International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 30-03-2025, Accepted: 29-04-2025, Published: 14-05-2025
Volume 11, Issue 5, 2025, Page No. 121-127

# Unmasking digital arrest: An emerging threat to modern society in India

**Uma**
Research Scholar, Department of Law, BPSMV, Khanpur Kalan, Sonipat Haryana, India

**Abstract**
The “Digital Arrest” phenomenons refers to a rising kind of cyber fraud in which perpetrators impersonate law enforcement or government authorities, often via phone or video calls or messaging, falsely accuse persons of crimes, claim a warrant or immediate warrant or arrest, and coercively extract money or personal data under fear of legal repercussions. This paper explores the nature, legal status, and modus operandi, sociologic and psychological impacts of digital arrest scams, situates the concept within existing legal frameworks, discusses challenges in enforcement and prevention, and provides recommendations for policy, law enforcement, and public awareness.

**Keywords:** Digital arrest, society, rights, laws

## Introduction

In recent decades, Indian society has witnessed the proliferation of digital communication tools likes smart phones, video calling, messaging apps, globalization of networks, and the increasing digital literacy gaps have led to the creation of fertile ground for new forms of cyber frauds. Among them, the “digital arrest” scam has gained prominence in India as frequently reported by media stories, government advisories, and public complaints. This term, while not yet formally recognized in legal dictionaries or criminal statutes, is being used increasingly in India to describe a scam where individuals are digitally coerced into compliance by fraudsters posing as law enforcement or government officials. These scams exploit both technological vulnerabilities and psychological manipulation, often leading to significant financial loss and emotional trauma for the victims. At the heart of this phenomenon lies a dangerous blend of impersonation, intimidation, and digital sophistication, where the illusion of legal authority is used to trap unsuspecting individuals.

The term “digital arrest” is, however, not a legal one it does not correspond with any recognized power under Indian criminal law for arrest via phone or video, etc. But its psychological effect is real, leading to significant financial loss and trauma.

## Defining “Digital Arrest”

Digital Arrest is a contemporary term used to describe a type of cyber-enabled fraud in which scammers impersonate law enforcement or government officials and falsely accuse individuals of criminal activity, coercing them into compliance through digital communication platforms. The concept of “arrest” in this context is entirely fictitious, as no actual legal authority is exercised. Instead, the illusion of legal power is used to manipulate, intimidate, and financially exploit victims. The term has gained widespread usage in India following a surge in such scams since 2023–24, but it has yet to be formally defined in legal statutes.

At its core, a Digital Arrest scam involves a fraudulent claim that the target is under investigation for a serious crime such as money laundering, drug trafficking, pornography, or misuse of identity documents like Aadhar or PAN. The scammers often claim to be calling from agencies such as the police, CBI, ED, NCB, or judicial bodies, and present a false narrative that the victim's involvement in a crime has been digitally verified. In many cases, the victim is told that a non-bailable warrant has already been issued or that they are under "digital surveillance."

What makes Digital Arrest unique from other forms of cybercrime is its reliance on psychological manipulation through a highly structured and often scripted impersonation. Scammers utilize voice calls, video calls, Whatsapp messages, and emails, sometimes backed by fabricated official documents, false FIRs, or screenshots of supposed government notices. They may also use fake uniforms, badges, virtual backgrounds mimicking police stations or courtrooms to reinforce the illusion of authority during video calls.

Victims, often caught off guard and under intense psychological pressure, are then coerced into transferring large sums of money to “settle” the matter, “verify” their identity, or pay a so called “digital bail” amount. In more severe cases, victims are forced to stay on continuous video calls for hours or even days, creating an atmosphere of control, surveillance, and panic. They are sometimes told not to contact family or legal counsel, leading to isolation and deeper manipulation.

It is important to note that no such legal process as a "digital arrest" exists under Bharatiya Nyaya Sanhita or any established global legal framework. In India, arrest procedures are governed by the new criminal law i.e. Bharatiya Nagarik Suraksha Sanhita, 2023 and involve formal steps including the issuance of warrants, documentation, and personal appearance. A person cannot be lawfully arrested through a phone call or video call, nor can they be asked to pay money to avoid arrest. The scam exploits the general public’s lack of legal awareness, fear of the police and judiciary, and trust in technology.

Thus, Digital Arrest is not a legal concept but a fraudulent construct, designed to exploit and extort. It blends elements of impersonation, intimidation, extortion, and cyber fraud, making it one of the most psychologically potent and financially damaging cybercrimes in recent years.

**Key Features**

### 1. Impersonation of Law Enforcement or Authorities

One of the defining aspects of a digital arrest scam is the impersonation of law enforcement or government agencies. Scammers pose as officers from police departments, central investigative agencies like the CBI or NCB, judicial officials, or regulatory authorities such as the RBI, TRAI, or customs. They often use fake names, identification badges, official-sounding ranks, and email addresses that mimic to real departments. On video calls, they may wear police uniforms or display false government insignia to make the deception more convincing.

### 2. False Accusations of Criminal Activity

The victim is typically informed that they are under investigation for a serious crime such as money laundering, drug trafficking, involvement in cybercrimes, possession of illegal materials, or the misuse of documents like Aadhar, passport, or SIM cards. In some cases, they are told their identity has been used in an international crime. The false allegations are designed to cause panic and urgency.

### 3. Use of Digital Communication Platforms

Digital arrest scams rely heavily on digital tools and communication platforms, making them scalable and hard to trace. Fraudsters contact victims through phone calls, Whatsapp, Telegram, Skype, emails, or video conferencing apps. On video calls, they simulate police stations or government offices using virtual backgrounds, official-looking documents, and props. This creates an illusion of legitimacy and reinforces the victim’s belief that the interaction is real.

### 4. Psychological Manipulation and Intimidation

The scam is built on creating a climate of fear. Victims are often told they will be arrested immediately, have their bank accounts frozen, face social humiliation, or go to jail. Some are threatened with public exposure or involvement of the media. The perpetrators often isolate the victim by asking them to remain on a video call continuously, discouraging them from speaking to friends, family, or lawyers. This coercive isolation increases compliance and prevents victims from seeking help.

### 5. Financial or Data Exploitation

Once trust or fear is established, scammers demand that victims pay money to avoid arrest or “resolve” the matter. These payments are termed as “security deposits,” “bail amounts,” “clearance charges,” or “verification fees.” The victim is asked to transfer funds via UPI, RTGS, NEFT, or international wire transfers. In some cases, personal and financial information is stolen, such as OTPs, bank details, or digital signatures.

### 6. Complete Lack of Legal Basis

The most important feature is that no such process as a “digital arrest” exists in any legal framework. Indian law requires arrests to follow formal procedures under the Bharatiya Nagarik Suraksha Sanhita, involving proper documentation and physical interaction by authorized officers. Therefore, any claim of arrest or legal action over a phone or video call demanding money is entirely illegal and fraudulent.

## Modus Operandi

The mechanism of a digital arrest scam is a sophisticated process that relies on a combination of psychological manipulation, impersonation of authority, technological tools, and rapid financial exploitation. While the specifics may vary, the core strategy follows a predictable pattern designed to intimidate the victim and elicit quick compliance.

### Initial Contact and Hook

The scam begins with unsolicited communication, often through a phone call, Whatsapp message, SMS, email, or video call. The caller claims to represent a government agency such as the police, Central Bureau of Investigation (CBI), Narcotics Control Bureau (NCB), Reserve Bank of India (RBI), customs department, or even a court.

The victim is informed that they are under investigation for a serious crime, often linked to money laundering, drug trafficking, misuse of Aadhar or SIM cards, or receiving illegal packages. The scammers use urgency and legal jargon to establish a sense of danger and legitimacy. Victims are told that they could face immediate arrest, bank account freezes, or criminal charges if they fail to cooperate.

### Escalation through Fear and Isolation

Once the initial threat is delivered, the scam escalates. The fraudster typically demands the victim to stay on a video call or to download a screen-sharing or meeting app (like Skype, Zoom, or Google Meet). The scammer might appear in police uniform, sitting in front of a digitally created police station or courtroom background. They may flash fake IDs, warrant documents, or show alleged evidence against the victim.

The victim is warned not to speak to anyone else, including friends or family. This forced isolation is a deliberate psychological tactic meant to heighten fear and reduce the chances of the victim verifying the scam or seeking help. The scammers maintain this pressure for hours or even days, with some cases involving continuous video surveillance.

### Coercion into Compliance

Once the victim is mentally overwhelmed, the scammers begin the next phase i.e. coercing payments or stealing data. The victim is told that they can avoid arrest or criminal charges by paying a refundable fine, deposit, or bail amount. These payments are framed as part of a “digital settlement process.”

The scammers often provide UPI IDs, bank account numbers, or international transfers details and pressure the victim to make immediate payments. In some cases, multiple transactions are requested over several hours. Sometimes, the scam also involves collecting sensitive data like bank login credentials, Aadhar numbers, or OTPs under the pretext of verification.

### Exit and Disappearance

Once the money is transferred or the victim begins to question the legitimacy of the process, the scammers abruptly terminate the communication. The phone numbers, Whatsapp accounts, or email addresses used are quickly deactivated or switched, making it difficult to trace them. Victims are often left confused, ashamed, and financially drained.

### Use of Technology and International Infrastructure

Many such scams originate from call centers based abroad or use VoIP (Voice over Internet Protocol), VPNs, and international SIM cards, making investigation difficult. Scammers also use social engineering scripts, fake websites, and spoofed caller IDs to enhance credibility.

In the digital arrest scam uses a multi-stage psychological and technological mechanism to trap, isolate, and exploit individuals under the illusion of lawful authority.

### Legal Status

The term "Digital Arrest" has gained popularity in recent years due to a sharp rise in cyber frauds where criminals impersonate government officials and threaten individuals with arrest over digital platforms. However, despite its growing notoriety, "digital arrest" has no legal basis in Indian criminal law. It is not a recognized legal procedure, and any claim or action made under the guise of a "digital arrest" is entirely fraudulent and unlawful.

### Non-Existence of "Digital Arrest" in Indian Law

Under Indian law, the concept of arrest is governed by the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). An arrest must follow proper legal procedures, such as:

- Issuance of a warrant or authorization by a competent authority,
- Physical presence and identification of the arresting officer,
- Communication of the grounds of arrest to the accused,
- Production before a magistrate within 24 hours.

None of these procedures can be lawfully executed via a phone call, Whatsapp message, video conference, or email. Hence, a "digital arrest" is not a legal mechanism recognized by the Indian judicial or policing system.

Therefore, any individual or group claiming to arrest someone digitally or demanding money to prevent a supposed arrest is acting outside the boundaries of the law, and their actions fall under criminal offences such as impersonation, extortion, cheating, and cybercrime.

### Applicable Legal Provisions

Although there is no dedicated law for "digital arrest," several provisions under existing statutes that can be applied to prosecute such acts:

**a.** Bharatiya Nyaya Sanhita, 2023

- **Section 319:** Punishment for cheating by personation
- **Section 318:** Cheating and dishonestly inducing delivery of property
- **Section 308:** Punishment for extortion
- **Section 336/338:** Forgery of purpose of cheating and use of forged documents
- **Section 61:** Criminal conspiracy

**b.** Information Technology Act, 2000

- **Section 66D:** Punishment for cheating by personation using computer resources
- **Section 66C:** Identity theft
- **Section 43:** Unauthorized access to computer systems and data
- **Section 72:** Breach of confidentiality and privacy

These sections provide a legal foundation to take action against individuals who perpetrate digital arrest scams. Section 66D; in particular, is directly applicable to such frauds since it criminalizes cheating by personation using electronic means.

### Challenges in Legal Enforcement

Despite the availability of relevant legal provisions, enforcing the law in digital arrest cases presents several challenges:

- **Anonymity of Offenders:** Scammers often use VoIP numbers, international SIMs, VPNs, and encrypted platforms, making it difficult to trace their identity and location.

- **Cross-border Jurisdiction:** Many of these scams originate from call centers located outside India (e.g., in South East Asia, the Middle East, or African countries), complicating jurisdiction and requiring international cooperation.

- **Delayed Reporting:** Victims often feel ashamed or confused, delaying complaints or refusing to report the crime at all, which leads to loss of evidence and time.

- **Lack of Awareness:** Most citizens are unaware that no police officer can arrest or threaten legal action over a phone call. This lack of legal literacy aids the scammer's manipulation.

- **Limited Cybercrime Infrastructure:** Although India has strengthened its cybercrime infrastructure, police departments in smaller towns may lack the technical expertise or resources to track digital crimes effectively.

### Enforcement Challenges

As digital arrest scams grow increasingly sophisticated and widespread across India, enforcement agencies face numerous challenges in investigating, preventing, and prosecuting such crimes. These scams exploit a combination of legal ignorance, psychological manipulation, and technological anonymity—making them particularly difficult to detect and dismantle using traditional policing methods. Below are the key enforcement challenges faced by law enforcement authorities:

### Anonymity and Cross-Border Operations

One of the biggest challenges in digital arrest scams is the anonymity of the perpetrators. Most scammers use VoIP (Voice over Internet Protocol) calls, international SIM cards, VPNs, and fake digital identities to conceal their location and identity. Many operations are run from outside India, often in cybercrime hubs across Southeast Asia, Africa, or the Middle East. This cross-border nature of cybercrime complicates jurisdiction and makes it difficult for Indian police to take direct legal action without international cooperation or mutual legal assistance treaties (MLATs).

### Lack of Legal Awareness among Victims

Most victims, especially the elderly and digitally inexperienced, are unaware that no law permits arrests via video or phone calls. Their lack of awareness about legal procedures makes them highly vulnerable to intimidation and manipulation. This results in delayed reporting or, in some cases, no reporting at all. Without timely complaints, law enforcement loses critical leads and opportunities for digital forensics.

**Technical and Infrastructure Limitations**

Many local police stations lack the technical tools and expertise to investigate complex cyber frauds. While metropolitan cybercrime units may be equipped with advanced tools, district-level enforcement mechanisms are often under-resourced. There is also a shortage of trained cybercrime investigators, digital forensic experts, and cross-domain collaboration between police, telecom, and financial authorities.

**Rapid Disposal of Evidence**

Scammers often operate through temporary or disposable infrastructure including burner phones, fake email accounts, and rapidly created bank accounts or UPI IDs. Once a scam is completed, they quickly dismantle the setup and move on. This short operational window makes evidence collection challenging. Additionally, digital traces are often hosted on foreign servers or encrypted platforms, making forensic retrieval slow and difficult.

**Legal and Procedural Delays**

Even when suspects are identified, prosecution is often delayed due to complex procedural requirements, such as inter-state coordination, forensic verification, and digital evidence authentication. Courts also face a backlog of cybercrime cases, and the lack of specific laws targeting impersonation-based digital scams slows down conviction rates. The absence of a well-defined legal category for "digital arrest" further complicates case classification and charge framing.

**Weak Inter-Agency Coordination**

Effective response to digital arrest scams requires collaboration between police, financial institutions, telecom companies, and cyber cells. However, in practice, this coordination is often fragmented. Delays in freezing fraudulent accounts, tracking IPs, or obtaining telecom data can allow scammers to escape undetected.

**Role of Enforcement Agencies**

The Indian government has taken steps to address rising cybercrime through:

- Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs.
- CERT-In (Indian Computer Emergency Response Team) for technical response and incident reporting.
- State Cyber Crime Cells for regional enforcement.
- Launch of the National Cyber Crime Reporting Portal (www.cybercrime.gov.in).

Additionally, police departments in states like Maharashtra, Karnataka, West Bengal, and Telangana have started issuing public alerts and press notes warning citizens about digital arrest scams.

**Need for Legal Reform and Public Education**

Given the increasing frequency and sophistication of digital arrest scams, there is an urgent need for:

- Dedicated laws or guidelines that recognize and define cyber-enabled impersonation frauds like digital arrest.
- Fast-track investigation and prosecution units for cybercrimes involving impersonation.
- Greater public legal awareness campaigns, including in regional languages, to educate citizens on their rights and the proper procedure for arrests.
- Stronger international collaboration to trace and dismantle cross border cybercrime networks.

**Comparative Perspectives**

The rise of digital arrest scams in India reflects a broader global trend in cyber enabled impersonation fraud. While the term "digital arrest" may be unique to the Indian context, similar tactics where scammers impersonate law enforcement or government authorities to extort money or data have been reported in various countries. A comparative perspective helps contextualize India's challenges, highlights international best practices, and underscores the need for cross border cooperation in cybercrime enforcement.

**United States: "Government Impersonation Scams"**

In the United States, the Federal Trade Commission (FTC) and Federal Bureau of Investigation (FBI) have long tracked a variant of digital arrest scams known as "government impersonation frauds".

Victims are contacted by individuals claiming to be from the IRS (Internal Revenue Service), Social Security Administration, or law enforcement agencies, and told that their social security number is linked to crimes like drug trafficking or tax evasion. They are then coerced into making payments via wire transfers, gift cards, or crypto currency to avoid arrest.

The FTC’s Consumer Sentinel Network reported over 100,000 impersonation scam complaints annually, with financial losses exceeding $500 million.

Legal Response:

- The U.S. has specific laws against fraud, identity theft, and impersonation of federal officials.
- Aggressive public awareness campaigns (e.g., “Hang Up on Fraud”) have helped reduce victimization.
- The Elder Justice Act addresses scams targeting older adults, who are frequently targeted by these frauds.

**China: “Police Video Call” Scams**

China has seen a significant rise in scams that resemble India's digital arrest model. Victims receive a call from someone posing as a police officer or customs agent, claiming a parcel in their name contains illegal items. The scammer then initiates a video call during which they show fabricated police documents and instruct the victim to transfer money to avoid legal consequences.

These scams often originate from overseas call centers, particularly in Southeast Asia, and target affluent or elderly citizens.

Legal and Technical Measures:

- China has implemented AI-based voiceprint verification and caller ID authentication to combat telecom fraud.
- The Public Security Bureau (PSB) works with Interpol and regional cybercrime task forces.

- China has also passed stricter Data Privacy and Anti-Telecom Fraud Laws (2021) to regulate digital communication.

**United Kingdom: "Fake Police" and Courier Fraud**

In the UK, similar scams are referred to as "Courier Fraud" or "Fake Police Scams." Victims are told by someone claiming to be from Scotland Yard or Action Fraud that their bank accounts are under investigation. To "protect" their money, they are told to transfer it to a "safe" account.

Older individuals are particularly at risk. The scam often involves multiple stages, including follow-up calls by people posing as bank officials or even police officers arriving at the victim's home.

Legal and Enforcement Strategies:

- Action Fraud, the UK's national fraud and cybercrime reporting centre, serves as a centralized platform for reporting such crimes.
- The Fraud Act 2006 and Computer Misuse Act 1990 provide legal backing.
- Banks are now obligated to use the "Confirmation of Payee" system to verify account holders before transfers.

**Australia: ATO and Border Force Scams**

In Australia, the Australian Taxation Office (ATO) and Australian Border Force are often impersonated in scams. Victims are told they owe money for customs violations or unpaid taxes and are threatened with arrest. Many are instructed to stay on the call and follow instructions, much like India's digital arrest tactics.

Government Actions:

- The Australian Competition and Consumer Commission (ACCC) run the Scam watch portal to monitor and warn about scams.
- Telecom companies are required by the Telecommunications (Consumer Protection and Service Standards) Act to implement scam-blocking technology.
- Australia also collaborates with international cybercrime units through the Five Eyes Alliance.

**Lessons for India**

India's "digital arrest" scam is part of a global ecosystem of impersonation fraud, but with unique local dimensions such as trust in uniformed authority, linguistic diversity, and variable digital literacy.

India can learn from international best practices:

- Centralized fraud reporting systems (like Action Fraud or Scam watch).
- Caller authentication and call-blocking infrastructure.
- Legal reforms that specifically address digital impersonation and emotional coercion.
- Targeted awareness campaigns to educate the public, especially the elderly.
- Cross-border cooperation for tracing scammers operating from international call centers.

Additionally, incorporating technological solutions, such as AI-based voice authentication, real-time scam databases, and secure digital ID verification, can significantly reduce victimization.

## Conclusion

The rise of digital arrest scams in India marks a dangerous evolution in cyber-enabled crimes, where fear, authority, and technology are weaponized to manipulate innocent individuals. These scams typically involve fraudsters impersonating law enforcement officials or government agencies, coercing victims often over Whatsapp or video calls into believing they are under investigation or facing imminent arrest. The victims are then tricked into transferring money under the pretext of bail, verification, or to avoid supposed legal consequences. This form of digital fraud, while technologically simple, is psychologically complex, exploiting public ignorance of legal procedures and the innate fear of authority. What makes this crime particularly insidious is that it doesn't rely on hacking or malware, but rather on deceit, impersonation, and emotional manipulation, creating a unique enforcement and legal challenge.

"Digital arrest" has no legal foundation under Indian law. The procedures for arrest, as codified in the Criminal Procedure Code (now updated under the Bharatiya Nyaya Sanhita, 2023), require physical custody, formal documentation, and judicial oversight. Arrests via phone calls or video chats are entirely illegitimate, yet the absence of a specific legal provision to address such impersonation-based digital frauds hampers effective prosecution. Currently, enforcement agencies must rely on generic sections of the IPC/BNS (such as cheating, impersonation, and extortion) and provisions from the IT Act, 2000 (such as Sections 66C and 66D), which, while helpful, are not adequately tailored to tackle the cross-border, anonymous, and tech-enabled nature of these crimes. Furthermore, the lack of a centralized database of such frauds, combined with low conviction rates and limited inter-agency coordination, further complicates the matter.

In response to this growing menace, a three-pronged strategy is required. *First*, legal reforms must be undertaken to specifically define and criminalize digital impersonation of public authorities, particularly when used to extort or threaten individuals. Such provisions must also include procedural guidelines for evidence collection and digital authentication. *Second*, institutional capacity-building is crucial. Dedicated cybercrime units at the district level, cross-agency cooperation, AI-powered fraud detection systems, and integration with telecom and banking networks are essential for real-time action and deterrence. *Finally*, citizen awareness is perhaps the most powerful tool in prevention. A digitally literate population that knows its legal rights and is trained to identify red flags is far less likely to fall prey. Public awareness campaigns run across TV, radio, social media, and even UPI/payment apps must clearly communicate that no government official or police officer can conduct an arrest or demand payments over phone or Whatsapp.

In conclusion, digital arrest scams are not just a cybercrime issue they are a threat to digital trust, personal dignity, and public confidence in the rule of law. Tackling them requires more than law enforcement; it calls for a holistic approach involving legal innovation, technological preparedness, institutional coordination, and civic empowerment. In the digital age, where governance and crime have both gone online, ensuring that citizens are protected from fraud and fear is not a privilege it is a fundamental right. India must rise to this challenge, not only to protect its people but also to set a global precedent for cyber resilience in the face of 21st-century threats.

In addition to that, digital arrest scams present a multi-dimensional enforcement challenge involving legal, technological, operational, and psychological aspects. To address these, India needs upgraded cybercrime infrastructure, better-trained personnel, legal reforms, and robust inter-agency and international cooperation. Without these, the digital arrest phenomenon may continue to escalate and evolve beyond the reach of traditional law enforcement models.

### Suggestions

The emergence of Digital Arrest scams a form of cyber-enabled impersonation fraud is a growing threat to digital trust and public safety in India. Victims are tricked into believing they are under investigation by law enforcement and coerced into paying "digital bail" or providing sensitive information. While existing legal provisions partially address such frauds, there is an urgent need for comprehensive policy, legal, and systemic reforms. Below are key recommendations:

### Recognize and Define “Digital Impersonation Fraud” in Law

India’s legal framework currently lacks a specific statutory definition for scams like digital arrest. Although provisions under the Indian Penal Code (IPC) (now replaced by the Bharatiya Nyaya Sanhita, 2023) and Information Technology Act, 2000 offer partial remedies (e.g., Sections 66D, 420), enforcement becomes inconsistent without targeted definitions. A new legal category or provision specifically addressing digital impersonation of public authorities, criminalizing the act of posing as a law enforcement officer via digital means with intent to cheat or extort should be introduced

### Strengthen Cybercrime Investigation Units

Many states lack well-trained cybercrime teams, especially at the district and rural levels. These scams often go uninvestigated due to lack of capacity, technical expertise, or coordination challenges between law enforcement agencies and financial or telecom service providers. Specialized cybercrime cells in every district with trained digital forensics experts should be created. Regular training and certification programs should be made mandatory for law enforcement personnel dealing with cyber cases.

### Centralized Digital Fraud Reporting and Redressal System

While India operates the National Cyber Crime Reporting Portal but awareness and responsiveness remain low. Victims often don’t know where or how to report such frauds. So, a 24x7 national cyber fraud helpline for immediate intervention must be established. Also, integrate this helpline with banking systems to enable rapid freezing of fraudulent accounts. Encourage UPI apps, banks, and telecom operators to display fraud alerts and reporting options directly within their platforms.

### Mandatory Caller Authentication and Telecom Regulation

Scammers use spoofed numbers and international VoIP calls to impersonate Indian officials. Victims are unable to verify the authenticity of these calls. To tackle this Mandate a caller ID verification system like the “KYC-based caller name display” proposed by TRAI to help users identify genuine calls. Telecom providers must deploy AI-based spam/fraud detection systems and work closely with law enforcement to track suspicious communication patterns.

### Monitoring & Intelligence Gathering

Government agencies to monitor emerging patterns block known fraudulent IDs or numbers; coordinate with telecoms for trace backs.

### Public Awareness and Digital Literacy Campaigns

A large number of victims fall for digital arrest scams due to fear, confusion, and lack of awareness about actual police procedures. A nationwide, multilingual campaign through TV, radio, social media, and banking/telecom apps to educate the public should be launched. Messages should emphasize:

- No police arrest happens over Whatsapp or phone calls.
- Government agencies do not demand payments via UPI or digital wallets.
- Citizens have the right to legal representation and due process.

### International Collaboration

Many scammers operate from outside India, using infrastructure based in other countries. Isolated national action is insufficient. International cooperation must be enhanced through Interpol, CERT partnerships, and MLATs (Mutual Legal Assistance Treaties) to track, extradite, and prosecute cybercriminals abroad.

To effectively combat digital arrest scams, India must move beyond reactive policing and adopt a multi-stakeholder, tech-enabled, and legally robust approach. Legal reform, institutional strengthening, public awareness, and international coordination must work in tandem to protect citizens in an increasingly digital world.

### References

1. Information Technology Act, Available at https://legislative.gov.in, 2000.
2. Ministry of Home Affairs. (n.d.). Indian Cyber Crime Coordination Centre (I4C). Available at https://cybercrime.gov.in
3. India Today. India's first 'digital arrest' conviction: Nine people sentenced to life imprisonment. Available at https://www.indiatoday.in/india/law-news/story/indias-first-digital-arrest-conviction-nine-people-sentenced-to-life-by-bengal-court-2758042-2025-07-19, 2025.
4. Times of India. Bengal’s first ‘digital arrest’ scam: 9 convicted in ₹1 crore fraud. Available at https://timesofindia.indiatimes.com/india/in-a-first-9-sentenced-to-life-by-court-in-bengal-for-digital-arrest-fraud/articleshow/122773681.cms, 2025.
5. Federal Trade Commission. (n.d.). Government impersonation scams. Available at https://www.consumer.ftc.gov/articles/0206-government-impersonation-scams
6. Australian Competition and Consumer Commission. (n.d.). Scamwatch. Available at https://www.scamwatch.gov.au

7. Action Fraud (UK). (n.d.). Courier fraud and fake police scams. Available at https://www.actionfraud.police.uk
8. PRS Legislative Research. (n.d.). Bill Track – Bharatiya Nyaya Sanhita and IT Act updates. Available at https://prsindia.org/billtrack
9. Indian Computer Emergency Response Team (CERT-In). (n.d.). Cybersecurity alerts and guidelines. Available at https://www.cert-in.org.in