Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The Legality and Practicality of Digital Arrest Warrants in India: A Critical Examination

Shivam Singh[a] Dr. Rajeev Kumar Singh[b]

[a]Amity University, Uttar Pradesh, Lucknow Campus, India [b]Assistant Professor, Amity University, Uttar Pradesh, Lucknow Campus, India

Received 17 March 2025; *Accepted* 18 April 2025; *Published* 22 April 2025

India's judiciary and police forces today are rapidly embracing digital technology to speed up their activities. As a result, new cybercrimes like e-arrest have also quickly evolved. The majority of cases involving digital arrest are very complex and hard to detect. Cybercriminals, despite the lack of official recognition, are always posing as police or court officers and using fake digital arrest warrants to deceive and blackmail unsuspecting victims. This paper examines the conditions that give rise to practical challenges, legislative conflicts, and the broader implications of the law for both local and national authorities. It also explores the types of evidence typically sought by the executive and judiciary, as well as the impact on victims, including the economic burden they bear. Furthermore, the paper critiques the current government's efforts to mitigate these risks and proposes innovative solutions, such as legal reforms, international cooperation, and capacity-building initiatives, to address the growing threat effectively.

Keywords: *digital arrest warrant, cybercrime, legal framework, digital scams.*

INTRODUCTION

Technology has significantly transformed the practice of law in the modern digital era, influencing nearly every facet of criminal procedure and law enforcement. One recent and

controversial development within the legal community is the concept of the 'Virtual Arrest Warrant.' Traditionally, judicial officers in India have issued arrest warrants through physical documentation in accordance with the Criminal Procedure Code (CrPC), which has now been replaced by the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2024. The emergence—and more accurately, the misinterpretation—of virtual arrest warrants has led to a host of complex legal and practical issues, primarily arising from fraudulent activities.

Although virtual arrest warrants are not officially recognised under Indian law, they are increasingly exploited in cyber scams.[1] In such schemes, fraudsters impersonate government or law enforcement officials, falsely accuse unsuspecting individuals of criminal offences, and coerce them into making online payments under the threat of arrest.[2] The anonymity afforded by technology, coupled with a general lack of public awareness regarding authentic legal procedures, exacerbates this problem.

From a practical standpoint, the misuse of virtual arrest warrants undermines public trust in legitimate law enforcement actions and highlights critical gaps in the existing legal framework. India's current legal regime, particularly the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita (BNS) 2023, does not explicitly recognise or regulate virtual arrest warrants, resulting in ambiguity about their legality and application.[3] This legal vacuum presents significant challenges for law enforcement agencies and legal practitioners in addressing cyber-enabled fraud.

Against this backdrop, the present study critically examines the legal ambiguities, practical difficulties faced by enforcement authorities, and proposes reforms aimed at improving legal clarity and operational effectiveness in dealing with virtual arrest warrants within the Indian context.

[1] 'India's 'digital arrest' scammers stealing savings' *Hindustan Times* (20 January 2025) <https://www.hindustantimes.com/technology/indias-digital-arrest-scammers-stealing-savings-101737350618503.html> accessed 03 March 2025

[2] 'Beware of 'Digital Arrest' Scam: Fraudsters Posing as CBI, ED Officials Target Indians' *Economic Times* (18 July 2023) <https://economictimes.indiatimes.com/news/india/digital-arrest-beware-of-the-new-cyber-scam-that-alleges-you-of-serious-crime-to-extort-money/articleshow/114762835.cms?from=mdr> accessed 03 March 2025

[3] Information Technology Act 2000

LEGAL FRAMEWORK GOVERNING ARREST WARRANTS IN INDIA

Traditionally, the criminal energy and method controlling arrest warrants in India had been codified in the Code of Criminal Procedure (CrPC), 1973, currently replaced by the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2024. By definition, an arrest warrant is a formal written order from a qualified courtroom authority authorising a law enforcement official to seize someone charged with a criminal offense and bring them before the court docket to guarantee their attendance throughout judicial proceedings.[4] Sections 70 to 81 of the BNSS, which maintain much of the procedural rigour of the previous CrPC while adding certain modern changes, clearly outline the issue and execution of arrest warrants.[5]

Section 70 of the BNSS states that an arrest warrant has to be in writing form, signed by the presiding judicial officer, bear the reliable court seal, and surely contain the accused's name, the specific offence charged, and instructions for the law enforcement's approximate execution.[6] These criminal clauses spotlight the want of physical papers and identification, for this reason suggesting that digital or electronic formats lack felony validity.

Furthermore, the BNSS underlines procedural protections to maintain man or woman rights, including precise warrant provider standards, execution time regulations, and the protocol for treating humans under arrest.[7] Especially, Section 74 of the BNSS states that warrants must usually be carried out within the issuing court's jurisdictional boundaries; it provides for execution beyond jurisdiction only under well-specified legal criteria.[8] These provisions goal to prevent arbitrary arrests and shield individuals from procedural abuses.

Moreover, essential in handling distinctive types of cybercrimes and digital fraud, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita (BNS), 2023, do no longer in particular well known or allow for digital or digital arrest warrants. Digital arrest warrants, particularly in the form unfold by way of net frauds, therefore, stay outdoor the mentioned legal framework and reflect a prime regulatory vacuum.

[4] K.N. Chandrasekharan Pillai, *R.V. Kelkar's Criminal Procedure* (7th edn, Eastern Book Company 2023)
[5] Bharatiya Nagarik Suraksha Sanhita 2024, s 81
[6] Bharatiya Nagarik Suraksha Sanhita 2024, s 70
[7] Bharatiya Nagarik Suraksha Sanhita 2024, s 75
[8] Bharatiya Nagarik Suraksha Sanhita 2024, s 74

Practically speaking, any virtual depiction of an arrest warrant that doesn't properly comply with the procedural policies and authenticity standards set out in the BNSS is deemed legally unlawful. Especially in a society greater prone to virtual manipulation and cyber fraud, this prison clarity is important for each judicial integrity and public self-belief.

THE EMERGENCE AND MODUS OPERANDI OF DIGITAL ARREST SCAMS

Various kinds of cybercrime have emerged with the arrival of digital communication technology and growing internet usage in India, including a disturbing new trend usually known as 'Digital Arrest Scams.'[9] These frauds prey on the general public's lack of awareness of legal processes and fear of legal action to steal money from unknowing victims.[10]

Typically, digital arrest scams involve cybercriminals impersonating officials from prominent law enforcement agencies such as the Central Bureau of Investigation (CBI), Enforcement Directorate (ED), state police, or even courts.[11] Fraudsters initiate contact primarily through phone calls, emails, or instant messaging platforms, asserting that a digital arrest warrant has been issued against the targeted individual for alleged involvement in serious crimes like money laundering, drug trafficking, financial fraud, or cybercrimes.[12]

These scams usually unfold through a carefully constructed modus operandi. Initially, perpetrators use spoofing technology to replicate official phone numbers, email addresses, or even fabricate realistic-looking documents bearing emblems or logos of government authorities, thereby lending apparent legitimacy to their claims. Victims, when confronted with these seemingly authentic credentials, experience intense psychological pressure, often prompting immediate compliance without verifying the claims independently.[13]

Following initial intimidation, scammers demand urgent payment, typically through online channels such as cryptocurrency wallets, UPI (Unified Payments Interface), bank transfers,

---

[9] Haran Mahadik, 'What are 'digital arrest' scams? Why do many Indians fall for them?' *The Indian Express* (11 December 2023) <https://indianexpress.com/article/technology/tech-news-technology/digital-arrest-scams-why-many-are-falling-for-them-9706065/> accessed 05 March 2025

[10] *Ibid*

[11] Beware of 'Digital Arrest' Scam: Fraudsters Posing as CBI, ED Officials Target Indians (n 3)

[12] Ruchika Garg, 'Digital arrest scams: All you need to know' *Hindustan Times* (09 January 2025) <https://www.hindustantimes.com/htcity/htcity-delhi-junction/digital-arrest-scams-all-you-need-to-know-101736409777645.html > accessed 07 March 2025

[13] Shashi Shekhar, 'The worrying rise of fraudsters on the prowl online' *Live Mint* (11 November 2024) <https://www.livemint.com/opinion/columns/fraud-online-cybercrime-criminal-intimidation-digital-arrests-cbi-11731246111792.html> accessed 07 March 2025

or digital wallets, claiming this would halt the enforcement of the purported digital arrest warrant. Victims are often warned explicitly against seeking external assistance, with threats of immediate arrest, imprisonment, or severe penalties, effectively isolating them and exacerbating their susceptibility to coercion.

One significant challenge arising from the widespread nature of these scams is the difficulty law enforcement agencies face in tracing the criminals, who often operate anonymously, employing proxy servers, VPNs (Virtual Private Networks), and encrypted communication channels.[14] Moreover, many scams originate outside Indian jurisdiction, complicating international legal cooperation and prosecution efforts.[15]

The emergence of digital arrest scams underscores an urgent need for public education and awareness about authentic legal procedures, as well as robust legal and technological responses to counteract such fraudulent activities effectively.

LEGAL CHALLENGES POSED BY DIGITAL ARREST SCAMS

The proliferation of digital arrest scams presents numerous legal challenges within India's current statutory and judicial framework. Foremost among these challenges is the lack of explicit statutory provisions addressing digital arrest scams or clearly defining 'Digital Arrest Warrants' under existing Indian laws, particularly under the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2024, and the Information Technology Act, 2000.[16] Consequently, ambiguity persists regarding the specific categorisation and prosecution of such offenses.

One critical legal challenge is from jurisdictional complexities. Cybercriminals frequently operate beyond national borders, using digital anonymity and encrypted communication channels, creating substantial barriers for Indian law enforcement to initiate investigations or prosecution effectively.[17] Jurisdictional issues become further complicated by the limited scope of mutual legal assistance treaties (MLATs) India holds with other countries, hindering timely international cooperation and information exchange.[18]

[14] Niti Aayog, *Cybercrime in India: Challenges and* Solutions 2023
[15] Reserve Bank of India, *Cyber Frauds and Consumer Protection (*2023)
[16] Bharatiya Nagarik Suraksha Sanhita 2024
[17] Reserve Bank of India, *Report on Cyber Frauds and Consumer Protection* (2023)
[18] Ministry of External Affairs, *Mutual Legal Assistance Treaties (MLATs) and Their Effectiveness* (2023)

Additionally, the absence of clear statutory definitions makes it difficult for courts to adequately classify these scams within existing categories of cybercrimes, such as identity theft, cheating, impersonation, or online fraud. Although parts of the Information Technology Act 2000 and Bharatiya Nyaya Sanhita (BNS), 2023, can be used to prosecute cyber-related frauds, they do not particularly cover the special characteristics of digital arrest schemes involving the impersonation of judicial or investigative agencies.[19]

The evidence issues related to digital crimes provide another major legal hurdle. Gathering acceptable digital evidence that satisfies the exacting standards under Section 65B of the Indian Evidence Act 1872, presents significant practical challenges that might compromise the effective prosecution of offenders.[20]

PRACTICAL IMPLICATIONS AND GOVERNMENT INITIATIVES

The rise of digital arrest scams has substantial practical implications, including financial loss, emotional distress for victims, and erosion of public trust in law enforcement and judicial systems.[21] Victims often suffer severe psychological impacts, including anxiety and a diminished sense of security, which can have lasting societal consequences.

Recognising the severity and widespread impact of these scams, the Government of India has initiated multiple preventive and responsive measures. A significant initiative is the establishment and expansion of the Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, which functions as a centralised mechanism for reporting, investigating, and preventing cybercrimes.[22]

Furthermore, the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) has been strengthened, offering citizens a streamlined platform for reporting cyber frauds, including digital arrest scams. Complementing these measures, the government launched the national

[19] Bharatiya Nyaya Sanhita 2023
[20] Indian Evidence Act 1872, s 65B
[21] 'Digital Arrest Scam: How fraudsters posing as 'officials' steal your money' *Financial Express* (16 December 2024) <https://www.financialexpress.com/money/digital-arrest-scam-how-fraudsters-posing-as-officials-steal-your-money-3692413/> accessed 09 March 2025
[22] 'About I4C' (*Ministry of Home Affairs*) <https://i4c.mha.gov.in/about.aspx> accessed 09 March 2025

Cyber Crime Helpline Number (1930) to provide immediate assistance to victims of cyber fraud.[23]

Additionally, the government has embarked upon extensive public awareness campaigns through various media platforms, alerting citizens about the methods used in digital arrest scams and educating them about proper legal procedures to mitigate their susceptibility to such fraud.[24] Despite these proactive initiatives, continued gaps in the enforcement capacity of local law enforcement agencies and limited technological resources persist, underscoring the need for increased investment in cyber forensic tools, specialised training, and international cooperation to effectively combat digital arrest scams.[25]

CONCLUSION

The emergence and proliferation of digital arrest scams in India pose significant legal and practical challenges, exacerbating vulnerabilities in India's existing legislative and law enforcement frameworks. Despite the absence of legal provisions explicitly recognising digital arrest warrants, the rampant misuse of technology to impersonate judicial and law enforcement officials highlights critical gaps in statutory clarity, procedural safeguards, and public awareness. These scams severely affect victims financially and emotionally, simultaneously undermining public trust in the legal and judicial processes.

Though admirable, the government's proactive measures—such as creating the Indian Cyber Crime Coordination Centre (I4C), improving reporting systems, and running public awareness campaigns need more support to fully handle the changing character of digital frauds.

RECOMMENDATIONS

To effectively combat digital arrest scams and bolster India's legal and institutional response, the following measures are recommended:

[23] Ministry of Home Affairs, 'National Cyber Crime Helpline '1930' Operationalised' (*Press Information Bureau*, 06 April 2022) <https://pib.gov.in/PressReleasePage.aspx?PRID=2101613> accessed 09 March 2025
[24] *Ibid*
[25] NITI Aayog, *Strengthening Cybercrime Investigation: A Policy Roadmap for India* (2023)

Amend Existing Laws: Update the Bharatiya Nagarik Suraksha Sanhita 2024 and the Information Technology Act 2000 to explicitly define and criminalise digital arrest scams, ensuring clear legal accountability.

Prohibit Forged Digital Documents: Enact legal provisions that explicitly ban the creation, dissemination, or use of fraudulent digital documents purporting to be from law enforcement or judicial authorities.

Enhance International Cooperation: Strengthen cross-border collaboration through bilateral treaties and multilateral frameworks to facilitate the investigation and prosecution of cybercriminals operating beyond national jurisdictions.

Empower Law Enforcement: Provide targeted cybercrime training, digital forensic tools, and infrastructure to law enforcement agencies to enhance their capacity to detect, investigate, and dismantle scam operations.

Promote Digital Literacy: Launch nationwide awareness campaigns aimed at educating the public on how to recognize and avoid cyber scams, particularly those involving fake legal threats.

Demystify Legal Processes: Conduct regular public workshops, seminars, and media outreach programs to improve understanding of legitimate legal procedures, reducing the likelihood of individuals falling prey to fraudulent intimidation.

Strengthen Digital Security Infrastructure: Implement robust cybersecurity protocols and real-time monitoring systems in coordination with telecom and internet service providers to detect and rapidly shut down scam networks.

By adopting these comprehensive measures, India can significantly reduce the incidence of digital arrest scams, protect its citizens from cyber-enabled fraud, and reinforce public trust in the credibility and effectiveness of its legal and judicial institutions.