perceived seriousness of digital arrest scams in India.
2. There is a significant relationship between respondents' perception of the adequacy of existing criminal laws and their belief that specific legal provisions are required to address digital arrest scams.

[13] (G. Sarkar, 2026)

ISSN: 2582-6433

3. There is a significant relationship between the professional background of respondents and their perception of the major challenges faced by law-enforcement agencies in investigating digital arrest scams.
4. There is a significant relationship between respondents' perception of the reasons victims believe digital arrest scammers and their preferred most effective preventive measure, particularly public awareness programmes.



The conceptual framework of the present study illustrates the relationship between the independent and dependent variables concerning digital arrest scams. Four independent variables are considered in the study, namely, awareness of digital arrest scams, perception of existing criminal laws, professional background, and perceived reasons for victim susceptibility. These variables are examined in relation to four corresponding dependent variables: perceived seriousness of digital arrest scams, perceived need for specific legal provisions, perceived law-enforcement challenges, and preferred preventive measures. The framework assumes that variations in respondents' awareness, perceptions, and professional backgrounds may influence their assessment of the seriousness of digital arrest scams, the adequacy of the existing legal framework, the challenges faced by law-enforcement agencies, and the measures considered effective for preventing such offences. The relationships represented in the framework provide the basis for formulating and testing the hypotheses of the study using appropriate statistical methods.

Limitation of the Study:

The present study, while offering useful empirical insights into perceptions of digital arrest scams and the legal vacuum in India, is subject to several limitations. The sample comprises only 55 respondents drawn largely through convenience sampling, with advocates and law students over-represented and the general public under-represented, which limits the generalisability of the findings and introduces self-selection bias. The study captures self-reported perceptions rather than objective measures of legal sufficiency or enforcement

ISSN: 2582-6433

effectiveness, and the absence of key stakeholders such as police officers, prosecutors, bank officials, and actual victims further narrows the perspective. The data was collected over a short period in September 2026 and does not account for regional variations across Indian states or evolving scam patterns. Certain questionnaire items contained overlapping or inconsistently labelled response options, and the dataset included duplicate entries and typographical inconsistencies, raising minor concerns about data integrity. The structured format also precluded qualitative depth, and the study did not examine actual FIRs, charge sheets, conviction rates, or judicial decisions, nor did it capture first-hand victim experiences. Notwithstanding these limitations, the study provides a useful exploratory snapshot of stakeholder perceptions and identifies clear directions for future research, including larger representative surveys, qualitative interviews with victims and enforcement officials, and doctrinal analysis of case outcomes.

Research Objectives:

- To assess the level of awareness about digital arrest scams among different professional groups.
- To evaluate the perceived seriousness of digital arrest scams in India.
- To examine perceptions regarding the sufficiency of existing criminal laws to punish digital arrest scam offenders.
- To determine whether respondents believe India has a specific legal provision directly addressing digital arrest scams.
- To identify the major challenges faced by law enforcement agencies in investigating digital arrest scams.
- To ascertain the most effective measures for preventing digital arrest scams.
- To understand the perceived reasons why victims, believe digital arrest scammers.

Research Questions

Corresponding to the objectives, the study addresses the following research questions:

- What is the level of awareness about digital arrest scams among advocates, law students, and the general public?
- How serious do respondents consider digital arrest scams in India?
- Do respondents consider existing criminal laws sufficient to punish digital arrest scam offenders?

ISSN: 2582-6433

- Do respondents believe India has a specific legal provision directly addressing digital arrest scams?
- What are the major challenges faced by law enforcement agencies in investigating digital arrest scams?
- Which preventive measures do respondents consider most effective?
- Why do respondents think victims are likely to believe digital arrest scammers?

Research Method and Instrument

The study adopted the survey method as the primary research method. A structured questionnaire was designed and administered through Google Forms, a widely accessible online survey platform. The questionnaire was designed to be self-administered, ensuring uniformity in the questions posed to all respondents and facilitating efficient data collection and analysis.

The questionnaire consisted of ten closed-ended and multiple-choice questions, designed to capture:

- Professional background of the respondent (advocate, law student, or general public);
- Awareness of digital arrest scams and the source of first awareness;
- Perceived seriousness of digital arrest scams in India;
- Perceived sufficiency of existing criminal laws to punish offenders;
- Belief regarding the existence of a specific legal provision directly addressing digital arrest scams;
- Perceived major challenges faced by law enforcement agencies;
- Perceived most effective preventive measures;
- Perceived reasons why victims believe digital arrest scammers; and
- Personal or vicarious exposure to suspicious calls claiming to be from police, CBI, ED, RBI, or other government agencies.

The response options for the questions were drawn from the literature and from the range of plausible positions identified in the doctrinal and policy discourse, ensuring that the instrument captured the key dimensions of the research problem.

Population and Sampling

The target population for the study comprised individuals with varying levels of legal knowledge and public awareness, specifically:

ISSN: 2582-6433

- Advocates (legal professionals);
- Law students; and
- General public (non-legal respondents).

The study adopted a non-probability convenience sampling technique. Respondents were approached through the researchers' networks and through the online distribution of the Google Form. A total of 55 responses were received and included in the analysis. While convenience sampling limits the generalizability of the findings, it was considered appropriate for an exploratory study of this nature, given the constraints of time and access, and the absence of a readily available sampling frame of persons aware of or affected by digital arrest scams.

Results and Analysis:

The primary statistical formula used for computing percentages in this descriptive study is:

Percentage (%) = (f/N) x 100

Where:

f = frequency of responses in a particular category

N = total number of valid responses

Respondent Profile:

Professional Background	Frequency (f)	Percentage (%)
Advocate	18	32.7
General Public	29	52.7
Law Student	8	14.5
Total	55	100.0

Table 1: Distribution of Respondents by Professional Background

The sample is dominated by general public respondents (52.7%), followed by advocates (32.7%) and law students (14.5%). This distribution is relevant because it allows comparison between legally trained respondents (advocates and law students, together 47.2%) and lay respondents (52.7%).

Awareness of Digital Arrest Scams

Awareness Level	Advocate (n=18)	General Public (n=29)	Law Student (n=8)	Total (N=55)
Yes, very well	8 (44.4%)	5 (17.2%)	0 (0%)	13 (23.6%)
Yes, to some extent	5 (27.8%)	1 (3.4%)	0 (0%)	6 (10.9%)

ISSN: 2582-6433

Heard the term but not aware of details	5 (27.8%)	20 (69.0%)	0 (0%)	25 (45.5%)
No	0 (0%)	3 (10.3%)	8 (100%)	11 (20.0%)
Total	18 (100%)	29 (100%)	8 (100%)	55 (100%)

Table 2: Awareness Levels by Professional Background

Awareness is highest among advocates; with 44.4% reporting they know digital arrest scams "very well" and only 27.8% having merely heard the term. In contrast, 69.0% of general public respondents had only heard the term without detailed knowledge, and 10.3% had no awareness at all. Notably, all law student respondents (100%) reported no awareness an unexpected finding that may reflect the timing of their legal education or the recency of the scam's prominence. Overall, 45.5% of all respondents had only heard the term without details, indicating a substantial awareness gap.

Social media is the dominant source of first awareness (45.5%), followed by friends and family (18.2%) and police cyber crime awareness programmes (14.5%). Traditional media (television/news) accounts for only 7.3%, suggesting that digital platforms are the primary channel through which the public learns about this cybercrime.

There is near-universal consensus on the seriousness of digital arrest scams: 74.5% rated them "very serious" and 16.4% rated them "serious," together accounting for 90.9% of respondents. Only 9.1% rated them "moderately serious." No respondent rated the scam as "not serious." The variation across professional groups is modest, with advocates (77.8%) and general public (75.9%) slightly more likely than law students (62.5%) to rate the scam as "very serious."

While 36.4% considered existing laws "not sufficient," 25.5% considered them "completely sufficient"—a counterintuitive finding given the documented legal vacuum. A further 5.5% considered them "partially sufficient" and 1.8% "mostly sufficient." Significantly, 30.9% left the question blank or provided no clear response, indicating either uncertainty or reluctance to opine on a technical legal question. The split between "not sufficient" and "completely sufficient" responses suggests that public and professional perceptions do not align neatly with the doctrinal position that no specific provision exists.

Respondents were evenly split, with 36.4% believing India has a specific legal provision and an identical 36.4% believing it does not. A further 5.5% answered "partially," and 21.8% left the question blank. This even split is analytically significant: it demonstrates considerable uncertainty and a lack of clear public and professional consensus on the existence of dedicated legal provisions, reinforcing the study's central premise of a perceived legal vacuum.

ISSN: 2582-6433

The responses are remarkably evenly distributed across the four identified challenges, each attracting approximately one-quarter of respondents. Identifying offenders, lack of technical resources, and cross-border nature each received 14 responses (25.5%), while tracing digital and financial transactions received 13 (23.6%). This even distribution suggests that respondents perceive multiple, equally significant structural impediments rather than a single dominant challenge—a finding consistent with the literature's emphasis on the multi-dimensional nature of enforcement difficulties.

Nearly half of all respondents (49.1%) selected "All of the above," indicating that victims are perceived as vulnerable to a combination of factors rather than any single cause. Among those who selected a specific reason, scammers' impersonation of government officials was the most frequently identified (27.3%), followed by fear of legal action (14.5%) and lack of cyber crime awareness (9.1%). This is consistent with the literature's emphasis on authority bias and the psychological coerciveness of the scam.

Among respondents who answered the question, 32.7% reported that someone known to them had received a suspicious call, and 10.9% reported personally receiving one—together accounting for 43.6% of respondents with direct or vicarious exposure. Only 12.7% reported no exposure, and 1.8% were unsure. The high proportion of blank responses (41.8%) limits the conclusiveness of this finding, but among those who responded, the data suggests that suspicious calls impersonating government agencies are widespread, affecting nearly half of all respondents with direct or indirect experience.

Conclusion

The study concludes that digital arrest scams are perceived as a serious and widespread threat in India, with 90.9% of respondents rating them "very serious" or "serious," and 43.6% of those who responded reporting personal or vicarious exposure to suspicious calls from fake government agencies. Yet this high perception of seriousness coexists with substantial uncertainty and division regarding the legal framework: respondents were evenly split on whether existing laws are sufficient and on whether India has a specific legal provision addressing digital arrest scams, with over one-fifth unable to answer either question. This disjunction between the perceived gravity of the threat and the perceived adequacy of the legal response is the empirical manifestation of the legal vacuum that this study set out to examine.

ISSN: 2582-6433

References

B.B. Meshram, M. K. (2025). From FIR to forensic analysis in the digital age: Legal powers, investigative models, and judicial oversight of cybercrime policing in India. *Journal of Law and Cyber Crime*, 1–11.

E. Singhal, N. T. (2026). Role of telcos and banks in preventing digital arrest scams. *The IUP Journal of Law Review*, 5–18.

G. Sarkar, S. L. (2026). A five-tier framework for understanding cyber-slavery and institutional misclassification: Evidence from 29,466 cases in Southeast Asia. *Crime & Delinquency*.

Gaur, H. (2026). Digital arrest fraud in India: Examining the legal and investigative challenges in combating emerging cyber scams. *International Journal of Social Science Research*, 563–576.

Ghodake, S. (2025). *A data-driven study of consumer vulnerability and behavioral responses to digital arrest scams in India and the role of data analytics in fraud prevention.* International Journal of Electronics and Computer Applications.

K. L. Karikalan, R. S. (2026). Cybercrime investigation in India after the 2023 criminal-law reforms: Integrating criminal liability, digital evidence, forensics and institutional enforcement. *International Journal of Science and Research Trends*.

Mangoli, R. (2025). Digital arrest scams in India: Challenges and solutions with special reference to Karnataka. *Journal of Social Science and Humanities Research*.

S. James Robert, V. S. (2026). *Digital arrest in the cyber age: a psychological perspective on fear, authority, and consciousness.* Frontiers in Psychology Forensic and Legal Psychology.

S. K. Pandey, A. P. (2025). Navigating digital arrest under India's cyber-forensics framework: Complexities, legal gaps, and pathways forward. *Journal of Forensic Justice*, 80–89.

Shree, G. S. (2026). Digital arrest scams in India: Doctrinal analysis of the legal framework, enforcement challenges and regulatory reforms. *Journal of Law and Legal Research Development*, 7–12.

Upadhyay, S. A. (2025). Contours and Webs of Digital Arrest Pandemic. *Journal of Communications Finance*, 44-49.

Yalala Rakesh, C. M. (2026). Evaluating the adequacy of Section 66D of the Information Technology Act, 2000 in prosecuting digital arrest and advanced personation scams. *International Journal of Law Management & Humanities*, 314–326.