DIGITAL ARREST: WHEN SCAMMERS BECOME POLICE, AND WHATSAPP BECOMES JAIL

Sneha Yadav*

ABSTRACT

'Digital Arrest' scams pose a significant challenge in the evolving landscape of cybercrime in India. These fraudulent schemes include cybercriminals impersonating police officers, government officials, or investigative agencies and using digital communication platforms such as WhatsApp and video conferencing applications to intimidate victims into believing they are under lawful arrest or investigation. This article examines the concept of digital arrest as a legal observation, clarifies that no such procedure exists under Indian law, and argues that arrests can only be made in accordance with India's statutory and constitutional safeguards. It further explores the criminal liability of perpetrators under laws and cyber offences. By drawing attention to the methods used by scammers, the legal remedies available to victims, and preventive measures for citizens, the article highlights the legal urgency of awareness among citizens and digital vigilance in combating this growing cyber threat.

Keywords: Digital Arrest, Digital Scam, Cybercrime, Constitutional Right.

INTRODUCTION

In the early days of the internet, cybercriminals were limited to defacing websites and pulling harmless pranks. Fast forward to today, and cybercrime has evolved into a sophisticated, ever-changing industry, with fraudsters constantly adapting to new technologies and targeting millions of unsuspecting victims.

The year 2024 witnessed a surge in cyber scams, particularly those involving digital arrest schemes. These scams have now expanded beyond basic online fraud, resembling large-scale operations akin to the infamous Jamtara scams. The targets of these frauds have become

*BA LLB, FOURTH YEAR, KANORIA SCHOOL OF LAW FOR WOMEN, JAIPUR.

increasingly diverse, including high-ranking officials, journalists, security personnel, and even innocent elderly individuals. Cybercrime has gone from a distant threat to a pervasive, everyday reality; Indians lost sensitive data and crores of rupees to digital arrest scams in 2024 alone.[1] Unlike general cyber fraud, a digital arrest scam involves criminals impersonating law enforcement officials to intimidate victims into transferring money or sharing sensitive information.[2]

'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime and digital arrest scams through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2022. Specific data regarding digital arrest scams is not maintained separately by NCRB.[3] This lack of separate categorisation makes it harder for LEAs to allocate the sources, enabling scammers to exploit the data gap. This data gap enables scammers to operate with impunity while LEAs struggle to track the exact scale of the threat.

INDIAN CYBER LAWS – SCENARIO AFTER DIGITAL ARREST SCAMS

Many complaints are being reported on the National Cyber Crime Reporting Portal (NCRP) regarding intimidation, blackmail, extortion and "Digital Arrests" by cyber criminals posing as Police Authorities, Central Bureau of Investigation (CBI), Narcotics Department, Reserve Bank of India (RBI), Enforcement Directorate and other Law Enforcement Agencies. Several victims have lost large amounts of money to such criminals. This is an organised online economic crime and is learnt to be operated by cross-border crime syndicates.

---

[1] Major Sadhna Singh, 'Digital Arrest the Modern Day Cyber Scam' (NITI Aayog, February 2025) <https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam> accessed 21 June 2026

[2] Union Bank, 'Digital Arrest Understanding' <https://www.unionbankofindia.bank.in/en/blog/digital-arrest-understanding-modus-operandi-current-trends-and-safety-tips > accessed 21 June 2026

[3] Shri Bandi Sanjay Kumar, 'Digital Arrest Scam' <https://www.pib.gov.in/Pressreleaseshare.aspx> accessed 21 June 2026

The National Cybercrime Threat Analytics Unit released guidelines that Scammers posing as law enforcement personnel often use threats of "digital arrest" to pressure victims. Real law enforcement won't arrest you digitally. There is no concept of Digital Arrest under any Indian law. Never share personal or financial information over the phone, email, or messaging apps without verifying the request. Always verify the identity of the caller or sender before taking any action; contact the nearest police station directly to verify the claim/identity. Speak to your relatives and friends before taking any action to transfer money. Report cyber frauds immediately at www.cybercrime.gov.in or by calling 1930. Regularly update yourself on the latest cybercrime and prevention tips; follow @cyberdost on social media.[4]

CYBERCRIME IN INDIA		
S.NO.	**CRIME**	**2024 &2025**
1	Fiscal losses owing common	20 lakh complaints in financial year 2024
2	INR 1,2 lakh crores (Phishing Crimes most common)	INR I,2 lakh by the end of 2025
3	Fraud on the Rise (Investment Scams & Identity theft)	Investment Scams INR 3,216 crores
4	Digital Arrest Fraud on the Rise in states	Tamil Nadu, Karnataka, and Telangana are major states which have seen rise of Digital Arrest in year 2024 & 2025

RESEARCH METHODOLOGY

Statistical data from various Indian Government websites, such as the Ministry of Home Affairs, NITI Aayog, Reserve Bank of India, Union Bank, National Cybercrime Threat Analytics Unit as Primary Sources of data and, many more, as well as review from journal

[4] Ministry of Home Affairs "Digital Arrest Scam" (National Cybercrime Threat Analytics Unit, 6 March 2025) <https://cybercrime.gov.in/pdf/Advisories/ADVISORYTAU-ADV-003DigitalArrest06.03.2025.pdf > accessed 21 June 2026

paper, annual reports, newspapers reports, and magazines based on the Article of Digital Arrest these data are cited as Secondary Sources of data. There are cases related to Digital Arrest that are also cited based on the judgment of High Courts and the Supreme Court. The study goal is to established, and highly descriptive research pattern based on the analyses of the above-mentioned data collection sources. The author acknowledges the lack of disaggregated NCRB Data on Digital arrest as a key limitation of this study.

UNDERSTANDING DIGITAL ARREST: DEFINITION

Digital Arrest is a severe cyber scam where the scammers impersonate law enforcement or government officials to trap victims in prolonged video calls on WhatsApp or Skype. They extort the victims with fabricated arrest warrants or frozen bank accounts. They demand huge sums of money. Their modus operandi involves intimidation and extortion. Digital Arrest Scam mostly target the individual of high status, senior citizens, highly educated professionals, and successful business executives.

In India, there is no separate law for 'Digital Arrest'; there are only preventive guidelines provided by the Government of India to prevent the Digital Arrest Scam. These scammers often attempt to isolate the victim and subsequently leverage the threat of fictitious consequences, such as arrest or imprisonment, to extort significant sums of money or part with personal information to prevent supposed legal action. These scams use tactics such as spoofed phone numbers, emails, and fake websites mimicking legitimate institutions.[5]

LEGAL POSITION IN DIGITAL ARREST: CAN ANYONE BE DIGITALLY ARRESTED?

Although there are no specific laws related to Digital Arrest, India provides a specific procedure for arrest, and there is no provision for Digital Arrest. In India, the arrest procedure is provided under Chapter V (Section 41-60A) of the Code of Criminal Procedure, 1973 (CrPC), which is replaced by Chapter V (Section 35-62) of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNNS).

[5] Ankoosh Mehta et al., 'Understanding the Digital Arrest in Indian Context' (*Dispute Resolution Blog*, 13 February 2025) <https://disputeresolution.cyrilamarchandblogs.com/2025/02/from-clicks-to-cuffs-understanding-digital-arrest-in-the-indian-legal-landscapes> accessed 21 June 26

No person can be legally digitally arrested in India. Supreme Court held that it requires the arresting officer to prepare an arrest wear clear identification, prepare an arrest memo witnessed by a family member, and report the arrest to a local police control room,[6] but Digital Arrest is unlawful detention which violates the Fundamental rights of an individual, which amounts to illegal confinement and violates Article 21 and Article 22 of the Indian Constitution.

CONSTITUTIONAL SAFEGUARD AND LEGAL PROVISION AGAINST ILLEGAL ARREST

Constitutional Safeguard: India provides constitutional safeguards under Article 21 and 22 of the Indian Constitution, which fall under the Right to Freedom in Part III. Article 21 guarantees the fundamental right to life and personal liberty, while Article 22 provides specific safeguards against arbitrary arrest and detention. Together, they ensure the state cannot take away a person's freedom without a just legal process.[7]

Legal Provision against Illegal Arrest: Although there is no separate legal provision for Digital Arrest in India, it can be governed and punished through the provisions of the following laws:

Bharatiya Nagarik Suraksha 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 for cheating and use of forged documents.
- Section 61: Criminal conspiracy.[8]

Information Technology Act 2000 –

- Section 66D: Punishment for Cheating by Personation using Computer Resources.
- Section 66C: Identity Theft.
- Section 43: Unauthorised Access to Computer Systems and Data.

---

[6] *D.K. Basu v State of West Bengal* (1997) 1 SCC 416

[7] Constitution of India 1950

[8] 'Unmasking Digital Arrest' (*International Law Journal*, 14 May 2025) <https://www.lawjournals.org/assets/archives/2025/vol11issue5/11210.pdf> accessed 21 June 26

- 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 criminalises cheating by personation using electronic means[9]

WHY DO THESE SCAMS SUCCEED?

Digital arrest scams succeed because they weaponise **fear, authority bias**, and **isolation** to manipulate victims into logical paralysis. Scammers do not need to hack your device; vice versa, they use psychological tricks to make you surrender your own money voluntarily. The following are the methods used by scammers in digital arrest scams:

Fake Authority Claims: The scammer pretends to be a law enforcement official or agent.

Threat of Arrest: Scammers then warn the victim about a supposed arrest warrant issued in the victim's name for unpaid taxes, customs violations, or other fabricated charges.

Request for Video Communication: Victims are often coerced into switching to video calls via platforms like WhatsApp or Skype to make the interaction appear more legitimate.

Fake Police Station Set-up: Scammers may create a convincing "police station" backdrop to gain the trust of the victim.

Demand for Money: Victims are then pressured to pay a fee, often via a bank transfer or UPI ID, to "settle the matter" and avoid arrest.

Real Cases of Digital Arrest Scam from the News Headlines –

Income Tax Fraud: A Mumbai-based professional received a call from someone posing as an income tax officer, threatening immediate digital arrest for unpaid taxes. The victim, fearing legal trouble, transferred ₹50,000 to the scammer.

Customs Violation Hoax: A Chennai resident was tricked into paying a hefty amount after being accused of customs violations related to an international parcel they had never ordered.

[9] *Ibid*

Social Media Targeting: An influencer was contacted on Instagram by someone claiming to be from a cybercrime department, accusing them of copyright infringement. They were asked to pay a "fine" to avoid further legal action.

These examples demonstrate how criminals exploit fear and authority to deceive victims.[10]

GOVERNMENT RESPONSES ON DIGITAL ARREST

To strengthen the mechanism to deal with cybercrimes including digital arrest scams in a comprehensive and coordinated manner, the Central Government has taken steps which, inter alia, include the following:

- The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cybercrimes in the country, in a coordinated and comprehensive manner.
- The Central Government has launched a comprehensive awareness programme on digital arrest scams which, inter alia, include: newspaper advertisement, announcement in Delhi Metros, use of social media influencers to create special posts, campaign through Prasar Bharti and electronic media, special programme on Aakashvani and participated in the Raahgiri Function at Connaught Place, New Delhi on 27.11.2024.
- I4C proactively identified and blocked more than 1700 Skype IDs and 59,000 WhatsApp accounts used for Digital Arrest.
- The Central Government has published a Press Release on Alert against incidents of 'Blackmail' and 'Digital Arrest' by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies.
- The Central Government and Telecom Service Providers (TSPs) have devised a system to identify and block incoming international spoofed calls displaying Indian mobile numbers that appear to be originating within India. Such international spoofed calls have been made by cyber-criminals in recent cases of fake digital arrests, FedEx scams, impersonation as government and police officials, etc. Directions have been issued to the TSPs for blocking such incoming international spoofed calls.
- Till 15.11.2024, more than 6.69 lakhs SIM cards and 1,32,000 IMEIs, as reported by Police authorities, have been blocked by the Government of India.

[10] 'Digital Arrest Understanding' (*Union Bank*) <https://www.unionbankofindia.bank.in/en/blog/digital-arrest-understanding-modus-operandi-current-trends-and-safety-tips > accessed 21 June 2026

- The 'National Cyber Crime Reporting Portal' has been launched, as a part of the I4C, to enable the public to report incidents pertaining to all types of cybercrimes, with special focus on cybercrimes against women and children. Cybercrime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.
- The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched in the year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, a financial amount of more than Rs. 3431 Crore has been saved in more than 9.94 lakh complaints. A toll-free Helpline number '1930' has been operationalised to get assistance in lodging online cyber complaints.
- To spread awareness on cybercrime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, digital displays on railway stations and airports across, etc.[11]

LEGAL REMEDIES AVAILABLE TO VICTIMS (POST SCAM)

While vigilance is the best defence, the following remedies are available to the victims of the Digital Arrest:

- Immediately report the incident to the National Cyber Crime helpline 1930 or at www.cybercrime.gov.in. Without any delay, and should not panic about the arrest. Do not share Aadhaar, OTP, or bank details with callers.
- Inform your bank to freeze transactions. Take screenshots of the WhatsApp call, numbers, and the messages shared with the scammer as evidence.

[11] Press Information Bureau Government of India Ministry of Home Affairs, 'Digital Arrest Scam' <https://www.pib.gov.in/Pressreleaseshare.aspx> accessed 21 June 2026

- File a First Information Report (FIR) at the nearest police station or on the CCTNS portal. Digital arrest is an offence under Section 316 and 308, Bharatiya Nyaya Sanhita, 2023.
- Preserve all evidence such as screenshots, video calls or messages, bank transaction IDs, and UPI IDs. Do not delete the WhatsApp chats.
- Seek legal assistance to file complaints under Section 35, BNSS for the arrest procedure violations and claim compensation.

PREVENTIVE MEASURES TO AVOID DIGITAL ARREST

Digital arrest is not a recognised legal procedure; genuine law enforcement agencies will never interrogate, threaten, or demand money over a prolonged phone call or video call. To prevent yourself from Digital arrest, immediately disconnect unsolicited calls, refuse to transfer funds, and verify such claims through official government channels. The following prevention measures must be taken to prevent Digital Arrest:

The Golden Rules –

Understand the Law: There is no legal provision in India for a "Digital Arrest". Every official requires physical presence and a warrant under Section 35, BNNS. Investigating officials never interrogate, threaten or demand money over phone and video calls.

Stay Calm and Disconnect: Scammers try to manipulate you. If you receive any threatening calls about legal action and they are posing to be government officials, immediately disconnect the call. A calm mind is the best defence or preventive measure against emotional manipulation.

Never Pay or Share Sensitive Information: Do not transact money, OTPs, Bank account details, or passwords under compulsion. Legitimate agencies will never ask for funds for "verification" or "clearing your name".

Steps to Take during a Suspicious Call –

Verify Identity: If someone claims to be from a government agency, ask for their full name, designation, and ID number. Hang up and verify this information by calling the official contact number of the department, not the number they provide.

Preserve Evidence: Take screenshots of the video call, call logs, and any forged documents sent by them to you.

Inform a Trusted Person: Scammers rely on isolating the victim. Immediately share the incident details with a family member or trusted friend.[12]

CHALLENGES TO CIRCULATE AWARENESS ABOUT DIGITAL ARREST

Despite the availability of relevant legal provisions, spreading awareness about "digital arrest" is a major challenge because scammers weaponise fear (modus operandi), highly mimic law enforcement, and operate across borders. Primary challenges include **psychological threat** at overrides critical thinking, **targeted AI deepfakes** that manipulate educated users, and **cross-border jurisdictional hurdles** that slow down actual police investigations.

The following are the major challenges to raise awareness among citizens:

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 centres 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.[13]

[12] Deeksha Dixit, 'Digital Arrest Scam' (27 December 2025) <https://www.pw.live/upsc/exams/digital-arrest-scam> accessed 22 June 2026

[13] 'Unmasking Digital Arrest' (*International Law Journal*, 14 May 2025) <https://www.lawjournals.org/assets/archives/2025/vol11issue5/11210.pdf> accessed 21 June 26

CASES OF DIGITAL ARRESTS IN INDIA

In 2025 and early 2026, a series of high-profile ‘digital arrest’ scams, where fraudsters pose as law enforcement or regulatory officials and virtually detain victims, were investigated across India. Notable cases and arrests include:

Bengaluru Tech Professional Scam 2024: In 2024, Bengaluru tech professionals were primarily targeted by devastating **‘**digital arrest’ scams, where fraudsters impersonated government officials to extort massive sums of money. In one of the most prominent cases, an IT executive lost ₹11.88 crore after scammers claimed her SIM card was linked to illegal activities[14].

Hyderabad Senior Citizen Scam 2024: One of the most notable scams targeting a senior citizen in Hyderabad in 2024 was a massive investment fraud where a 66-year-old retired resident was conned out of ₹13.16 crore. The fraudsters orchestrated a sophisticated online investment and business scam through WhatsApp by adding the victim to a fake stock broking group and impersonating assistants of reputed brokerages like Upstox and International Brokers (IB).[15]

Noida Woman Defrauded through Virtual Detention (2023): In a prominent case, a woman was kept under "digital arrest" after receiving an IVR call falsely claiming her Aadhaar card was used for illegal activities in Mumbai. Scammers posing as CBI and police officers forced her into transferring Rs 11.11 lakh via Skype.[16]

Pune Retired Judge Case 2025: A retired judge from Pune became the victim of a digital arrest scam in which he lost over Rs 1 crore to a cyber-criminal who posed as an IPS officer

[14] ‘Digital Arrest Scam’ *The Hindu* (17 November 2025) <https://www.thehindu.com/news/national/karnataka/senior-it-executive-in-bengaluru-loses-over-31-crore-in-digital-arrest-scam/article70289620.ece > accessed 22 June 2026

[15] Digital Arrest Scam to senior citizen’ *The Hindu* (05 September 2024) <https://www.thehindu.com/news/cities/Hyderabad/hyderabad-based-senior-citizen-conned-of-1316-crore-in-investment-fraud-three-arrested/article68605965.ece> accessed 22 June 2026

[16] ‘Noida woman defrauded through Virtual Detention, 2023’ *The Times of India* (04 December 2023) <https://timesofindia.indiatimes.com/city/noida/noida-logs-first-case-of-digital-arrest-woman-duped-of-over-rs-11-lakh/articleshow/105683261.cms > accessed 22 June 2026

and threatened to arrest him under the National Security Act. A First Information Report (FIR) was registered at the Cyber Crime Police station of Pune.[17]

SUGGESTIONS

The emergence of Digital Arrest scams, a form of cybercrime-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:

- Strengthen the cybercrime unit and laws in urban as well as rural areas because rural areas are most vulnerable to cybercrime.
- Define and recognise 'Digital Arrest' under Indian Law in a specific provision.
- Organise schemes and camps to spread awareness among citizens about 'Digital Arrest' in rural and urban areas.
- Centralise the redressal system for digital fraud and digital arrest for speedy and fast trial.
- International collaborations to fight the situation so that the cross-border fraud issue can be resolved.
- Compulsory call authentication and telecom regulation to protect the citizens.
- Strengthen the official units and investigation agencies of the government to protect citizens from digital arrest.

CONCLUSION

The rise of digital arrest scams in India marks a dangerous evolution in cyber-enabled crimes, where fear, authority, and technology are weaponised 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

[17] 'Digital Arrest Scam with Retired Judge' *The Indian Express* (08 July 2025) <https://indianexpress.com/article/cities/pune/digital-arrest-fraud-retired-judge-rs-1-crore-10114542/ > accessed 22 June 2026

they are under investigation or facing imminent arrest. To get bail, the victim transfers money without verification.

'Digital arrest' has no legal provision 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. In present, enforcement agencies must rely on procedures of sections of the IPC/BNS (such as cheating, impersonation, and extortion) and provisions from the IT Act, 2000 (such as Sections 66C and 66D). Yet there is no provision for cross-border fraud. They are difficult to trace and prosecute.

In response to these growing cases of digital arrest, strict rules are required. Legal reforms must be undertaken to specifically define and criminalise 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. 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. Citizen awareness is perhaps the most powerful tool in prevention.

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, governance and crime have both gone online. In addition to that, digital arrest scams present a multidimensional 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.