Page 4026 - 4035 **DOI:** *https://doij.org/10.10000/IJLMH.119405*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Digital Arrest in India: Navigating Challenges and Legal Framework

NIDHI GUPTA[1]

ABSTRACT

With the introduction of the World Wide Web, the whole communication technology has been revolutionized. Noteworthy changes and achievements can be witnessed in the field of Information and Communication Technology by continuous progress and innovation of technology. But it has also resulted in new types of cybercrimes called 'digital arrest.' The advancement of technology has led to the formation of the digital era in which cyber threats are also evolving. Innovative forms of cybercrimes have originated in recent times. In digital arrest, deceiving tactics are used by the cybercriminals by impersonating themselves as officials from law enforcement agencies with the main objective of extorting and receiving a hefty sum of money from individuals. This paper examines the concept of digital arrest in the context of India, rising sparks of cyber criminality as far as digital arrest is concerned by taking into consideration the reports published by NCRB, PTI, etc. The paper highlights the existing legal provisions dealing with digital arrest, such as the Information Technology Act, 2000, and the Indian Penal Code, 1860 (now Bhartiya Nyaya Sanhita, 2023). However, the paper analyzes certain challenges that acts as a loophole in ensuring the security of individuals, such as lack of awareness, rigid enforcement mechanisms, rapid increases in technology, etc. Government initiatives play an important role in providing a solution to the existing problem of such crimes. At last, the paper offers probable recommendations that can be adopted by the different stakeholders to ensure justice for the victims of digital arrest and suggestions that can curb the menace of this type of crime committed virtually, ensuring a sound and secure digital ecosystem in India.

***Keywords**: Communication Technology; Digital Arrest; Cyber Criminality; Impersonating; Digital Ecosystem.*

I. INTRODUCTION

Almost every facet of life has been touched by the recent developments and expansion of computer and digital engrossment of the economies. These developments have brought new challenges in the form of cybercrimes, proving them to be new stakeholders causing threats in this digital realm[2]. In recent years, internet usage and digital services have increased to a large

[1] Author is a PhD Scholar at Uttaranchal University, India.

[2] Pawan Sood & P. Bhushan, *A Structured Review and Theme Analysis of Financial Frauds in the Banking*

 [ISSN 2581-5369]

extent, which has unfortunately resulted in the rise of digital crimes. The traditional form of crimes was mainly confined to cuts and knives, theft, extortion, etc., but digitalization has changed the outlook of criminals towards the commission of crimes, as now they are in the form of bits and bytes. One of the most fascinating forms of cybercrime is the 'digital arrest.' It is a type of scam in which victims are put under pressure and forced to remain on a video call with the fraudsters until and unless their greedy demands are fulfilled. Posing themselves as officials from government departments and law enforcement agencies, trying to extort money from their target audience over video calls[3]. They try to pressurize the target audience by asking them to transfer hefty sums of money, and if not done, they will construct and lodge false legal cases. In the age of the internet, digital arrest has become a significant concern where they exploit the trust and confidence of people from the lawful authorities, creating a growing menace globally[4]. These cybercriminals take the help of the dark art of manipulating psychological thinking, and most importantly, a devastating effect is caused by way of a social engineering technique by posing them as a bank representative, creating a panic- like situation where someone is having access to your account and asking the victim about the financial credentials such as passwords, PINs, OTPs, etc. Digital arrest is a terminology used as a cybercrime technique in which cybercriminals create a psychological situation in which they claim to have the victim's family members and friends being involved in criminal activities like drug trafficking, money laundering, organ trafficking or their important documents such as Aadhaar card or PAN card being linked to some illegal activities, making the target individual believe in the fake situation created for him and getting arrested over the video call for hours till their wishes are fulfilled. The first focus of this paper is to highlight the concept of digital arrest, the rising sparks of cyber criminality, preferably in terms of digital arrest in India, causing a major challenge in the smooth functioning of the economy, thereby affecting the trust and confidence of people in the concerned authorities, and what are the acts that fall under the category of digital arrests.

The paper also aims to analyze the legal framework and legislative provisions concerned with the penalization of digital arrest incidents, taking into consideration different legislation such as IT Act, 2000, IPC (now BNS), etc. On the other hand, it also explores various incidents of digital arrest that occurred in different cities. The overall findings of the paper are clubbed together into practical suggestions and recommendations as to what changes could be made in

Industry, 9 Asian J. Bus. Ethics 305, 305-21 (2020), available at https://doi.org/10.1007/s13520-020-00111-w.

[3] Jyoti Chauhan, *Digital Arrest: An Emerging Cybercrime in India*, Issue 6 Int'l J.L. Mgmt. & Human. 7, 1632 (2024).

[4] Saroj Shekhar Mallick, Digital Arrest Scams in India: Challenges and Solutions Under the IT Act, 2000 (Dec. 25, 2024) https://ssrn.com/abstract=5076535 or http://dx.doi.org/10.2139/ssrn.5076535.

the existing technologies and legal frameworks to overcome the menace of digital arrest and to safeguard India's future digital perspectives.

(A) Methodology

The design and execution of this study are based upon the doctrinal research. The information that has been used in this study is a collection from secondary sources and is based upon the review of the existing literature relevant to the topic of study. Evaluations from various academic publications, inclusive of reputed journal articles, reference books, and conference papers. Other materials that act as components of secondary resources were taken from the internet, which is relevant to the paper and contributes much to the analysis.

II. DIGITAL ARREST IN INDIA: AN INEVITABLE CHALLENGE

Science and technology are having control over almost everything, heading towards a technology-friendly era. Every sector is grabbing advantage out of technology, but it is also giving an invitation for the cybercriminals to take benefit out of the vulnerabilities attached to such technologies, becoming a key problem for mankind[5]. India is witnessing a gradual increase in the number of digital crimes that have changed the evolving landscape of cyber jurisprudence[6]. Digital arrest usually occurs like a fraudulent scheme in which fraudsters impersonate themselves as law enforcement officers or government officials, causing deception to the ones who are digitally arrested by making them believe that they are going to face criminal charges or arrest because of their involvement in illegal activities, unpaid taxes, evasion of taxes, etc. Here, the main aim of the scammer is to frighten the victim over the phone, video call, social media, or email to pay the required sum of money or share personal information.

(A) How digital arrest scam work?

Digital arrest is a new form of cybercrime that can be committed in the following ways:

- Message: Contact with the victim is established by way of an SMS, email, or WhatsApp text. The number is shown to have been linked with criminal and illegal activities such as pornography, money laundering, etc., and asking the victim to call a specific number to avoid chances of digital arrest.
- Video Call: Here, a video call is made from Skype or WhatsApp impersonating themselves as officials from government agencies like CBI, ED, etc. Appropriate uniform are worn by

[5] A. Singh et al., *Cyber-Crime and Digital Forensics: Challenges Resolution*, 2023 Int'l Conf. on Computer Comm. & Informatics (ICCCI), Coimbatore, India, 1-7 (2023), https://doi.org/10.1109/ICCCI56745.2023.10128333.
[6] Keshav Patel & Gyamar Nemey, *Digital Arrest: The Intersection of Law Enforcement and Media in the Digital Age* (Feb. 20, 2025) https://ssrn.com/abstract=5146128.

them, deceiving the victim into believing in the fact that they truly belong to government agencies.

- False Allegations- Serious accusations are made against the victim during the call, creating a panic-like situation for the victim to fulfill their demands.
- Continuous Intimidation- By posing as cops and government officials, cyber fraudsters put force on the victim by maintaining a continuous presence on the call. This is done to ensure that the victim is not able to have consultation with others.
- Extortion- A demand for hefty sum of money is made to clear the charges against the victim. Mule accounts are created to transfer funds from the victim's account to mule accounts[7].

(B) Rising sparks of cyber criminality

As far as digital arrests are concerned, there is a great surge in the number of incidents of digital arrest, which almost tripled in 2024 as compared to the year 2022. The below-mentioned National Cyber Crime Reporting Portal (NCRP) data relates to digital arrest scams and was furnished by Minister of Home Affairs, Mr. Bandi Sanjay Kumar.

Year	Incidents (in lakhs)	Amount involved (in crore)
2022	39,925	91.14
2024	1,23,672	19,35.51

Fig.1: Incidents of Digital Arrests[8]

In the above Fig. 1 it can be clearly seen that incidents of digital arrests and its interconnected cybercrimes are almost thrice to the number of incidents occurred in 2022. The defrauded amount is approximately 21 times more than what it happened to be in 2022.

In a recent case, a 45-year-old woman, her daughter, and her elderly father were digitally arrested and were put on virtual hostages on video call for two days, digitally extorting Rs. 8.10 lakh from them by way of forged documents of CBI and ED. They threatened them by constructing a fictitious money laundering case against them. Fortunately, the accused were identified and got arrested[9].

[7] "*Digital Arrest: Beware of the New Cyber Scam That Alleges You of Serious Crime to Extort Money*," Econ. Times (Feb. 2025), https://economictimes.indiatimes.com/news/india/digital-arrest-beware-of-the-new-cyber-scam-that-alleges-you-of-serious-crime-to-extort-money/articleshow/114762835.cms?from=mdr.

[8] "*Digital Arrests: Cyber Crimes Tripled During 2022-24, Defrauded Amount Jumped 21 Times: Govt*," PTI News (2025), https://www.ptinews.com/story/national/digital-arrests-cyber-crimes-tripled-during-2022-24-defrauded-amount-jumped-21-times-govt/2369315.

[9] "*Delhi Police Busts Gang Behind Digital Arrest Fraud: Four Held*," PTI News (2025),

 [ISSN 2581-5369]

On 10th February, 2025, a family was put under digital arrest for up to 5 days by unknown people posing as government officials and was duped of Rs. 1 crore. Here, the victim received a call from an unknown number asking the victim to have a word with the Telecom Regulatory Authority of India (TRAI), intimidating that his SIM card would be blocked. The victim was put under pressure when he was told that his case is being handled by the Cyber Crime Branch of Mumbai as his name is involved in 24 other cases of extorting money. That's how the victim and his family member were digitally arrested over a video call, resulting in paying Rs. 1.10 crore to fraudsters[10].

Similarly, a shocking incident was reported from Noida that a 78-year-old retired banking official became a victim of digital arrest for 15 days, thereby losing a huge sum of Rs. 3.15 crore. He received a call from a person portraying him as an official from TRAI, informing him that a criminal case has been registered against him at Colaba, Mumbai, as his SIM card number seems to be involved in illegal activities, including 'hawala transactions'[11].

Two individuals from Gujarat were arrested by the Cyber Crime Police for digitally arresting a doctor and duping them of Rs.3 crore. This scam revolves around when a 54-year-old female doctor received a call from an unknown number posing as an officer from the Telecom Department telling her that her number is linked to money laundering and other unlawful activities and is going to be blocked within 2 hours. When allegations were denied by the doctor, her call was transferred to a Skype call, where another posed himself as an IPS officer from Delhi. A fake court order issued by Chief Justice of India, D.Y. Chandrachud, was shown to her, and she was asked to prove her innocence, but before that. she was required to deposit a huge sum of money in a designated bank account. She was given assurance that if proved not guilty, her money would be refunded. Under pressure and duress, she was forced to deposit a total of Rs. 3 crores into the accounts provided by the scammers[12]. In a similar case, Chairman and Managing Director of Vardhman Group, S.P. Oswal was duped of Rs. 7 crores by the fraudsters impersonating them as officials from government agencies, including CJI of India,

https://www.ptinews.com/story/national/delhi-police-busts-gang-behind-digital-arrest-fraud-four-held/2445914.

[10] "*Family of 3 Digitally Arrested for 5 Days, Cheated of ₹1 Crore*," Times of India (2025), https://timesofindia.indiatimes.com/city/noida/family-of-3-digitally-arrested-for-5-days-cheated-of-1-crore/articleshow/118140061.cms.

[11] "*Ex-Banker, 77, Put Under Digital Arrest for 15 Days in Noida Flat; Also Attends Fake SC Hearing*," Times of India (2025), https://timesofindia.indiatimes.com/city/noida/ex-banker-77-put-under-digital-arrest-for-15-days-in-noida-flat-also-attends-fake-sc-hearing/articleshow/119270968.cms.

[12] "*Doctor Conned of ₹3 Crore in Digital Arrest Scam by Gujarat Scammers*," Hindu (2025), https://www.thehindu.com/news/national/telangana/doctor-conned-of-3-crore-in-digital-arrest-scam-by-gujarat-scammers/article69155399.ece.

 [ISSN 2581-5369]

D. Y. Chandrachud[13].

Therefore, from the above incidents, it is evident that the scammers involved in causing digital arrests were having personal information of the victims, which helped them to dupe their targets. The target group of these people are entrepreneurs, businessmen, or rich people who can satisfy their greedy demands. But this does not mean that they do not target middle-class people. These crimes are the result of two scenarios; firstly, fear in the mind of the victim of being trapped in criminal activity and duress to face penal consequences, and secondly, ignorance and lack of awareness of the latest crimes in society.

III. LEGAL PROVISIONS RELATED TO DIGITAL ARREST

Digital arrest is new species of cybercrime that has originated in recent times, that's why there is no particular legislation to deal with it, but there are general primary laws that governs it:

a. Information Technology Act, 2000

In the year 2000, the need for legislation dealing with cyber offences arose. As a result, the IT Act, 2000 was enacted as a foundation of India's cyber law, covering a wide range of cyber offenses and providing punishments for the same. Law enforcement agencies are also empowered under it to investigate, arrest, and prosecute offenders. Section 66 covers offenses like data theft and unauthorized access to accounts, and personal information and punishes the defaulter with imprisonment of up to 3 years or a fine up to 5 lakh rupees or both. While Section 66 C provides for the offense of identity theft and punishes all those who use monograms, digital seals, and signatures for the purpose of defrauding the target victim, it is punishable with imprisonment up to 3 years and a fine, which may be extended up to 1 lakh rupees. On the other hand, Section 66D punishes all those who cheat another by impersonating themselves by using a computer or computer resources, being held liable with a similar punishment as under Section 66C.

Under Section 70B, the Central Government has been empowered to establish the India Computer Emergency Response Team, called CERT-In. It is an office under the Ministry of Electronic and Information technology that looks after the cybersecurity incidents. Strengthening of security-related defense in India is under its control and performs various functions in the area of cyber security such as the collection and analysis of data, real-time cyber incident reports, etc.

[13] "*Digital Arrest and ₹7 Crore Heist: How Vardhman Group Head Was Tricked*," Bus. Standard (2024), https://www.business-standard.com/companies/news/digital-arrest-and-rs-7-crore-heist-how-vardhman-group-head-was-tricked-124100100832_1.html.

b. Bhartiya Nyaya Sanhita (BNS)

Earlier known as the Indian Penal Code, 1860, it is now replaced with the modern criminal general legislation called the Bhartiya Nyaya Sanhita, 2023, which also has some provisions related to digital crimes. The new concept of organized crime and its punishment has been introduced in BNS. It punishes all those who commit cybercrimes either singly or jointly. Similarly, Section 204 BNS is a penal provision making a defaulter liable for impersonating a public servant, whereas Section 351(4) deals with the punishment for the offense of criminal intimidation by anonymous communication and making a demand of a huge sum of money.

c. Bhartiya Nagarik Suraksha Sanhita (BNSS)

The Code of Criminal Procedure, 1973, now known as the Bhartiya Nyaya Sanhita, 2023, is a procedural code that provides full-fledged guidelines as to what procedure needs to be followed for arrest in cases relating to digital offenses. Law enforcement agencies have been given enormous power to confiscate that equipment and devices that seem to be used in such offenses, block access to social media accounts, and freeze the bank accounts as part of the investigation. But unfortunately, Sanhita lacks in providing express provisions for digital arrest.

IV. CHALLENGES IN DIGITAL ARREST

a. Anonymity of Perpetrators

It is difficult to trace the perpetrator as their identity is unknown, creating a challenge to trace and penalize them.

b. Jurisdictional Issues

If any digital arrest incident is taking place in India, this does not mean that the fraudsters are operating from India itself. They often operate across borders, creating problems for the law enforcement agencies because of jurisdictional issues.

c. Lack of Awareness

People became easy targets of cyber fraudsters because they lacked awareness regarding the modus operandi used by them. Insufficient knowledge regarding cybercrimes, and digital arrest scams makes them more vulnerable, resulting in them becoming easy targets for fraudsters.

d. Technological Complexities

Advanced tools and techniques such as AI and deepfake technology, are being used by the scammers to impersonate themselves as law enforcement officials, making it difficult to track and identify them.

 [ISSN 2581-5369]

e. Psychological Manipulation

It is very much challenging to combat such types of crimes, as some of the incidents are not even reported because the victims are exploited and put under fear, making them feel hesitant to report such incidents.

V. GOVERNMENT INITIATIVE

As to overcome or combat the issue of digital arrest, necessary steps have been taken by the Ministry of Home Affairs by setting up the 'Indian Cyber Crime Coordination Centre (I4C) ' wherein it aims to deal with cybercrimes in a comprehensive and coordinated manner. Following are some of the key initiatives:

- With a view to raising the level of awareness and promotion of Cyber Crime Helpline No. 1930 and the National Cyber Crime Reporting Portal (NCRP), a caller tune has been launched by collaboration between I4C and the Department of Telecommunications (DoT). It is broadcast in different languages, overcoming the problem of different languages been understood among various states.
- Identification and blocking of 3962 Skype IDs and 83,668 WhatsApp accounts that were being used for digital arrest.
- Alert against incidents of blackmail and digital arrest by cyber criminals impersonating themselves as police, CBI, law enforcement agencies, bank officials, etc., has been published by the Central Government in the form of a press release.
- 7.81 lakh SIM cards and 2,08,469 IMEIs have been blocked by the Government of India.
- In 2021, IC4 has started the 'Citizen Financial Cyber Fraud Reporting and Management System' for reporting financial frauds instantly, with the help of which around Rs. 4,368 crores have been saved related to 13.36 lakh complaints.
- With a view to addressing the problem of transnational cybercrimes targeting Indians, a committee has been established that comprises law enforcement officers and intelligence agencies.
- Social media accounts such as X (@CyberDost), Facebook (CyberDostI4C), Instagram (CyberDostI4C), radio campaigns, and Cyber Safety and Security Awareness weeks are some of the initiatives taken by the Central Government to spread awareness on cybercrimes[14].

[14] Press Release: "*Cyber Crimes and Digital Arrest Scams*," Press Info. Bureau (Mar. 12, 2025),

 [ISSN 2581-5369]

- Advisories have been issued by the Ministry of Home Affairs to educate the people about the digital arrest scam as a set confined pattern is used by the scammers called 'modus operandi'. Precautionary measures have been listed in the advisory that needs to be followed by the society as most of the cases IVR calling and impersonation tactic is used where they pose as member of government agencies by using spoofed or computer -generated numbers. They intimidate and digitally confine the victim.

VI. RECOMMENDATIONS

The tactics used by the cybercriminals are hard to find and analyze; that's why it becomes crucial to be aware of such tactics. Some of the suggestions and recommendations have been discussed below:

a. **Beware of Fraudsters:** The numbers used by the cybercriminals are computer-generated and looks similar to a genuine one, causing difficulty for the target audience to identify between genuine and fake callers. That's why we must spread awareness regarding the illegal motive behind such calls. If anyone receives such calls, they first have to hang up the call and report it to the concerned authorities, who will take immediate action.

b. **Strengthening Law Enforcement:** Specialized training in technology and advanced tools needs to be delivered to the law enforcement authorities and other concerned personnel that would result in enhancing the capabilities of cybercrime identification and prevention effectively and efficiently.

c. **International Collaboration:** Such crimes are not only limited to one country, but they are prevalent in almost every country depending upon technology. As a result, cooperation is required to be facilitated between countries to ensure that these crimes are addressed globally.

d. **Seek Legal Advice:** Necessary legal advice must be taken by one who falls prey into digital arrest. Legal experts would be better people who would help the victim as how to overcome this situation. Assistance from relatives and friends could also be taken.

e. **Reporting Suspicious Activities:** Upon receiving any message, phone call, or email that seems to be suspicious, the person has to report it to the local police or cybercrime helpline number 1930 or file a complaint on the National Cyber Crime Reporting Portal (NCRP). On receiving a complaint, immediate action would be taken against the suspicious caller or mail sender.

https://pib.gov.in/PressReleasePage.aspx?PRID=2110809.

 [ISSN 2581-5369]

VII. CONCLUSION

While the digital arrest is not universally defined, but a notable threat is going to affect the cybersecurity of the nation in the form of a digital arrest. People's lack of awareness and weakness play a major role in the cyber fraudster' ability to coerce the target victim, using it to create a sense of fear in their minds. Across the country, there is an increase in the number of complaints being reported on the National Cyber Crime Reporting Portal (NCRP) related to digital arrest, virtual extortion, blackmailing, etc., whereby people lose a large sum of money. This scam falls under the category of organized crime that is highly organized in the sense that they collect important credentials of the target victim and use this information to insist them to deliver the required amount in so-and-so mule accounts. Therefore, in order to curb this ever-evolving menace, necessary efforts have to be made, especially the people of the society need to be proactive and aware. Even though they are digitally arrested, they should not share their personal or financial information with them over a phone call or email[15]. Technological measures could be adopted, such as artificial intelligence integrated with blockchain technology. Blockchain algorithms can be used as a tool to track and trace illicit transactions, whereas machine learning algorithms help in identifying the suspicious transactions on a real-time basis. All these technologies assist in procuring and recording digital evidence. Necessary efforts must also be taken on the part of the legislative authorities to frame comprehensive legislation or add necessary provisions in the existing Information Technology Act, 2000, that can deal with cybercrimes, including digital arrest, so that a secure and reliable digital ecosystem is maintained in Indian cyberspace.

*****

[15] D. Sarala, *"Analysis of a Digital Arrest Scam: Impersonation of Law Enforcement Officials,"* Int'l J. All Res. Educ. & Sci. Methods, https://www.ijaresm.com/uploaded_files/document_file/D._Sarala_jolU.pdf.