

---

# DIGITAL ARREST IN INDIA: THE LAW BEHIND THE SCAM

---

Vishwadipti Sinha, BBA LLB (Hons.), Amity Law School, Patna

## ABSTRACT

The increasing use of digital communication has also created new opportunities for cyber fraud. One such fraud is commonly known as a “digital arrest” scam, where criminals impersonate police officers or other authorities and use phone or video calls to threaten victims with arrest and legal action. The Ministry of Home Affairs has clarified that there is no concept of “digital arrest” under Indian law. This article examines the legal reality behind such scams and explains how existing laws relating to arrest, cheating and impersonation may apply to the conduct of scammers. It also discusses how the use of personal information, video calls, threats and false claims of legal authority can make these scams convincing to victims. The article further explains the difference between a genuine arrest and the false claims made during a digital arrest scam. A lawful arrest must have a legal basis and follow the procedure established by law, whereas a scammer attempts to create fear by making the victim believe that the person on the other side of the call has legal authority. The article also examines relevant provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 that may become applicable depending on the conduct of the scammer. The article further highlights the challenges involved in preventing such fraud, particularly the misuse of personal information, the pressure created through threats and the difficulty victims may face in identifying false claims of legal authority. It suggests greater public awareness, independent verification of official claims, careful handling of confidential information and timely reporting of suspicious activity. It argues that understanding the actual legal procedure of arrest, along with greater digital awareness, can help individuals recognise such scams and avoid acting under fear or pressure. The article concludes that legal safeguards and public awareness must work together to reduce the misuse of legal authority through digital communication.

**Keywords:** Digital Arrest, Cybercrime, Online Fraud, Impersonation, Cheating, Arrest, Bharatiya Nyaya Sanhita, Cyber Awareness

## 1. Introduction

Technology has transformed communication by making it faster, easier and accessible across long distances. Phone calls, video calls and instant messaging allow people to communicate without physical interaction, but this convenience has also created new opportunities for cybercriminals to deceive others. What makes the so-called “digital arrest” scam particularly frightening is the manner in which scammers pretend to be police officers or other legal authorities.<sup>1</sup> They do not merely demand money; they create the impression that the law itself is speaking to the victim. In my view, this misuse of legal authority is one of the most concerning aspects of the scam because it exploits people’s trust in the very institutions that are supposed to protect them.

A basic question that arises in such cases is whether a person can actually be arrested through a phone call or video call. The answer is no. The Ministry of Home Affairs, through its cybercrime advisory, has clarified that there is no concept of “Digital Arrest” under Indian law.<sup>2</sup> A lawful arrest must have a legal basis and must follow the procedure prescribed by law; it cannot be created simply by a person claiming over a phone or video call that someone is under arrest. Therefore, the fear created by a so-called digital arrest is based on a false representation of legal authority rather than an actual arrest.

The scam becomes more convincing when the fraudster creates an atmosphere that appears to be connected with a genuine legal proceeding. Scammers may introduce themselves as police officers or other officials and communicate through phone or video calls while using official-sounding language and making serious allegations against the victim. The situation is often presented as urgent, leaving little time for the person to question or verify the claim. In my view, the real strength of this scam lies not only in the technology used, but in the false credibility created by presenting the scammer as someone who represents the law.

This article examines the legal reality behind digital arrest scams, the provisions that may apply to such fraudulent conduct, the challenges faced in preventing these scams, and the safeguards that can help protect individuals from such misuse of legal authority.

---

<sup>1</sup>National Cybercrime Threat Analytics Unit (NCTAU), Indian Cyber Crime Coordination Centre (I4C), Advisory on “Digital Arrest” Scam, TAU/ADV/003 (6 March 2025).

<sup>2</sup>National Cybercrime Threat Analytics Unit (NCTAU), Indian Cyber Crime Coordination Centre (I4C), Advisory on “Digital Arrest” Scam, TAU/ADV/003 (6 March 2025).

## **2. Understanding the “Digital Arrest” Scam.**

A digital arrest scam is a form of cyber fraud in which a person is made to believe that they are involved in a serious legal matter and are being monitored or arrested through a phone or video call. The scammer may obtain or refer to personal information such as an Aadhaar number, passport details, or other confidential information to make the situation appear genuine. The victim is then threatened with legal action, damage to their reputation, or other serious consequences if they do not follow the scammer’s instructions.

Scammers generally approach victims through phone calls, WhatsApp messages, or video calls. They may already possess some personal information about the victim, which makes their claims appear more convincing. Instead of simply asking for money, they create fear and confusion by presenting the matter as an urgent legal issue. This pressure may make the victim less likely to stop and verify whether the person on the other side is actually a police officer or any other lawful authority.

The impression of dealing with the law is often created through impersonation. Scammers may present themselves as police officers or other officials, use official-looking backgrounds or clothing, and communicate in a serious and authoritative manner.<sup>3</sup> They may also refer to personal details of the victim to create the impression that the caller has access to official records. By combining these methods, the scammer attempts to make a false situation appear like a genuine legal proceeding.

The situation becomes particularly frightening because the victim is placed under continuous pressure. The scammer may create a sense of urgency and threaten the victim with arrest, legal consequences, or damage to their dignity and reputation. Under such pressure, a person may believe that the caller is telling the truth and may act without properly verifying the claim. Therefore, the effectiveness of a digital arrest scam lies not only in the use of technology but also in the misuse of fear, personal information, and public trust in legal authorities.

## **3. The Legal Reality of Arrest in India**

The term “digital arrest” can be confusing because arrest is a legal process and cannot simply

---

<sup>3</sup> Indian Cyber Crime Coordination Centre (I4C), National Cybercrime Threat Analytics Unit, Advisory on “Digital Arrest” based cybercrime in India, TAU/ADV/003 (6 March 2025).

be created through a phone or video call. A person cannot be legally arrested merely because someone calls them and says that they are under arrest.<sup>4</sup> There must be a legal basis for the arrest and the procedure prescribed by law must be followed. Therefore, when a scammer tells a person that they are “digitally arrested,” the statement itself does not create a lawful arrest. It is a false claim used to create fear and make the victim believe that they are dealing with a real legal authority.

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) provides the legal framework relating to arrest in India. Section 35 of the BNSS deals with the situations in which a police officer may arrest a person without a warrant.<sup>5</sup> This means that the power to arrest is subject to legal conditions and cannot be used simply because someone claims to be a police officer. In a digital arrest scam, however, the scammer tries to create the impression that such legal power is being exercised against the victim.

The law also provides safeguards after a person has been arrested. Section 57 of the BNSS provides that an arrested person is to be taken or sent without unnecessary delay before the appropriate Magistrate or officer in charge, subject to the provisions relating to bail.<sup>6</sup> Section 62 further states that no arrest shall be made except in accordance with the BNSS or any other applicable law. These provisions show that arrest is connected with a proper legal procedure and cannot be replaced by threats made through a phone or video call.

The Supreme Court has also emphasised safeguards relating to arrest and custody in *D.K. Basu v. State of West Bengal*.<sup>7</sup> The Court laid down requirements intended to prevent misuse of arrest and custodial powers, including proper identification and documentation by the arresting officers and informing a relative or friend about the arrest. These safeguards show that the exercise of legal authority must remain subject to accountability and procedure.

Therefore, the main legal reality behind a digital arrest scam is that there is no separate legal procedure through which a person can simply be “digitally arrested” over a phone or video call. The scammer creates the appearance of a legal proceeding and uses that appearance to frighten

---

<sup>4</sup> National Cybercrime Threat Analytics Unit (NCTAU), Indian Cyber Crime Coordination Centre (I4C), Advisory on “Digital Arrest” Scam, TAU/ADV/003 (6 March 2025).

<sup>5</sup> The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023 Section 5

<sup>6</sup> The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, § 57.

<sup>7</sup> *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416.

the victim. Understanding the actual legal procedure of arrest can help people recognise that such threats are not the same as a lawful arrest.

#### **4. Legal Provisions Applicable to Digital Arrest Scams**

Digital arrest scams do not involve a separate offence called “digital arrest.” Instead, the actions of the scammer may fall under different existing laws depending on what the scammer does. The main problems involved are usually impersonation, cheating and threats. Understanding these acts helps explain how the existing legal system can deal with such scams.

One common feature of these scams is impersonation. The scammer may pretend to be a police officer, government official or another person in authority. The purpose is to make the victim believe that the person on the other side of the call has genuine legal power. Section 319 of the Bharatiya Nyaya Sanhita, 2023 deals with cheating by personation.<sup>8</sup> Therefore, when a person uses a false identity to deceive another person, this provision may become relevant depending on the facts of the case.

Another important aspect is cheating. The scammer may create a completely false legal situation and then ask the victim to transfer money or follow certain instructions. Section 318 of the Bharatiya Nyaya Sanhita, 2023 deals with cheating.<sup>9</sup> In a digital arrest scam, the victim is first made to believe the false story and is then pressured to take an action that benefits the scammer.

Since these scams are carried out through phones, video calls and other digital means, cyber law may also become relevant. Section 66D of the Information Technology Act, 2000 deals with cheating by personation using a communication device or computer resource.<sup>10</sup> This shows that existing laws can be applied to the conduct involved in a digital arrest scam even though “digital arrest” itself is not a separate legal form of arrest.

Thus, the important point is that the law does not need to recognise “digital arrest” as a separate type of arrest in order to deal with the scam. The actual conduct of the scammer can be examined under existing laws relating to impersonation, cheating and the use of digital means.

---

<sup>8</sup> The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, § 319.

<sup>9</sup> The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, § 318.

<sup>10</sup> The Information Technology Act, 2000, No. 21 of 2000, § 66D.

This makes it important for people to understand that the threatening appearance of a legal proceeding does not give the scammer any genuine legal authority.

## **5. Why the Scam Appears Convincing to Victims**

Digital arrest scams often appear convincing because scammers create an environment of fear and urgency. They may use official-looking backgrounds, uniforms, legal language and personal information of the victim to make their claims seem genuine. The use of video calls can also make the situation appear more serious and real.

Another reason is the pressure placed on the victim. The scammer may threaten immediate arrest, legal action or damage to the victim's reputation. Because the victim is given very little time to think or verify the information, they may follow the scammer's instructions out of fear.

The scam therefore works not only through technology but also through the misuse of trust and fear. By pretending to represent the law, scammers make victims believe that they must immediately obey their instructions.

## **6. Challenges in Addressing Digital Arrest Scams**

One of the major challenges in dealing with digital arrest scams is the lack of awareness among people about how such scams operate. Many victims may not immediately realise that the person contacting them is impersonating a legal authority. The use of personal information, video calls and official-looking communication can make the fraud difficult to identify.

Another challenge is the fear created by the scammer. When a person is suddenly told that they are involved in a criminal case or may be arrested, they may panic and follow instructions without verifying the information. This gives scammers an opportunity to misuse the victim's fear and obtain money or other information.

Therefore, preventing such scams requires not only legal action but also greater public awareness. People should know that no one can create a "digital arrest" simply through a phone or video call and that suspicious claims of legal authority should be independently verified.

## **7. Possible Legal and Institutional Safeguards**

Awareness is one of the most important ways to prevent digital arrest scams. People should be

made aware that there is no concept of “digital arrest” under Indian law and that genuine legal authorities do not create an arrest merely through a phone or video call.<sup>11</sup> Public awareness campaigns can help people recognise such false claims and avoid acting under pressure.

People should also avoid sharing confidential information, financial details or documents with unknown callers. If someone claims to be a police officer or another authority, the person should independently verify the claim through official channels instead of relying on the contact details provided by the caller.

Law enforcement agencies and cybercrime authorities also have an important role in preventing such scams. Quick reporting, public awareness and effective investigation can help reduce the impact of these frauds. A combination of legal action and digital awareness can therefore help protect people from the misuse of legal authority through technology.

## **8. Conclusion**

Digital arrest scams show how technology can be misused to create fear and falsely represent legal authority. Although the term “digital arrest” is commonly used by scammers, it does not represent a separate legal procedure in India. A lawful arrest must have a legal basis and follow the procedure established by law.

The problem, however, is not limited to the misuse of technology. Scammers also misuse people’s trust in police and other legal authorities. By using personal information, video calls and threats, they create a situation in which victims may act without properly verifying the claim.

Legal provisions can help deal with the conduct involved in these scams, but public awareness is equally important. People should understand that a threatening phone or video call does not itself amount to a lawful arrest. Greater awareness, quick reporting and effective action can help reduce the impact of such scams and protect people from the misuse of legal authority in the digital age.

---

<sup>11</sup> National Cybercrime Threat Analytics Unit (NCTAU), Indian Cyber Crime Coordination Centre (I4C), Advisory on “Digital Arrest” Scam, TAU/ADV/003 (6 March 2025).