DIGITAL ARREST SCAMS IN INDIA: EXAMINING THE LEGAL FRAMEWORK, ENFORCEMENT MECHANISMS AND JUDICIAL RESPONSE

Madhurima G, LL.M. (Criminal Law), School of Law, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.[1]

Janvi Ashika G, Assistant Professor, School of Law, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.[2]

ABSTRACT

Digital technology has ushered in India plenty of change in governance, money transactions and communication and also helped in the rise of new high-end cyber financial frauds. One new threat is that of the "digital arrest" where the fraudster pretends to be a police officer, investigating agency or any other government body and make it look like they are conducting a criminal investigation or that they are going to arrest the victim and therefore, extort money from the victim via phone call, video call or online platform. Though the term 'digital arrest' is a term of public discourse, there is no definition of the term in Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000 or any existing laws in India. No police force in the world has the authority to arrest, detain or investigate anyone as a result of a phone call or video call or based on anything that is transmitted through the internet. The paper adopts a doctrinal technique for analysing the law relating to digital arrest scams in India. It explores the fraudster's modus operandi, applicability of existing statutory measures, institutional and technological barriers, recent judicial cases and enforcement measures of the Government. The study comes to the conclusion that the public trust is being exploited by criminals, due to the lack of authenticated digital communication protocols, as they use social engineering, artificial intelligence, voice cloning, deepfake technologies and impersonation. The paper also examines recent examples of digital arrest scams, and judicial response to it. It concludes that while the existing legislation has adequate tools to prosecute crimes such as cheating, forgery, impersonation, extortion, and identity theft, the problem would require the adoption of authenticated digital communication systems, more inter-agency cooperation, international cooperation, financial protection,

[1] LL.M. (Criminal Law), School of Law, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.

[2] Assistant Professor, School of Law, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.

dedicated cybercrime enforcement, and more digital legal literacy. These are the reforms that are needed to ensure that people can have greater confidence in digital governance and to tackle the evolving threat of digital arrest scams.

Keywords: Digital Arrest, Cyber Fraud, Government Impersonation, Digital Due Process, Cybercrime Enforcement, Bharatiya Nyaya Sanhita, 2023.

Introduction

India has been evolving into a digitised country where internet is an integral part of communication, banking, education, business, e-commerce and accessing government services. In total, there were 850.95 million internet users as of March 2023[3]. The growing digitization of life has created more efficient and convenient ways to do things, but it has also resulted in a dramatic increase in cybercrime and cyber security risks. The number of cybercrime cases involving communication devices has risen from 50,035 in 2020 to 65,893 in 2022, according to the Ministry of Home Affairs.[4] Likewise, in the return reply Minister of State for Finance in the Lok Sabha, said that the losses due to digital banking, credit card and ATM fraud have increased from ₹44.22 crore in 2019-2020 to ₹177.05 crore (2023-2024)[5]. These statistics are just a few indicators of the increased risks people face from financial fraud online.

Digital arrest scam is one of the latest modus operandi of cybercrime wherein criminals pose as police officers or officials with CBI, ED or Customs and make calls or video calls to individuals. Victims are tricked into committing crimes, including money laundering, drug trafficking or cybercrime and threatened with arrest or prosecution unless they send funds or reveal personal information. The term digital arrest is used all the time but has not been defined anywhere in the Indian law[6] and no law enforcement agency in India can arrest, detain or investigate a person via a phone call or video call or any online platform. Unusually, criminals take advantage of this public ignorance, relying on fear, psychological pressure and official

[3] Lok Sabha Debates on March 15,2023 available at: https://sansad.in/getFile/loksabhaquestions/annex/1711/AU2351.pdf?source=pqals (last visited on July 11,2026)

[4] Lok Sabha Debates on August 6,2024 available at: https://गृहमंत्रालय.सरकार.भारत/MHA1/Par2017/pdfs/par2024-pdfs/LS06082024/2504.pdf

[5] "Over Rs 177 Crore Lost on Account of ATM, Credit Card, Internet Banking Frauds", *The Economic Times*, Aug 05, 2024,available at https://economictimes.indiatimes.com/industry/banking/finance/banking/over-rs-177-crore-lost-on-account-of-atm/credit-card-internet-banking-frauds/articleshow/112287077.cms (last visited on July 11,1016)

[6] Uma, "Unmasking Digital Arrest: An Emerging Threat to Modern Society in India", 11 International Journal of Law 121 (2025).

fake documents to make their threats seem credible. Often the person is compelled to video call on Skype or WhatsApp for hours and hours and is coerced into sending money. The scams often lead to financial loss, identity theft, privacy intrusion and often to severe psychological trauma.

Digital arrest scams have become increasingly serious, and have captured the attention of the highest level of government. On his Mann Ki Baat TV programme broadcast on 27 October 2024, the Prime Minister advised people to be alert for such scams and warned that no government agency could carry out any investigation or arrest through a phone or video call.[7] In Re: Victims of Digital Arrest Related to Forged Documents, the Supreme Court of India noted that these scams are spread at par with pandemic wherein both the scale of victimisation and the organised nature of crime is noted. The developments demonstrate a need for more robust legal protections, effective enforcement of cybercrime and more public awareness. In this context, this paper critically assesses the current statutory provisions and enforcement procedures for combating digital 'arrest scams' in India.[8]

What Are Digital Arrest Scams?

Cyber Crime in India has become one of the fastest-growing crimes due to the increasing digitalisation, internet penetration, online banking, and e-commerce. Cybercriminals are creating new tools to carry out financial fraud on the Internet, misuse of identity, etc. The online arrest scam has become one of the most high-tech financial frauds. Due to improved enforcement and public awareness drives, the reported digital arrest scam cases have gone down in the recent past. However, the offence continues to pose a serious threat which has been increasing with time because of the changing nature of crime, an organised way of committing fraud. Further, it has serious financial and psychological impact on the victim.

The term 'digital arrest' does not appear in the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, or any other existing legislation in India. No law enforcement agency in India, from the Central Bureau of Investigation to the Narcotics Control Bureau, the Enforcement Directorate or the State Police can arrest, detain or investigate anybody using a phone call, video call or any other online platform. The term digital arrest and online detention

[7] Kawaljit Singh & Dr. Harish Kumar, "Digital Arrest Using Artificial Intelligence Generative Deepfake Media Content in Post-Truth Society", 13 Journal of Research in Humanities and Social Science 192 (2025).
[8] Supra

are not a recognized form of arrest, says cyber security experts[9]. In practice, digital arrest is defined as a fraudulent activity on the internet where people pose as police or law enforcement officials with the intention of stealing money or acquiring confidential information. Generally, the criminals contact their target by way of a phone or video call and accuse them of committing an offence such as the use of money laundering, cybercrime or drug trafficking. They also use fake identification, spoofing phone numbers and other tricks to convince their target they are legitimate law enforcement officers.[10] From a legal standpoint, there should be a clear distinction between Digital Arrest and a true arrest under Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS). Digital Arrest cannot fulfill any of the legal requirements set forth in Section 35-62 of BNSS 2023 including lawful jurisdiction, cognizable jurisdiction, warrant and that an authorised officer must follow the law when performing his/her duties. It is essentially an act of criminal impersonation that has been enacted in order to benefit from the individual's ignorance of criminal law.

Pattern of Criminal Activity

Digital arrest scams have become technologically advanced and are getting harder and harder to identify and investigate. The dark web marketplace for stolen personal data and malware tools has also come under the spotlight in relation to the planning and execution of such frauds. The use of artificial intelligence to clone voices and create fake video calls that look like authentic government officials, making it harder to trace the calls, has also been reported in relation to the planning of these fraud schemes.[11] Typically, digital arrest scams are conducted in three stages. During the first phase, the victim is contacted by someone claiming to be from a bank, courier or other official and alleging that they have an issue with the victim's account, or a suspicious parcel. The caller will then instruct the victim to contact the police and then send him to another person via WhatsApp or Skype. In the second phase; the scammer pretends to be a police officer, possibly using a police uniform during video chat to look legitimate. The victim is falsely accused of being involved in a serious crime and is threatened with legal action. The final step involves a victim being contacted by a person pretending to be a senior member of a government agency, instructing the victim to comply with the many directions,

[9] Bhawna Vijay, "The Evolution of Digital Arrest Cyber-Crimes in India: Trends and Patterns Preventive Measures", 7 International Journal of Sociology and Humanities 2 (2025)
[10] Government of India, "Digital Arrest: The Modern-Day Cyber Scam", (NITI Aayog)
[11] Sh. Aditya Hriday Upadhyay, "Contours and Webs of Digital Arrest Pandemic", 2 Journal of Communications Finance 45 (2025)

such as transferring funds. Scams are well-planned, and the scammers are frequently trained to play certain parts.

Scams that involve offenders being arrested digitally are mostly not random acts they function in a way where the offender has completed a prior reconnaissance of the intended victim through the knowledge of the victim's personal information and financial information. This allows the offender the ability to tailor the scam to fit the victim and provide credibility to the scam. The offender places intense psychological pressure on the victim by using fake arrest or criminal warrants, fake financial documents, and distorted video recordings through the use of social engineering methods, so that the victim has an extreme amount of fear and is further isolated from outside assistance. The offender will instruct the victim not to contact family members or attorneys so that the victim will not receive information contradicting the offender's stories, thus keeping the victim isolated.[12]

The last step of the scam is extracting money from the victim. They are asked to pay via an untraceable route such as UPI transfers, cryptocurrency, or prepaid gift cards. Once they have paid up, the fraudsters disappear, and the victim realises their mistake when trying to verify the truth behind the story with genuine authorities. The illegally acquired cash is then split up, circulated between several accounts, before being wired out to foreign shores, a well-planned layering technique that makes tracking impossible and recovery unlikely.

Reported Incidents:

1. Retired Bengaluru Teacher Loses ₹24 Crore in Digital Arrest Scam: One of Bengaluru's biggest digital arrest scam happened in 2026 where a 74 year old retired teacher was cheated of ₹24 crore by fraudsters pretending to be cops. The victim was falsely implicated in a money laundering case and kept under constant video surveillance where she was forced to make ₹24 crore transferred over 26 transactions into 23 mule's bank accounts between February and April 2026. The fraud came to light when the bank manager became suspicious on being approached for another loan against pledging 1kg gold. A joint probe by Karnataka State Cyber Command (KSCC) & NCRP resulted in the arrest of 6 accused and about ₹1.60 crore recovered by

[12] N. Likhitha Prasad, "The Illusion of Authority: Understanding Digital Arrest in India", 1 Canonsphere Law Review 9 (2025)

freezing mules accounts.[13]

2. Faridabad Bank Clerk Kept Under "Digital Arrest" for 56 Hours: An alarming digital arrest case came to light in Faridabad, Haryana, where a 55-year-old bank employee was mercilessly mentally tortured by cyber conmen for almost 56 hours. Impersonating CBI and TRAI officials, the fraudsters wrongfully accused him of linking his Aadhaar to a ₹6.6 crore money laundering case and threatened him with immediate arrest. Overpowered with fear and constantly videotaped, he transferred ₹5 lakh thinking it will be 'verified' by the RBI. It all came out when his peculiar conduct alarmed locals who alerted his family.[14]

3. 67-Year-Old Woman Defrauded of ₹16 Lakh in a Digital Arrest Scam: In one such digital arrest scam reported in Thiruvananthapuram, a 67-year-old woman lost ₹16.36 lakh after fraudsters impersonating officials of the Central Bureau of Investigation (CBI) called her up on WhatsApp video and allegedly showed her an arrest warrant. They claimed her Aadhaar number was used in a money laundering case in Mumbai and backed their claim by showing fake documents bearing a stamp of a Notary Public. Scared of being arrested and facing legal action, the victim shared her bank details and transferred ₹16.36 lakh through nine transactions before realising she was being duped and approaching the Cyber Police.[15]

4. Recent Enforcement Action: CBI's Operation Chakra-VI: One of the biggest recent enforcement action on digital arrest scams is the Central Bureau of Investigation's (CBI) Operation Chakra-VI. In June 2026, the CBI carried out "coordinated searches" at over 80 locations spread over 16 States/UTs in more than 200 cases of digital arrest fraud. Around 60 specialised teams were deployed to take down organised cybercrime networks involved in impersonation and financial fraud. Investigations revealed that the accused "had raised shell companies and had been using 'Mule Bank Accounts' to launder around ₹2 crores amassed from digital arrest fraud." A major breakthrough came in the form of a fraudulent website with a URL almost identical to the official website of the Supreme Court of India. Allegedly, the

---

[13] "Retired Teacher Cheated of ₹24 Crore in Digital Arrest Scam in Bengaluru, 6 Arrested", *The Hindu*, May 25, 2026, available at: https://www.thehindu.com/news/national/karnataka/two-held-for-allegedly-duping-elderly-bengaluru-woman-of-24-crore/article71017200.ece (last visited on 13 July,2026)

[14] Mahesh Buddi, "Under 'Digital Arrest', 55-Year-Old Man Made to Go from Faridabad to Bihar", *Times Of India*, Nov. 27, 2024,available at: https://timesofindia.indiatimes.com/city/gurgaon/digital-arrest-man-duped-in-cbi-money-laundering-scam/articleshow/115703688.cms (last visited on 13 July,2026)

[15] "Digital Arrest Scam: 67-Year-Old Woman Defrauded of Rs 16 Lakh", *New Indian Express*, June 16, 2026 https://www.newindianexpress.com/cities/thiruvananthapuram/2026/Jun/16/digital-arrest-scam-67-year-old-woman-defrauded-of-rs-16-lakh (last visited on 13 July, 2026)

accused uploaded forged court orders, arrest warrants, and other fake documents pretending to be issued by courts and law enforcement agencies to create an illusion of authenticity and terrorise victims to transfer money. During the searches, CBI seized mobile phones, digital devices, banking details, and other incriminating material. The operation also showed that the accused targeted both Indians as well as foreigners. Operation Chakra-VI proves that digital arrest scams are no longer one-off crimes but a job carried out by organised crime networks using advanced technology, fake digital IDs, shell companies, money laundering networks, and whatnot.[16]

Government Initiatives to Combat Digital Arrest Scams

1. Constitutional and Institutional Framework.

The State Governments and the Central Government both share the responsibility of preventing the investigation, and prosecution of cybercrimes, including digital arrests scams. Article 246 of the Constitution of India mentions "Police" and "Public Order" as State Subject under Seventh Schedule. As such, it is mainly the responsibility of the State Police and other law enforcement agencies to deal with such offences. However, the Center supports the States by the issuance of guidelines, financial support and strengthening the capacity of investigating agencies through various schemes.[17]

2. Indian Cyber Crime Coordination Centre (I4C) and Reporting Mechanisms.

The Indian Cyber Crime Coordination Centre (I4C) was established by the Home Ministry to enhance the country's response to cyber crime. It is the central agency that co-ordinates all the actions against cyber-crimes. Citizens can file online reports of cyber crimes through the national cyber-crime reporting portal of the Government. Once a complaint is lodged, it is sent to the relevant State or Union Territory police to investigate it as per law.

Apart from the above measure, the Citizen Financial Cyber Fraud Reporting and Management System launched in 2021 is another important step. With this, victims of such fraud can report immediately so that banks and enforcement agencies can freeze suspicious transactions before

[16] Devesh K. Pandey, "Digital Arrest Scams: CBI Conducts Searches at Over 80 Locations Across India", *The Hindu*, June 26, 2026, https://www.thehindu.com/news/national/digital-arrest-scams-cbi-conducts-searches-at-over-80-locations-across-india/article71144963.ece (last visited on 14 July 2026)
[17] Government of India, "Digital Arrest Scam" (Ministry of Home Affairs, 2024)

the money gets transferred further. By November 2024, complaints worth ₹3,431 crore saved through this mechanism had been registered in more than 9.94 lakh complaints. The government has launched the cyber helpline number 1930 to report any cyber fraud and take action immediately.

3. Measures Taken to Combat Digital Arrest Scams

The Government has implemented a number of specific measures aimed at combating digital arrest fraud. The I4C has successfully blocked a total of over 1,700 Skype IDs and 59,000 WhatsApp accounts that were being used by cyber criminals to impersonate government officials and defraud victims. A total of over 669,000 SIM cards plus 132,000 IMEI numbers have also been blocked for connection to cyber crime activities.[18]

In the fight against the use of fake Indian mobile numbers, the Government is working with telecommunications providers to identify and block calls made by international telecommunications companies from 'spoofed' mobile numbers to Indian mobile numbers such calls are often made from countries other than India and are used in digital arrest fraud. Therefore, the blocking of calls using 'spoofed' mobile numbers has been identified as an important method of combating impersonation fraud.

4. Public Awareness and Preventive Measures

With regards to enforcement, the government has also been focusing on educating citizens about digital arrest scams. Awareness campaigns have been carried out using newspapers, television, radio, announcements made in the Delhi metro, social media and in-person outreach. CyberDost a part of the I4C regularly posts safety tips using X, Facebook, Instagram, and Telegram. In addition, the government has held Cyber Safety and Security Awareness Week and provided educational materials for both students and the public in order to encourage safe practices online.[19]

5. The **Cyber Fraud Mitigation Centre (CFMC)**, which was created to improve coordination among stakeholders involved in combating cyber fraud, is part of the Indian Cyber Crime Coordination Centre (I4C). The CFMC integrates authorities from banks, financial institutions, payment services, telecommunications, IT intermediaries, as well as State and Union Territory

---

18 Id
19 Government of India, "Steps Taken to Address the Issue of Digital Arrest Scams", (Ministry of Home Affairs, 2025)

based law enforcement agencies to facilitate the rapid exchange of data and the immediate intervention into, and investigation of, cyber frauds.[20]

6. The Government of India has launched several technology centric initiatives under the Indian Cyber Crime Coordination Centre (I4C) to boost cybercrime investigation and inter-agency coordination. A project of this kind is a Geographic Information System (GIS) based software, called **Pratibimb Module**, which helps law enforcement agencies locate and track cybercriminals. It is an online platform which enables investigating agencies to map out mobile phone numbers of complaints related to cybercrime in real time, analyze criminal networks and facilitate coordinated enforcement action across jurisdictions. Details given to the Lok Sabha reveal that the Pratibimb Module has aided in thousands of arrests and in establishing linkages between cyber criminals across the country and helped in many cyber investigation requests.

The Ministry of Home Affairs has also initiated another important step **Samanvay Platform** to improve coordination between law enforcement agencies. The platform can be used as a centralised platform for sharing cybercrime information and for analytical evaluation of the cybercrime complaints received by various States and UTs. The platform enables the identification of inter-state connections between crimes and criminals, which allows for the sharing of information, more efficient investigations and promotes coordinated efforts to combat organised cybercrime activities.[21]

These efforts reflect the Government's growing use of technology-enabled solutions for the investigation, intelligence sharing and enforcement of cybercrime. These are especially relevant in fighting against the organised cyber attack, such as the digital arrest scam where the perpetrator may be from another State / jurisdiction.

The Statutory Framework for Combating Digital Arrest Scams

While there is no dedicated legislation governing digital arrest in India, various provisions of the existing criminal and cyber laws are applicable to prosecute those involved in such offences.

[20] Government of India, "Union Home Minister and Minister of Cooperation, Shri Amit Shah addresses first Foundation Day celebrations of I4C as the Chief Guest at Vigyan Bhavan in New Delhi, launches major initiatives for prevention of cyber crime" (Ministry of Home Affairs,2024)

[21]Vajiram Content Team, Pratibimb Module, Vajiram & Ravi available at: https://vajiramandravi.com/current-affairs/pratibimb-module/ (last visited on 14 July,2026)

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) has some provisions under which penalty can be invoked to prosecute offenders in digital arrest scams. The term "digital arrest" does not exist in the BNS or in any Indian law but the actions of fraudsters engaged in such schemes, can be held liable under many existing crimes.

a. The crime of impersonation of a public servant is included in Section 204 of the Bharatiya Nyaya Sanhita, 2023. This is especially applicable when it comes to digital arrest scams since the offenders are often pretending to be from police or agencies like the Central Bureau of Investigation (CBI), Enforcement Directorate (ED), Customs Department or other government bodies, thereby gaining the victim's confidence and intimidation. Whoever violates this provision shall be punished by imprisonment for a term of not less than 6months up to three years and by fine.

b. Another important section of the crime that applies to digital arrest scams is Section 318: Cheating. Fraudsters pretend to be engaged in a criminal activity like money laundering, drug trafficking or identity theft, and convince the victim to send money, pretending that this will prevent the victim's arrest or help the investigation. Sentence for the offence is up to seven years imprisonment and a fine.

c. The forgery of legal documents and their use in such scams are covered in Section 336 of the Bharatiya Nyaya Sanhita 2023. They usually attempt to establish a fake arrest warrant, court order, identity card, official notice or other document to make their threat look real and victims think that legal proceedings have been started against them. Offences depending on the nature of the forgery are punishable by up to seven years imprisonment and a fine.

d. Also, Section 308-criminal extortion is triggered when someone obtains money by placing a victim under fear of some legal sanction such as arrest or prosecution or the loss of property. The key to these scams are making victims give their money away through intimidation and psychological manipulation, instead of legal authority. The penalties for the crime of extortion under this provision include up to 10 years imprisonment and a fine.

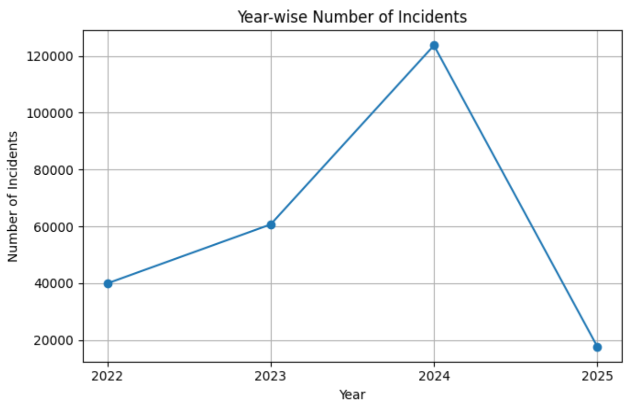
Information Technology Act, 2000 Provisions

The Information Technology Act, 2000 also has certain provisions which are relevant and specific to the prosecution of offences committed by digital arrest scams.

a. Section 66C of the Information Technology Act, 2000, deals with the offence of identity theft. It makes the use of another person's electronic signature, password, unique identification feature or other electronic identity, dishonest or fraudulent, a criminal act. The same applies to the digital arrest scams where the fraudsters use the name of a genuine organisation and/or stolen personal information, Aadhaar details, passwords, digital signature or other electronic credentials to commit fraud. Whoever is convicted under this provision faces imprisonment up to 3 years and a fine of up to ₹1 lakh.

b. Section 66D of the Information Technology Act, 2000, has a specific criminal provision relating to cheating by personation through computer resources or communication devices. The provision is one of the most important implications that exist with relation to digital arrest scams as most of the time these are committed via phone call, video call, email, social media, or other digital means of communication. Impersonating police officers, officers of the Central Bureau of Investigation (CBI), the Enforcement Directorate (ED), officials of the Customs Department, bankers or other government agencies, the fraudsters lure the victim into believing that he or she is being investigated or even arrested, and then get him or her to transfer funds. The punishment for the offence is up to three years imprisonment and a fine of up to ₹1 lakh.

Statistical Analysis of Digital Arrest Scam Cases in India (2022–2025)



[22]

[22]Data.gov.in, "Year-wise Number of Incidents of Digital Arrest Scams and Related Cyber Crimes Reported on National Cyber Crime Reporting Portal from 2022 to 2025", available at: https://www.data.gov.in/resource/year-

Interpretation: The chart shows the trend of digital arrest scams reported in India over the years from 2022 to 2025. The number of reported incidents increased from 39,925 cases in 2022 to 60,676 cases in 2023, before reaching a peak of 1,23,672 cases in 2024. In 2025 however, there was a marked decrease, with reported cases dropping to 17,264. The Ministry of Home Affairs (MHA) said this drop has been seen due to awareness campaigns across the country, which included through SMS, caller tunes, public ads and through public awareness programmes like the Prime Minister's Mann Ki Baat. Authorities have warned that digital arrest scams remain a serious cybercrime issue, though just 35% of the victims had fallen victim to an online scam. Many of the digital arrest scams are reportedly being run by organised scam networks from Southeast Asia.[23]

Judicial Response

1. **Kuldeep Sharma v State of Madhya Pradesh**[24] Recently, the Madhya Pradesh High Court refused to grant bail in a high-profile cyber fraud case that was called "digital arrest". The complainant a senior citizen was contacted on video calls by persons claiming to be law enforcement authority. They wrongly implicated her in a 'black money scam' and threatened to arrest her. The fraudsters managed to put her under "digital arrest" for 25 days by continuously intimidating her through video calls from June 1, to June 25, 2025. They took advantage of her age and fear and convincing her that her funds needed to be "verified" by the court. She and her husband transferred almost ₹59 lakhs in coercion to various bank accounts. The fraudsters sent a fake bail order to her mobile phone, even after that, they asked for an extra ₹10 lakhs. The accused had applied for bail, whereas prosecution opposed the bail, saying that it is an organised cyber syndicate and the investigation is still in a critical stage tracing funds, identifying beneficiaries and the role of each accused.

Justice Rajesh Kumar Gupta refused bail for two reasons:

a. Such cyber offences involve technical evidence, electronic devices and digital evidence

---

wise-number-incidents-digital-arrest-scams-and-related-cyber-crimes-reported-national (last visited on 15 July, 2026)

[23] Ananya Bhardwaj, "After 465% Spike in 2024, MHA Data Shows Digital Arrest Scams Are on a Decline in India", *ThePrint* Feb. 18, 2026, available at: https://theprint.in/india/governance/after-465-spike-in-2024-mha-data-shows-digital-arrest-scams-are-on-a-decline-in-india/2857002/ (last visited on 14 July 2026)

[24] 2026 LiveLaw (MP) 32

that can be tampered, granting bail at this stage could impact upon the investigation/trial and would also give the opportunity to influence witnesses or manipulate electronic evidence".

b. The prosecution case on the prima facie establishes that the complainant was subjected to what can be termed as a "digital arrest" while under the guise of police and investigating authorities, where she was constantly threatened and psychologically bullied and coerced to transfer huge sums of money on the false allegation of her involvement in a black money scam and receipt of bail. The way the complainant was purportedly digitally confined and forced to hand over her life savings is a "well-thought-out and well-organised cyber fraud" Thus, the bench dismissed the bail application.

2. The Rajasthan High Court has denied bail to the accused who allegedly extorted ₹2.02 crore from an elderly couple through impersonating Cyber Police officials and fake arrest. The Court noted that the digital arrest scam is an organised cybercrime and expressed concern on the lack of appropriate cybercrime investigation infrastructure and technical skills. The Court made a number of directions to the State Government recognising the rising menace of cybercrime.[25] The important directions were:

a) Setting up a Rajasthan Cyber Crime Control Centre along the lines of Indian Cyber Crime Coordination Centre (I4C).

b) Investigating specialised cybercrime units and accredited digital forensic laboratories are strengthened.

c) The increased use of AI by banks in identifying mule accounts and suspicious transactions. More AI technology in banks for the detection of mule accounts and suspicious transactions.

d) Improved supervision of SIM card suppliers, call centres, digital platforms and e-commerce companies.

[25] Adnan Haidar Bhai v. State of Rajasthan, 2025 SCC OnLine Raj 6059

e) Designation of specialist cyber prosecutors and cyber law specialists.

f) Public awareness programmes and enhancing digital literacy to avoid cyber fraud.

3. The Rajasthan High Court termed the digital arrest scam as one of the most dangerous type of cybercrime and said it raised grave concerns regarding the growing trend of such scams. The Court explained that there are no provisions in Indian law to recognise "digital arrest" and no law enforcement body has the power to arrest, detain or investigate any person through a phone call, video call or any other platform like that. It said that it was imperative to promote awareness of this kind of fraudulent practices among the public by creating awareness programmes using print and electronic media, and social media. The Court also noted that all lawful arrests must rigorously follow the procedure laid down in the BNSS, 2023, which requires identification of the officer in charge of the arrest and a preparation of an arrest memo. It also advised the Central and Rajasthan State Governments to submit reports on measures taken to combat digital arrest frauds, as well as encouraged the Reserve Bank of India and the Government to improve fraud prevention in the case of fund transfer and cybercrime prevention.[26]

Challenges in Combating Digital Arrest Scams in India

a. Lack of a Dedicated Legal Framework

No dedicated law exists in India concerning digital arrest fraud.

The current method used to prosecute offenders includes general legal provisions relating to criminal cheating, impersonation, extortion, forgery, and the Information Technology Act of 2000. This lack of dedicated legislation leaves an element of risk regarding how to deal with the unique aspects of this form of cybercrime.

b. Lack of Authenticated Digital Communication Protocols

Although Indian criminal law has different provisions to prosecute digital arrest scams, an important institutional weakness arises out of lack of authenticated digital communication

[26] Nupur Agarwal, "No Provision For Law Enforcement To Conduct Arrests Via Video Calls: Rajasthan HC Takes Suo Motu Cognizance Of 'Digital Arrest Scams' ", available at: https://www.livelaw.in/high-court/rajasthan-high-court/rajasthan-high-court-suo-motu-cognizance-digital-arrest-scams-281745 (last visited on 14 July 2026)

protocols for law enforcers. While India has started digitising official processes (e-summons, online complaints portal etc.), there exists no universally accepted mechanism for citizens to ascertain the authenticity of official video calls/emails supposedly issued by LEAs. Visual cues such as police uniforms, official insignias, govt logos etc. can be easily faked in digital space, thereby rendering these scams much more believable.[27]

c. Anonymity of Cybercriminals

Fraudsters typically use various technology solutions such as Virtual Private Networks (VPNs) or encrypted communications, spoofed telephone numbers, false identities, anonymous online accounts to disguise their identity and whereabouts and make it very difficult to investigate or prosecute them.[28]

d. Transnationality of Cybercrime

The majority of digital arrest scams originate from outside of India and are operated by organised cyber criminal enterprises. Jurisdictional limitations, differing legal systems, and delays in obtaining the necessary international assistance hinder the ability to conduct effective investigations.[29]

e. Difficult to Detect

The sophistication of digital arrest fraud makes it difficult to recognise. Even individuals who are educated and possess digital literacy skills have fallen victim to these cyber criminal's fear tactics, urgency, and false sense of authority created by the scams.

f. Lack of Awareness

Additionally, there is a significant lack of public knowledge about this type of fraud as a result, victims often mistakenly assume that they have a firm legal basis to digitally arrest individuals involved in committing fraud against them or their funds. Victims frequently believe an

[27] "Digital Arrest Scams in India: Legal Gaps, Criminal Liability and the Need for Digital Due Process Reform", *Free Law* Feb. 17, 2026, https://www.freelaw.in/legalarticles/Digital-Arrest-Scams-in-India-Legal-Gaps-Criminal-Liability-and-the-Need-for-Digital-Due-Process-Reform (last visited on 15 July 2026)
[28] Kawaljit Singh& Dr. Harish Kumar, "Digital Arrest Using Artificial Intelligence Generative Deepfake Media Content in Post-Truth Society", 13 Journal of Research in Humanities and Social Science 195 (2025)
[29] Dr. R. N. Mangoli, "Digital Arrest Scams in India: Challenges and Solutions with Special Reference to Karnataka", 11 IJRDO - Journal of Social Science and Humanities Research 14 (2025).

individual who has fraudulently represented himself as a member of the police, CBI, ED or some other legitimate governmental agency.

Recommendation:

1. To bridge this 'digital due process' gap, India needs to create a statutory framework for authenticated digital communications by law enforcement agencies. Official digital summons and notices should be digitally signed by authorised officers under the IT Act, 2000 and have a QR-code/certificate-based verification linked to a central government authentication portal. This would allow citizens to instantly check the authenticity of official communications and significantly limit imposter driven scams. Banks could also explore more stringent verification or cool-off periods for abnormal big value transactions by vulnerable seniors, while telecom regulators need to strengthen caller IDs for verified government messages.

2. Given that many digital arrest scams are perpetrated by cross-border criminal networks, India should deepen international cooperation through bilateral agreements, information sharing mechanisms and joint investigations with foreign law enforcement agencies. This would help trace the offenders, disrupt transnational cybercrime gangs and recover funds stolen in such a manner.

3. Central and State Governments should undertake sustained digital legal literacy campaigns to educate citizens about lawful arrest, rights of accused persons under criminal law, ways to verify official digital communications, and use of emergency cybercrime reporting mechanisms such as the National Cybercrime Helpline and National Cyber Crime Reporting Portal. Special focus should be given on senior citizens and other vulnerable groups that fall prey to digital arrest scams.

4. FIU–INDIA, along with banks and other financial entities, should strengthen real-time monitoring of suspicious transactions, and accelerate the identification and freezing of mule accounts used to launder proceeds of digital arrest scams. Improved information sharing amongst banks, payment service providers, and law enforcement agencies will help quicker recovery of fraudulently transferred funds and disrupt organised cybercrime networks.

5. Specialised cybercrime benches or dedicated cybercrime courts should be established to ensure the expeditious investigation and adjudication of complex cyber fraud cases, including digital arrest scams. Such specialised forums would strengthen judicial expertise in cyber offences, reduce delays in criminal proceedings, and improve the overall effectiveness of cybercrime enforcement.

CONCLUSION

One of the most sophisticated forms of cyber enabled financial fraud facing India today are 'digital arrest' scams though there is no legal definition of 'digital arrest' under Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Information Technology Act, 2000, or any other law in India. No agency has the power to arrest, detain or even investigate anyone over a phone/video call or online. Yet these are highly organised scams using technology, impersonation, social engineering and victim illiteracy about criminal procedures to extract money.

This study finds that while provisions of the BNS,2023, BNSS,2023, IT Act, 2000, and BSA, 2023 have a legal basis to prosecute crimes like cheating, personation, ID theft, forgery and offences related to electronic evidence, they fail to address institutional gaps enabling 'digital arrest'. The absence of authenticated digital communication and growing AI/voice clone, deep fake technology and cross border cybercrime nexus has created a significant "digital due process gap" for the fraudsters to leverage trust on public institutions and citizen's fear of prosecution.

Thus, addressing 'digital arrest' requires a comprehensive approach with stronger institutional safeguards, tech innovations, better investigations, financial security and sustained legal awareness. Authenticated digital communication systems, better coordination between LEAs, banks and telcos, and regular public legal literacy can drastically minimise possibilities of impersonation based frauds. As India grows digitally, strengthening procedural safeguard and public trust in official digital communication will become crucial to protect people from new cyber enabled frauds and ensure trust in rule of law.