International Journal of Enhanced Research in Management & Computer Applications,
ISSN: 2319-7471, Volume 14 Issue 5, May 2025

# Digital Arrest as an Emerging Cybercrime in India: Legal, Social and Ethical Dimensions

**Ish Kumar**

Assistant Professor, Chhotu Ram Institute of Law, Rohtak, Haryana

## ABSTRACT

**This paper explores the critical issue of digital arrest scams, a growing cybercrime phenomenon in India that involves fraudulent impersonation of law enforcement agencies through digital platforms to intimidate and extort victims. The introduction outlines the rise of this scam, driven by technological advancements such as voice cloning and deepfake videos, which enable criminals to simulate legal authority and manipulate individuals. The paper offers a clear definition of digital arrest as a cyber-enabled fraud involving impersonation, coercion, and deception primarily executed through electronic communication. It further categorises the crimes involved under cheating, extortion, identity theft and criminal intimidation, highlighting the severity of financial, psychological and social consequences suffered by victims and communities.**

**The study examines the legislative framework addressing digital arrest scams in India, focusing on relevant provisions under the IT Act and the BNS. It discusses government initiatives like the Indian Cybercrime Coordination Centre, public awareness campaigns, and reporting mechanisms designed to empower citizens and law enforcement. Judicial responses, including landmark convictions and critical court rulings, are analysed to demonstrate the evolving legal stance that reinforces the fraudulent nature of digital arrests and the necessity for strict penalties. An international perspective is provided through treaties and comparative legal analysis with countries such as the United Kingdom, the United States, Singapore, and Australia.**

**The challenges section details operational difficulties faced by Indian law enforcement, including jurisdictional barriers, technological complexities, resource constraints and limited public awareness. The paper emphasises the urgent need for dedicated legislation explicitly criminalising digital arrest scams, enhancing investigative capacity and expanding public education. Recommendations call for international cooperation, mandatory compliance by telecom and financial sectors and improved grievance redressal systems. Through a comprehensive approach integrating legal precision, technology and community engagement, India can better protect citizens and effectively combat the increasing threat posed by digital arrest scams.**

**Keywords: digital arrest, cyber fraud, online scams, cybercrime, online platforms.**

## INTRODUCTION

Digital arrest is an alarming and emerging form of cybercrime in India, characterised by deceptive tactics in which fraudsters impersonate law enforcement or government officials through digital platforms. These criminals threaten victims with false allegations of serious offences and coerce them into paying money or divulging sensitive information, often through intimidating phone calls, fake messages, and forged documents. The scam exploits the fear of legal consequences and the victim's limited understanding of authentic legal procedures. This makes digital arrest a complex issue, intertwining legal ambiguities with serious social and ethical consequences that affect individuals and the broader community. The incidence of digital arrest scams in India has seen a significant rise over recent years, reflecting the growing nexus between crime and digital technology. According to government data reported on the National Cybercrime Reporting Portal, there were 39,925 incidents recorded in 2022 with losses amounting to approximately Rs 91.14 crore. These figures almost tripled by 2024, with 1,23,672 reported cases and a staggering increase in financial fraud to Rs 1,935.51 crore. In just the first two months of 2025, 17,718 cases were reported involving defrauded amounts exceeding Rs 210 crore. The government has responded by blocking over 7.81 lakh SIM cards and more than 2 lakh IMEIs linked to these scams, illustrating the scale of the problem and the administrative efforts underway to contain it.[1] Notable judicial instance reflecting the gravity of digital arrest scams is the recent suo

[1] Ministry of Home Affairs, Incidents of Digital Arrest, Mar 25, 2025, available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2114750, (Last visited on April 12, 2025).

moto case[2] taken by the Rajasthan High Court. The court recognised digital arrest scams as one of the most insidious cybersecurity threats. It directed both the State and Central Governments to take prompt action to curb the scam. The bench emphasised the absence of any legal provision permitting arrest via digital means such as video calls and called for extensive public awareness campaigns using various media outlets to dispel misconceptions about legal arrest procedures. Additionally, the court instructed the RBI and other financial institutions to formulate mechanisms to prevent payment transfers to fraudsters. This case highlights judicial recognition of digital arrest as a serious crime requiring coordinated legal and regulatory intervention. The social ramifications of digital arrest are extensive, going beyond merely financial loss. Victims often face intense psychological distress, including fear, anxiety, and humiliation, which can affect their families and communities. The emotional trauma can disrupt the social fabric, leading to isolation or distrust among victims towards legitimate authorities and digital platforms. Moreover, the pervasive fear generated by such scams undermines public confidence in digital communication and governance, particularly in a country rapidly transitioning to digital financial and administrative services. Such societal impacts necessitate strong awareness initiatives and support systems for victims.[3] Ethical concerns arise from the exploitation of vulnerable sections of society by digital arrest scammers.

The crime strategically targets those with limited digital literacy and legal knowledge, including the elderly and economically disadvantaged groups, leveraging fear and ignorance. This exploitation reveals critical ethical challenges about digital inclusion, equity, and the responsibility of state and societal actors to protect these vulnerable populations. The ethical imperative to build digital resilience requires collaborative efforts to enhance education, promote transparency, and develop accessible complaint and redressal mechanisms for cybercrime victims.[4] From a legal perspective, digital arrest encompasses various offences such as impersonation, fraud, forgery, and extortion, often executed through elaborate schemes that cross geographical boundaries. The fragmented nature of related laws complicates timely investigation and prosecution, especially as scam operations frequently originate outside India. Enforcement agencies face challenges in tracking and apprehending perpetrators amid jurisdictional complexities and technological sophistication. Despite efforts to enhance cyber forensic capabilities and inter-agency coordination, continuous evolution in scam tactics demands adaptive legal and technological responses anchored in victim protection and swift justice.[5] The rapid digitalisation of financial and communication systems in India has increased both convenience and vulnerability. With more citizens engaging in online banking, mobile payments and government e-services, the attack surface for digital arrest scams expands correspondingly.

Fraudsters leverage cutting-edge techniques such as voice manipulation and fake digital identities, which complicate detection and prevention efforts. This dynamic necessitates a proactive approach combining technological innovation, legal vigilance and public sensitisation to reduce risks and enhance user confidence in digital ecosystems. Comprehensive prevention of digital arrest requires a coordinated multi-stakeholder response. The government has initiated several campaigns and platforms focusing on cybercrime awareness and reporting, such as CyberDost and the Indian Cyber Crime Coordination Centre. Public education and capacity building among law enforcement agencies are equally vital to increasing detection and response efficiency. Enhanced cooperation between financial institutions, telecom providers, and cyber police ensures the timely blocking of fraudulent channels and secure transaction frameworks.[6] These integrated efforts are essential to creating a safer digital environment, encouraging trust and protection for all users. It is a growing cybercrime in India that presents complex challenges that transcend legal dimensions, deeply impacting social trust and ethical norms. Its prevalence underscores the urgent need for a balanced, multifaceted strategy focusing on legal rigour, social support, ethical responsibility, and technological innovation. Strengthening public awareness and institutional readiness will be crucial in safeguarding individuals from this pernicious cyber threat and sustaining India's digital transformation with security and confidence.

**Digital Arrest**

Digital arrest, as explained by the Hon'ble Prime Minister during the "Mann Ki Baat" episode on 27th October 2024, refers to a fraudulent act where scammers impersonate law enforcement or government officials through digital means such as calls or messages, falsely claiming that the victim is under investigation and facing immediate arrest. This intimidation tactic compels individuals to pay money or disclose sensitive information out of fear, despite no lawful basis for such digital or remote arrests. The Prime Minister stressed that lawful arrests require following formal

[2] Suo Motu: Tackling the Issue of 'Digital Arrest Scams v. UOI, CW/1311/2025.
[3] Dr. Ruchi Gupta, "Scammed into Silence: A Study of Digital Arrest Cybercrimes in India Through the Lens of AI Manipulation, Legal Loopholes, and Socio-Financial Impact", 14 *Journal of Neonatal Surgery*, 2025.
[4] Major Sadhna Singh, Digital Arrest: The Modern-Day Cyber Scam, available at: https://securitylinkindia.com/eMagazine/February2025.php, (Last visited on April 12, 2025).
[5] Ministry of Home Affairs, Lok Sabha Question No. 3100, Aug 2025, available at:https://mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/RS20082025/3100.pdf, (Last visited on April 12, 2025).
[6] Press Information Bureau, Government of India, "Government Initiatives on Cyber Crime Awareness," October 2024, available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2082765, (Last visited on April 12, 2025).

procedures and cannot be executed through unverified digital communication channels.[7] According to the Indian Cyber Crime Coordination Centre, Cyber Crime Portal, digital arrest is a cybercrime involving impersonation, coercion and fraud executed through electronic communication to simulate official arrest or legal threats. The NITI Aayog's detailed report defines digital arrest as unlawful digital manipulation designed to create fear of legal consequences, prompting victims to comply with extortion demands. This definition highlights the scam's basis in psychological manipulation and misuse of digital infrastructure to deceive and exploit individuals. The Ministry of Home Affairs and the Indian Cyber Crime Coordination Centre also recognise digital arrest scams as a significant and evolving cyber threat in India, emphasising the use of fake digital identity and intimidation tactics to defraud citizens.[8] The definition of digital arrest as a cybercrime involving impersonation, coercion, and fraud through electronic communication is elaborated in key government reports and legal analyses specific to the Indian context.

**Criminal Elements and Categories in Digital Arrest**

Digital arrest encompasses multiple categories of crimes that are executed through digital platforms to intimidate and exploit victims. Research indicates that these scams primarily involve impersonation offences, where cybercriminals falsely represent themselves as law enforcement officers, court officials, or representatives from regulatory agencies such as the Central Bureau of Investigation, Narcotics Control Bureau, or Income Tax Department. The fraudsters employ sophisticated digital manipulation techniques, including deepfake technology, to create convincing video calls and audio communications that simulate authentic official interactions. The criminal activities associated with digital arrest include cheating and fraud, where perpetrators deceive victims into believing they are under investigation for serious crimes such as money laundering, drug trafficking, or financial terrorism.

These accusations are often supported by fabricated evidence, including fake legal documents, arrest warrants, and court orders designed to enhance credibility and instil fear. Criminal intimidation forms another significant component, as scammers use threats of immediate arrest, imprisonment, or asset confiscation to coerce victims into compliance with their demands. Additionally, digital arrest crimes encompass extortion and financial fraud, where victims are forced to transfer money under false pretences of securing bail, paying compliance bonds, or proving their innocence. Identity theft and data manipulation are also integral elements, as criminals often use stolen personal information to create believable narratives and enhance their deceptive schemes. The psychological manipulation involved includes cyberstalking and harassment, particularly when victims are forced to remain on continuous video calls for extended periods, creating a sense of digital captivity that amplifies the trauma and ensures victim compliance.[9]

**Societal Impacts of Digital Arrest Scams**

1. Digital arrest scams erode public trust in law enforcement and judicial systems, as victims and bystanders struggle to distinguish genuine official communication from fraudulent messages, leading to widespread fear and suspicion.
2. Financial stability of individuals and families is severely compromised when victims are coerced into paying large sums under false legal threats, often resulting in long-term economic hardship and debt.
3. The psychological distress caused by prolonged intimidation and isolation during these scams can lead to anxiety, depression and a lasting sense of vulnerability, especially among elderly or socially isolated individuals.
4. Communities face social stigma and reputational damage when victims are reluctant to report incidents, fearing shame or disbelief, which perpetuates underreporting and allows criminals to operate with impunity.
5. The diversion of law enforcement resources to investigate and prosecute digital arrest cases strains police and judicial capacity, delaying response to other crimes and undermining overall public safety efforts.

**Government Legislative Measures and Initiatives to Combat Digital Arrest Scams**

India's approach to tackling digital arrest scams is supported by legislative provisions and numerous government initiatives aimed at prevention, reporting and investigation. Under the Information Technology Act, 2000, Section 66D punishes cheating by impersonation through digital means with imprisonment of up to three years and a fine of ₹1 lakh. The Bharatiya Nyaya Sanhita, 2023, prescribes penalties ranging from three to ten years' imprisonment for offences including cheating under Section 415, cheating by personation under Section 419, and extortion under Section 423. To enhance public awareness, the Ministry of Electronics and Information Technology collaborated with the Department of Telecommunications to introduce automated caller tunes in multiple regional languages during 2022-23, cautioning people against fake arrest calls. Telecom operators were also instructed by the Department of Telecommunications to send regular SMS alerts to subscribers about active digital arrest scams[4]. On 27th November, the PIB in Delhi issued an important press release highlighting the Central Government's efforts to raise awareness about cybercrime, including digital arrest scams. These efforts include sending informative messages via SMS and actively engaging on social media platforms such as X (formerly Twitter) (@CyberDost), Facebook (CyberDostI4C), Instagram (cyberDostI4C),

[7] Prime Minister Narendra Modi, Mann Ki Baat, 27 October 2024, available at: https://www.pmindia.gov.in/en/news_updates/mann-ki-baat-episode-86-october-27-2024/ (Last visited on April 12, 2025).

[8] Supra note 1.

[9] Rishabh Chaudhary, "Dr. Kanika Aggarwal, AI-Driven Digital Arrest Scams: Legal Gaps in Regulating Deepfake Impersonation", 6 *International Journal of Research Publication and Reviews*, 2025.

and Telegram (cyberdosti4c). Ongoing radio campaigns and collaborations with MyGov amplify publicity across various media channels. The government also organises Cyber Safety and Security Awareness weeks in partnership with States and Union Territories. To educate the youth, handbooks designed for adolescents and students have been published, while newspapers run advertisements on digital arrest scams. Public announcements are made on Delhi metro trains about digital arrest and other cybercrime tactics and social media influencers are engaged to create special posts to spread awareness. Digital displays have been set up in railway stations and airports nationwide, ensuring widespread visibility of the campaign and reaching diverse communities. The Ministry of Home Affairs established the Indian Cyber Crime Coordination Centre (I4C) in 2020, which manages the National Cyber Crime Reporting Portal, allowing citizens to lodge complaints and track their progress online.

The RBI, in January 2022, mandated banks and payment service providers to install real-time fraud monitoring systems and immediately block transactions linked to impersonation fraud. Moreover, the Cyber Surakshit Bharat initiative organizes training workshops for law enforcement personnel, and the CyberDost campaign offers helpline support and digital literacy programs specifically designed to protect vulnerable groups. Victims of digital arrest scams can report incidents through the National Cyber Crime Reporting Portal or their local police cybercrime cells, supplying relevant evidence like screenshots, call logs, and transaction records. Looking ahead, there is a pressing need for the government to introduce a specific offence targeting digital arrest scams, standardise procedures for grievance redressal, improve international cooperation for cross-border investigations, and require telecom and financial institutions to conduct regular compliance audits to prevent scams. Despite these efforts, the lack of a dedicated law for digital arrest highlights the urgent requirement for legal reforms, clearer procedural frameworks, and ongoing public education to effectively address this growing cyber threat.[10]

**International Treaties Approaches to Digital Arrest**

Fundamental rights to privacy are well established in international treaties and increasingly recognised in the digital environment. Article 12 of the Universal Declaration of Human Rights states that no one shall be subject to arbitrary interference with their privacy, and everyone has the right to legal protection against such infringements. Similarly, Article 17 of the International Covenant on Civil and Political Rights protects individuals from unlawful or arbitrary interference with their privacy or attacks on their reputation, extending these safeguards equally to online platforms. Since 2013, the United Nations General Assembly and Human Rights Council have adopted multiple resolutions emphasizing the right to privacy in the digital age, notably in 2019 and 2020, reaffirming states' obligations to respect this right in cyberspace.

Treaties such as the ICCPR, the Universal Declaration of Human Rights, and the WIPO Internet Treaties require countries to enact laws that protect against violations of individual privacy, including prohibitions on the deliberate alteration or deletion of electronic records and information. In addition, regional instruments like the European Union's General Data Protection Regulation offer robust protections against online fraud and misuse of personal data. The UN Convention against Transnational Organised Crime (Palermo Convention) obliges signatory states to criminalise activities carried out by organised criminal groups and establish frameworks for legal assistance, extradition, and international cooperation. The Council of Europe's Budapest Convention on Cybercrime was the first international treaty harmonizing laws to combat cybercrime through improved investigation techniques and cross-border collaboration. These conventions set international standards against cyber-enabled crimes, including digital impersonation and fraud.[11]

**Judicial Pronouncements**

Several significant judicial pronouncements have shaped the legal understanding and enforcement response to digital arrest scams in India. In Noida Cybercrime Case No. FIR/12/2023, Noida Cybercrime Police Station, the trial court's order in March 2024 recognized the novel modus operandi of digital arrest, recording that the accused had impersonated Delhi Police officers through spoofed calls and fabricated arrest warrants to extort ₹11.2 lakh from the victim, thereby setting a precedent for prosecuting such scams under Section 420 for cheating and Section 384 for extortion of the IPC as well as Section 66D for cheating by personation of the Information Technology Act.[12] In January 2025, the Rajasthan High Court in Suo Motu Writ Petition, directed both the State and Central Governments to launch nationwide awareness campaigns on legitimate arrest protocols and instructed the RBI to devise mechanisms for blocking transactions linked to digital arrest scammers, affirming the judiciary's proactive role in consumer protection against cyber fraud.[13] The landmark conviction in the Kalyani Nadia case, delivered by the Sessions Court, sentenced nine members of a cross-border syndicate to life imprisonment for defrauding victims of over ₹1 crore by simultaneous

[10] Jyoti Chauhan, "Digital Arrest: An Emerging Cybercrime in India", *International Journal of Law Management & Humanities*, 2024.
[11] Ibid.
[12] Noida logs first case of 'digital arrest', woman duped of over Rupees 11 Lakh, Times of India, available at: https://timesofindia.indiatimes.com/city/noida/noida-logs-first-case-of-digital-arrest-woman-duped-of-over-rs-11-lakh/articleshow/105683261.cms, (Last visited on April 12, 2025).
[13] Supra note 2.

impersonation of multiple enforcement agencies, illustrating the application of Sections 120B, 420, 384, and 66D in a cohesive prosecution strategy.[14] Most recently, case involved fraudsters attempting to extort Rs 2 crore from retired Bombay High Court judge Vijay Daga through a digital arrest scam. The perpetrators contacted him via a video call, falsely accusing him of involvement in a criminal case and threatening immediate arrest unless the demanded amount was paid. Demonstrating alertness and integrity, Justice Daga promptly reported the incident to the Nagpur Cyber Police, enabling authorities to trace the call to the Rajasthan-Gujarat border and commence investigations. This incident reflects the audacity and psychological manipulation used by scammers who target even prominent figures and underscores the urgent need for enhanced protections and swift law enforcement action against such digital extortion attempts.[15] Collectively, these judgments underscore the judiciary's evolving jurisprudence on digital arrest, reinforcing the principle that lawful arrest must adhere to statutory safeguards and that any attempt to simulate legal threats through digital means is unequivocally fraudulent and punishable.

**Challenges in Combating Digital Arrest Scams**

1. The absence of a distinct offence for digital arrest in Indian statutes hampers targeted prosecution, as authorities must piece together charges under cheating, extortion and impersonation provisions, leading to fragmented legal responses and inconsistent sentencing.
2. Jurisdictional challenges arise when scam operations are conducted from foreign servers or involve transnational networks, complicating evidence gathering, extradition and mutual legal assistance processes under existing frameworks.
3. Rapid advancements in digital technologies, including voice cloning and deepfake video calls, outpace legislative updates and strain law enforcement's technical capabilities, making it difficult to authenticate communications and trace perpetrators.
4. Limited digital literacy and awareness among large segments of the population leave victims vulnerable to sophisticated scams, as many do not recognise the signs of fraudulent legal threats or know the proper channels for verification and reporting.
5. Resource constraints and insufficient training in cyber forensics within many police units hinder timely investigation and prosecution, leading to delays that embolden scammers and frustrate victim confidence in the justice system.
6. Data privacy regulations and the need to protect sensitive personal information can restrict law enforcement's access to critical digital evidence, necessitating careful balancing between investigative needs and individual privacy rights.
7. Procedural inadequacies, such as the lack of streamlined protocols for blocking fraudulent communication channels and freezing illicit financial transactions, delay preventive action and allow scammers to repeatedly exploit victims before authorities can intervene effectively.

## CONCLUSION

Digital arrest has emerged as a significant cybercrime challenge in India, reflecting the broader complexities of the digital age's impact on legal and social frameworks. The scam's modus operandi fraudsters impersonating law enforcement or government officials using sophisticated technology exploits fear and misinformation, inflicting profound financial and psychological harm on victims. Despite existing provisions under the Information Technology Act and the Bharatiya Nyaya Sanhita, these general laws fall short in addressing the unique features of digital arrest scams, such as the use of voice cloning, deepfake videos, and transnational operations. The lack of a dedicated statutory offence leaves gaps that impede swift investigation and consistent prosecution. Government initiatives, including the establishment of the Indian Cyber Crime Coordination Centre, the National Cyber Crime Reporting Portal, caller tune advisories and SMS alerts, have made commendable progress in raising public awareness and facilitating reporting mechanisms. Campaigns like CyberDost broaden outreach to vulnerable groups, offering helpline support and digital literacy education vital for prevention.

However, technological advancements and evolving criminal methods continue to test the capacities of law enforcement and regulatory bodies, underscoring the urgent need for legal and operational reforms. International experience provides valuable lessons in this context. Jurisdictions such as the UK, the US, Singapore and Australia have developed targeted legislation and judicial frameworks specifically recognising digital impersonation and fraud as serious offences. Their laws often include detailed provisions addressing electronic deception, advanced technological tools in crime and mechanisms for international cooperation. India's current reliance on more general provisions contrasts with these focused approaches, highlighting a clear opportunity for legislative modernisation and enhanced

[14] Rajesh Saha, India's first digital arrest conviction: 9 sentenced to life by Bengal court, available at: https://www.indiatoday.in/india/law-news/story/indias-first-digital-arrest-conviction-nine-people-sentenced-to-life-by-bengal-court-2758042-2025-07-19, (Last visited on April 13, 2025).

[15] Digital Arrest Scam: Former Bombay High Court Judge Targeted in Digital Extortion Scam," ET Legal World, July 12, 2025, available at: https://legal.economictimes.indiatimes.com/news/litigation/former-bombay-high-court-judge-targeted-in-digital-extortion-scam/122421942 (Last visited on April 13, 2025).

cross-border collaboration. To effectively combat digital arrest scams, India must enact specific laws defining these offences with clear penalties and procedural guidelines. There must also be a strengthening of investigative infrastructure, consistent training for law enforcement, and expanding public education campaigns. International partnerships should be harnessed to improve intelligence-sharing and coordinated actions against transnational fraud networks. Only through a comprehensive and adaptive approach, integrating legal precision, technological innovation, and public awareness, can India hope to mitigate the growing threat of digital arrest and protect its citizens fundamental rights and financial security in the digital era.

**Recommendations**

[1]. The government should introduce dedicated laws explicitly criminalising digital arrest scams, with clear definitions, adequate penalties and procedural safeguards to enable effective prosecution and deterrence.
[2]. Strengthening cyber forensics units and providing specialised training to law enforcement agencies is essential to keep pace with evolving technologies like voice cloning and deepfakes used by scammers.
[3]. Continuous nationwide education programs using multiple media, including regional languages and vulnerable group-focused initiatives like CyberDost, should be intensified to help citizens recognise and report digital arrest attempts.
[4]. Streamlining the National Cyber Crime Reporting Portal for user-friendliness and ensuring timely grievance redressal will boost victim confidence and facilitate quicker law enforcement responses.
[5]. Given the transnational nature of many digital arrest syndicates, India must actively strengthen bilateral and multilateral agreements for intelligence sharing, extradition, and joint investigations.
[6]. Regulatory bodies like the Department of Telecommunications and the Reserve Bank of India should enforce regular audits and fraud detection mandates on service providers to prevent misuse of communication and payment channels in digital arrest scams.