
DIGITAL ARREST SCAMS AND THE EVOLUTION OF CYBER FRAUD LAWS IN INDIA

Nitish Kumar P, B.A.LL.B., PES University, Bengaluru¹

ABSTRACT

India's rapid digitalisation has transformed governance, commerce and financial transactions while simultaneously creating new opportunities for sophisticated cybercrime. It has revolutionised how the government, commerce and the financial world are governed, but it has also opened opportunities for high-tech cybercrime. The fast-growing scam is the "digital arrest scam"² in which the fraudsters pretend to be from a law enforcement agency or government official and ask the victim to wire money to a criminal account in order to fund an investigation. These scams are not purely technological in nature, but instead use social engineering, intimidation and use of public authority to trick victims into reacting. While the Indian legal framework offers avenues for prosecution of various elements of these offences through existing laws, including the Information Technology Act, 2000³, the Bharatiya Nyaya Sanhita, 2023 (BNS)⁴, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the framework is largely reactive and fragmented. This article examines the enactment of the Cyber Fraud legislation in India, highlights the application of existing legislation in the context of Digital Arrest Fraud, practical issues involved in Cybercrime Investigations and Cybercrime Prosecutions and proposes reforms for improving Cybercrime Governance in India. It affirms that the fight against digital arrest scams should be carried out through a coordinated strategy, which includes some legislative changes, technological innovation, cooperation between institutions and raising awareness among citizens.

Keywords: Digital Arrest Scam, Cyber Fraud, Information Technology Act, Bharatiya Nyaya Sanhita, Electronic Evidence, Cybercrime, and Social Engineering.

¹ B.A. LL.B., PES University, Bengaluru.

² Ministry of Home Affairs, Government of India, *Advisory on Digital Arrest Scams* (2024).

³ Information Technology Act, 2000.

⁴ Bharatiya Nyaya Sanhita, 2023.

I. Introduction

In the past decade, India has experienced an unprecedented shift towards digital transformation. Many such initiatives, like Digital India⁵, the rapid pace of internet penetration, Aadhaar authentication and the popularity of the Unified Payments Interface (UPI)⁶, have revolutionized the economic and administrative landscape of the country. Today, there are millions of electronic transactions taking place every day, of course, which enhance efficiency, financial inclusion and access to government services. With this digital revolution, however, there are more possibilities for the cybercriminal, too, and cyber-enabled financial frauds⁷ are becoming more sophisticated.

Since the beginning of the days of hacking through emails, spoofing and Malware attacks, Cybercrime in India is now far from what it was in the beginning. Nowadays, modern criminals will take advantage of the psychology of the people instead of the vulnerabilities in technology, which is known as the social engineering approach⁸. Advanced scam variations on this theme include digital arrest scams. The scams involve various individuals pretending to be from agencies such as the Central Bureau of Investigation (CBI)⁹, Enforcement Directorate (ED), Customs, Reserve Bank of India (RBI)¹⁰ or police. The victims are told that they are committing crimes such as money laundering, financial fraud or narcotics trafficking and will be arrested if they do not cooperate in an alleged investigation.

The modus operandi is usually lengthy video calls, fake legal documents, spoofed caller-ID and fake arrest warrants. Victims are instructed to transfer funds into accounts falsely represented as government verification or escrow accounts. Offenders capitalize on the fears, urgency and faith that victims have in public institutions, leaving victims to do their own investigation without any voluntary transfer of money. Digital arrest scams are, then, to an extent, different from the usual cyber frauds, in that they are not, for the most part, based on access.

⁵ Ministry of Electronics and Information Technology, *Digital India Programme*.

⁶ National Payments Corporation of India, *Unified Payments Interface Annual Report*.

⁷ National Crime Records Bureau, *Crime in India Report 2023*, Cyber Crime Chapter.

⁸ Kevin D. Mitnick, *The Art of Deception* (Wiley Publishing, 2002).

⁹ Central Bureau of Investigation, Official Website.

¹⁰ Reserve Bank of India, Official Website.

As these scams are emerging, the effectiveness of the law in India is a serious question. Offences related to cheating, Identity theft, personation, forgery, etc., are distributed across different legislations such as the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023. Together, these laws convey the requisite powers to prosecute, but do not mention digital arrest scams as a particular category of organised financial crime. Consequently, investigators may need to trigger more than one provision at the same time, and the procedures may be different or may be implemented differently.

This article thinks it is a structural flaw in the Indian Cyber Crime system, that is the digital arrest scam. The law effectively punishes many aspects of the crime, but fails to provide an integrated legislative and institutional framework specifically directed towards the prevention, investigation and prosecution of this new type of cyber fraud. Hence, the article investigates the evolution of cyber fraud law in India, explores whether the legislation can be extended to cyber fraud, observes the challenges of the investigative agencies, contrasts the stance of the Indian legislation and other foreign legislations and suggests reforms for cyber fraud governance in the digital era to combat cyber frauds. Hence, the article discusses the evolution of cyber fraud laws in India and the applicability of existing laws, challenges faced by the investigative agencies and comparative analysis with foreign approaches and proposes the reforms in cyber fraud governance in the digital era.

II. Understanding Digital Arrest Scams and the Evolution of Cyber Fraud Laws in India

Digital arrest scams are one of the most sophisticated types of cyber-financial fraud that are happening in India. The scams are not designed by using other cybercrimes like phishing, malware, or hacking, but rather by using what is referred to as social engineering¹¹, a science that makes individuals do tasks they wouldn't normally do out of concern, or deceptive methods, or abuse of authority. The scamsters pretend to be from the Central Bureau of Investigation (CBI), Enforcement Directorate (ED), Narcotics Control Bureau (NCB) or Police departments to make the victim believe that they are somehow related to a crime, such as money laundering, financial fraud, tax evasion or narcotics trafficking. The victims face threats of arrest, their bank accounts are frozen, or criminal proceedings are initiated against them if they

¹¹ Kevin D. Mitnick, *The Art of Deception*.

do not comply with the "investigating officers".

The usual pattern of the *modus operandi* is regular. Someone pretending to be from a government agency calls or video calls the victim. To gain credence, fraudsters use spoofed phone numbers, identity cards with altered information, fake arrest warrants or fake judicial documents. Victim is instructed to stay in touch via continuous video calls, prevented from contacting family members or legal counsel and coerced to put money into bogus government-controlled "verification" or "escrow" accounts. Once it is transferred, the funds are swiftly channelled along a succession of mules or are transformed into digital currency, and it is difficult to trace back.

It's important to note that, as with all these scams, they don't rely on technical vulnerabilities but rather psychological ones. Offenders can render the victim unable to verify or rationalize his or her decision through the atmosphere of urgency and legal intimidation. Therefore, digital arrest scams are not only a serious financial scam but also a well-organised cybercrime which weakens the faith in the law enforcement institutions and in the digital governance.

Digital arrest scams are also linked to overall cyber crimes in India. The primary areas of cybercrime in the early 2000s were hacking, spamming, email spoofing, software piracy and unauthorised access to computer systems. The Information Technology Act, 2000, provided legal support to electronic records and provided for offences relating to unauthorised access to computers, identity theft and cyber fraud. The Information Technology (Amendment) Act, 2008, reaffirmed the law by extending the definition of intermediary liability, identity theft and cheating by personation through computer resources and putting them as criminal acts.

After the inception of the Digital India Programme¹² and the swift roll-out of UPI, internet banking, mobile wallets and services based on Aadhaar, the Indian Digital landscape has undergone a paradigm shift. The improvements, however, transformed the nature of cybercrime in terms of financial inclusion and the ease of doing business. Over time, criminals shifted their focus from technological exploits to exploiting human behaviour by phishing, OTP fraud, QR code fraud, investment fraud, fake customer care, and lastly, digital arrest fraud. This transformation demonstrates the greater importance of the power of the mind over technology

¹² Ministry of Electronics and Information Technology, *Digital India Programme*.

in cybercrime.

The most significant changes in the law are related to the replacement of the Indian Penal Code, the Code of Criminal Procedure and the Indian Evidence Act by the Indian laws Bharatiya Nyaya Sanhita, 2023 (BNS)¹³, Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and Bharatiya Sakshya Adhiniyam, 2023 (BSA)¹⁴. These acts amended the Indian criminal law system but did not include any specific laws which address digital arrest scams. Rather, investigators are still going the old method as a mixture of various miscellaneous misdemeanour, personation, criminal intimidation, forgery, conspiracy and electronic evidence¹⁵ offences. It also indicates the absence of a dedicated law to tackle new organised financial fraud techniques through cyber means, which is what can be prosecuted.

The shift from 'technology-driven legislation' to 'protection of electronic transactions and electronic identities' signifies the gradual progression of cyber fraud laws in India. As digital arrest scams become more sophisticated, though, it is important to have more proactive policies in place. The current use of AI, caller ID spoofing, encrypted communication and digital payments, behavioural manipulation are part and parcel of cybercrime problems which were not envisioned by the Indian cyber laws. This necessitates a thorough analysis of the effectiveness of the existing legal system to meet these challenges in the face of the new ones.

III. Legal Framework, Investigative Challenges and Comparative Perspectives.

India presently has a set of legislations to address digital arrest frauds, such as the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)¹⁶, and Bharatiya Sakshya Adhiniyam, 2023 (BSA). All of these laws give the police sufficient powers to combat crime, but none target digital arrest scams as a new type of cybercrime. Thus, investigators must use multiple provisions at once, creating a disjointed enforcement system.

The Information Technology Act 2000 is the main legislation relating to cyber offences.

¹³ Bharatiya Nyaya Sanhita, 2023.

¹⁴ Bharatiya Sakshya Adhiniyam, 2023.

¹⁵ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1

¹⁶ Bharatiya Nagarik Suraksha Sanhita, 2023.C

Section 66C of the Information Technology Act, 2000¹⁷. outlaws dishonest use of electronic signatures, passwords or unique identification characteristics to commit identity theft, and Section 66D¹⁸ tackles cheating by personation involving computer resources or a communication device. These provisions come into effect automatically in situations where a person who is an offender pretends to be a police officer or a government official on the phone lines, via video conferencing or through online communications. Likewise, Sections 43¹⁹ and 72²⁰ deal with unauthorised access to computer systems and privacy violations²¹, which are often connected to digital arrest scams that involve the abuse of personal data acquired in the course of other data breaches or phishing attacks.

However, the primary thrust of the IT Act is on the technological aspect of cybercrime. It will not suffice to apply only moderate psychological pressure, virtual detention or organised impersonation of the public authorities in the frame of digital arrest scams. So, investigators have to act on the basis of the Bharatiya Nyaya Sanhita 2023 to proceed with the substantive criminal charge.

These are common crimes committed during a BNS digital arrest: cheating, personation, criminal intimidation, forgery, extortion and criminal conspiracy. The victim is induced to think that a crime is being committed against him/her and he/she has to give the money that is needed for investigations and/or verifications. The fraudsters also fake arrest warrants, fake court documents and fake ID cards to increase the believability of the fraud. Where two or more persons are involved in the collation of information, impersonation, money laundering and movement, it may go as far as to be an 'organised criminal conspiracy'.

Another important factor is the Bharatiya Sakshya Adhiniyam, 2023, which is a key piece since digital evidence is the fundamental basis of prosecution for digital arrests. The primary pieces of evidence in the investigation and trial include call recordings, WhatsApp conversations, emails, records of UPI transactions, bank statements, IP logs, CCTV feeds and recordings of video conferencing. This is an added challenge to courts as AI, voice cloning, and deepfake videos become more common. Therefore, the need for proper forensic practices and judges'

¹⁷ Information Technology Act, 2000, § 66C.

¹⁸ Information Technology Act, 2000, § 66D.

¹⁹ Information Technology Act, 2000, § 43.

²⁰ Information Technology Act, 2000, s. 72.

²¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

knowledge of the progress of technology and the future developments of technology are critical to the electronic evidence challenges.²²

Bharatiya Nagarik Suraksha Sanhita 2023 provides for the electronic search, seizure of electronic devices and retention of electronic records for procedural investigation. But it is the speed with which investigative agencies react, not their statutory powers, that is the key to good enforcement – the money is transferred to another jurisdiction and the digital evidence is deleted before the investigation.

Despite this legislation, there are many challenges in implementation. Transnational criminals usually behind these scams employ encrypted communication sites and spoofed caller ID, virtual private networks (VPN) and cryptocurrency²³ payments. Fraudulently obtained funds are generally disbursed into multiple mule accounts in minutes, making asset recovery very difficult. This means that there is a need for immediate coordination between banks, payment intermediaries, telecommunications operators, internet service providers, cyber forensic laboratories and law enforcement agencies to be successful in investigating such a crime. Freezing bank accounts and/or 'freezing' bank accounts until electronic evidence is captured and collected greatly reduces the likelihood of successful prosecution and restitution for the victim.

Lack of Digital Forensic is also a big challenge. Electronic evidence is easily altered, deleted, remotely encrypted or even erased from a computer, and the preservation and analysis of electronic evidence will require specific forensic skills. The rise in AI has also made investigations more difficult as fraudsters can now create a realistic voice clone, make fake documents and deep fake videos that can fool victims and make it harder to prove their authenticity. Therefore, there is a need to enhance the forensic resources and continued education of investigators, prosecutors and judges.

It is seen that there are some jurisdictions that have been more preventive than India. Singapore's²⁴ financial institutions have to put measures in place to detect fraud, and the government promotes public awareness of fraud, including the ScamShield app. There are both criminal and regulatory controls in Singapore. The criminal prosecution and criminal

²² Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

²³ Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators*.

²⁴ Computer Misuse Act (Singapore).

coordination/banking protection mechanisms have been established in the United Kingdom²⁵, as have the rules which allow customers to confirm the identity of the beneficiary of the funds before they are transferred (the "Confirmation of Payee" service). Australia²⁶ also has a whole-of-government approach with dedicated agencies, regulation of telecommunications, behavioural analysis, and a National public awareness campaign.

The jurisdictions highlight the need for good governance beyond the criminal law in combating cyber fraud. Other key strategies to prevent victimisation are preventive regulation, development of new technologies, coordination of institutions, and public education. India's legal framework to address challenges arising from modern-day cybercrime has definitely evolved and is a reactive approach. Several laws have been enacted for different purposes, but since there is no specific legislation targeting digital arrest scams, they have to be utilised to stop scams. Increased criminal liability should not be the only way in which improvements can be developed in the future, but an integrated cyber fraud governance framework should be developed that can prevent, detect and respond to increasing sophistication in cyber deception.

IV. Recommendations and the Way Forward.

It is evident that digital arrest scams have become a new phenomenon, and there is a need to have a holistic and proactive approach towards the escalating number of cybercrimes in India. Instead of new criminal laws, there is a need to focus on enhancing the coordination of legal, regulatory and technological mechanisms.

First, the Legislature should look at adopting a statutory definition of digital arrest scams. Having a clear legal definition of these offences would clarify the distinction between these offences and the existing cyber fraud definition and recognise the unique characteristics (digital impersonation of public authorities, psychological coercion and financial extraction). This would have led to uniformity in the investigation and prosecution of existing laws and in their interpretation by the judges.

Secondly, the regulation of financial institutions and payment service providers needs to be increased. Banks must embrace AI technologies²⁷ to identify fraudulent transactions, user

²⁵ Fraud Act 2006 (UK).

²⁶ Australian Cyber Security Centre, ScamWatch.

²⁷ Reserve Bank of India, Annual Report 2024.

behaviour, and risky transfers that could indicate forced scams. New security checks for unusually high purchases and instant alerts to consumers can substantially minimise monetary losses without sacrificing the efficiency of digital payment solutions.

Thirdly, telecommunications companies must enhance caller authentication to minimise the number of times caller ID is spoofed, one of the most common techniques employed by fraudsters. Better coordination amongst telecom²⁸ operators, banks²⁹ and law enforcement would help in the quick identification of fraudulent communications and help preserve electronic evidence.

Moreover, there is a need to make capacity building in digital forensics a part of the discussion. Training should be provided to investigative agencies continuously in areas of AI, blockchain analysis, digital evidence preservation, and Cyber forensic investigation. Modern technological infrastructure, as well as specialized forensic laboratories, are also crucial for reliable and scientifically valid electronic evidence to the courts.

However, international cooperation is necessary to further strengthen transnational digital arrest scams. The Government of India should also enhance its bilateral and multilateral collaboration to exchange information, extradition, collect digital evidence and recover assets. Enhanced cooperation with foreign financial intelligence units and law enforcement agencies will enhance the investigation of cybercrime that is organised transnationally.

Last but not least, a greater awareness among the general public regarding the laws should be an integral part of India's cybersecurity policy. Government agencies, educational institutions, banks, and digital platforms should carry on the awareness campaign, highlighting that none of the legitimate investigating agencies makes arrests via video call, demand the confidential banking details via phone calls, or guide the citizens towards transferring money into verification accounts. When there are more people who understand what is happening, there are fewer chances of social engineering techniques being used to lay the foundations for digital arrest scams.

²⁸ TRAI Regulations on Unsolicited Commercial Communications. ²⁹ RBI Master Directions on Digital Payments Security Controls.

These collectively form a shift of the traditional criminal justice model to a new governance model, in which the law, technology, financial regulation and institutional coordination work in harmony with citizen awareness. This is necessary to respond to the changing landscape of cyber crime financial crime.

V. Conclusion

The economic revolution in India has brought in a lot of opportunities in the realm of economic growth, financial inclusion and technological innovations. It has also been instrumental in the emergence of ever-more sophisticated financial crimes via cyber technology. The digital arrest scam is a major advancement in cyber fraud as it incorporates the technology, psychology, institutions and financial networks. These scams rely on victims' trust of government entities and their actions, rather than on technological weaknesses, as do the more traditional cyber offences.

The present law of India, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, the Information Technology Act, 2000 and Bharatiya Sakshya Adhiniyam, 2023, already have sufficient statutory provisions to prosecute numerous facets of digital arrest scams. However, the absence of a coordinated and effective legal framework can result in a lack of consistency in the implementation of the law, delays in investigations and asset recovery. More traditional means of cybercrime enforcement remain challenging, as do the use of artificial intelligence, encrypted communication, caller ID spoofing and cryptocurrencies.

This demonstrates that a robust governance framework in the fight against cyber fraud is not simply one of criminal penalties – Singapore, the UK and Australia have proved this. The prevention of cyber victimisation is also an issue, and can be addressed with cutting-edge technologies to track fraud, cooperation between institutions and continuous public awareness campaigns. India has already taken a great leap forward by setting up special cybercrime units, the Indian Cyber Crime Coordination Centre (I4C) and digital reporting systems. Such actions, however, should be matched with stiffer rules and regulations; increased cooperation between countries; enhanced digital forensic tools, and a National strategy specifically for digital arrest scams.

In sum, digital arrest scams are a prime example of how cybercrime has changed and adapted to the digital era. With evolving technology, India's legal approach should shift from a reactive

to a more proactive nature, focusing on prevention, technological resilience, and institutional cooperation. Digital governance needs a comprehensive and flexible legal structure to ensure sufficient safeguards for new forms of financial crime that take place through digital channels.