International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2024 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

IJLRES

Digital Arrest in India: Decoding the Mechanism, Real-Life Cases and Protective Measures of Victims

Afiya Parveen[a]

[a]The Tamil Nadu Dr. Ambedkar Law University, Chennai, India

Received 16 November 2024; Accepted 17 December 2024; Published 20 December 2024

With the rapid advancement of technology in India, the concept of digital arrest emerged. Unlike physical detention, in digital arrest, scammers impersonate law enforcement agents and make false allegations towards the victims to deceive them and gain at their expense. Scammers trick the victim by stating that they are under digital arrest and would be released upon the payment of the required sum to their account. The study aims to provide in-depth knowledge about the concept of digital arrest and its modus operandi. Through an analysis of real-life case studies, the paper dissects the challenges and brings to light the protective measures people can take to safeguard themselves against digital arrest scams. In addition, the article critically examines the Government's effort (14C) towards combating digital arrests. It aims to support the ongoing dialogues on digital arrests by contributing insights into the government's effort, the challenges and the measures to safeguard the people from the jeopardies of digital arrest scams.

Keywords: *digital arrest, false allegations, modus operandi, government's effort.*

INTRODUCTION

In the digital era, the rapid advancement of technology has given rise to several cybercrimes such as identity theft, data breaches, deepfakes, and so on. In addition, cybercriminals have made their way towards a new concept called digital arrest. According to the National Cybercrime Portal report from January to April, the Chief Executive Officer (14C) Rajesh Kumar stated that Indians have lost Rs. 120.30 crore in digital arrests[1]. Digital arrest is a way of online fraud where cybercriminals disguise themselves as police officer, law enforcement agent, or government officials to defraud the victims and make them believe that they are under a digital arrest[2]. However, the operations of digital arrests by cybercriminals have given rise to critical legal and ethical questions. What is the modus operandi of digital arrest? What are the legal frameworks that exist to protect individuals and safeguard them against digital arrest? These questions help to comprehend the equilibrium between effectual law enforcement and the protection of constitutional rights. Prime Minister Narendra Modi, on his 115th episode of Man Ki Baat, talked about this dangerous game and stated that there are three steps to digital security. The first step is to 'Stop'- to remain calm and composed and not to share personal information with the scammers. The second step is to 'Think'- No Government Agency would threaten people on the phone and demand money, if that's the case then something is wrong. The final step is to 'Take action'- dial 1930 and report the case on cybercrime.gov.in[3]. The Indian Cybercrime Coordination Centre (14C) set up by the Ministry of Home Affairs has reported that till November 15, 2024, the government of India has blocked more than 6.69 lakhs of SIM cards and 1,32,000 IMEIs. As of now, a sum of more than Rs.3431 crore has been conserved from the hands of cybercriminals[4]. This study aims to analyze the modus operandi and real-life cases related to digital arrests. And to identify key challenges and explore the protective measures against the victims. Eventually, this study aims to contribute to the ongoing dialogues on digital arrest by

[1] 'Indians lost Rs 120 crore in digital arrest frauds in January-April 2024' *The Indian Express* (New Delhi, 28 October 2024) <https://indianexpress.com/article/india/indians-lost-rs-120-crore-in-digital-arrest-frauds-in-january-april-2024-9641952/> accessed 08 November 2024

[2] Anurag Sharma, 'The Growing Problem of Digital Arrest Scams in Bharat' (*Vivekananda International Foundation*, 26 November 2024) <https://www.vifindia.org/article/2024/november/26/The-Growing-Problem-of-Digital-Arrest-Scams-in-Bharat> accessed 08 November 2024

[3] 'PM's address in the 115th Episode of 'Mann Ki Baat'' (*PMINDIA*, 27 October 2024) <https://www.pmindia.gov.in/en/news_updates/pms-address-in-the-115th-episode-of-mann-ki-baat/> accessed 08 November 2024

[4] 'Cases of Digital Arrest Scams' (*Ministry of Home Affairs*, 27 November 2024) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2077948> accessed 08 November 2024

proposing practical recommendations to deal with increasing cyber threats on digital arrest in this rapidly growing digital era.

MODUS OPERANDI OF DIGITAL ARRESTS

Spam Calls: Cybercriminals impersonate themselves as police officers, CBI officers, Law enforcement agents, or Government officials and reach out to the victims via WhatsApp calls, text, etc. They also depict themselves as officers wearing uniforms in their WhatsApp profiles, which easily makes people believe they are original officers.

False Allegations: Cybercriminals make false allegations about the victim's involvement in illegal activities such as drug dealing, illicit funds integration, etc. They even intensify the condition. Victims are frightened by stating that their loved ones are in danger due to their involvement in such illegal activities[5].

Claim for Money: Scammers order the victims to stay on the call and bar them from contacting anyone for help, building a sense of loneliness. By producing fake arrest warrants and by using deepfake videos, fraudsters threaten the victims to make payments of fixed sums to reduce the period of imprisonment or to release them.

Digital Arrest Strategy: Cybercriminals force victims to transfer money ordered by them immediately, and a few of them are subjugated to digital arrest. Making the victim stay on the call until they pay towards the account directed by the cyber criminals ultimately builds a feeling of custody and exigency[6].

REAL-LIFE CASES

Retd. Army Personal Tricked of Rs 83 Lakhs in Digital Arrest: On October 15, 2024, Puri received a call from an unknown number stating that his contact number would be switched off within 2 hours. Further, he was connected to customer service, and they informed him about using his mobile number to coerce people. A person identifying himself as SI Mishra stated that

[5] Prashant Shekhar, 'Digital Arrest Fraud- Concerns and Way Forward- Explained Pointwise' (*ForumIAS*, 29 October 2024) <https://forumias.com/blog/digital-arrest-fraud-concerns-and-way-forward-explained-pointwise/> accessed 08 November 2024

[6] 'Digital Arrest Scam: Modus Operandi' (*Stay Safe Online*) <https://staysafeonline.in/concept/digital-arrest-scam/Modus%20Operandi> accessed 08 November 2024

he would be connected to the cyber cell and another person named Roshan informed him that his number was also used for money laundering to the tune of Rs. 80 lakhs and for threatening people. Following this, Puri got a video call from Roshan and Kashyap from CBI, who instructed him to remain on the video call. They informed him that he would be digitally arrested and would be released after the completion of certain procedures. On October 16, Puri received a picture from them stating a man had been arrested for using his number. Further, they ordered him to withdraw all his savings into his wife's account and transfer the same to the account instructed by the scammer, making him believe that they would refund him within six hours. And to add, they even informed him that they would recommend an award for him from the centre for his cooperation in solving the crime. This video call continued till the evening. In this present case, Puri complained about the scammers Mishra and Roshan under sections 316(2), 318(4), 336(3), 338, and 340 of the IPC[7].

Mumbai Woman Forced to Strip, Tricked of Rs. 1.7 Lakhs in Digital Arrest: On November 19, 2024, a 26-year-old woman working in a pharmaceutical company received a call from an unknown number who addressed themselves as a police officer. They informed her that her name had cropped up during an investigation related to a money laundering case connected to Naresh Goyal. The fraudsters menaced her with arrest. During the video call, she was informed that she was under digital arrest and asked to book a hotel to continue the interrogation. Once she had checked into a hotel, the fraudsters asked her to transfer a sum of Rs. 1.7 lakhs and also forced to strip during the video call, stating that it was done for body verification. Later realizing that she had been tricked, she filed a complaint on November 28, 2024, and as of now, the investigation process is in process[8].

Scientific Assistant Tricked of Rs.71 Lakhs in Digital Arrest: On September 1, 2024, a person working at Raja Ramanna Advanced Technology Centre as a scientific assistant received a call from a gang of fraudsters. One of the members identified himself as Telecom Regulatory Authority of India. He made a false allegation towards the victim, stating that unlawful advertisements and messages about women harassment were forwarded to numerous people via

[7] H T Correspondent, 'Retd Major General duped of Rs 83 lakh in 'digital arrest'' *Hindustan Times* (24 October 2024) <https://www.hindustantimes.com/cities/chandigarh-news/retd-major-general-duped-of-83-lakh-in-digital-arrest-101729714258360.html> accessed 08 November 2024

[8] Paras Harendra Dama, 'Mumbai Woman Made to Strip, Duped Of Rs 1.7 Lakh In 'Digital Arrest' Shocker' *NDTV* (01 December 2024) <https://www.ndtv.com/india-news/digital-arrest-mumbai-woman-made-to-strip-duped-of-rs-1-7-lakh-in-digital-arrest-shocker-7145284> accessed 08 November 2024

the SIM card issued in his name. Further, the scammers threatened the victim, stating that an arrest warrant had been issued against him in a case related to money laundering and human trafficking. In addition to this, another member of the gang presented himself as a CBI officer and carried out a spurious interrogation via video call. Out of dread, the victim deposited a sum of Rs. 71.33 lakhs in diverse accounts as per the instructions of the fraudsters[9].

Man Tricked of Rs.30.65 Lakhs in Digital Arrest: On October 19, 2024, the victim received a call from an unknown number who addressed himself to be from the Mumbai Sahar Police Station and stated that a charge sheet had been filed against him for the commission of online fraud which had been committed using a mobile number which has been registered in his name. Further, on the same day, he got a video call from another person dressed in a police uniform who identified himself as Mohan Kumar. The caller stated that an account had been opened by someone in his name at the SBI branch in Mumbai and performed forgery summing to roughly Rs.3.9 Crore through human trafficking. On detention, the person stated that he had given Rs.38 Lakhs to the victim as a commission. Upon the denial of the false allegation by the victim, the fraudsters threatened him by stating that all his bank a/c had been frozen and an arrest warrant had been issued against him. Out of dread, he transferred as per the instruction of the caller Rs. 2.65 lakhs on October 21, 14 lakhs on October 22 and Rs.14 lakhs. Later, realising that he had been tricked, he filed a complaint to the cybercrime helpline 1930[10].

73-Year-Old Retired Lecturer Tricked of Rs. 45.5 Lakhs in Digital Arrest: On November 12, 2024, a 73-year-old retired lecturer named Purshottam Sharma received a call from an unknown number stating that the authorities had seized a package containing illicit drugs. The fraudsters further added that Sharma's Aadhar card number was linked to the package, incriminating him in a money laundering case. To avoid the arrest, the caller provided Sharma with the contact number of an alleged CBI officer in Ahmedabad and ordered him to cooperate with the investigation process. The fraudster appeared in a police uniform during the WhatsApp video call with Sharma and instructed him to provide his bank account details. The retired lecturer was tricked by the scammers and was made to transfer a sum of Rs.45.5 Lakhs.

[9] 'Scientist Duped of Rs 71 Lakh After "Digital Arrest" By Fraudsters In Madhya Pradesh: Cops' *NDTV* (05 October 2024) <https://www.ndtv.com/india-news/scientist-duped-of-rs-71-lakh-after-digital-arrest-by-fraudsters-in-madhya-pradesh-cops-6718350> accessed 08 November 2024

[10] Naina J A, 'Digital arrest strikes again! Man loses Rs 30.65 lakh in Karnataka' *Deccan Herald* (09 November 2024) <https://www.deccanherald.com/india/karnataka/digital-arrest-strikes-again-man-loses-rs-3065-lakh-in-karnataka-3269319> accessed 08 November 2024

To make him believe, the scammers even provided him with duplicate receipts, alleging to be from the Supreme Court and signed by the registrar. Later on, realizing that he had been tricked, he filed a complaint by approaching the Rachakonda cybercrime police[11].

THE GOVERNMENT'S EFFORTS TOWARDS COMBATING DIGITAL ARREST

- The Indian Cybercrime Coordination Centre (14C) has been established by the Ministry of Home Affairs to deal with all kinds of cybercrimes which take place in the country in a very organised and systematic manner.
- A system has been developed by the Central Government and Telecom Service providers to detect and bar incoming transnational spoofed calls appearing to be an Indian mobile number to deceive people as if they had originated within India.
- The Cyber Fraud Mitigation Centre (CFMC) has been set up at 14C, where the delegates of various financial sectors and law enforcement agencies are functioning collectively to deal with cybercrimes. A Suspect registry of identifiers of cybercriminals has been set up at 14C in conjunction with financial institutions.
- 'Report and Check Suspect' has been launched by the Central Government on https://cybercrime.gpv.in, which helps the citizens to search for 14C's database of cybercriminals via the option 'Suspect Search'. 14C plays a key role in detecting and blocking fraudulent IDs that are utilized for digital arrests.
- Under 14C, Seven Joint Cyber Coordination Teams (JCCTs) have been set up to protect the entire country. These areas have been selected based on the severity and considering the hotspot areas where cyber crimes take place frequently, such as Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam and Guwahati.
- To allow people to report cases in connection with all kinds of cybercrimes, the National Cybercrime Reporting Portal has been introduced as a subset of 14C. All the cases reported in this portal are addressed and managed by the state/ Union Territory Law Enforcement Agency.

[11] 'Retired lecturer losses Rs 45 lakh to 'Digital arrest' scam: WhatsApp call; fake Supreme Court receipts; Google Pay, Paytm payments and more' *Times of India* (22 November 2024) <https://timesofindia.indiatimes.com/technology/tech-news/retired-lecturer-loses-rs-45-lakh-to-digital-arrest-scam-whatsapp-call-fake-supreme-court-receipts-google-pay-paytm-payments-and-more/articleshow/115523377.cms> accessed 08 November 2024

- To get help in filing online cyber complaints, a cost helpline number '1930' has been put in place, which makes it way easier for the victims to get legal aid. And 14C has provided cyber hygiene training to 7,330 officials and more than 40,151 NCC Cadets[12].

CHALLENGES IN DIGITAL ARRESTS

False Allegations to Cause Dread: One of the major concerns involved in digital arrests is that scammers pose false allegations toward the victims, accusing them of their involvement in illegal activities such as money laundering, illicit drug trade, human trafficking, etc. And even in some cases, the fraudsters make false claims towards the victim about the involvement of their family members in such illicit activities, which ultimately makes the victim panic and follow the instructions of the fraudsters.

Adverse Effect on Psychological Factors: Scammers often represent themselves as law enforcement agencies, police officers or government agents, and they take various steps towards deceiving the people and making them believe they are original officers. In addition to this, fraudsters often instruct the victims to stay on the call until their demands are met, which creates feelings of loneliness, anxiety, stress and depression.

Hindrances in Locating the Scammers: Digital arrest scams are carried out by scammers dwelling inside as well as outside the country, therefore, it becomes very difficult to identify and accuse the original perpetrators. In addition, the fraudsters direct the victims to make payments via untraceable modes such as e-gift cards, bank transfers, etc.

Monetary Losses: Scammers often trick the victims by stating that they will release them from the charge of illegal activities if they follow the directions given by them. Victims get out of trouble, follow the instructions given by the scammer and make huge sums of payment towards the bank account provided by them, resulting in huge financial losses for the victims.

[12] Cases of Digital Arrest Scams (n 4)

PROTECTIVE MEASURES TO BE TAKEN TO AVOID BECOMING A VICTIM OF DIGITAL ARREST

Stay Calm and Composed: On receiving a sceptical call from scammers posing as law enforcement agents, Government agents or police officers, people should remain calm and composed. Understand and assess the allegations made towards the people about their involvement in illegal activities. This helps to prevent them from becoming prey of the perpetrator.

Do Not Share Personal Information: Law enforcement agencies generally do not claim money from people through calls. If someone asks you to make a payment immediately, confirm their accreditations and refrain from making payments. Abstain from revealing personal and confidential information, like bank account details, to strangers or scammers.

Verify the allegations and Request Supporting Materials: Once the scammers make false allegations towards people's involvement in drug trading, money laundering, human trafficking, etc, they should assess the allegations and accusations on their own. Try contacting any authorized body and cross-check the veracity of the claims made by the scammers.

Report the Case to the Concerned Authority: On the occurrence of the digital arrest scams, people should immediately report the incident to the concerned authority or police officer or file a complaint through the toll-free helpline number 1930. Timely actions can help to avoid becoming a victim of digital arrest.

Public Awareness: One of the most important steps to be taken to prevent these offences is to create awareness among the people regarding digital arrests and their modus operandi. Education initiatives should be taken to train people on how to identify and ward off scams of this type.

CONCLUSION

In the contemporary era, the entire world is driven by the force of the internet and digital services. It has created many openings for scammers to deceive people and get enriched at their expense. Digital arrest is a growing concern in the field of cybercrime. In contrast to physical arrest, it is entirely online, which is specially introduced to deceive victims and make them believe that prompt actions, i.e., transfer of money, would shield them from intense conditions[13]. One of the key challenges involved in digital arrest is that scammers impersonate themselves as Law enforcement agents, police officers, CBI officers or government agents to commit this type of cybercrime. Scammers often deceive their victims by using fear as a tool, which helps in making the people believe that they are in a very serious danger of undergoing stringent legal punishments[14]. Digital arrest causes dread and hurts the psychological factors of the victims. It becomes very challenging to locate the scammers as they use untraceable mechanisms. To avoid becoming a victim of digital arrest, people should verify the allegations made towards them and cross-check with the concerned authority the veracity of the allegations. Generally, people in rural and semi-urban areas become prey to the perpetrators as they are unaware of this growing concern named digital arrest. The key to combating the increasing growth of digital arrests is to create awareness among the people regarding digital arrests and the necessary steps to be taken after encountering this type of cybercrime. The intimidation of digital arrest can proficiently be controlled only through cumulative initiatives and the collaboration of law enforcement agents with technological firms.

[13] Abhinandan, 'What Is The "Digital Arrest" Scam & How To Avoid It?' (*Authbridge*, 15 November 2024) <https://authbridge.com/blog/what-is-the-digital-arrest-scam/> accessed 08 November 2024

[14] Isha Sharma, 'Digital Arrest Fraud' (*CyberPeace*, 07 December 2023) <https://www.cyberpeace.org/resources/blogs/digital-arrest-fraud> accessed 08 November 2024