The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DIGITAL ARREST SCAMS: INDIA'S DEEPFAKE DILEMMA AND FIGHTBACK

Gunjan Chopra

INTRODUCTION: The Midnight Knock

*It's late at night. You're unwinding, perhaps scrolling through your phone, when a WhatsApp video call pops up from an unknown number. You answer, and a stern-faced "**CBI officer**" appears on screen. His badge shines, his uniform is exemplary and his tone is perfectly official. He accuses you of involvement in a money laundering racket, flashes a digital **"arrest warrant**" with your name and photo, and threatens that a police team is en route to your house. He insists you stay on the call for **"national security reasons**," forbids you from contacting anyone, and demands you to transfer money to "settle" the case. The officer's face and voice are undoubtedly convincing-thanks to **deepfake technology**. **Terrified,** you comply with the terms, isolated and coerced into draining your savings. **And by the time you realize it's a scam. The money is gone.***

This is not a scene from a thriller film. It's the reality of *digital arrest scams*- a new, high-tech **cybercrime** wave sweeping India. As these cases exploded in number, the government responded with its most ambitious counter-offensive action: ***Operation Chakra- V,*** a comprehensive, multi-agency initiative led by the **CBI** and the **Indian Cyber Crime Coordination Centre (I4C).**

The Anatomy of a Digital Arrest Scam

A **digital arrest scam** is a form of cyber fraud where criminals impersonate law enforcement or government officials. Victims are accused of serious crimes-*money laundering, drug trafficking, or identity theft*-and threatened with immediate arrest unless they pay a

"*settlement*" or provide *sensitive personal information*. The scam typically unfolds as follows:

Step 1: The Hook

Scammers contact victims via phone, Whatsapp, Telegram, or Skype, often using phone numbers that *appear official*. The caller claims to be from the police, *CBI, Narcotics Control Bureau, or even the RBI.*

Step 2: The Deepfake Deception

Here's where technology makes things terrifying. Using ***deepfake AI***, scammers generate videos or audio clips that *convincingly mimic real officials*-sometimes even using the faces and voices of actual officers or celebrities. Victims are shown fake *arrest warrants*, *court orders*, or even ***a fake "police stations" setup*** to heighten the illusion.

Step 3: The Threat

The victim is accused of a serious crime-money laundering, drug trafficking, or cybercrime. The scammer shares personal details (often found on social media or leaked databases) to build credibility. And the threats escalate: *"If you disconnect, you'll be arrested. Cooperate, or your family will be notified."*

Step 4: The Digital Detention

Victims are ordered to stay on a video call, sometimes for hours or days. They are *isolated* from friends and family, forbidden from contacting anyone, and subjected to relentless *psychological pressure.*

Step 5: The Extortion

The "*official*" demands immediate payment-sometimes in *multiple installments*- to "settle" the case. Victims are told to transfer money to bank accounts, *cryptocurrency wallets*, or through payment apps. Some are forced to *record confessions* or provide sensitive personal data.

Step 6: The Escape

Once the money is transferred, ***the scammers vanish.*** Victims are left *traumatized*, *ashamed*, and often *too embarrassed* to report the crime.

It is important to note that the term *"digital arrest" is a fiction*-**there is no such legal provision in India**. It's a *psychological weapon*, used to fear and urgency, making victims more likely to comply.

The Deepfake Threat: When Seeing Isn't Believing

A terrifying evolution in these scams is the use of **deepfake technology**. With AI, scammers can create videos and audio that perfectly mimic law enforcement officials, judges, or even the victim's family members. Deepfakes are used to *impersonate* police or government officials in live video calls, *forge audio messages* from trusted sources, *fabricate evidence*, such as fake arrest warrants or court orders or simulate the voices and faces of family members etc. increasing the psychological pressure.

This blur fiction makes the scam almost impossible to detect, even for tech-savvy individuals. The rapid spread of deepfake apps and AI tools has put this power in the hands of cybercriminals, making their threats more convincing and their demands more urgent.

The Digital Arrest Crisis: Numbers That Shock

The digital arrest scam epidemic has grown at an alarming pace. According to official data:

- **2022: 39,925 cases**, **₹91.14 crore** lost
- **2023: 60,676 cases, ₹339.03 crore** lost
- **2024: 1,23,672 cases**, **₹1,935.51 crore** lost
- **Jan–Feb 2025: 17,718 cases**, **₹210.21 crore** lost

Losses have multiplied *21-fold* in just three years. **In 2024** alone, Indians lost nearly **₹2,000 crore** to digital arrest scams. The government has blocked over **83,000 WhatsApp accounts**, nearly **4,000 Skype IDs**, and more than **7.8 lakh SIM cards** linked to these frauds. Experts believe *the true scale is even greater*, as many victims do not report their losses due to shame, fear, or lack of awareness. The *psychological impact* is immense, with victims suffering not just financially, but emotionally and socially.

Victims' Stories: The Human Toll

The impact goes beyond money. Victims suffer deep psychological trauma, shame, and social isolation. It is not the case that only uneducated people have been the victims of these scams. The digital arrest scam has affected very educated people of India, be it a doctor, a businessman, a social media influencer, a retired professor or a retired army officer. They have been defrauded by these scammers and lost crores of rupees. It was due to a lack of awareness of the fact that there is a thing called 'Digital Arrest' in legal procedure.

Here are some real-life cases:

1. The 86-Year-Old Mumbai Woman's Ordeal (2024–2025)

An 86-year-old woman from Mumbai became the victim of one of India's longest-running digital arrest scams, losing more than ₹20 crore over several months. The scam began when she received a call from individuals posing as police officers, who claimed her Aadhaar card had been misused to open a bank account involved in illegal activities like money laundering. The scammers threatened her with legal action, saying both she and her family would be implicated unless she cooperated. To avoid these *fabricated* charges, she was *coerced* into transferring large sums to numerous bank accounts. Throughout the ordeal, the fraudsters kept her under "digital arrest," instructing her *not to share* her situation with anyone and using fake video calls with people impersonating police and government officials to create a sense of *urgency* and *authenticity*.

2. Mr. Gupta's Bharatpur Scam (2025)

Mr. Gupta, a retired resident from Bharatpur, Rajasthan, received a WhatsApp call from someone claiming to be a Srinagar police officer. The caller alleged that Mr. Gupta's son, an engineer in Jammu & Kashmir, was involved in *anti-national activities* and would be booked under terror charges. Exploiting the fact that Mr. Gupta could not reach his son, the scammer **demanded ₹5 lakh** as a "*surety*" and told him he was under ***"digital arrest***," instructing him to remain isolated and not communicate with anyone. Under immense *emotional pressure and panic*, Mr. Gupta ended up transferring ₹1.2 lakh before realizing he had been duped by a financial scam.

3. Padma Bhushan Recipient S.P. Oswal's Ordeal (August 2024)

In August 2024, Padma Bhushan awardee and Vardhman Group chairman S.P. Oswal was defrauded **of ₹7 crore** after being kept under digital arrest by cybercriminals posing as CBI officers. The scammers set up a *fake Supreme Court hearing* over Skype, with an impersonator playing the Chief Justice of India. They presented convincing documents, including a fabricated Supreme Court case paper, and *coerced* Mr. Oswal into adhering to a "*24-hour surveillance order"* with strict requirements, such as not blocking his camera and not contacting anyone *without their consent*. Over two days, Oswal was manipulated into transferring the money, believing he was complying with legal authorities.

These cases show how digital arrest scams exploit fear, authority, and isolation to manipulate victims into handing over vast sums of money. The scammers' use of technology, *impersonation*, and *psychological pressure* makes these crimes particularly devastating and difficult to detect.

Why India Is at a Vulnerable stage:

Several factors make India a hotspot for digital arrest scams:

1. The Digital Boom

India has over **800 million internet users**, with millions joining the digital economy every year. Many are *first-time users*, *unfamiliar* with cyber risks and *digital privacy*.

2. Social Engineering

Scammers exploit cultural respect for authority and fear of legal trouble. Even educated, tech-savvy individuals can be manipulated when threatened with arrest or public disgrace.

3. Telecom and Banking Loopholes

The **KYC norms** and **weak verification** at telecom and banking points-of-sale enable fraudsters to obtain SIM cards and open mule accounts with fake documents.

4. Data Breaches

Criminals access *leaked personal data*, making their threats more credible and their manipulation more effective.

5. International Syndicates

Many scams originate from ***call centers*** in Myanmar, Cambodia, and other countries, making enforcement and extradition challenging.

6. Low Cyber Literacy

Despite rapid digital adoption***, cyber hygiene*** and awareness remain low, especially among the elderly and rural populations.

Legal Framework for Digital Arrest Scams under Indian Law

There is **no legal provision** or **recognition** of "***digital arrest***" under Indian laws. Law enforcement agencies in India do not have the authority to arrest or detain anyone through digital means such as video calls, emails, or instant messaging. Any claim of a ***"digital arrest***" is fraudulent and not supported by any statute or regulation.

Key Legal Provisions Addressing Digital Arrest Scams

1. Information Technology Act, 2000:

This is the cornerstone of India's cyber law framework. **Section 66C** penalizes identity theft, and **Section 66D** deals with cheating by impersonation using computer resources, which are directly applicable to digital arrest scams. **Section 43** and **Section 43A** address unauthorized access and data theft, providing for compensation and penalties. **Section 70B** empowers the ***Indian Computer Emergency Response Team (CERT-In)*** to handle and respond to cyber incidents, including scams.

2. Bharatiya Nyaya Sanhita, 2023 (formerly IPC):

Provisions such as impersonation of a public servant, ***cheating, forgery, extortion, and criminal intimidation*** **(Sections 204, 351(4), etc.)** are invoked in digital arrest scam cases. These sections provide for imprisonment and fines for offenders who impersonate officials, threaten victims, or extort money using digital means.

3. Bharatiya Nagarik Suraksha Sanhita, 2023 (formerly CrPC):

The code governs the procedure for arrests, searches, and seizures, including in cybercrime cases. It allows law enforcement agencies to *confiscate* electronic devices, *freeze accounts*, or *block access* to digital platforms during investigations, but does not allow for digital arrest as a mode of lawful detention.

4. Bharatiya Sakshya Adhiniyam, 2023 (BSA)

Sections 65A and 65B provide for the admissibility of electronic records and digital evidence in court.

5. Digital Personal Data Protection Act, 2023:

Strengthens data privacy and mandates higher standards for handling personal data, indirectly supporting the fight against digital impersonation and fraud.

6. Judicial and Government Response

The **Rajasthan High Court** and **other courts** have clarified that there is *no concept of digital arrest in Indian law*, and any such threats are illegal. Notices of arrest must be served through traditional, legally recognized means, not via WhatsApp or video calls. The Government has issued advisories, blocked thousands of fraudulent accounts, and launched public awareness campaigns to educate citizens about the illegality of digital arrest scams and the proper procedures for lawful arrest

Operation Chakra-V: India's Multi-Pronged Counterattack

Honourable Prime Minister of India, **Shri Narendra Modi**, in the '***Man Ki Baat***' radio programme, in **October 2024**, *warned* citizens of India against the digital arrest scam, which can eat up their hard-earned savings. The central government and Telecom Service providers have devised a system to identify and block spoofed calls. To increase awareness among the masses, *caller tunes* to increase the awareness of online scams are released. Social media, electronic media, newspaper advertisements and announcements in Delhi Metros have been modes of spreading awareness among the masses. Adding to the awareness the government has released *a toll-free number 1930* to assist people in lodging online cyber complaints.

Recognizing the scale and sophistication of digital arrest scams, the Indian government launched **Operation Chakra-V** in **2025-*a comprehensive, multi-agency initiative*** led by the **CBI** and the **Indian Cyber Crime Coordination Centre (I4C).**

Operation Chakra-V's strategy is both broad and deep:

Authorities have conducted *coordinated raids* across multiple states, targeting *illegal SIM card vendors*, mule account operators, and call centers that serve as the ***backbone*** of these scams. In one high-profile operation, police in ***Uttar Pradesh*** arrested over twenty individuals involved in the supply of *pre-activated SIM cards* to scam syndicates. In ***Mumbai,*** a major racket was busted where former telecom employees had been leaking VIP customer data to fraudsters, enabling highly targeted attacks.

Financial institutions have been roped in to freeze thousands of suspicious accounts linked to scam proceeds. The **I4C**, in partnership with the **RBI** and **leading banks,** has implemented real-time transaction monitoring to identify and halt fraudulent transfers. In several cases, crores of rupees have been recovered from *shell companies* and *mule accounts* before they could be laundered overseas.

Technology has played a key role. Cybercrime units have deployed *AI-driven analytics* to skim through millions of *call records*, identifying *patterns* and *keywords* commonly used in digital arrest scams. This intelligence has led to the takedown of dozens of WhatsApp groups and Telegram channels used for recruiting money mules and spreading scam scripts.

Public awareness is another pillar of ***Operation Chakra-V***. The government has launched monthly "*Cyber Jagrukta Diwas*" (Cyber Awareness Day) events, where police and cyber experts conduct workshops in schools, colleges, and corporate offices. Viral *video campaigns* dramatize real-life scam stories, teaching viewers how to recognize and resist digital arrest tactics.

International cooperation has also been crucial. Indian agencies have *shared intelligence* with counterparts in ***Southeast Asia, the Middle East, and the United States***, leading to joint operations against scam call centers in ***Cambodia and Myanmar***. The **FBI** and **INTERPOL** have provided expertise in tracking *cryptocurrency* flows and identifying *cross-border money laundering routes.*

Global Lessons and International Cooperation in Digital Arrest Scams

Digital arrest scams are not unique to India; *they have become a cross-border menace,* with criminal syndicates operating from multiple countries and targeting victims worldwide. International cooperation is essential in combating these scams, as syndicates often exploit legal and jurisdictional gaps between nations.

Countries such as **Singapore, the United States**, and members of the **European Union** have established bilateral and multilateral agreements to facilitate the rapid sharing of intelligence, the freezing of suspect bank accounts, and the extradition of key suspects. India has joined global initiatives such **as INTERPOL's cybercrime task forces** and the **Budapest Convention on Cybercrime**, which provide frameworks for joint investigations and evidence sharing.

One notable example is the *collaboration* between **Indian and Southeast Asian authorities**, which led to the *dismantling of a major scam hub in Cambodia* that targeted Indian citizens. Similarly, **the FBI has** assisted Indian agencies in tracing *cryptocurrency transactions* used to launder scam proceeds, resulting in the recovery of significant amounts of stolen funds.

Despite these successes, challenges remain. Criminals frequently use *encrypted messaging* apps and *cryptocurrency wallets* to evade detection. *Jurisdictional hurdles*, differences in legal standards, and delays in mutual legal assistance can slow down investigations. Continuous international dialogue, *harmonization* of cybercrime laws, and regular joint training exercises are needed to keep pace with the evolving threat.

Recommendations: Strengthening India's Defences Against Digital Arrest Scams

To effectively counter digital arrest scams, India must adopt a **multi-layered strategy** that addresses prevention, enforcement, *victim support*, and international collaboration. Recommendations, specifically in the context of digital arrest scams, include:

1. Legal and Regulatory Measures

Establish *clear legal provisions* criminalizing digital impersonation of law enforcement and judiciary, with stringent penalties for those found guilty. Mandate telecom and financial

institutions to *implement robust KYC* and real-time *transaction monitoring* to detect and block accounts used for digital arrest scams. Create a *fast-track judicial mechanism* for the freezing and recovery of scam proceeds, ensuring that victims can reclaim their losses swiftly.

2. Law Enforcement and Victim Support

Set up *dedicated cybercrime units* in every district, equipped with the *latest forensic tools* and staffed *by trained investigators* and victim counsellors. Launch a nationwide victim support helpline offering psychological counselling, *legal advice*, and assistance with reporting and recovering losses. Foster *continuous training* for police and prosecutors on the latest scam tactics and digital evidence gathering.

3. Public Awareness and Education

Integrate *digital scam awareness modules* into school and college curricula, emphasizing the tactics used in digital arrest scams. Conduct regular outreach campaigns targeting vulnerable groups, especially the elderly and those less familiar with digital technology. *Partner with private sector organizations* and *NGOs* to spread awareness through workshops, seminars, and digital media.

4. International Cooperation

Strengthen bilateral and multilateral agreements for the sharing of intelligence, freezing of assets, and extradition of scam ringleaders. Participate actively in global cybercrime task forces and conventions, ensuring India's voice is heard in shaping international cyber policy. Develop joint *training and capacity-building programs* with international partners to stay ahead of emerging scam techniques.

Conclusion: Building Resilience in a Digital Age

Digital arrest scams represent a ***new frontier in cybercrime***-one that exploits not just technology, but human psychology and social trust. **Operation Chakra-V** has demonstrated India's resolve to fight back through enforcement, technology, and international partnership. *Yet, the ultimate defence lies in awareness, education, and community support.*

As the digital landscape evolves, so must our strategies. Every citizen, institution, and policymaker has a role to play in building a safer digital India. *The next time your phone rings with a threat of arrest, remember: pause, verify, and report.* ***In this fight, knowledge is power-and resilience is our greatest asset.***