

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 8 | Issue 2

2026

© 2026 International Journal of Legal Science and Innovation

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in the International Journal of Legal Science and Innovation 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 Legal Science and Innovation, kindly email your Manuscript to submission@ijlsi.com.

Jurisdictional Dilemmas of Digital Arrest in Cross Border Cybercrime in India

AAYUSH VERMA*, SHRIKANT AMBDKAR**, AND BHAVYA MITTAL***

ABSTRACT

“Digital arrest” is a form of cyber-enabled fraud in which offenders impersonate police officers, investigators, regulators, customs officials, or judicial authorities and create the false appearance that a victim is under criminal investigation or custody. Victims may be kept on video or telephone calls for hours and pressured to transfer money to accounts controlled directly or indirectly by the offenders. The distinctive legal difficulty is geographical. The caller may be in another State or another country; the victim may be in Lucknow or another Indian city; the first recipient account may be located in a different State; later transactions may cross several jurisdictions; and the digital infrastructure used for communication may be situated abroad. This article examines whether Indian criminal law can determine the appropriate forum for such a distributed offence. It argues that Indian law possesses substantial domestic jurisdictional capacity: the place where electronic communication is received, the place where the consequence occurs, and the place where property is delivered can connect the offence to an Indian court. The principal domestic difficulty is the multiplicity of potentially competent forums. The cross-border problem is different: Indian law may prescribe jurisdiction over foreign conduct, yet foreign evidence, platforms, and accused persons remain beyond direct coercive reach. The article proposes a “Digital Arrest Jurisdiction Nexus” based on five factors (act, communication, victim, consequence, and evidence) and a six-stage procedure for investigators and courts.

Keywords: *Digital Infrastructure, Territorial Jurisdiction, Cybercrime, Electronic Evidence, Cyber Fraud*

I. INTRODUCTION

Imagine a retired government employee sitting at home in Lucknow when a video call appears on her phone. The caller is dressed as a police officer and claims that a parcel booked in her name has been intercepted. The caller produces fabricated documents, threatens immediate physical arrest, and directs the victim to transfer her savings to a “verification account.” The

* Author is a Ph.D. Scholar at School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India.

** Author is a Student at School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India.

*** Author is an Independent Researcher, India.

victim is told not to disconnect the call and not to speak to relatives. By the time the deception is discovered, the money may already have moved through several bank accounts and, in some cases, beyond India. This hypothetical captures the central feature of digital arrest fraud: the offence is psychologically experienced in one place but technically and financially distributed across many places. The expression “digital arrest” does not describe a legally recognised form of arrest. It is a label for a method of cyber-enabled cheating, impersonation, intimidation and, depending on the facts, extortion or organised crime. The Ministry of Home Affairs has characterised digital arrest scams as organised online economic crime that is “learnt to be operated by cross-border crime syndicates.”¹ The absence of a statutory offence called “digital arrest” does not diminish the legal significance of the phenomenon. Rather, it requires investigators to identify the substantive offences involved and then apply ordinary rules of criminal jurisdiction to an extraordinary factual structure. The central problem addressed in this article is therefore not whether digital arrest is criminal. Indian law already contains several offences capable of addressing the conduct. The more difficult question is: which court may lawfully inquire into and try a digital arrest case when the accused, victim, financial intermediaries, communication systems and evidence are located in different jurisdictions? The ordinary territorial principle assumes that an offence has a reasonably identifiable place of commission. Cybercrime challenges that assumption because an unlawful act can be initiated in one jurisdiction, received in another, produce financial consequences in a third, and depend upon evidence stored in a fourth.

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)² provides the starting point. Section 197 establishes the ordinary rule that every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.³ Sections 198,⁴ 199⁵ and 202,⁶ however, recognise situations in which an offence is committed partly in one local area and partly in another, in which an act produces a consequence in another place, or in which cheating is practised through electronic communications. These provisions are particularly important because they prevent territorial jurisdiction from being reduced to the physical location of the accused.

¹ Home Ministry Warns Against Fraudsters Posing as Government Officials for Intimidation and Extortion, NEWSONAIR (May 14, 2024, 6:21 PM), <https://newsonair.gov.in/home-ministry-warns-against-fraudsters-posing-as-government-officials-for-intimidation-and-extortion>.

² The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India) [hereinafter BNSS]. Sections 197 to 209 of the BNSS re-enact, with amendments, §§ 177 to 189 of the Code of Criminal Procedure, 1973, No. 2, Acts of Parliament, 1974 (India).

³ BNSS § 197.

⁴ BNSS § 198.

⁵ BNSS § 199.

⁶ BNSS § 202.

The article uses Lucknow as a recurring hypothetical location. Lucknow is not treated as an empirical case study; it is simply an ordinary victim's city through which the jurisdictional rules can be tested. The article asks four principal questions. First, what constitutes the place of commission of a digital arrest offence? Second, can the victim's location independently establish jurisdiction? Third, how do the BNSS provisions concerning electronic communications operate in practice? Fourth, what changes when the accused, infrastructure or evidence is located outside India?

The central conclusion is qualified but important. For the domestic dimension of a digital arrest case, Indian law is substantially capable of identifying a competent forum. Sections 199 and 202 of the BNSS are especially significant because they connect jurisdiction to the consequence of the offence and to the sending or receipt of electronic communications.⁷ The more serious difficulty emerges where multiple Indian courts are simultaneously competent or where crucial evidence and accused persons are outside India. In those circumstances, jurisdiction to prescribe does not automatically become jurisdiction to enforce. The law therefore requires a structured approach that identifies all legitimate territorial connections and then selects the forum best placed to secure effective justice.

II. DIGITAL ARREST AS A CYBERCRIME OF DISTRIBUTED COMMISSION

A. Meaning and characteristics

Digital arrest is best understood as a pattern of cyber-enabled deception rather than as a standalone offence. The offender commonly begins with a fabricated communication concerning a parcel, financial account, identity document or alleged criminal activity. The communication is then escalated by transferring the victim to a person impersonating a police officer, customs officer, investigator, regulator or other public authority. The victim is informed that she is implicated in a serious crime and is placed under a fictional "digital arrest." The objective is to create an atmosphere in which ordinary verification becomes psychologically difficult. The Ministry of Home Affairs has described these operations as organised online economic crime linked to cross-border syndicates.⁸ This characterisation matters for jurisdictional analysis because the apparent "offender" speaking to the victim may be only one participant in a larger network. One person may make the call; another may control a mule bank account; another may move the money; and a principal organiser may be located abroad.

⁷ BNSS §§ 199, 202.

⁸ *Home Ministry Warns Against Fraudsters*, *supra* note 1.

Treating the telephone caller as the entire offence can therefore obscure the geographical distribution of criminal responsibility.

B. The distributed structure of the offence

A completed digital arrest fraud may contain at least six territorial components. First is the place from which the fraudulent communication originates. Second is the place where the victim receives the communication and experiences the coercion. Third is the place from which the victim transfers money. Fourth is the location of the first recipient or mule account. Fifth are the locations of subsequent accounts or conversion points. Sixth is the location of the digital infrastructure, including servers, internet-based calling services and platform data. The accused may be located in yet another place.

C. Why territoriality becomes difficult

Territorial jurisdiction traditionally serves several purposes. It identifies the State most directly affected by the offence, facilitates evidence collection, gives courts proximity to witnesses and protects the accused from arbitrary assertion of criminal authority. Digital arrest weakens the geographical assumptions behind each purpose. Evidence may be distributed among banks, telecom providers and technology platforms. The victim may be in Lucknow, the first mule account in West Bengal and the principal organiser in another country. The accused cannot reasonably predict a forum from the location of the device alone because the offence is deliberately designed to conceal location. The “peace” disturbed by the offence is also distributed: the victim’s State suffers the immediate harm, another State may contain the money trail, and a foreign country may contain the principal actors.

The appropriate response is not to abandon territoriality but to reinterpret its connecting factors in light of electronically distributed conduct. The BNSS already provides the statutory tools necessary for such an interpretation.

III. TERRITORIAL JURISDICTION UNDER INDIAN CRIMINAL LAW

A. The general rule under Section 197

Section 197 of the BNSS provides the ordinary territorial rule: every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.⁹ The word “ordinarily” is significant because the subsequent provisions create exceptions and additional bases of jurisdiction.

⁹ BNSS § 197.

B. Section 198 and multiple places of commission

Section 198 permits inquiry or trial by a court having jurisdiction over any of the local areas concerned where it is uncertain in which of several local areas an offence was committed, where an offence is committed partly in one local area and partly in another, where it is a continuing offence, or where it consists of several acts done in different local areas.¹⁰ Digital arrest fits naturally within this structure. The deceptive communication may originate in one State, the victim may receive it in another, and the transfer of property may occur through a bank located elsewhere.

C. Section 199 and the place of consequence

Section 199 provides that where an act is an offence by reason of something done and a consequence that has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction the thing was done or the consequence ensued.¹¹ In digital arrest cases, the consequence is principally the victim's loss of property.

This makes the victim's location particularly significant. If a victim in Lucknow receives the deceptive communication, authorises a transfer from Lucknow and suffers depletion of funds as a result, Lucknow is not merely the place where the complaint was filed. It is a place where an essential consequence of the offence occurred. This distinction is important because territorial jurisdiction cannot be based merely on a complainant's later decision to travel to a particular city.

The reasoning is consistent with the historical judicial approach in *Mobarik Ali Ahmed v. State of Bombay*, where the Supreme Court recognised jurisdiction in India even though the accused was in Karachi and the relevant representations were made through letters, telegrams and telephone calls.¹² The case illustrates that physical presence of the accused is not indispensable where the fraudulent communication produces its legal effect within India.

D. Section 202 and electronic communications

Section 202 is particularly valuable for digital arrest cases because it expressly addresses cheating practised by means of electronic communications, letters or telecommunication messages.¹³ It permits inquiry or trial where the communication was sent or received and further recognises, for cheating and dishonestly inducing delivery of property, the place where the property was delivered by the deceived person or received by the accused.

¹⁰ BNSS § 198.

¹¹ BNSS § 199.

¹² *Mobarik Ali Ahmed v. State of Bombay*, AIR 1957 SC 857 (India).

¹³ BNSS § 202.

This provision provides at least three obvious connections in a typical digital arrest case. The first is the place from which the deceptive communication was sent. The second is the place where it was received. The third is the place where the victim's property was delivered or the accused received it.

E. Section 206 and conflicting forums

The consequence of Sections 198, 199 and 202 is that more than one court may be competent. Section 206 provides a mechanism for resolving the question where two or more courts have taken cognizance of the same offence: the High Court concerned decides which of them shall inquire into or try it.¹⁴ The provision is useful after competing proceedings have arisen, but it is less satisfactory as a preventive mechanism. It does not provide a detailed pre-litigation test for choosing the best forum.

IV. DETERMINING THE PLACE OF COMMISSION IN DIGITAL ARREST CASES

A. Place of origin of the fraudulent communication

The originating location of the call is an obvious territorial connection because it represents the place from which the offender acted. Section 202 expressly recognises the place from which the communication was sent.¹⁵ Yet this factor is often difficult to establish. Digital arrest operations may use virtual numbers, internet-based calling applications, routing services and compromised infrastructure. The apparent number displayed to the victim may not reveal the physical location of the caller.

B. Place of receipt

The place where the victim receives the communication is usually the most accessible jurisdictional fact. A victim sitting in Lucknow when the call arrives provides a direct factual connection between the communication and Lucknow. Section 202 expressly recognises receipt as a basis of jurisdiction.¹⁶

C. Place of consequence

The place where the financial loss is suffered provides an additional basis under Section 199.¹⁷ The key is to identify a consequence that is part of the offence itself. *Y. Abraham Ajith v.*

¹⁴ BNSS § 206.

¹⁵ BNSS § 202.

¹⁶ BNSS § 202.

¹⁷ BNSS § 199.

Inspector of Police cautions that mere presence of a complainant in a place does not confer jurisdiction when the alleged acts occurred elsewhere.¹⁸

Digital arrest cases are different when the victim receives the communication and loses money in the same place. The victim's location then represents not a coincidental residence or later filing location but the site of receipt, coercion and financial consequence. *Swaati Nirkhi v. State (NCT of Delhi)*, adopting the reasoning in *Y. Abraham Ajith*, similarly treats the place of trial as the place where the cause of action, the bundle of facts constituting the offence, arose rather than any incidental connection.¹⁹

D. Place of delivery or receipt of property

Section 202 also identifies the place where property is delivered by the deceived person or received by the accused.²⁰ This creates a further layer in digital arrest cases because money may pass through a sequence of accounts. The first mule account may be in West Bengal, a second account in Delhi, and a later conversion may occur through a cryptocurrency service without a fixed Indian location.

The first transfer is relatively straightforward: the victim's property leaves the victim's control and enters the first recipient account. Later transfers raise a more difficult question. If the operators of successive accounts are themselves accused of the underlying cheating, their locations may generate additional jurisdictional connections. If they are instead treated as separate facilitators, money laundering actors or witnesses, the jurisdictional analysis may differ.

E. The cluster rather than the single point

The better doctrinal approach is therefore to recognise a cluster of connecting factors. A digital arrest case may lawfully involve jurisdiction at the victim's location, the place of communication, the place of financial consequence, the first recipient location and the location of other relevant acts. The BNSS does not insist that one of these factors must be selected before the others are considered.

V. THE LUCKNOW ILLUSTRATION: ONE VICTIM, MANY COURTS

Consider a retired government employee residing in Lucknow who receives a video call from persons claiming to be police officers in Mumbai. She is falsely told that a parcel containing

¹⁸ *Y. Abraham Ajith v. Inspector of Police*, (2004) 8 SCC 100 (India).

¹⁹ *Swaati Nirkhi v. State (NCT of Delhi)*, Transfer Petition (Crl.) No. 262 of 2018, ¶¶ 14–15 (Mar. 9, 2021) (India), <https://indiankanoon.org/doc/95311661/>.

²⁰ BNSS § 202.

illegal articles has been seized. She is pressured into transferring ₹8 lakh. Investigation reveals that the call was routed through a VoIP service whose immediate technical origin cannot be fixed, though evidence suggests an overseas location. The first recipient account is in West Bengal, the funds move to a second account in Delhi, and part of the money is later converted into cryptocurrency through a platform without a fixed physical presence in India. Under Sections 199 and 202, Lucknow has a strong jurisdictional basis.²¹ The communication was received there; the financial consequence occurred there; and the victim delivered property from there. The police need not first identify the foreign caller before recognising Lucknow as a competent forum. At the same time, West Bengal may have a jurisdictional connection because property was received there. Delhi may also have a connection if the second account is operated by a person treated as an accused in the cheating transaction. The result is not a single jurisdiction but several potentially valid jurisdictions.

From a policy perspective, Lucknow may nevertheless be the most effective initial forum. The victim is there. The victim's device, bank records, testimony and screen recordings are likely to be immediately available there. The first transfer can also be traced from the victim's account. West Bengal may become particularly important for freezing and investigating the first mule account. Delhi may be relevant for subsequent transactions. The example therefore demonstrates the distinction between jurisdiction and forum selection. The first question is whether a court is legally competent. The second is which competent court should lead the investigation and ultimately conduct the trial. Indian law answers the first question more clearly than the second.

VI. COMPETING JURISDICTIONS WITHIN INDIA

The National Cyber Crime Reporting Portal and the 1930 helpline provide an administrative mechanism for reporting and coordinating cyber fraud.²² These mechanisms can help connect the victim's complaint with State cybercrime units and financial institutions.²³ Yet administrative coordination does not itself determine the court of trial. Section 206 remains available when competing proceedings arise, but it is essentially a dispute resolution mechanism.²⁴ It does not rank the territorial connections. Consequently, investigators require a

²¹ BNSS §§ 199, 202.

²² *National Cyber Crime Reporting Portal*, MINISTRY OF HOME AFFAIRS, <https://cybercrime.gov.in> (last visited Sept. 6, 2026).

²³ MINISTRY OF HOME AFFAIRS, *Digital Arrest Scam*, PRESS INFO. BUREAU (Dec. 10, 2024, 4:36 PM), <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2082761®=3&lang=2> (written reply in the Lok Sabha: complaints on the portal and their conversion into FIRs are handled by the State and Union Territory law enforcement agencies, the Citizen Financial Cyber Fraud Reporting and Management System exists for immediate reporting of financial fraud, and the toll-free 1930 helpline gives assistance in lodging online cyber complaints).

²⁴ BNSS § 206.

practical hierarchy. The victim's location ordinarily has the strongest operational claim because the victim is the principal witness and the first evidence is generated there. The first-layer financial location is next because it may offer the earliest opportunity to freeze and identify the recipient. Deeper layers are useful but progressively less suitable as the sole basis for initial forum selection.

VII. CROSS-BORDER DIGITAL ARREST AND EXTRATERRITORIAL JURISDICTION

Section 1(5) of the Bharatiya Nyaya Sanhita, 2023 (BNS) extends the Sanhita to specified offences committed outside India, including offences by Indian citizens beyond India and offences committed by any person outside India that target a computer resource located in India.²⁵ The computer-resource limb is potentially relevant where the conduct is directed at an Indian device or resource, although the precise meaning of "targeting" may require judicial development in digital arrest cases. The Information Technology Act, 2000 (IT Act) provides another extraterritorial basis.²⁶ Section 75 applies the Act to offences or contraventions committed outside India by any person, irrespective of nationality, where the act or conduct involves a computer, computer system or computer network located in India.²⁷ This wording is potentially broader than the "targeting" formulation because it focuses on involvement with an Indian computer resource.

Section 208 of the BNSS provides a procedural mechanism for offences committed outside India by Indian citizens, or by other persons on ships or aircraft registered in India, and requires the previous sanction of the Central Government before such an offence is inquired into or tried in India.²⁸ Construing the corresponding Section 188 of the Code of Criminal Procedure, 1973, the Supreme Court has held that the sanction requirement applies only where the entire offence is committed outside India and is not attracted where part of the offence occurs in India.²⁹ This is highly relevant to digital arrest because the receipt of the fraudulent communication and the financial consequence can occur in India even if the caller remains abroad.

Thus, a digital arrest directed at a victim in Lucknow can often be treated as partly committed in India. The cross-border location of the accused does not automatically deprive Indian courts of jurisdiction. The practical problem is instead securing the accused and the evidence.

²⁵ The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), § 1(5) [hereinafter BNS].

²⁶ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) [hereinafter IT Act].

²⁷ IT Act § 75.

²⁸ BNSS § 208.

²⁹ *Sartaj Khan v. State of Uttarakhand*, Criminal Appeal No. 852 of 2018, 2022 LiveLaw (SC) 321, ¶¶ 13–14 (India) (construing the Code of Criminal Procedure, 1973, § 188); see also *Ajay Agarwal v. Union of India*, (1993) 3 SCC 609 (India).

VIII. ELECTRONIC EVIDENCE AND THE LIMITS OF JURISDICTION

Digital arrest cases depend heavily on electronic evidence. Relevant material can include call detail records, IP logs, device data, screen recordings, bank transaction records, KYC documents, subscriber information and platform records. The Bharatiya Sakshya Adhiniyam, 2023 (BSA) recognises electronic and digital records as documentary evidence subject to the statutory conditions in Section 63.³⁰

Foreign-held evidence creates a different problem. An Indian production order has no automatic coercive effect in another State. If a foreign technology company holds subscriber information or server logs, Indian investigators may need the cooperation of the company or the relevant foreign authorities. The evidentiary difficulty is intensified by data retention periods. A request made after the relevant logs have been deleted cannot recover information merely because Indian jurisdiction exists.

IX. INTERNATIONAL COOPERATION: MUTUAL LEGAL ASSISTANCE AND EXTRADITION

Mutual legal assistance is central to cross-border digital arrest investigations. India may obtain foreign evidence through letters rogatory or through mutual legal assistance mechanisms where treaties exist. Such processes, however, can be slow. Digital evidence may be deleted within a period shorter than the time required for formal international requests. The second major mechanism is extradition. Under the Extradition Act, 1962 and applicable treaties, India may seek surrender of an accused located abroad.³¹ Extradition ordinarily involves dual criminality and may be affected by nationality rules and other grounds of refusal. A foreign-based organiser may therefore remain outside the immediate reach of Indian criminal process even where Indian jurisdiction is legally established.

Interpol cooperation can assist with locating wanted persons and coordinating international policing.³² A Red Notice, however, is not itself an arrest warrant; each member country applies its own law in deciding whether to arrest the person and what legal value to give the notice.³³ Interpol should therefore be understood as a coordination mechanism rather than a substitute for extradition.

³⁰ The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India), § 63.

³¹ The Extradition Act, 1962, No. 34, Acts of Parliament, 1962 (India).

³² *Red Notices*, INTERPOL, <https://www.interpol.int/How-we-work/Notices/Red-Notices> (last visited Sept. 6, 2026).

³³ *Id.*

X. JUDICIAL AND INSTITUTIONAL RESPONSE

Indian judicial doctrine concerning remote cheating predates the internet. *Mobarik Ali Ahmed* demonstrates that an accused acting outside India may nevertheless be tried in India where the deceptive conduct produces its effect within India.³⁴ The principle is highly relevant to digital arrest because the modern statute now expressly recognises electronic communications. At the other end of the doctrinal spectrum, *Y. Abraham Ajith* warns against treating mere presence or filing of a complaint as sufficient to establish jurisdiction.³⁵ The case supports a disciplined victim-centric approach: the forum must be connected to an element or consequence of the offence, not simply to the complainant's later movement.

Significant institutional developments have also come through the Supreme Court's suo motu proceedings concerning victims of digital arrest and forged documents, begun on a complaint that forged Supreme Court orders had been used to hold a senior citizen in a so-called digital arrest and extort money.³⁶ By its order of 1 December 2025, the Court made the Central Bureau of Investigation the primary agency to investigate digital arrest scams, directed the States and Union Territories to accord consent under Section 6 of the Delhi Special Police Establishment Act, 1946, directed the Bureau to coordinate with Interpol, impleaded the Reserve Bank of India to assist the Court on using artificial intelligence to identify mule accounts and freeze the proceeds of crime, directed information technology intermediaries to cooperate with the investigation and preserve data, and directed the expeditious establishment of Regional and State Cybercrime Coordination Centres.³⁷ These measures respond to the very fragmentation identified by the territorial analysis.

XI. CRITICAL DOCTRINAL ANALYSIS

First, the statutory framework was not designed for the degree of multilateral distribution seen in contemporary digital fraud. Sections 199 and 202 are sufficiently broad to capture multiple locations, but they do not explain how jurisdiction should be ranked when a single offence produces five or more relevant territorial nodes.³⁸ Second, there is no clear statutory hierarchy among multiple competent forums. Section 206 can resolve a dispute after competing

³⁴ *Mobarik Ali Ahmed*, AIR 1957 SC at 860.

³⁵ *Y. Abraham Ajith*, (2004) 8 SCC at 103.

³⁶ *SC Takes Strong Note of Rising Digital Arrest Scams, Seeks Centre and CBI Response*, NEWSONAIR (Oct. 17, 2025, 2:20 PM), <https://www.newsonair.gov.in/sc-takes-strong-note-of-rising-digital-arrest-scams-seeks-centre-and-cbi-response>.

³⁷ *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, Order, ¶¶ 5–6, 11 (Dec. 1, 2025) (India), <https://indiankanoon.org/doc/67470969/>.

³⁸ BNSS §§ 199, 202.

proceedings arise, but investigators need guidance before duplication occurs.³⁹ Third, victim-centric jurisdiction remains under-specified in relation to layered transactions. The clearest consequence is the victim's loss. Less clear is whether every subsequent gain or movement of money should independently generate jurisdiction for the underlying offence. Fourth, the most serious gap is enforcement. Indian law may establish jurisdiction over foreign conduct, but jurisdiction cannot compel foreign States or companies to cooperate. This is not a weakness that domestic legislation can entirely solve. Fifth, institutional coordination remains partly dependent on administrative and judicial arrangements rather than a comprehensive statutory framework. The Supreme Court's directions in the suo motu proceedings represent an important response, but judicial directions should not become a permanent substitute for legislation where structural coordination is required.

XII. TOWARDS A MULTI-NEXUS JURISDICTIONAL FRAMEWORK

A. Five connecting factors

The Act factor asks where the accused performed the relevant fraudulent conduct, so far as that can be identified. The Communication factor asks where the deceptive electronic communication was received. The Victim factor identifies the place where the victim was physically present and subjected to coercion. The Consequence factor identifies where the financial loss and corresponding wrongful gain occurred. The Evidence factor identifies where the material evidence needed to prove the case is located and can practically be obtained.

The five factors are not a mathematical test. One factor can be sufficient to establish jurisdiction where the statute permits it. The framework instead serves two purposes: first, to identify all legally competent forums; and second, to select the forum best placed to produce an effective prosecution.

B. Six-stage procedure

Stage One is offence identification. Investigators should specify the suspected offences under the BNS and the IT Act rather than treating "digital arrest" itself as a statutory offence.

Stage Two is territorial mapping. Each of the five factors should be marked as established, probable or unknown.

Stage Three is jurisdictional identification. Investigators should identify every Indian court possessing statutory jurisdiction under Sections 197–202 of the BNSS.⁴⁰

³⁹ BNSS § 206.

⁴⁰ BNSS §§ 197–202.

Stage Four is forum selection. Where multiple courts qualify, the forum with the strongest combination of victim availability and accessible domestic evidence should ordinarily lead, subject to the facts and applicable institutional arrangements. Section 206 should be used when a genuine dispute cannot otherwise be resolved.⁴¹

Stage Five is cross-border classification. Investigators should separately identify which elements are outside India and determine whether Section 1(5) of the BNS,⁴² Section 75 of the IT Act,⁴³ or other applicable provisions support extraterritorial application.

Stage Six is coordinated enforcement. The chosen forum should immediately identify the international evidence and enforcement steps required, including preservation requests, mutual legal assistance, extradition processes and Interpol coordination where appropriate.⁴⁴

C. Why the framework is necessary

The framework does not create new jurisdiction. It organises jurisdiction that already exists. Its value is therefore interpretive and administrative. It prevents the mistaken assumption that the first police station receiving a complaint is necessarily the only possible forum, while also preventing endless multiplication of proceedings.

The framework is complementary to the institutional directions in the Supreme Court's proceedings. A central investigative agency can address who investigates; the nexus framework addresses why a particular court is competent and why that court should ordinarily become the principal forum. Investigation and adjudication are related but distinct questions.

XIII. CONCLUSION

Digital arrest exposes a fundamental tension in contemporary criminal law. The offence is technologically borderless, but criminal jurisdiction remains substantially territorial. Yet the Indian legal framework is more adaptable than a simple territorial model might suggest. Within India, Sections 197–202 of the BNSS provide several bases for jurisdiction.⁴⁵ Section 198 accommodates offences distributed across local areas. Section 199 recognises the place where a consequence ensues.⁴⁶ Section 202 specifically recognises cheating through electronic communications and connects jurisdiction to the place of sending, receipt and delivery or receipt of property.⁴⁷ These provisions make the victim's city, such as Lucknow, a strong jurisdictional

⁴¹ BNSS § 206.

⁴² BNS § 1(5).

⁴³ IT Act § 75.

⁴⁴ The Extradition Act, 1962, No. 34, Acts of Parliament, 1962 (India); *Red Notices*, *supra* note 32.

⁴⁵ BNSS §§ 197–202.

⁴⁶ BNSS § 199.

⁴⁷ BNSS § 202.

forum where the victim receives the communication and suffers the financial consequence there. The domestic difficulty is therefore not a vacuum of jurisdiction. It is multiplicity. West Bengal may be connected to the first mule account; Delhi may be connected to a subsequent account; another State may contain an accused facilitator; and the victim's city may contain the most important evidence. The law needs a method for choosing among these legitimate forums. The cross-border dimension is more difficult. Section 1(5) of the BNS and Section 75 of the IT Act provide bases for applying Indian law to specified foreign conduct.⁴⁸ But the power to prescribe cannot by itself arrest an accused abroad or compel a foreign platform to disclose data. Mutual legal assistance, extradition and international police cooperation are therefore indispensable.⁴⁹ The five-factor Digital Arrest Jurisdiction Nexus proposed here (act, communication, victim, consequence and evidence) offers a practical way to organise these issues. It does not replace statutory jurisdiction; it makes its application more systematic. The accompanying six-stage procedure separates identification of offences, mapping of territorial connections, selection of forum and cross-border enforcement.

Ultimately, the key doctrinal lesson is that “where did the cybercrime happen?” is the wrong question if it assumes only one answer. The better question is: “Which legally recognised territorial connections exist, and which competent forum is best positioned to secure justice?” For a victim in Lucknow, Indian law can generally answer the first part. The continuing challenge is making that jurisdiction effective against people, money and evidence beyond India's borders.

⁴⁸ BNS § 1(5); IT Act § 75.

⁴⁹ The Extradition Act, 1962, No. 34, Acts of Parliament, 1962 (India); *Red Notices*, *supra* note 32.