Rewind: Arrested on a screen — Inside India’s digital arrest fraud

telanganatoday.com/rewind-arrested-on-a-screen-inside-indias-digital-arrest-fraud

Telangana Today February 7, 2026

Digital arrest fraud exposes how fear, weak enforcement and regulatory gaps collide, proving that awareness is no substitute for urgent regulatory action

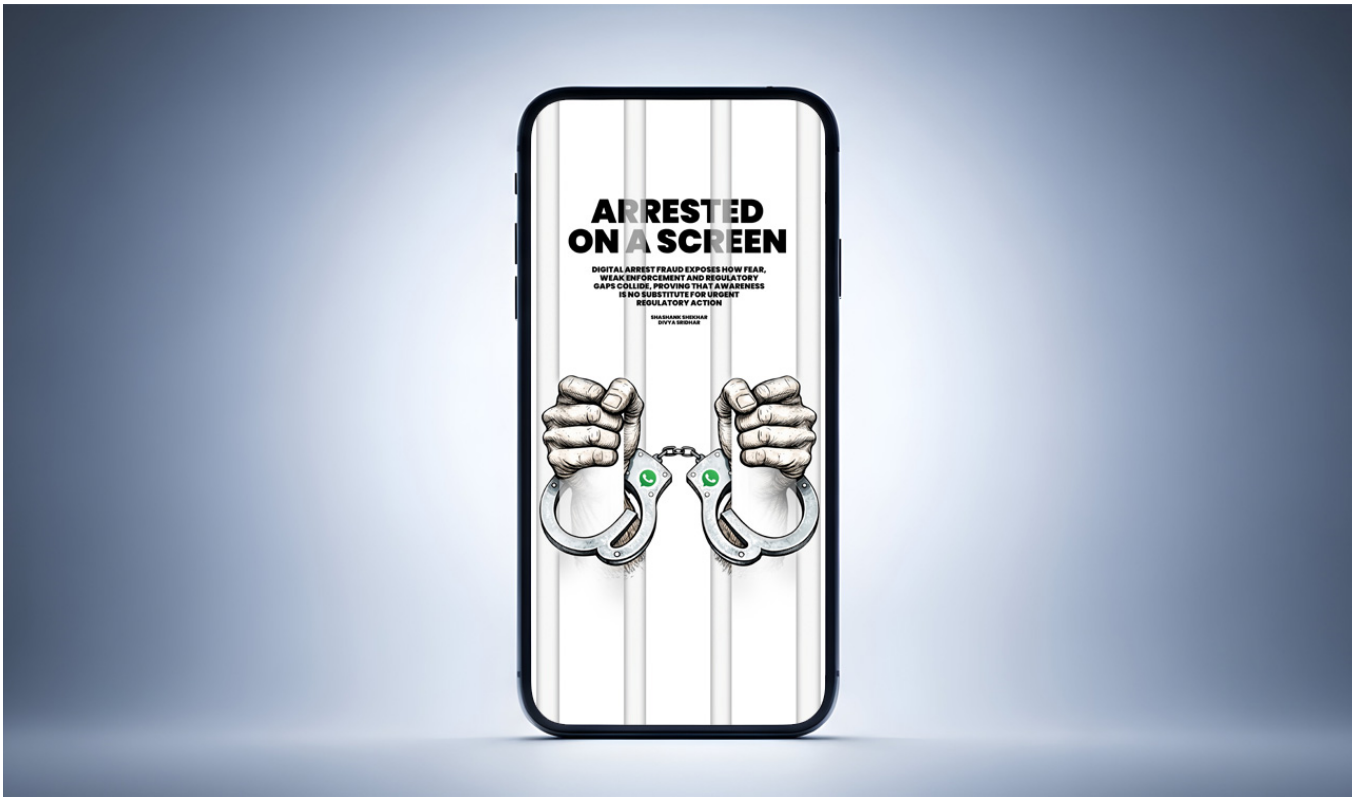

Illustration: GuruG

By Shashank Shekhar, Divya Sridhar

In recent months, thousands of citizens have been ‘arrested’ without even stepping into a police station. A video call flashes a uniform and a forged warrant on screen, accompanied by a stern voice warning of immediate detention unless the victim cooperates. What unfolds is not law enforcement, but fraud, a sophisticated cybercrime now commonly known as ‘digital arrest’.

Also Read

- Digital Arrest, the con that thrives on fear of law enforcement
- Editorial: New ideas to fight digital arrest

The name itself is a misnomer. Indian law does not have any concept of arrest via video call or screen-shared warrant. Yet the success of this scam lies in how convincingly it imitates the rituals and language of the criminal justice administrative system. Cybercriminals have turned authorities under the law into a tool of deception, weaponising the fear of law itself.

The Illusion of Authority

Digital arrest fraud generally entails the impersonation of law enforcement personnel or officials from agencies such as the Central Bureau of Investigation (CBI), Enforcement Directorate (ED), or Customs authorities. Victims are informed of their association with money laundering, narcotics trafficking, or courier fraud schemes. The situation intensifies rapidly: separation from family, constant surveillance via video calls, and requests for “verification payments” to prevent arrest.

The efficacy of this scam arises not merely from technological expertise, but from its psychological design. The threat of arrest carries stigma, uncertainty and panic. When presented with seemingly official attributes, it eclipses rational scepticism. That such tactics succeed highlights a deeper vulnerability — not merely digital illiteracy, but legal illiteracy.

Why the Fraud Works

Digital arrest **scams** thrive at the intersection of fear and asymmetry. Most citizens encounter the criminal justice system at the moment of crisis. The laws relating to arrest, search, seizure, rights of the accused, requirement of physical custody or judicial oversight remain poorly understood. This knowledge gap gives criminals the opportunity to substitute procedure with performance.

Further, the perceived imbalance of power between authorities and individuals discourages questioning. Victims fear that refusal to comply may itself be considered an offence. In such an environment, urgency replaces verification. The fraud succeeds, not in the absence of law, but in the shadow of how law is commonly perceived: distant, punitive and beyond question. It does not exploit a legal vacuum; it exploits public fear of the law.

It’s a scam — If it’s on a screen and demands money

- **The Video Call Arrest:** Indian law enforcement will never arrest you, record a statement, or serve a warrant via WhatsApp, Skype, or Zoom
- **The ‘Secret’ Probe:** Genuine officials will never ask you to stay on a video call for hours or prevent you from contacting a lawyer or family member.
- **Money demands:** No government agency will ever ask for a “verification deposit” or “security payment” into a private bank account.

Is the Law Ineffective?

It would be incorrect to argue that India lacks legal tools to address the issue of **digital arrest.** India’s legal framework sufficiently contains provisions such as Personating a public servant (Section 204 BNS), Cheating (Section 318 BNS), Cheating by personation (Section 319 BNS), Criminal Intimidation (Section 351 BNS), Extortion (Section 308 BNS), Cheating by personation using a computer resource (Section 66D, IT Act), and Identity theft (Section 66C, IT Act). Dedicated cybercrime portals and helplines exist, with repeated advisories issued by enforcement agencies.

The problem lies in the enforcement deficit and institutional lag. Cybercriminal networks operate across jurisdictions, often beyond Indian borders. Between 2020 and 2022, according to the National Crime Records Bureau (NCRB) report, only about 1.6% of registered cybercrime cases led to convictions across all States — ie, just 2,706 convictions of the roughly 1,67,000 cybercrime cases.

According to the 'Crime in India' report, the number of cases registered under the **cybercrimes** category rose to 86,420 in 2023 from 65,893 cases in 2022. The crime rate under this category increased from 4.8% in 2022 to 6.2% in 2023. Conviction rates remain poor, investigation is slow, and recovery of funds continues to be the exception rather than the norm. The law on paper struggles against the speed and scale of digital crime in practice. When law exists only on paper and criminals act with impunity, deterrence collapses, and advisories ring hollow without enforcement.

State's Response and Its Limits

A detailed reply by the Ministry of Home Affairs in the Lok Sabha on December 2, 2025, illustrates that to strengthen enforcement, the government has established the Indian Cyber Crime Coordination Centre (I4C), launched the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) for public reporting, and operationalised the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), which has helped save over Rs 7,130 crore through more than 23.02 lakh complaints.

Through coordinated action, authorities reported blocking over 11.14 lakh SIM cards and 2.96 lakh IMEIs linked to cybercrime, alongside multi-agency efforts including the Cyber Fraud Mitigation Centre and enhanced forensic support to state law enforcement. The government has also rolled out nationwide awareness campaigns through media, caller-tunes and outreach programmes to educate citizens about such scams. These are necessary steps.

However, advisories function primarily as awareness tools. They do little for victims in the moment of crisis, when fear eclipses recall. They also do not impose systemic obligations on digital intermediaries whose platforms enable such scams at scale. Awareness without structural safeguards leaves citizens exposed. Awareness is not protection. The response to digital arrest fraud must, therefore, move beyond alerts towards a comprehensive regulatory strategy.

Prevention: Stop Before It Starts

Effective prevention must begin by stripping digital arrest fraud of its core asset: the appearance of lawful authority. This requires a clear institutional rule that no law-enforcement agency may initiate arrest, investigation or monetary demands through video calls, messaging platforms or private numbers. Such communication protocols must be standardised nationally and publicly notified, with agencies restricted to verifiable channels — official landlines, registered email domains, and in-person procedures — leaving no ambiguity for **citizens** to exploit.

Telecom service providers should be assigned obligations that are technically feasible and within existing regulatory reach. Rather than behavioural surveillance, the focus must be on number integrity and misuse control. Telecom operators should strictly implement caller line identification verification to prevent the spoofing of law enforcement numbers, with flagged numbers subject to time-bound suspension and mandatory re-verification rather than discretionary blocking.

Prevention: Minimising Harm to Victims

Even the most robust preventive framework cannot eliminate fraud entirely. Protection, therefore, must be designed around speed, certainty and victim support, not post-facto sympathy. Financial harm in digital arrest scams escalates within minutes, making immediate fund freezing the single most effective protective measure. While complete recovery remains challenging due to rapid cross-border fund transfers, the UK's approach *(see Lessons from the UK)* offers instructive precedent. Under English law, financial institutions are required to implement verification protocols before processing transfers, particularly for large sums to new payees. Until verification is completed, transfers should be frozen. Similar mandatory verification mechanisms could significantly slow the movement of fraud proceeds, creating critical windows for intervention.

Lessons from the UK

The United Kingdom's experience with Authorised Push Payment (APP) scams, where victims are tricked into authorising payments to fraudsters, offers valuable lessons for India. Recognising the scale of the problem, in 2024, the Payment Systems Regulator introduced mandatory reimbursement requirements for most APP scam victims, with banks required to reimburse victims up to 85,000 pounds within five business days unless the customer acted with gross negligence. This shift placed greater responsibility on financial institutions, incentivising stronger fraud prevention. Alongside deposit protection (up to 85,000 pounds) under the Financial Services Compensation Scheme, the approach demonstrates how regulation can balance consumer protection with institutional accountability.

Banks and payment intermediaries should be placed under a statutory obligation to act on first complaints through the cybercrime reporting system, with clear timelines for provisional freezes and account marking, rather than leaving victims to navigate fragmented grievance processes. Police responses must be similarly structured. **Cybercrime** complaints should trigger time-bound acknowledgements, standard operating procedures and designated points of contact, reducing both delay and intimidation for victims. Treating such complaints as routine financial disputes rather than coercive crimes undermines confidence and recovery.

Protection must also extend beyond financial remediation to include legal and psychological support, especially for elderly and first-time victims. A system that approaches victims with suspicion or moral judgement not only compounds trauma but also actively discourages reporting, allowing fraud networks to continue unchecked.

Prohibition: Making Impersonation Costly

Finally, prohibition requires sharper deterrence. While enhanced penalties alone may not deter sophisticated criminal networks, they become effective when coupled with comprehensive enforcement. Impersonation of public authority in digital spaces should attract stringent penalties, recognising the unique coercive power such acts wield. However, the focus must extend beyond individual perpetrators to systematic ecosystem disruption.

This requires coordinated action across multiple fronts: asset seizure and confiscation of proceeds; international cooperation through mutual legal assistance treaties and real-time information sharing; and aggressive targeting of facilitators — mule account holders, SIM card suppliers, payment gateway operators, and call centre infrastructure providers.

Technology companies and telecom operators that enable such operations must face regulatory consequences for non-compliance. Jurisdictions harbouring these networks, often neighbouring countries with weak enforcement, must also face diplomatic and economic pressure to act.

Punishing individual callers is insufficient; the **goal** must be dismantling the ecosystem that sustains digital arrest fraud. This requires disrupting financial channels through stronger Know Your Customer (KYC) norms, real-time transaction monitoring, swift account freezes, and proactive law enforcement investigation using cyber forensics.

Arrest is Physical

Digital arrest fraud exposes a simple truth about modern governance: as public services move online, the symbols of authority have become easier to imitate than to verify. The answer is not to abandon technology, but to ensure that legality travels with it. In a constitutional democracy, arrest is not a threat over a call, or a payment extracted through fear: it is a serious act carried out openly, through procedure and accountability. When citizens are made to believe otherwise, what is lost is not just money, but trust.

The state's task is therefore urgent: to make the law visible, understandable and impossible to fake. The legitimacy of law depends not only on its enforcement, but on its recognisability, and in an age of digital deception, that recognisability must be built, protected and constantly reinforced.

(Shashank Shekhar is Assistant Professor of Law, Lloyd Law College. Divya Sridhar is Assistant Professor of Law, Jindal Global Law School)