Clicks to Cuffs: The Jurisprudence of Fear, Extortion, and "Digital Arrests" in Cyber Fraud

ABSTRACT

Imagine a phone call claiming your bank account is linked to a crime, followed by a video call with someone in a police uniform, showing a fake arrest warrant bearing your name. No handcuffs, no police station, just a screen, a script, and enough fear to make people hand over their life savings. This is "digital arrest," now among India's most damaging cyber scams, costing citizens thousands of crores in recent years. This paper examines digital arrest as both a legal and psychological problem. It explains the scam's mechanics, scammers posing as CBI, ED, or police officials, using fake documents and mock courtrooms to pressure victims into panic-driven transfers, and traces the legal provisions currently used to prosecute such cases, mainly borrowed from the IT Act and Bharatiya Nyaya Sanhita, showing why these fall short in the absence of a dedicated offence. Drawing on real cases, including a West Bengal court judgment, it explores why the scam succeeds through fear and authority rather than technical skill, and proposes recommendations: recognising digital arrest as a distinct offence, tightening financial safeguards, and expanding public awareness.

Keywords – Digital-arrest, cyber-fraud, legal reforms, Psychological manipulation.

I. INTRODUCTION

In Avengers: Infinity war, Thanos needed a gauntlet and Six Magical stones to erase half of the existence with a single snap. Today's scammers need neither – just a phone call and some minutes of manufactured fear to erase someone's whole life savings. No stones, no sorcery – only a stolen identity, a doctored warrant and a script rehearsed enough to sound like an actual law. This is the reality of digital arrest a new form of digital scam which is rapidly growing all over India. According to National Human Rights Commission (NHRC) Indians have lost around Rs.52,976 crores to cyber-enabled frauds over the past six years, with nearly 8% of the losses linked to "digital arrest" scams.[1]

Recently, Prime Minister Narendra Modi addressed the nation in his 'Mann Ki Baat' and raised concern against the 'digital arrest'. He played an audio-video clip that showed a man in

[1] Nat'l Hum. Rts. Comm'n, NHRC, India Organises an Open House Discussion on "Safeguarding Human Rights Against Digital Arrest Scams" in Hybrid Mode (June 9, 2026), https://nhrc.nic.in/media/press-release/nhrc,-india-organises-an-open-house-discussion-on-safeguarding-human-rights-against-digital-arrest-scams-in-hybrid-mode (last visited July 22, 2026).

a police uniform, asking the victim to share his Aadhaar number to save his mobile number from being blocked. Digital arrest is the name given to a cybercrime technique where scammers send messages, make calls or video calls to the person and manipulate him by impersonating law enforcement officials or investigating agencies and asks for ransom as a fine or sometimes personal information for the purpose of fake verification.

Despite remarkable developments in digital laws, including Sections 43, 66C, and 66D of the Information Technology Act, 2000, little has fundamentally changed. What has changed is the scale of fraud and earlier digital scams mainly relied on weaknesses in software, while this modern scam instead exploits psychological weaknesses. As before, we remain largely unable to curb it

This paper seeks to examine the phenomenon of "digital arrest" as both a legal and psychological crisis unfolding across modern India. It begins by tracing the legal developments that govern cyber fraud and impersonation in India. before identifying the loopholes and enforcement gaps that allow such scams to persist despite this legal architecture. The paper further explores the psychological and technological factors that make digital arrest uniquely effective, distinguishing it from conventional cybercrime, and examines major reported incidents across India to understand recurring patterns in method, targeting, and impact. Finally, it offers a set of recommendations aimed at closing existing gaps.

II. UNDERSTANDING DIGITAL ARREST

The term **"digital arrest"** is a piece of modern cyber-parlance. It is not an actual legal procedure, but rather a psychological tactic and scam developed by cybercriminals to extort victims through intimidation and virtual confinement. A digital arrest is a cyber-technique that is based on psychological confinement rather than physical detention. Scammers impersonate judges, police officers, and officials from agencies such as the Central Bureau of Investigation, Customs Department, Income Tax Department, Narcotics Control Bureau and the Reserve Bank of India. They Maliciously accuse the victims of crimes like money laundering, drug trafficking, or suspicious parcel movements.[2]

[2] GRMI, Digital Arrest Scam: Real Incidents, Concerns, Challenges and Way Forward (Jan. 19, 2026), https://grm.institute/blog/digital-arrest-scam-real-incidents-concerns-challenges-and-way-forward/ (last visited July 22, 2026).

The scam usually begins with a simple phone call - the pretext can vary widely, from an undelivered parcel or KYC verification to a blocked SIM card, or alleged involvement in a crime - but the intent is always the same- to create just enough doubt for the victim to stay on the line. As the conversation progresses, the scammer uses aggressive tactics to instil panic, often claiming that the victim or any of his relatives is involved in serious crimes like money laundering, cybercrime, or drug trafficking. They support the same using forged documents, doctored videos, and even spoofed phone numbers, the scammers create an air of legitimacy, pushing the victim to believe the legitimacy.[3]

At the moment when the person being targeted begins to believe in the deception, the scammer is already set to accomplish their goal: they either request financial details to get access to the victim's money or demand cash claiming these funds as a "fine" with the promise to refund the victim of the amount once the so-called "investigation" is complete. This usually leads to the shedding of the needed money from some savings or even debts which also allow the person to repay the scammer. After money has been sent to the scammer, they close the account and disappear, leaving the victim in despair and unaware of what to do.

The helplessness that people feel in this situation does not occur out of the blue. It is directly connected with the difference between digital arrest and crimes that the law was designed to deal with. The laws do not apply here because they have no means to deal with the cases like these due to little public awareness about the problem and the inability to act in case they recognize the scam.

First, a traditional arrest requires a physical officer to detain the accused in person, whereas digital arrest requires no such physical presence, scammer and victim interact entirely in virtual form. This is one of the primary reasons apprehending the scammer proves so difficult: perpetrators typically operate using fake ID cards, spoofed mobile numbers, and VPNs, making it nearly impossible to trace their actual location or IP address. Second, while conventional cybercrime typically relies on malicious links, unauthorized device access, or installed malware to compromise a victim, digital arrest requires none of this, no location is breached and no device is technically compromised. The crime occurs entirely within the

[3] Major Sadhna Singh, Digital Arrest: The Modern-Day Cyber Scam, NITI Aayog (Apr. 16, 2025), https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf (last visited July 22, 2026).

victim's judgment and fear response, leaving little to no technical trace for investigators to follow. Third, in traditional crime, money is taken by force or stealth, often without the victim's knowledge until after the fact; in digital arrest, however, the victim willingly and knowingly transfers the money themselves, genuinely believing they are paying a legitimate fine or clearing their name of false charges. As a result, there is no clear moment at which the act registers as theft while it is happening, the victim only recognizes the fraud after the transaction is complete, by which point it is already too late to intervene. Finally, traditional crimes are often instantaneous, a single act over in moments, whereas digital arrest can extend over hours or even days, with victims kept continuously on video calls and explicitly instructed not to disconnect or contact anyone, turning the crime into a sustained state of psychological captivity rather than a single criminal act.

III. LEGAL FRAMEWORK GOVERNING DIGITAL ARREST IN INDIA

India does not have any specific legal framework that addresses digital arrest scams. Instead of that, the offences are prosecuted under a combination of cybercrime legislation, criminal law provisions and regulatory measures which have the goal of preventing identity theft, online impersonation, financial fraud and unauthorised access to digital systems.

The primary legislation to provide for protection is the Information Technology Act, 2000 which criminalises several acts generally used in digital arrest scams.[4] Section 43[5] talks about civil liability for unauthorised access to computer systems, unauthorised downloading of data and damage to digital infrastructure. Section 66C[6] provides for punishment of fraudulent use of electronic signature, password or any other unique identification credential of another person and Section 66D[7] provides for punishment for cheating by personation by use of computer resources or communication devices. These provisions provide the legal basis to prosecute offenders who act as law enforcers or government officials on digital platforms.

Criminal liability is also attracted under the Bharatiya Nyaya Sanhita, 2023[8] which has replaced the Indian Penal Code, 1860 along with the Information Technology Act. Depending upon the facts of each case, offences of cheating, criminal intimidation, extortion, forgery and

---

[4] *Information Technology Act, 2000, No. 21 of 2000, India Code (2000), https://www.indiacode.nic.in/handle/123456789/1999*
[5] *Information Technology Act, 2000, No. 21 of 2000, § 43 (India).*
[6] *Information Technology Act, 2000, No. 21 of 2000, § 66C (India).*
[7] *Information Technology Act, 2000, No. 21 of 2000, § 66D (India).*
[8] *Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, India Code (2023).*

personation may be invoked against perpetrators who force victims to transfer money under false caveat of arrest or criminal investigation. Both cyber-specific and general criminal provisions are there to ensure that digital arrest scams are not treated as merely technological offences but as serious crimes of deception, coercion and financial exploitation.

This legal response is also supported by the regulatory framework. The Ministry of Home Affairs has established the Indian Cyber Crime Coordination Centre (I4C) as the central agency to coordinate the investigation and awareness activities connected with cybercrime. The Reserve Bank of India has issued guidelines to banks for strengthening fraud identification and consumer protection mechanisms[9], whereas the Telecom Regulatory Authority of India has introduced measures to check spam communications, caller ID manipulation and abuse of telecom networks.[10] Together these statutory and institutional frameworks form the response of India to the rising danger and threat of digital arrest scams.

IV. LOOPHOLES AND ENFORCEMENT GAPS

India's legal response to digital arrest scams continues to face serious enforcement challenges despite several statutory provisions and institutional mechanisms. The rapid growth of cyber-enabled fraud has revealed weaknesses in the current legal system, showing that effective enforcement is not only about the existence of legal provisions but also about their capacity to respond to new forms of digital deception. The law has had a hard time keeping up with the ever more sophisticated nature of these offences, as scammers keep improving their methods.

One of the most obvious gaps is the lack of a clear legal definition of "digital arrest." At the moment, these scams are dealt with under a mix of provisions relating to cheating, impersonation, identity theft, criminal intimidation and cyber fraud.[11] However, these offences, while covering different aspects of the crime, do not recognise digital arrest as a specific type of fraud with its own modus operandi. Often, the lack of any specific statutory recognition is a reason for fragmented investigations, inconsistent application of legal provisions and difficulties in proper recording and analysis of the scale of the problem. A

---

[9] *Reserve Bank of India, Master Directions on Cyber Resilience and Digital Payment Security Controls for Non Bank Payment System Operators, RBI/DPSS/2024-25/01 (July 30, 2024).*

[10] *Telecom Regulatory Authority of India, The Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR, 2018), No. 1 of 2018.*

[11] *Shailesh K. Pandey & Ansh Parashar, Navigating Digital Arrest Under India's Cyber Forensics Framework: Complexities, Legal Gaps, and Pathways Forward, 4* NFSU Journal of Forensic Justice *80 (2025).*

clear legal offence would allow for more focused policy making and law enforcement strategies, as well as greater consistency in prosecution.[12]

Enforcement is further complicated by the borderless nature of cybercrime. Organised networks often run digital arrest scams across different jurisdictions, with the scammers routing calls through overseas servers, employing virtual private networks, and hiding behind encrypted communication platforms. Money transfers are often moved through a number of bank accounts, cryptocurrency wallets or mule accounts, making the investigation trail harder to detect and follow. These cross border operations require timely and adequate international cooperation but effective investigation and prosecution are often obstructed by differences in domestic laws, procedural requirements and delays in mutual legal assistance.[13] This generates a major obstacle in identifying and taking action against masterminds behind such scams.

Also worrying are the delays that mark investigation and recovery mechanisms. By the time victims report the offence, the fraudulent transactions are often spread across a number of accounts or withdrawn completely, greatly reducing the chances of financial recovery.[14] Technical expertise, manpower and digital forensic resources often constrain the investigative agencies. Coordination between banks, telecom service providers and law enforcement agencies is not always smooth. These delays mean victims are not only stuck in legal uncertainty for longer, but it also comes with serious financial and emotional costs. [15]Therefore, improving investigative capacity, improving coordination between agencies and creating faster mechanisms for freezing and recovering fraudulently transferred funds are necessary for ensuring that legal safeguards are effective on ground and not just on paper.

V. FACTORS CONTRIBUTING TO THE RISE OF DIGITAL ARREST SCAMS

To understand the alarming rise of digital arrest scams, it’s not enough to see them just as a product of technology or criminal innovation. But at their core these scams play on very

---

[12] *Saroj Shekhar Mallick, Digital Arrest Scams in India: Challenges and Solutions Under the IT Act, 2000, SSRN Electronic Journal (Dec. 25, 2024).*

[13] *United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (Feb. 2013), available at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*

[14] *Federal Bureau of Investigation, Internet Crime Report 2024 (Internet Crime Complaint Center, 2025), available at https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf*

[15] *Shailesh K. Pandey & Ansh Parashar, Navigating Digital Arrest Under India's Cyber Forensics Framework: Complexities, Legal Gaps, and Pathways Forward, 4* NFSU Journal of Forensic Justice *80 (2025).*

human instincts, using emotions, trust and vulnerability to manipulate even the most careful of people. Their success is not the result of simple, sophisticated trickery but their ability to tap into the psychology of fear, along with modern technology and existing social inequalities.

Psychology is one of the greatest factors behind these scams. The fraudsters deliberately create an atmosphere of fear by accusing victims of involvement in serious offences such as money laundering or cyber crime.[16]They often pose as police officers, investigators, or government officials, based on the natural tendency to obey perceived authority. The pressure is amplified by the creation of artificial deadlines and threats to victims that any delay will result in immediate arrest, seizure of assets or public humiliation. The fear that accompanies those moments bypasses rational thought, and makes people more likely to continue with it without questioning whether the interaction is real.[17]

Technology has made those manipulative tactics even more believable. Caller ID spoofing allows scammers to appear as legitimate government agencies, and artificial intelligence advancements have enabled voice cloning, deepfakes and digitally generated impersonations which look really real. These technologies are making it tougher and tougher to differentiate between real and fake communication, making it more difficult to identify deception. As technology becomes more and more accessible, the barriers to sophisticated and orchestrated fraud keep getting lower and simpler.

The socio demographic vulnerabilities which these scams exploit are equally as important. Elderly people, who are more likely and shown to have a greater trust in institutional authority, are specifically at risk. So are those with limited digital literacy who might find it difficult to differentiate between legitimate official communication and carefully planned out fraud.[18] Isolation, unfamiliarity with emerging technologies and lack of immediate guidance increases their proneness in many cases. Digital arrest scams thus thrive and operate at the nexus of human psychology, technological sophistication and unequal digital preparedness, making it one of the most subtle yet dangerous forms of cyber enabled fraud today.

---

[16] Rimjhim Singh, Digital Arrest and Fear Scams: Why Educated Users Fall for Cyber Fraud, Bus. Standard (June 25, 2026, 1:20 PM), https://www.business-standard.com/technology/tech-news/digital-arrest-scam-fear-educated-elderly-victim-users-fall-cyber-fraud-126062500485_1.html (last visited July 22, 2026).

[17] Abhijnan Rej, India's Digital Arrest Scams, Lowy Inst. Interpreter (Sept. 10, 2025), https://www.lowyinstitute.org/the-interpreter/india-s-digital-arrest-scams. (last visited July 22, 2026).

[18] GRMI, Digital Arrest Scam: Real Incidents, Concerns, Challenges and Way Forward, GRMI Blog (Jan. 19, 2026), https://grm.institute/blog/digital-arrest-scam-real-incidents-concerns-challenges-and-way-forward/ (last visited July 22, 2026).

VI. MAJOR REPORTED INCIDENTS IN INDIA

Incident 1: - A 68-year-old woman in Kottayam, Kerala, was scammed of Rs.1.86 crore in a "digital arrest" fraud. Posing as CBI officials, scammers falsely accused her of money laundering and threatened her with arrest via a WhatsApp video call, pressuring her into transferring the money in four instalments during September 2025. In a similar case, musician Jerry Amaldev was saved from losing Rs.3 lakhs after his bank manager spotted a suspicious account and alerted police. Investigating the Kottayam case, the CBI carried out raids across six cities on February 25, 2026, arresting three people, including the main accused in Goa, for running mule accounts and crypto transactions used in the fraud..[19]

Incident 2: - SP Oswal, Chairman of the Vardhman Group, was defrauded of Rs.7 crores in an elaborate digital arrest scam. Scammers contacted him via WhatsApp, posing as CBI officials, and claimed his Aadhaar details had been misused in a fake passport and financial fraud case. To make the scheme convincing, they wore fake CBI uniforms, used a backdrop featuring the CBI logo, and staged a fake virtual courtroom complete with fabricated documents. They contacted Oswal daily over video calls, keeping him under the illusion of "digital arrest" for two days, and even sent him a fake Supreme Court arrest warrant over WhatsApp.

Fearing financial and reputational harm, Oswal paid Rs.7 crores to the scammers when they demanded money for his "bail." After realising he had been duped, he filed a complaint with the Cyber Crime Department of Ludhiana Police. The Enforcement Directorate later took over the money laundering and digital arrest investigation, and police managed to recover over Rs.5 crores. The case underscores the growing sophistication of cybercriminals exploiting fear and impersonation tactics to target even high-profile individuals.[20]

Incident 3: - A 74-year-old retired professor from Kalyani, Nadia district, West Bengal, was kept under a month-long "digital arrest" by fraudsters posing as Mumbai Police officials in fake uniforms. Accused of financial fraud, he was shown fabricated documents and warned via WhatsApp calls, leading him to transfer nearly Rs.1 crore, his savings, fixed deposits,

---

[19] Cent. Bureau of Investigation, CBI Launches "ABHAY" – AI-Powered Notice Verification System: Empowering Citizens to Verify CBI Notices and Defeat "Digital Arrest" Fraud (May 15, 2026), https://cbi.gov.in/press-detail/NzU5Ng== (last visited July 22, 2026).

[20] *Aditi Pangotra & Neeraj Soni, Corporate Leader Duped by Digital Arrest Scam: A New Era of Cyber Fraud, CyberPeace (Oct. 8, 2024), https://cyberpeace.org/resources/blogs/corporate-leader-duped-by-digital-arrest-scam-a-new-era-of-cyber-fraud* (last visited July 22, 2026).

mutual funds, and even mortgaged jewelry, into mule accounts before the scammers vanished.

He filed a complaint on the National Cyber Crime Reporting Portal, and the Cyber Crime Branch traced the mastermind to Cambodia, beyond MLAT reach, though the local network was dismantled. Despite defense arguments over the lack of a legal definition for "digital arrest" and missing forensic evidence, the prosecution succeeded using Locard's Exchange Principle and Section 106 of the Evidence Act (now Section 109 of the BSA), shifting the burden of proof to the accused, who failed to explain the transactions.[21]

Incident 4: - A pharmaceutical businessman and his wife lost Rs.58.1 crore in a digital arrest scam that began in August 2025. Scammers convinced them of a money-laundering probe using fake video clips of police stations, CBI/ED offices, and a mock courtroom, pressuring the couple into transferring their entire savings over several weeks with false promises of reimbursement.

After the scammers went silent, the couple filed a complaint with the Maharashtra Nodal Cyber Police. Investigation revealed an international network linked to Cambodia, Dubai, and Hong Kong, led by mastermind Vijay Khanna operating from abroad. Funds were traced through 13 layers involving 27 mule accounts across Maharashtra, Gujarat, and Rajasthan. The first arrest was Gujarat businessman Jayeshbhai, who allegedly received Rs.15.3 crore for routing the money, marking one of India's biggest digital arrest scams.[22]

VII. RECOMMENDATIONS

Enhancing Proactive Cybercrime Policing- There is a need to switch the focus of law enforcement from addressing fraud post occurrence to implementation of preventive measures. The dedicated units dealing with cybercrime must be provided regular training to meet the new challenges and threats related to cybercrime like voice cloning based on AI, deep fakes and encrypted communication channels, cross-border fraud etc. Moreover, the department must keep pace with the criminals in terms of the technological capacity.

---

[21] State of West Bengal v. Jatin Anup Ladwal, Sessions Case No. 51 of 2025 (Court of Add'l District & Sessions Judge, Kalyani, Nadia, July 17, 2025) (India), https://sikkimjudicialacademy.nic.in/sites/default/files/PPTs/Digital%20Arrest%20Judgement.pdf. (last visited July 22, 2026).

[22] *Ahmed Ali, Rs 58 Crore Digital Arrest Fraudsters Opened 10K Mule Accounts: Cops, Times of India (Jan. 9, 2026, 1:05 AM IST), https://timesofindia.indiatimes.com/india/rs-58-crore-digital-arrest-fraudsters-opened-10k-mule-accounts-cops/articleshow/126421857.cms* (last visited July 22, 2026).

Creation of Mechanism for Institutions Coordinating Instantaneously- There is a need to develop a system allowing smooth coordination between law enforcement agencies, banks, telecommunication companies, financial service providers and technology companies. The rules aimed at freezing suspicious accounts and tracing transactions instantly might greatly assist in recovering robbed money.

Raising the Awareness of the Public- It is time to revise approaches to public education institutions and move beyond simple cyber hygiene by explaining people the details of digital arrest scams including impersonation of police officers, manipulation of victims and misleading information about arrests.

Elevate the Accountability of Financial and Technological Intermediaries- Banks must utilize cutting-edge fraud detection solutions which would identify suspicious transaction patterns in real-time. Telecom providers should also improve caller verification to minimize fake calls coming from government numbers. Furthermore, digital platforms must take prompt action against accounts impersonating authorities.

Focus on Efficient Execution and Victim Help- Instead of the addition of new offenses, the need is for a more rapid investigation process, simpler complaint system, higher international collaboration, and regular assessment of cybercrime enforcement processes. It is vital to render legal assistance to victims, provide psychological help, and make compensation easier to obtain in order to compensate for the financial and emotional consequences of a crime.

VIII. CONCLUSION

Digital arrest represents a disturbing evolution in cybercrime, one that succeeds not through technical vulnerabilities but through fear, authority, and psychological manipulation. By posing as police officers, investigators, or government officials, scammers exploit citizens' trust in public institutions, ensnaring even educated professionals, business owners, and senior citizens alike. As this paper has shown, India's legal framework, comprising the IT Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, is robust on paper, yet the absence of clear legal recognition for digital arrest, combined with jurisdictional barriers and limited public awareness, continues to hamper enforcement. The gap, therefore, lies not in the absence of law but in its enforcement, one that tougher penalties alone cannot close. What is needed instead is coordinated institutional response, faster recovery mechanisms, technological safeguards, and sustained public awareness, so that law, enforcement, financial institutions, and citizens evolve together against a threat that will only continue to adapt.