Page 773 - 786 **DOI:** *https://doi.org/10.63108/IJLMH.13115*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Synthesizing 'Digital Arrest' into a Standalone Offence and the Gaps in Indian Law under the Bharatiya Nyaya Sanhita, 2023

J. MOHAMED IBRAHIM*

ABSTRACT

"Digital arrest" scams are among the fastest-growing cybercrimes today. A scammer appears on a video call dressed as a police officer, judge or government official, flashes fake arrest warrants, makes frightening legal threats and keeps the victim on the call for hours, sometimes days. Cut off from family and friends, frightened and exhausted, victims end up paying large sums of money to avoid going to jail. Indian law does not recognise "digital arrest" at all. The phrase does not appear in the Bharatiya Nyaya Sanhita (BNS), 2023, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, or the Information Technology (IT) Act, 2000; it is simply a popular label. When these cases reach the police, several different provisions therefore have to be pieced together: Section 204 BNS (personating a public servant), Section 308 BNS (extortion), Section 318 BNS (cheating), Section 336 BNS (forgery), Section 66C of the IT Act (identity theft) and Section 66D of the IT Act (cheating by personation using a computer resource). These provisions were written for ordinary crimes. Each covers only a piece of the scam, and none covers the crime as a whole. There is no offence of "digital confinement" either: the wrongful confinement provision (Section 127 BNS) was written with physical detention in mind, and so does not fit a victim held captive over a video call. Cases are also often charged as cheating (Section 318), even though they look more like extortion (Section 308): victims do not pay because they were promised a gain, but because they are afraid of being arrested. Reliance on so many scattered provisions leads to confusion and gaps in the law. It slows the freezing of stolen money and often results in weak punishment for the organised gangs behind these scams.

Keywords: *Digital arrest, Bharatiya Nyaya Sanhita, 2023, cyber fraud*

I. INTRODUCTION

A "digital arrest" is a fake arrest staged by cybercriminals to extract money from their victims.[1]

* Author is a Student at SASTRA Deemed University, Thanjavur, Tamil Nadu, India.

[1] *CBI, ED, Police Don't Arrest People Through Video Calls: Indian Cyber Crime Coordination Centre*, THE TRIBUNE (Oct. 6, 2024), https://www.tribuneindia.com/news/india/cbi-ed-police-dont-arrest-people-through-video

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The criminals call or message a victim and claim that a parcel sent in the victim's name contains illegal items (such as drugs or fake passports), or that the victim's government identity numbers, telephone numbers or bank accounts are linked to serious crimes such as money laundering or terrorism.

The scam works through several calculated steps:

- The call is transferred to persons pretending to be police officers, officers of central investigating agencies or customs officials.
- The scammers sit in front of backdrops designed to look like real police stations or courtrooms. They wear official-looking uniforms and display forged arrest warrants or legal notices.
- They order the victim to stay on a live video call (on WhatsApp, Zoom, Skype and similar platforms) continuously, sometimes for hours, days or even weeks, and tell the victim that hanging up, leaving the camera's view or talking to family will count as "resisting arrest" and will bring real police to the door.[2]
- Once the victim is isolated, the scammers make the victim transfer his or her life savings into specified bank accounts, claiming that the money is needed for "identity verification" or as a "security deposit" that will be refunded later.

In 2022 there were about 39,925 complaints of digital arrest and related cybercrime, with losses of about ₹91 crore. In 2024 the figure rose to 1,23,672 complaints, with losses of about ₹1,935 crore.[3] Reported cases began to decline in 2025 as public awareness and government intervention took effect.[4] By November 2025 the Supreme Court had been informed that almost ₹3,000 crore had been extorted from victims of cyber fraud, particularly of digital arrest scams.[5]

-calls-indian-cyber-crime-coordination-centre/ (reporting the advisory of the Indian Cyber Crime Coordination Centre (I4C)); NITI AAYOG, *Digital Arrest: The Modern-Day Cyber Scam*, https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf.

[2] *CBI, ED Don't Nab via Video Calls: Advisory to Curb 'Digital Arrest'*, THE TRIBUNE (Oct. 7, 2024), https://www.tribuneindia.com/news/india/cbi-ed-dont-nab-via-video-calls-advisory-to-curb-digital-arrest/ (fraudsters confine victims to their premises by making them keep their phone cameras on).

[3] MINISTRY OF HOME AFFAIRS, Reply to Rajya Sabha Unstarred Question No. 1505 (Mar. 12, 2025), https://rsdebate.nic.in/bitstream/123456789/757210/1/PQ_267_12032025_U1505_p268_p273.pdf; *Digital Arrests, Cyber Crimes Tripled During 2022–24, Defrauded Amount Jumped 21 Times: Govt*, THE WEEK (Mar. 12, 2025), https://www.theweek.in/wire-updates/national/2025/03/12/del54-rsq-cybercrime.html (39,925 cases and ₹91.14 crore in 2022; 1,23,672 cases and ₹1,935.51 crore in 2024).

[4] Ananya Bhardwaj, *After 465% Spike in 2024, MHA Data Shows Digital Arrest Scams Are on a Decline in India*, THEPRINT (Feb. 18, 2026), https://theprint.in/india/governance/after-465-spike-in-2024-mha-data-shows-digital-arrest-scams-are-on-a-decline-in-india/2857002/ (17,264 cases and ₹644 crore in 2025); *Indians Lost INR 1,935 Cr to Digital Arrest Scams in 2024: Govt*, INC42 (Mar. 14, 2025), https://inc42.com/buzz/indians-lost-inr-1935-cr-to-digital-arrest-scams-in-2024-govt/.

[5] Ritwik Choudhury, *Shocking, Will Deal with Iron Hands: Supreme Court on Extortion of ₹3,000 Crore in Digital Arrests*, BAR & BENCH (Nov. 3, 2025), https://www.barandbench.com/news/litigation/shocking-will-deal-with-iron-hands-supreme-court-on-extortion-of-3000-crore-in-digital-arrest-scams (reporting that the Supreme Court

The Supreme Court and High Courts, among them the Rajasthan High Court, have accordingly stepped in, directing central and state authorities to improve public awareness, banking safeguards and coordination between law enforcement agencies.[6]

The legal problem is that "digital arrest" does not exist in law. Under Indian law, including the new Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), there is no procedure by which a person can be arrested over a telephone or video call, and genuine law enforcement officers do not arrest anyone online.[7]

Because "digital arrest" is not named in the law, police and prosecutors must combine separate charges under the Bharatiya Nyaya Sanhita, 2023 (BNS) and the Information Technology Act, 2000 (IT Act), such as cheating, personation and extortion.[8]

The question this paper addresses is whether combining existing laws is enough to prosecute these criminals effectively, or whether India should create a new and specific criminal offence of feigning governmental authority in order to trap and rob people online.

---

was informed that "almost ₹3,000 crore" had been extorted in cyber frauds, particularly digital arrest scams); BUSINESS STANDARD (Dec. 1, 2025), https://www.business-standard.com/industry/news/sc-orders-cbi-probe-digital-arrests-pan-india-cybercrime-125120101046_1.html.

[6] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Pet. (Crl.) No. 3 of 2025 (SC Oct. 17, 2025) (India), https://api.sci.gov.in/supremecourt/2025/59769/59769_2025_2_7_65003_Order_17-Oct-2025.pdf (cognisance taken); *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Pet. (Crl.) No. 3 of 2025, ¶¶ 5–6 (SC Dec. 1, 2025) (India), https://api.sci.gov.in/supremecourt/2025/59769/59769_2025_1_28_66412_Order_01-Dec-2025.pdf (CBI to investigate digital arrest cases; interim directions); *Digital Arrest Scam: Supreme Court Takes Suo Motu Cognizance, Issues Notice to Centre, CBI*, DECCAN HERALD (Oct. 17, 2025), https://www.deccanherald.com/india/digital-arrest-scam-supreme-court-takes-suo-motu-cognizance-issues-notice-to-centre-cbi-3767349; NEWS ON AIR, https://www.newsonair.gov.in/sc-takes-strong-note-of-rising-digital-arrest-scams-seeks-centre-and-cbi-response; Satya Prakash, *SC Tells CBI to Probe Pan-India Digital Arrest Scam, Role of Bank Staff*, THE TRIBUNE (Dec. 2, 2025), https://www.tribuneindia.com/news/cybercrimeindia/sc-tells-cbi-to-probe-pan-india-digital-arrest-scam-role-of-bank-staff; *Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059 (decided Nov. 27, 2025) (India), https://indiankanoon.org/doc/107652351/; *"Present Machinery Can't Handle Traditional Cybercrimes, AI/Deep Fake Challenges": Inside Rajasthan High Court's Detailed Directions to Curb Cybercrimes*, SCC TIMES (Dec. 5, 2025), https://www.scconline.com/blog/post/2025/12/05/raj-hc-issues-directions-to-curb-cybercrimes/.

[7] *CBI, ED, Police Don't Arrest People Through Video Calls*, *supra* note 1; The Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, INDIA CODE (2023) [hereinafter BNSS], § 43(1) (an arrest is made by actually touching or confining the body of the person, unless the person submits to custody by word or action); *Mann Ki Baat's 115th Episode: PM Modi Warns of 'Digital Arrest', Urges People to Stay Vigilant*, FREE PRESS JOURNAL (Oct. 27, 2024), https://www.freepressjournal.in/india/mann-ki-baats-115th-episode-pm-modi-warns-of-digital-arrest-urges-people-to-stay-vigilant (the Prime Minister's broadcast of Oct. 27, 2024); VIVEKANANDA INTERNATIONAL FOUNDATION, https://www.vifindia.org/print/13130; *Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059, ¶ 3 (India) (recording the prosecution's submission that "digital arrest" is "not defined in any Act"); Sanjay Raman Sinha, *Courts vs Clicks: Rajasthan High Court Sounds the Alarm*, INDIA LEGAL (Feb. 5, 2026), https://indialegallive.com/cover-story-articles/il-feature-news/cyber-fraud-digital-arrests-deepfakes-rajasthan-high-court/.

[8] The Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023) [hereinafter BNS], https://www.indiacode.nic.in/handle/123456789/20062?view_type=browse; The Information Technology Act, No. 21 of 2000, INDIA CODE (2000) [hereinafter IT Act], https://www.indiacode.nic.in/handle/123456789/1999.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

II. Legal and Technical Background

A. Understanding the scam

Callers use either spoofed numbers or numbers registered over the internet, and they reach victims through common modes of communication: telephone calls, messaging applications and video applications. They dress as officials or display government emblems and symbols, and they send PDF notices created with editing software. The money taken is transferred to accounts known as "mules". These accounts simply relay the money onward, and it is typically converted into cryptocurrency or sent out of India. In many instances the gangs have operated from overseas, which makes detection difficult. Speed is of the essence: the money is often dispersed within a matter of hours.[9]

The acts involved can be classified into five stages:

1. Introduction: the caller claims that the victim has sent a package containing illegal substances, or that the victim's phone number has been implicated in an offence.
2. Progression: a video call follows, usually when a "senior" officer takes over.
3. Restriction: the victim is made to remain on the call and is told that the matter is confidential, and is often asked to report back at set intervals.
4. Taking: the scammers ask for money.
5. Transfer: mule accounts receive the money and relay it to other accounts until it is dispersed.[10]

This is a series of offences: spoofing and personation, forgery and the use of technology, coercion, fraud and, finally, the laundering of money. Each is governed by a separate provision, as discussed below, but together they form a chain of events committed in succession.

B. Victims

Why do people fall for these scams? As in a lottery scam, the fraud offers the victim nothing of value; the difference is that it appeals to fear of an authoritative figure. Most people know not

[9] Bhardwaj, *supra* note 4 (calls placed from "scam farms" in Thailand, Cambodia and Myanmar); Vibha Sharma, *India Cracks Down on 'Digital Arrest' Scam: Over 6.69 Lakh SIM Cards and 1.32 Lakh IMEIs Blocked*, The Tribune (Nov. 28, 2024), https://www.tribuneindia.com/news/india/india-cracks-down-on-digital-arrest-scam-over-6-69-lakh-sim-cards-and-1-32-lakh-imeis-blocked/ (system to block incoming international calls spoofed to display Indian numbers); Vivekananda International Foundation, *supra* note 7; Prakash, *supra* note 6 (mule accounts and the role of bank staff).

[10] *Digital Arrest Scams: ED Charge Sheet & I4C Advisory to Protect Citizens*, Vajiram & Ravi (Nov. 8, 2025), https://vajiramandravi.com/current-affairs/digital-arrest-scams-ed-charge-sheet-i4c-advisory-to-protect-citizens/ (funds "funneled through 'mule' accounts, converted to cryptocurrency, and transferred abroad").

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

to ignore a police officer or a summons from a court, and the length of the calls and the stream of instructions leave victims in a daze, with no time to think for themselves.[11]

The instruction not to tell anyone does most of the work. Whether the victim is told that the case is sensitive or that the family will be drawn in if they are told, the victim believes it, and any doubts that family or friends might have raised are never voiced. This isolation further restricts the victim, and restriction plays a large part in these scams. This account is drawn from official sources and news reports rather than from empirical research, and it is offered as a hypothesis about why victims comply.

C. Laws applicable

The provisions relevant to these scams are the following:

- Section 204 BNS: personating a public servant.[12]
- Section 308 BNS: extortion, that is, putting a person in fear in order to obtain money.[13]
- Section 318 BNS: cheating, that is, fraudulently inducing a person to part with money.[14]
- Section 336 BNS: forgery, as of fake warrants and notices.[15]
- Section 66C of the IT Act: identity theft, that is, the fraudulent use of another person's unique identification features.[16]
- Section 66D of the IT Act: cheating by personation using a communication device or computer resource, that is, fraud carried out through technology.[17]

Not all of these provisions fully apply. Some cover parts of the crime and not others:

- Section 204 BNS punishes pretending to hold a public office and acting under colour of that office, but it is not directed at the extraction of money from the person deceived.

---

[11] *CBI, ED, Police Don't Arrest People Through Video Calls*, *supra* note 1 ("Don't Panic, Stay Alert"); *Mann Ki Baat's 115th Episode*, *supra* note 7 ("Stop, Think, Take Action"); VIVEKANANDA INTERNATIONAL FOUNDATION, *supra* note 7.

[12] BNS, *supra* note 8, § 204; Prashant Kanha, *Section 204 BNS: Bhartiya Nyaya Sanhita, 2023 & Equivalent IPC Section* (June 19, 2024), https://www.prashantkanha.com/section-204-of-bhartiya-nyaya-sanhita-2023-bns-equivalent-ipc-section/; https://www.indiacode.nic.in/handle/123456789/20062?view_type=browse.

[13] BNS, *supra* note 8, § 308; https://devgan.in/bns/section/308/.

[14] BNS, *supra* note 8, § 318; UTTAR PRADESH POLICE, *Corresponding Section Table of Bharatiya Nyaya Sanhita 2023 (BNS)*, https://uppolice.gov.in/site/writereaddata/siteContent/Three%20New%20Major%20Acts/20240628171056482 3BNS_IPC_Comparative.pdf.

[15] BNS, *supra* note 8, § 336; https://www.latestlaws.com/bare-acts/central-acts-rules/bns-section-336-forgery-/.

[16] IT Act, *supra* note 8, § 66C; https://www.unodc.org/cld/en/legislation/ind/the_information_technology_act_2000/chapter_xi/sections_66c66d/sections_66c-66d.html.

[17] IT Act, *supra* note 8, § 66D; https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&sectionId=13089&sectionno=66D&orderno=80; https://indiankanoon.org/doc/1965344/.

- Section 308 BNS (extortion) applies where a person is put in fear of injury and thereby induced to give up property. This is close to the conduct in these scams, save for the question whether fear of imprisonment counts, which is discussed below under "It should be extortion".
- Section 318 BNS (cheating) again covers deceiving a person out of money. It is probably the section most often invoked, because of its familiarity and because it matches what complainants report.
- Section 336 BNS (forgery) covers the fake warrants, notices and emblems.[18]
- Sections 66C and 66D of the IT Act deal specifically with the use of technology.

Section 127 BNS (wrongful confinement) may also play a role, as discussed below under "Detaining people".

Section 111 BNS, on organised crime, could also be used against the gangs that commit these crimes. It requires proof, however, that a person or group is engaged in a "continuing unlawful activity" as, or on behalf of, an organised crime syndicate, which the section ties to more than one charge-sheet filed within the preceding ten years.[19]

D. Procedures

Procedures are in place to block and retrieve money: the national cybercrime helpline 1930 and the National Cyber Crime Reporting Portal.[20] Under the BNSS, the police may seize property connected with an offence (Section 106), and a court or Magistrate may, on a police application, attach proceeds of crime, if necessary by an interim order made without notice where notice would defeat the attachment (Section 107).[21] Because these crimes are carried out within hours, such procedures are essential. Having the law is good, but a law that is not used efficiently achieves little.

[18] BNS, *supra* note 8, § 336; https://www.latestlaws.com/bare-acts/central-acts-rules/bns-section-336-forgery-/.
[19] BNS, *supra* note 8, § 111(1) & Explanation (ii) (defining "continuing unlawful activity"); UTTAR PRADESH POLICE, *supra* note 14 (listing § 111 as a new section with no IPC equivalent), https://uppolice.gov.in/site/writereaddata/siteContent/Three%20New%20Major%20Acts/20240628171056482 3BNS_IPC_Comparative.pdf.
[20] *CBI, ED, Police Don't Arrest People Through Video Calls*, *supra* note 1 (directing victims to helpline 1930 and www.cybercrime.gov.in); *Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059, ¶¶ 10–11 (India).
[21] BNSS, *supra* note 7, §§ 106, 107(1), 107(5); https://indiankanoon.org/doc/105332178/; *Section 107 of BNSS*, DRISHTI JUDICIARY (June 17, 2025), https://www.drishtijudiciary.com/current-affairs/section-107-of-bnss.

III. Analysis

A. None of the sections covers the entire offence

No single section covers impersonating an official in order to extort money. Section 204 covers only the false identity, and Section 336 the forged documents; neither reaches the threats. The technology offences in Sections 66C and 66D are directed at identity theft and at cheating by personation through a communication device or computer resource; like Section 318, they rest on deception rather than intimidation. Each of these sections would have to be invoked and proved separately by the police, so that every charge-sheet becomes longer and more convoluted, and easier for the defence to dissect.[22]

The problem is not only the manner in which a case can be presented. Every charge requires its own proof of intention and its own evidence. If one element fails, for instance if a document is proved not to have been made by the accused, the charge-sheet as a whole is weakened, even where the bigger picture tells a different story. A single offence could capture all the acts accurately.

Sentencing also comes into play. The ceilings for most of the offences listed above are not high: three years under Section 204 BNS and under each of Sections 66C and 66D of the IT Act, and seven years under Sections 308(2), 318(4) and 336(3) BNS.[23] Where a person is convicted at one trial of several offences, Section 25(1) BNSS leaves it to the court, considering the gravity of the offences, to order the sentences to run concurrently or consecutively; where they run concurrently, the offender serves no more than the longest single term.[24] That outcome is unfair to a person who was emotionally coerced for days into parting with his or her life savings.

B. It should be extortion

Obtaining money by deception is cheating under Section 318. But, as noted above, no one in these scams is trying to persuade the victim to hand over money for a higher return. The scammers are trying to make the victim fear arrest and to force payment, which is extortion. Where a person threatens another with harm and makes that person surrender property out of

---

[22] IT Act, *supra* note 8, §§ 66C–66D; https://www.unodc.org/cld/en/legislation/ind/the_information_technology_act_2000/chapter_xi/sections_66c66d/sections_66c-66d.html; BNS, *supra* note 8, §§ 204, 336; https://www.prashantkanha.com/section-204-of-bhartiya-nyaya-sanhita-2023-bns-equivalent-ipc-section/; https://www.latestlaws.com/bare-acts/central-acts-rules/bns-section-336-forgery-/.

[23] BNS, *supra* note 8, §§ 204 (not less than six months and up to three years), 308(2) (up to seven years), 318(4) (up to seven years), 336(3) (up to seven years); IT Act, *supra* note 8, §§ 66C–66D (up to three years each); https://www.prashantkanha.com/section-204-of-bhartiya-nyaya-sanhita-2023-bns-equivalent-ipc-section/; https://devgan.in/bns/section/308/; https://www.latestlaws.com/bare-acts/central-acts-rules/bns-section-336-forgery-/; https://www.unodc.org/cld/en/legislation/ind/the_information_technology_act_2000/chapter_xi/sections_66c66d/sections_66c-66d.html.

[24] BNSS, *supra* note 7, § 25(1).

that fear, the offence is extortion under Section 308, whether the harm threatened is imprisonment or damage to reputation. The pretence of official status only makes the threat more credible.[25]

Correct classification benefits not only complainants but also those prosecuting the case. Labelling the crime as cheating instead of extortion understates it, and potentially opens the case to an inquiry into whether the victim was in fact deceived. Charges can be framed in the alternative, but correct labelling starts the case in the right direction.[26]

A counter-argument is that a threat of imprisonment is not a threat of harm: a caller who claims to be a police officer and says that he will come to arrest the victim might be thought to threaten nothing unlawful. The Sanhita answers much of this objection. Section 2(14) defines "injury" as any harm whatever illegally caused to any person in body, mind, reputation or property, and Section 308(6) punishes putting, or attempting to put, a person in fear of an accusation of having committed an offence punishable with death, imprisonment for life or imprisonment for up to ten years, in order to commit extortion, while Section 308(7) punishes extortion committed by putting a person in such fear.[27] Even so, express statutory language on threats of fabricated legal process would save courts time in deciding these cases.

Cheating and extortion should not, moreover, be treated as mutually exclusive in this situation. A caller who pretends to be another person cheats, but the same caller also pressures the victim into handing over money, which is extortion.

C. Detaining people

A person detained against his or her will is protected by Section 127 BNS. That provision, however, sits awkwardly with a situation in which no one has been physically confined, and it could be applied only if a court were prepared to extend it to such facts.[28] Investigators have already invoked it: the two FIRs lodged at Ambala by the couple whose complaint gave rise to the Supreme Court's suo motu proceedings invoke Section 127(2) BNS together with Sections

[25] BNS, *supra* note 8, §§ 308, 318; https://devgan.in/bns/section/308/; UTTAR PRADESH POLICE, *supra* note 14 (corresponding to IPC §§ 383 and 415), https://uppolice.gov.in/site/writereaddata/siteContent/Three%20New%20Major%20Acts/20240628171056482 3BNS_IPC_Comparative.pdf.

[26] Sinha, *supra* note 7 (describing digital arrest as "nothing more than an extortion technique designed to induce panic and compliance"); *see also Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059, ¶¶ 1, 4 (India) (FIR registered under, among others, §§ 308(2) and 308(6) BNS, which the Court treated as serious).

[27] BNS, *supra* note 8, §§ 2(14), 308(6)–(7).

[28] BNS, *supra* note 8, § 127; https://devgan.in/bns/section/127/.

308(2), 318(4) and 336(3), among others.[29] Whether a court will sustain a charge of wrongful confinement where there was no physical restraint remains to be seen.

Victims of digital arrest have been told not to leave their location and have been prevented from telling others what was happening. This resembles confining a person at home, where the person is stopped from calling others for help or informing them of the situation.[30]

D. Money gets frozen too slowly

Recovery is where the real test lies. Because money has to be traced and frozen within hours, the tools to do so must be available. There are at present the reporting portal, the 1930 helpline and the provisions of the BNSS that allow the seizure of property and the attachment of proceeds of crime (Sections 106 and 107). All of these, however, depend on an FIR being registered and on the offence being classified correctly. If a case is not classified properly, or looks like a minor instance of cheating, banks will be reluctant to act and states may dispute jurisdiction over the offence (the state of the victim against the state of the mule account). The Supreme Court has also taken suo motu cognisance of these scams.[31] The problems can be broken down as follows:

- Classification: whether the case is recorded as cheating of a small amount, or as continuing extortion by a person pretending to be a government official, affects how officials react at the first instance.
- Jurisdiction: the state where the victim resides, the state where the receiving account is held and possibly another state may all be involved.
- Legal constraints: banks want proper instructions before they hold funds in a customer's account, and there can be repercussions if innocent account-holders have their money frozen.[32]

A specific offence would assist both classification and the legal footing for action. With proper labelling, those responding can act more quickly, and banks would have grounds to freeze an

[29] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Pet. (Crl.) No. 3 of 2025, ¶ 2 (SC Oct. 17, 2025) (India) (FIRs Nos. 76/2025 and 77/2025, Cyber Crime Branch, Ambala, registered under §§ 127(2), 308(2), 318(4), 336(3), 338, 340(2) and 61(2) BNS).

[30] *CBI, ED Don't Nab via Video Calls*, *supra* note 2.

[31] *CBI, ED, Police Don't Arrest People Through Video Calls*, *supra* note 1; BNSS, *supra* note 7, §§ 106–107; *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Pet. (Crl.) No. 3 of 2025 (SC Oct. 17, 2025) (India); https://www.deccanherald.com/india/digital-arrest-scam-supreme-court-takes-suo-motu-cognizance-issues-notice-to-centre-cbi-3767349; https://www.business-standard.com/industry/news/sc-orders-cbi-probe-digital-arrests-pan-india-cybercrime-125120101046_1.html.

[32] *Headstar Global Pvt. Ltd. v. State of Kerala*, Crl. M.C. No. 3740 of 2025, 2025 LiveLaw (Ker) 339 (India), https://www.livelaw.in/high-court/kerala-high-court/kerala-high-court-rules-police-cannot-freeze-bank-account-section-107-bnss-295027 (police may seize property under § 106 BNSS, but a bank account suspected to hold proceeds of crime may be attached only on a Magistrate's order under § 107); *Section 107 of BNSS*, *supra* note 21.

individual's funds temporarily. Coordination between jurisdictions must also be addressed, as discussed under "Proposed reforms" below.

E. Low deterrence

Because arrests mainly fall on those who provide their accounts to the fraudsters, many cases will be closed against minor offenders. At present several sections break this offence into smaller pieces carrying lower penalties, which will not deter those who carry it out on a large scale and across borders. Section 111 BNS can apply, but its requirements may be difficult to prove. Section 75 of the IT Act extends that Act to offences committed outside India where the conduct involves a computer, computer system or computer network located in India, but finding and arresting offenders in foreign countries depends on mutual legal assistance treaties, which operate extremely slowly.[33]

Deterrence comes from the likelihood of being caught, the speed of punishment and its severity. The present patchwork does little for the first two, and the punishments are not especially severe either. This is not to say that higher punishments will raise the rate of arrest, but a distinct offence may deter those who would otherwise sell their accounts or phones to others, since they would know what the charge is.

F. Offence labelling

The label attached to an offence can play a large part in how a victim feels about the experience. A victim who feels that he or she was simply cheated out of money by believing what a scammer said may not come forward, out of embarrassment. An offence framed around the offender's false representation of governmental authority may help victims to see what was done to them and to come forward sooner. Such an offence would also help the government to spread the message that no one can be "digitally arrested".

Two further points arise from other legislation:

1. Labelling crimes can work. The criminal code already labels organised crime as a distinct offence (Section 111 BNS), and a distinct offence could likewise be created to represent the conduct involved in these scams.[34]
2. Another offence that helps victims to come forward is coercive control. Some countries have created an offence where one person controls another through fear and

[33] IT Act, *supra* note 8, § 75; https://indiankanoon.org/doc/1965344/; BNS, *supra* note 8, § 111; https://uppolice.gov.in/site/writereaddata/siteContent/Three%20New%20Major%20Acts/20240628171056482 3BNS_IPC_Comparative.pdf; Bhardwaj, *supra* note 4 (overseas operations).

[34] BNS, *supra* note 8, § 111; https://uppolice.gov.in/site/writereaddata/siteContent/Three%20New%20Major%20Acts/20240628171056482 3BNS_IPC_Comparative.pdf.

intimidation; in the United Kingdom, for example, the offence of controlling or coercive behaviour applies within intimate or family relationships. This model merits further study than this paper can give it.[35]

G. Proposed reforms

i. Structure of the offence

The offence should be drafted to fit the conduct rather than the popular name. Its ingredients might be that the accused:

- falsely represents or implies that he or she has some legal standing or authority;
- does so by electronic communication;
- makes threats or inducements related to the law; and
- thereby obtains money or property from the victim, or prevents the victim from getting in touch with others.

The offence should also be punishable when attempted, since a victim suffers prolonged intimidation even if saved from having to part with money. Where the offence is directed at the elderly or vulnerable, is committed by a gang, or involves the use of fake insignia or documents, it should carry heavier sentences, both minimum and maximum. The sentences should exceed those for the individual offences, so that the case is not reduced to a charge of cheating. The precise sentences are best left to Parliament.

ii. Recommendations

- Create an aggravated offence of extortion with impersonation, with increased minimum and maximum sentences, covering a person who falsely portrays himself or herself as having legal standing through electronic communication and thereby obtains money from another.
- Create an offence of coercing a person, by electronic communication, to withhold contact from others, which would close the gap left by Section 127 without broadening its definition.
- Ensure that these offences are registered under Section 308 BNS read with Sections 204 and 336 BNS and Sections 66C and 66D of the IT Act, and not under Section 318 alone.

---

[35] Serious Crime Act 2015, c. 9, § 76 (UK), https://www.legislation.gov.uk/ukpga/2015/9/section/76/enacted; HOME OFFICE, *Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework* (Dec. 2015) (archived July 27, 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1174578/Controlling_or_coercive_behaviour_-_statutory_guidance.pdf.

- Provide guidelines to banks on when they may freeze accounts and how quickly they should do so.[36]
- Conclude legal assistance treaties with other countries and develop ways to restrict the use of spoofed numbers.[37]
- Repeatedly remind the public that there is no such thing as a digital arrest.

iii. Changes to the registration of these crimes

This is probably the most cost-effective and simplest reform. Police stations could be instructed that, on receiving these complaints, they are to register them as extortion and associated offences where possible, and to record in the report that the caller falsely claimed legal standing and ordered the complainant to stay away from others. The accused could then be charged with all the offences of which they are guilty. Banks should be made aware of these situations and act immediately once a complaint is registered, and the courts would receive the crime in its full nature.[38]

iv. A rule for quick, time-limited freezing

Care is needed with such a rule, since it may affect more people than the criminals themselves. It would apply for a fixed period, after which someone would have to reconfirm that the funds must stay frozen, failing which they would be released automatically. The owner of the funds should be notified and allowed to dispute the freeze, and the bank should allow a set amount to be used in an emergency where the account-holder is clearly not involved in the crime. The existing law provides part of this: the Indian Cyber Crime Coordination Centre's system allows suspected fraud money to be put on hold; the BNSS allows a court or Magistrate to order interim attachment without notice; and the Kerala High Court has held that the police cannot themselves attach an account suspected to hold proceeds of crime but must apply to the Magistrate under Section 107. A rule of this kind would allow freezing to happen quickly but fairly.[39]

---

[36] *Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059, Directions 9–15 (India) (directions to banks and financial institutions, including use of the Reserve Bank of India's "Mule Hunter" tool); *Inside Rajasthan High Court's Detailed Directions*, *supra* note 6; *Rajasthan High Court Orders Strict Cyber Safety Measures Statewide*, NEWKERALA (Nov. 28, 2025), https://www.newkerala.com/news/o/rajasthan-hc-directs-state-govt-implement-cyber-safety-measures-802.

[37] Sharma, *supra* note 9 (over 6.69 lakh SIM cards and 1.32 lakh IMEIs blocked up to Nov. 15, 2024); VIVEKANANDA INTERNATIONAL FOUNDATION, *supra* note 7.

[38] Sinha, *supra* note 7 (direction to simplify the registration of cyber fraud complaints); *Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059, Direction 3 (India) (toll-free number for the automatic registration of FIRs).

[39] BNSS, *supra* note 7, § 107(5); https://indiankanoon.org/doc/105332178/; *Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059, ¶ 10 (India) (I4C system "to freeze and put on hold fraud money"); *Rajasthan High Court Issues Sweeping Directions for Cyber Safety Reforms: Rejects Bail in 'Digital Arrest' Extortion Case Under IT Act*, 24LAW (Dec. 3, 2025), https://24law.in/story/rajasthan-high-court-issues-sweeping-directions-for-cyber-safety-reforms-rejects-bail-in-digital; *Headstar Global*, *supra* note 32; *Section 107 of BNSS*,

v. Help from other countries

Some problems cannot be solved within India's borders. Quicker assistance is needed from the countries in which these scams frequently originate, together with steps to stop callers from spoofing Indian numbers. Some measures already exist: a system to identify and block incoming international calls spoofed to display Indian numbers has been put in place, and the Supreme Court has directed the CBI to seek the cooperation of Interpol. It is much easier to cut off the communication than to recover the funds.[40]

IV. COUNTERARGUMENTS

"Current laws are sufficient." It may be argued that the offences described above already exist and that courts have applied them sensibly. That may be true, in the sense that offenders can be convicted. But it does not help with deterrence, it does not describe correctly what the offenders did, and it does not help to freeze assets.[41]

"A new crime cannot be added for every new trick." If that were done, there would be hundreds of offences. The proposal, however, is a defined type of offence, as set out above: extortion and impersonation conducted online, in which a fake authority figure tells the victim to cut off contact with friends and family. The term "digital arrest" need not be mentioned at all.

"The problem is enforcement, not the absence of laws." Communication between banks, telecom providers, the police and others will indeed play a key role in catching and preventing these crimes, which is why procedure has been addressed alongside the substantive offence.[42]

"Bigger punishments will not affect criminals in other countries."[43] This argument has some force. But correctly identifying what happened to victims helps the case, as discussed above, and allows funds to be frozen more quickly. It will also allow those involved within India to be punished.

---

supra note 21.

[40] Bhardwaj, *supra* note 4 (scam farms in Southeast Asia); Sharma, *supra* note 9; *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Pet. (Crl.) No. 3 of 2025, ¶ 6(vi) (SC Dec. 1, 2025) (India) (CBI to seek the cooperation of Interpol); Prakash, *supra* note 6.

[41] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Pet. (Crl.) No. 3 of 2025, ¶ 5 (SC Dec. 1, 2025) (India); BUSINESS STANDARD, *supra* note 5; Prabhanu Kumar Das, *Supreme Court Orders Pan-India CBI Probe on Digital Arrest Scams, Orders States to Give Consent for Investigation*, MEDIANAMA (Dec. 2, 2025), https://www.medianama.com/2025/12/223-supreme-court-cbi-probe-digital-arrest-scams/.

[42] *Adnan Haidar Bhai v. State of Rajasthan*, 2025 SCC OnLine Raj 6059, Direction 8 (India) (quarterly coordination meetings with banks, telecom service providers and intermediaries); *Inside Rajasthan High Court's Detailed Directions*, *supra* note 6; *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Pet. (Crl.) No. 3 of 2025, ¶ 6(viii) (SC Dec. 1, 2025) (India) (Regional and State Cybercrime Coordination Centres); Prakash, *supra* note 6.

[43] Bhardwaj, *supra* note 4 (cross-border "scam farms").

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

"Innocent account-holders may have their accounts frozen." This is a real risk, which is why any freeze should be limited in time and the account-holder told the reason for it. Yet if as much time is allowed to pass as at present, the purpose of freezing assets is defeated.[44]

V. Conclusion

There is a gap that "digital arrest" exploits. No single offence currently fits it, so several are pieced together to bring it within the present law. That approach fails to represent what the victim experienced and does not address the victim's detention. An offence that addresses what is actually happening would allow money to be frozen faster and may stop more people from committing these crimes.[45]

This is not to say that existing laws should be scrapped and replaced. What is needed is a law that identifies a crime in which a person falsely poses as an official to obtain money or to stop the victim from contacting anyone, together with a standard entry that police stations can use when recording complaints, and a power to hold money that may have been transferred to those involved.

Laws of this kind help to stop criminals, because the authorities know what to look for and how to handle it. People should be able to answer the telephone secure in the knowledge that a caller threatening "arrest" is not the government.

This study has limitations. Statistics were not available on how many cases are charged under each provision, how long it takes to freeze assets, or how many cases are successfully prosecuted. Such data would test the claim that cheating is over-used, and would show whether assets are frozen more readily when particular charges are brought.[46]

There are many other jurisdictions with which these proposals could be compared. Some have been touched on above, and the comparison is left open for further work.[47]

*****

[44] *Headstar Global*, *supra* note 32; *Section 107 of BNSS*, *supra* note 21; BNSS, *supra* note 7, §§ 106–107; Bhomesh R. Bellam, *Section 107 BNSS: A Sword Too Heavy for the Hands that Hold It*, SCC Times (Sept. 5, 2026), https://www.scconline.com/blog/post/2026/09/05/section-107-bnss-property-attachment-forfeiture/.

[45] *CBI, ED, Police Don't Arrest People Through Video Calls*, *supra* note 1.

[46] Naina J A, *Over Rs 40 Crore Lost to Cyber Crimes in 2024 in Mangaluru*, Deccan Herald (Dec. 30, 2024), https://www.deccanherald.com/amp/story/india%2Fkarnataka%2Fover-rs-40-crore-lost-to-cyber-crimes-in-2024-in-mangaluru-3335912 (about 5,498 complaints on the National Cyber Crime Reporting Portal, of which 215 were converted into FIRs); Ministry of Home Affairs, *supra* note 3.

[47] Serious Crime Act 2015, c. 9, § 76 (UK), https://www.legislation.gov.uk/ukpga/2015/9/section/76/enacted.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]