DIGITAL ARREST AS FINANCIAL CRIME: MONEY LAUNDERING TRAILS, PROCEEDS OF CRIME, AND ED-CBI OVERLAP

Gautam Bahuguna, B.A. LL.B. (Hons.), Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

Dr. Ujjwal Kumar Singh, Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

ABSTRACT

India's growing digital arrest fraud is a new form of financial crime combining elements of cyber fraud and cash demands using authority impersonation of state police with demands for immediate cash transfers, adding an actual and immediate opportunity to mask placement of criminal proceeds. This article examines this phenomenon, not as a unique and distinct statutory crime, but in the form of a composite fact pattern that may be legally addressed through existing criminal law and the financial tracing, and, if the criminal threshold is satisfied, the Prevention of Money Laundering Act of 2002. This study seeks to construct the legal evolution from Coercive Extraction, to Proceeds of Crime, and finally to a Coercive Multi-Agency Investigation using doctrinal study of the Indian statutes, parliamentary debates, legal and policy official pronouncements, and the case law. The central legal question does not lie with the newness of the term "digital arrest", but with the investigator's ability to determine the underlying offence, trace the transferred value, and demonstrate a substantial relationship between the criminally operated property and the criminal nexus to a schedulable offence. The case analyses suggest that the complexity of these cases exacerbates the overlap, and in this regard, state police, the central bureau of investigation, and enforcement directorates, with a primary focus on sequencing, jurisdiction, and evidence in balance to legal enforcement. Simultaneously, the author notes that the rapid reporting, the preservation of electronic evidence, temporary freezing of suspicious transfers, and victim-centred mechanisms for recovery, are just as important as prosecution, if not more so. The author concludes that digital arrests should be seen as the perpetration of a financial crime, in stages: first, a coercive extraction offence; second, a potential laundering offence; and third, a test of whether the Indian criminal process can be precise, doctrinally, while simultaneously responding to the preservation of victim protective, and impacted, an quick enough to preserve collateral.

Keywords: Digital arrest; cyber-enabled financial crime; proceeds of crime; predicate offence; money laundering; Enforcement Directorate; Central Bureau of Investigation; electronic evidence; mule accounts; victim restitution.

1.1 INTRODUCTION

Depending upon the cyber deceit, trick-based fraud, and financial fraud, digital arrest fraud is an emerging field. It is an area of concern in Indian law more so as a composite of various existing crimes rather than as a separate unique legal issue. The problem is therefore not whether digital arrest exists in the abstract, but rather how criminal law, legal procedures, and anti-money laundering laws respond to the situation when an identifiable sting of fear is associated with the movement of money.[1]

Digital arrests usually begin with the impersonation of law enforcement officials. Scammers pose as police officers, Central Bureau of Investigation officers, Enforcement Directorate officers, Reserve Bank of India officers, and officers from the narcotics division, and intimidate the target to stay on the line as they threaten the target with arrest, asset freezes, prosecutions, and other criminal charges until they get the target to send money. The Indian Ministry of Home Affairs and the Indian Cyber Crime Coordination Centre have described this pattern multiple times in their advisories, which is telling because it shows that the State is acknowledging this scam as a repeating operational model.

The Home Affairs Ministry stated that the National Crime Records Bureau does not categorize digital arrest scam statistics separately. That administrative gap does matter in doctrinal terms. It suggests that, for legal analysis to remain coherent, the nomenclature of offences must remain plural. This means a legal composition approach must be employed by the courts and investigators which includes extortion, cheating, personation, intimidation, forgery, electronic evidence, and subsequent legal composition of money laundering if the statutory threshold is crossed. Therefore, a lack of a separate category should not be seen as a lack of doctrinal significance.

What makes digital arrest especially serious is the financial dimension. The scam is not only designed to defraud, but to economically compel the victim to commit an immediate, unconsidered, unadvised, unbanked, and un-cautioned transfer. The first illegality is coercive

[1] Jonathan Clough, *Principles of Cybercrime* 96 (Cambridge University Press, Cambridge, 2nd edn., 2015).

extraction, but the second, and often more sophisticated, illegality is the conversion of the extracted money into layered, concealed, or quickly evaporated assets. This is the reason why looking at the issue from a cyber-fraud perspective is inadequate, and why the expression of proceeds of crime becomes analytically necessary.[2]

Digital arrests should be considered as 'acts' of financial crime, and the consequence of this crime should be viewed as a series of steps unfolding in stages. The first stage refers to the scheduled or predicate offence. The second stage concerns if the transferred value becomes proceeds of crime as per the Prevention of Money-Laundering Act, 2002. The third stage concerns institutional overlap, particularly where State police, the Central Bureau of Investigation, and the Enforcement Directorate act in relation to the same chain of transactions, but under different legal frameworks.

The analysis is doctrinal and focused predominantly on Indian law. It attempts to respond to a practical problem of growing importance, using various sources, including, but not limited to, the Indian statutes, Parliament website, Official Advisory, Supreme Court ruling, and answer the questions When a victim is digitally pressured to pay, what do the investigators need to prove to go from fraud to laundering, from a complaint to an attachment, and from one investigative agency to another, while avoiding the collapsing of legally defined thresholds and telling the narrative of public outrage.

1.2 DIGITAL ARREST AS PREDICATE FINANCIAL CRIME

The initial objective is to accurately categorize digital arrest. Although the phenomenon seems new since the coercive process is remote, screen-based, impersonated, and seamlessly paid through digital means, the legal components in play are not as novel. They include inducement, coercion, deception, and extraction. Conceptually framing it as a predicate financial crime is a means to sidestep both under-criminalisation and doctrinal overreach.[3]

1.2.1 Concept and Modus Operandi

Digital arrest scams often start with fake triggers such as packages with illicit materials, fraudulently linked bank accounts, or arrest warrants for a criminal investigation. Victims are

[2] Vishwanath Paranjape, *Cyber Crimes & Law* 118 (Central Law Agency, Allahabad, 2nd edn., 2019).
[3] Tessa Cole, "How Are Financial Institutions Enabling Online Fraud? A Developmental Online Financial Fraud Policy Review", 30 *Journal of Financial Crime* 1458 (2023).

almost always subjected to isolation, are instructed not to speak to family members, banks, or lawyers, and enduring multiple video call isolation instructions not to speak to family members, banks, or lawyers. Victims are frequently instructed to show certain documents, provide a bank balance, or are placed in a position where they must remain on camera for long periods of time. The architecture of fear is doing the work of changing the nature of the crime from an asserted voluntary transfer to a legally nuanced extraction.[4]

What legally appears to be consent is fragile. A victim paying money under the direction of a scammer posing as an arresting officer telling the victim that there is an operational hold on their bank accounts does not demonstrate normal commercial freedom. Rather, this is far closer to an extortionate collapse under an impersonation of the state. The use of fake warrants, phony case numbers, spoofing, and fake departmental identities as callers increases the crime, since the authority being impersonated is not a private individual, but the state.[5]

The direct consequence of these procedures is that police must consider these types of complaints as disclosing identifiable offences when the fact pattern includes deception and coercive transfer. The constitutional bench in *Lalita Kumari v. Government of Uttar Pradesh*,[6] stated that where a piece of information reveals a cognizable offence, the reporting of that offence is a must, and is only subject to a very stringent few pre-reporting inquiry exceptions. In the case of complaints regarding digital arrest, the costs of delay in registering a case are even more pronounced, in that the delay allows the perpetrators of the fraud to disperse the defrauded funds in a manner that is not susceptible to recovery.

1.2.2 Penal Mapping

The Bharatiya Nyaya Sanhita, 2023 gives an adequate wide-reaching range of penal codes to accommodate the behaviour without having to create some new doctrinal category. Depending on the facts the scam could be classified as extortion, cheating, cheating by personation, criminal intimidation, forgery, the use of forged documents, and conspiracy. Better for us is functional mapping as opposed to nominal innovation. Instead of describing digital arrests as

[4] Digital Arrest Scam, *available at:* https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2082761 (last visited on March 29, 2026).
[5] The Growing Problem of Digital Arrest Scams in Bharat, *available at:* https://www.vifindia.org/article/2024/november/26/The-Growing-Problem-of-Digital-Arrest-Scams-inBharat (last visited on March 28, 2026).
[6] (2014) 2 SCC 1.

a standalone offence, courts should focus on particular elements that are evidence-based. This approach improves the quality of charges and subsequent anti-money laundering investigations.[7]

This mapping has substance. It ascertains whether the factual foundation can support a laundering case. The anti-money laundering law only punishes some of the movements of money that are suspicious. It punishes the process or activity that touches the property that resulted from a crime that is classified as a scheduled offence. That's why at the earliest stage, the precise identification of the underlying wrong is not a mere drafting exercise, but is the doctrinal bridge that connects the victim's complaint to the subsequent financial investigation. A poorly constructed predicate case will often yield a poorly constructed laundering case.[8]

Digital arrests bring to light the significance of technology-neutral statutory interpretation. While means of coercion can include messaging apps, video apps, calls to the victim using a spoofing service, or digitally manipulated documents, the harm is still recognizable by criminal law. The law of extortion or cheating is still applicable, regardless of the fact that the victim is threatened via a screen. The only thing that changes is the evidentiary environment: screenshots, bank drop notifications, call records, instructional recordings, and device logs.

Therefore, the substantive law and the law of proof have to be applied together from the start.

1.2.3 Financial-harm Structure

Digital arrest cases differ from typical cheating complaints in the financial structure involved in the crime. Offenders' accounts that victims are made to transfer money to are usually not the end stop. The accounts are used to split and layer money, cash out, and funnel the money through gateways to other mule accounts. The victims are made to transfer the money during the coercive act, but the crime does not stop there. It is only the first step of a much larger financial operation.[9]

The subsequent national figures demonstrate the magnitude of the cyber-fraud landscape in which digital arrest functions. While the figure 1 captures data on cyber fraud as a whole, it

[7] Prashant Mali, *Cyber Law & Cyber Crimes* 143 (Eastern Book Company, Lucknow, 2nd edn., 2015).
[8] D. P. Mittal, *Law Relating to Information Technology, E-Commerce, E-Governance & Cyber Crimes* 165 (Eastern Book Company, Lucknow, 1st edn., 2024).
[9] Ajay Kumar Goel, "Pandemic and Online Financial Frauds Regulatory Issues and Challenges", 5 *International Journal of Law Management & Humanities* 601 (2022).

shows the increased volume of reported incidents of cybercrime and the increased volume of reported losses, which justifies a research paper's vertical bar, horizontal bar, line, or dual-axis chart.

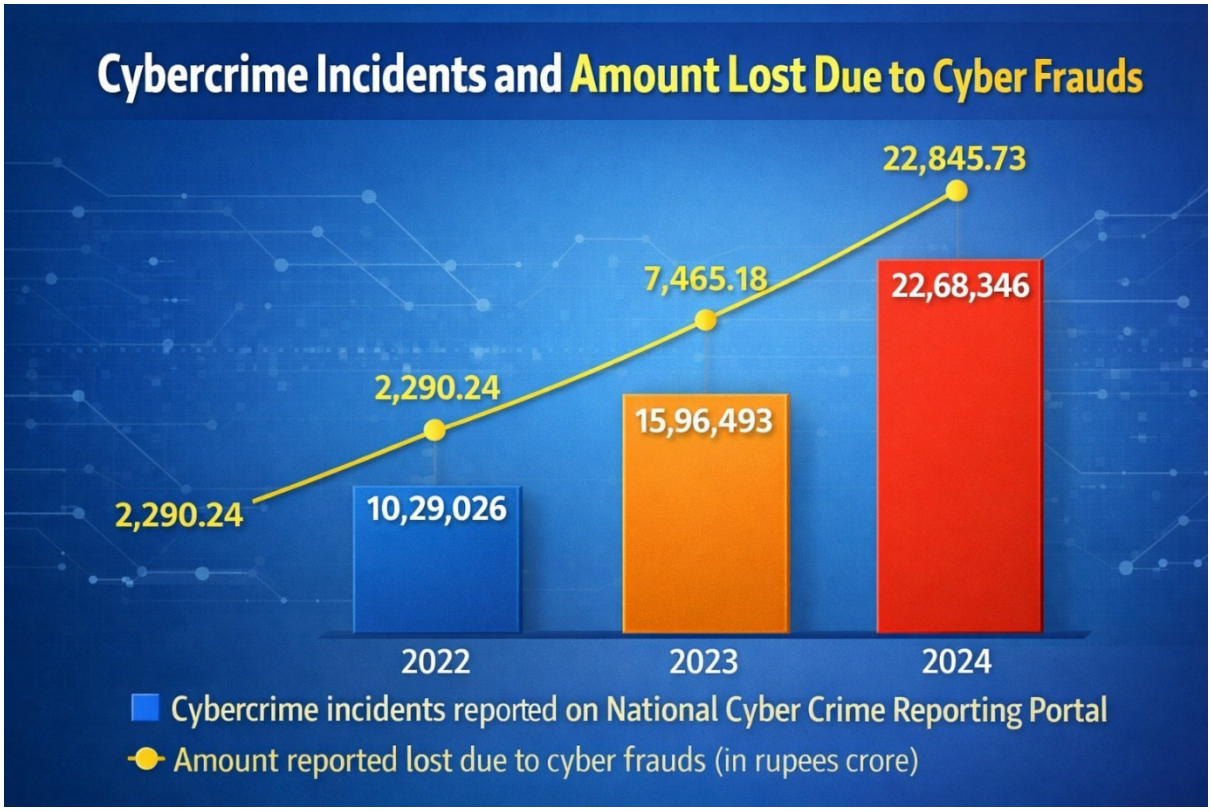

Figure 1. India incidents of cybercrime and reported losses, 2022 to 2024.[10]

The Figure 1 demonstrates doctrinally that the legal system is dealing not with local deception but with an ever-widening field of cyber-enabled extraction. When the monetary curve outstrips the incident curve, the mere fact that more cases are reported is an understatement. It also suggests that the focus of the targeting may be of higher value, scams may be better scripted, victims may be more fearful, and extraction and laundering channels may be more efficient.

This is why digital arrest should be understood as a type of crime of forced relocation and then concealment opportunity. The first part is a broad criminal law issue pertaining to extortion, fraud, impersonation, and threats. The second part poses a more complex issue as to whether

[10] Lok Sabha Unstarred Question No. 432: Cases of Cybercrime, *available at:* https://www.mha.gov.in/MHA1/Par2017/pdfs/Par2025-pdfs/LS02122025/432.pdf (last visited on March 21, 2026).

the diverted money could be classified as laundered through the legal processes of possession, concealment, acquisition, use, or the disposition of the money as untainted. The second part of this analysis can only be as good as the first part is strong and well-defended.[11]

1.3 PROCEEDS OF CRIME AND MONEY LAUNDERING ARCHITECTURE

The Prevention of Money Laundering Act, 2002 has not criminalised all transactions that are morally questionable, or economically damaging. It criminalises specific relationships of criminal acts, some sort of the property, and subsequent dealing with that property. In the case of digital arrests, the hardest questions deal with the statutory nexus: what is the tainted property, how is the derivation proven, and when does movement constitute laundering?[12]

1.3.1 Scheduled Offence Requirement

The key element in law is defining "proceeds of crime" in section 2(1)(u) and formulating the crime in section 3 of the Prevention of Money Laundering Act, 2002. The definition of "proceeds of crime" is not definitional, it is a jurisdictional limit. The Enforcement Directorate has to prove that the said property was acquired or gained, directly or indirectly, from a criminal act involving a scheduled offence. There has to be more than a mere suspicion about the unexplained money.[13]

In *Vijay Madanlal Choudhary v. Union of India*,[14] the Constitution Bench restated the fact that the anti-money laundering laws are linked to the commission of a crime concerning a scheduled offence, even if the laundering offence is different from the predicate crime. This is a common misunderstanding. Laundering is different in that it punishes the subsequent dealing with the 'tainted' property. However, it is also dependent because the taint must come from a scheduled criminal activity. Without that, there is no statutory basis for the laundering claim.

The later decision in Pavana Dibbur v. Directorate of Enforcement further clarified this issue. The Supreme Court stated that an individual does not have to be an accused in the predicate case to be subject to a laundering claim, but there must be some criminal activity pertaining to

[11] Ioannis A. Bolimos, Kim-Kwang Raymond Choo, "Online Fraud Offending Within an Australian Jurisdiction", 24 *Journal of Financial Crime* 277 (2017).
[12] Prevention of Money Laundering Act, 2002 (PMLA), *available at:* https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html (last visited on March 27, 2026).
[13] Abhijeet Sharma, *Money Laundering: Prevention, Law & Practice* 177 (Eastern Book Company, Lucknow, 1st edn., 2023).
[14] [2022] SCC Online SC 929, (2023) 12 SCC 1.

a scheduled offence. This is of particular significance to the cases of digital arrests because these types of frauds have 'peripheral' account holders, 'helping' or 'relating' persons who only come into the picture after the money has moved. Their liability is determined by culpable knowledge and nexus, and not by mere relational proximity.[15]

Yash Tuteja v. Union of India[16] further developed the reasoning by stating that, without a predicate or scheduled offence the complaint is deficient. Therefore, a complaint under the Prevention of Money Laundering Act, 2002, cannot exist as an isolated financial claim. In terms of digital arrest litigation, the prosecutors have a greater burden. Simply stating the presence of fear, transfer, and suspicious accounts is insufficient. They must articulate the offence and criminality of the value transfer and how the transferred value linked to it.

The statutory bridge opens when the underlying facts align with offences that fit scheduled entries, and the victim's money can be linked to the crime. The analysis must proceed as follows: a) identify the predicate act, b) ascertain the property obtained as a result of that act, and c) demonstrate the subsequent process or activity related to that property. Procedurally speaking, jumping to anti-money laundering terminology without the aforementioned steps is a legal non sequitur.

1.3.2 Tracing and Layering

Because the origination of the transfer is typically electronic and time-stamped, digital arrest cases are especially suited for financial tracing. Specifically, movements as a result of device IDs and de-linked branch withdrawals are discernible with far greater precision than older cashbased fraud on the Detectable. Unified Payments Interface (UPI) transactions) and Participating banks' KYC (Know Your Customer) records, as well as the banks' KYC records, may also reveal and expose moved cash/inflows. However, just because something is traceable, does not mean it is legally sufficient. Although a visible trail shows the movement of something, it does not mean that all subsequent holders intended to participate in the illegitimate movement of the item or to legitimize it.[17]

[15] Jai Anant Dehadrai, *Prevention of Money Laundering Act, 2002: A Practitioner's Guide* 201 (Eastern Book Company, Lucknow, 1st edn., 2024).
[16] (2024) 8 SCC 465.
[17] Aaron Spensley, "Untangling Laundered Funds: The Tracing Requirement Under 18 U.S.C. § 1957", 75 *Stanford Law Review* 1157 (2023).

The mule-account infrastructure is massive, and official documents now describe it as such. The Ministry of Home Affairs told Parliament in December 2025 that the suspect registry has more than 18.43 lakh suspect IDs, and that 24.67 lakh Layer 1 mule accounts have been ingrained in the entities, with declined transactions worth over ₹8,031.56 crore. This information is important for doctrinal analysis as it demonstrates that the laundering ecology of cyber fraud is no longer incidental, but rather structured, layered, and institutionally apparent.[18]

Nonetheless, the prosecution must prove nexus, regardless of movement across several accounts. While a layered trail may support a concealment inference, such an inference is contextual, depending on the velocity of the transfers, the relational proximity of the account holders, fabricated documents for account openings, patterned communications, directives, or communications to/from a supposed controller of the fraud. The Supreme Court's proceeds of crime rulings demand some actuality of proximity between the property and the defined criminal conduct. The mere circulation of funds does not suffice.

1.3.3 Attachment and Confiscation

When the Enforcement Directorate alleges that a certain property is linked to proceeds of crime, the next step is normally a provisional attachment under section 5, and then, in order, adjudicative review under section 8 of the Prevention of Money-Laundering Act, 2002. Ideally, attachments are protective and not punitive, and their purpose is to ensure that there will not be frustration of confiscation proceedings. However, in the real world, attachments are frustrating and can cause severe disruptions to business and family financial arrangements, and cause great reputational damage, long before there is a final adjudication. For this reason, the nexus issues in such cases are particularly sensitive.[19]

Digital arrests often lead to challenging attachment disputes, particularly when combined with previously legitimate assets. In Pavana Dibbur v. Directorate of Enforcement, the Supreme Court focused on the challenges of temporal and transactional nexus, especially when an asset exists prior to the alleged criminal activity, or when the accused alleges an independent

[18] Stefan D. Cassella, "Toward a New Model of Money Laundering: Is the "Placement, Layering, Integration" Model Obsolete?", 21 *Journal of Money Laundering Control* 494 (2018).
[19] Restitution of Properties/Assets, *available at:* https://www.enforcementdirectorate.gov.in/performance/restitution-of-properties-assets/ (last visited on March 25, 2026).

funding source. This line of reasoning applies strongly to the money trails of digitally arrested assets, as recipients typically contend that the account or asset in question was lawfully in existence prior to the contested transfer.[20]

A reliable doctrinal approach must separate three types of dealings: first, dealings with property that was directly received from the fraud; second, dealings with property that was purchased using such proceeds; and third, dealings with property that is simply linked to a person of interest, but there is no evidence to suggest that the property is linked to the fraud. Only the first two categories align with the framework of the prohibitive statute. The third category is an example of true reach. The strength of the anti-money laundering regime is that it targets the change of value that has been derived from crime, not the change of value based on a vague and unsubstantiated economic theory. The distinction will have to be applied at all phases of the digital attachment and confiscation decree for the prosecutions on digital arrests to be plausible.

1.4 ENFORCEMENT DIRECTORATE AND CENTRAL BUREAU OF INVESTIGATION OVERLAP

The issue of overlap between the Enforcement Directorate and the Central Bureau of Investigation is best understood as layered jurisdiction rather than a problem of bureaucratic rivalry. Different legal actions can arise from the same set of facts as one agency may deal with the predicate offence while another agency deals with the offence of laundering. The problem is to maintain legal distinction while not losing the coordinate effort of investigators.[21]

1.4.1 Institutional Mandates

Investigations by the Enforcement Directorate fall under the Prevention of Money Laundering Act of 2002. The Central Bureau of Investigation, however, has a statutory base under the Delhi Special Police Establishment Act of 1946 and investigates what are termed as notified offences, typically involving corruption, serious financial crimes, or other matters that are constitutionally or statutorily required to be assigned to them. State police are primary because “police” and “public order” are State subjects and a number of digital arrest complaints are the

[20] ARIN-AP, *available at:* https://www.enforcementdirectorate.gov.in/international-cooperation/arin-ap/ (last visited on March 24, 2026).
[21] Aaditya Gore, "Case for a Common Investigative Procedure for All Agencies", 6 *Commonwealth Law Review Journal* 339 (2020).

result of local reporting, local bank collaboration, and local First Information Reports.[22]

The Central Bureau of Investigation has specific transnational relevance in cyber-financial crime. In March 2025, the Ministry of Home Affairs notified Parliament that the National Central Bureau of the Central Bureau of Investigation uses INTERPOL for communication with foreign law enforcement and that the Central Bureau of Investigation is the lead agency for the G7 24/7 cybercrime data-preservation-request-in emergencies network. This is especially relevant when the digital arrest infrastructure, servers, or accounts chain transgress the borders of India.[23]

The scenario is therefore layered. A single digital arrest case starts with a cybercrime complaint at a local level, branches into interstate letters of a financial tracing, and cross-border aid or laundering. None of these stages automatically displaces the other. The central doctrinal concern is that laundering jurisdiction is not a circumvention of the federal balances of power concerning police authority, and Central Bureau of Investigation jurisdiction is not triggered simply because a case is serious, digitally mediated, and of serious financial magnitude.

1.4.2 Parallel Proceedings

It is legally possible for parallel proceedings to occur, as the predicate case and laundering case are not the same. One of these could go at a First Information Report, investigation, and a final report or charge-sheet. The other could go at an Enforcement Case Information Report, summons, a search, attachment, and a complaint to the Special Court. The fact that there are overlapping facts does not mean that there is a merger of causes. Each process has its own statutory thresholds, procedural incidents, and consequences for liberty. That distinction is central to doctrinal clarity in digital arrest litigation.[24]

The combined lawsuits of *P. Chidambaram v. Central Bureau of Investigation*[25] and *P. Chidambaram v. Directorate of Enforcement*[26], continue to be useful to illustrate how the same factual context can support separate actions before different agencies. While the cases do not

[22] What We Do, *available at:* https://enforcementdirectorate.gov.in/about-us/what-we-do/ (last visited on March 29, 2026).
[23] Central Bureau of Investigation, *available at:* https://cbi.gov.in/about-us?search=what-we-do (last visited on March 28, 2026).
[24] P.S.P. Suresh Kumar, *Law Relating to CBI & ED Including Recent & Landmark Judgments* 184 (Vinod Publications (P) Ltd., New Delhi, 3rd edn., 2025).
[25] (2020) 13 SCC 337.
[26] (2019) 9 SCC 24.

concern virtual arrests, they illustrate the structural principle that one investigation does not wipe out the legal autonomy of other investigations. Courts, however, are aware of the effects of parallel investigations on arrests and bail, and the strategic unfairness of an investigator.[27]

In order to understand how the digital case arrests work, one must see how the prosecution is unable to, in a casual way, draw legitimacy from one process to rationalize another. A strong case regarding fraud does not, by itself, respond to the question regarding the proceeds of crime, and a strong narrative with respect to laundering does not eliminate weaknesses with respect to the predicate case. Also, one shouldn't let institutional overlap obscure the difference between the evidence of impersonation and the evidence of concealment. The more the actors involved, the more crucial it becomes to trace the factors to the legal element they prove, and to whom the legal jurisdiction derives any authority to collect the evidence.

1.4.3 Federal and Constitutional Limits

Under the Delhi Special Police Establishment Act of 1946, the Central Bureau of Investigation's authority within individual States is determined by the Act's extension and consent provisions. However, constitutional courts still have the authority in particular cases to compel the CBI to investigate. In *State of West Bengal v. Committee for Protection of Democratic Rights*, *West Bengal*,[28] the Constitution Bench ruled that the High Courts and the Supreme Court may, in the exercise of judicial review, direct such investigation in the absence of consent from the State, but that authority should be used very judiciously.[29]

This principle is relevant for digital arrest cases with inter-state or international dimensions. Some fraud schemes use geographically dispersed models for their call centres and for their bank accounts domiciled in one State while their victims are in another and their operational platforms are outside India. Here, if the piecemeal and structurally shallow investigations fail to follow the whole fraud, the constitutional justification for requesting the CBI to investigate becomes stronger. *State of West Bengal v. Committee for Protection of Democratic Rights*, *West Bengal*[30] cautions that one should not consider transfer as an everyday solution.

---

[27] K. K. Khandelwal, Anu Singh, *A Treatise and Commentary on the Prevention of Money Laundering Act, 2002 (In 2 Volumes)* 129 (OakBridge Publishing, Gurugram, 1st edn., 2025).
[28] (2010) 3 SCC 571.
[29] Sameer Sharma, "Independence and Temporality: Examining the PMLA in India", 23 *Journal of Money Laundering Control* 208 (2020).
[30] *Supra* note 30.

A more sustainable model is cooperative federalism under technological coordination as opposed to reflexive centralisation. The latest Standard Operating Procedure concerning the National Cybercrime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System develops a victim-centric coordination mechanism and keeps State police structurally responsive to the coordination mechanism. In digital arrest cases, the best institutional response is often coordinated sequencing, not just agency substitution.[31]

1.5 EVIDENCE, ARREST, AND REMEDIES

Any credible piece of writing about digital detention must conclude where the litigation truly heats up: the intersection of proof, detention, procedure, and retrieval. These digital cases are, figuratively and literally, bank slips and legal compliance documents in the waist of digital communication. They are also influenced by the arrested reasoning and the velocity with which banks get to freeze collusive transfers before the money disappears.[32]

1.5.1 Electronic Evidence

Cases of digital arrests usually have a lot of evidence. Victims have call logs, screenshots of video calls, fake message fake message alerts, transaction notifications, dummy account info sent by the fraud, and recordings of the coercive interaction. The Bharatiya Sakshya Adhiniyam, 2023, adds digital records to the breach of law that preserves the admissibility of records, while section 63 provides the conditions for considering computer output as evidence in the form of documents. For cyber fraud prosecutions, this legal consistency is imperative.[33]

The *Anvar P. V. v. P. K. Basheer*[34] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[35] cases have been important in that they have said that the evidentiary value of electronic documents must be taken seriously. The courts have said that the way documents can be relied upon and used depends more on the way the documents can be proven to be admissible than on the subjective belief of the judge. Even though we have now the Bharatiya Sakshya Adhiniyam, 2023, the important learning from the evidence still remains that the

[31] Kirty Ranjan Rani, "Federalism Under Indian Constitution Vis-à-vis CBI Investigation", 7 *International Journal of Legal Developments & Allied Issues* 25 (2021).
[32] Note on Conman, *available at:* https://www.enforcementdirectorate.gov.in/media/note-on-conman/ (last visited on March 27, 2026).
[33] Kush Kalra, *Law of Electronic Evidence with Reference to New Criminal Laws* 91 (Vinod Publications (P) Ltd., New Delhi, 3rd edn., 2025).
[34] (2014) 10 SCC 473.
[35] (2020) 7 SCC 1.

prosecution has the burden of proving, not just what was displayed on the screen, but also how the displayed screen constitutes evidence that is admissible.[36]

This underlines the importance of determining a preservation strategy. Victims are urged to report the crime as soon as possible via the helpline and the portal. Simultaneously, investigators are challenged to take the necessary steps to preserve all potential evidence related to the crime, which includes the data associated with the relevant platforms, banking records, and materials contained on the devices, before such evidence is no longer available. In cases with a cross-border dimension and/or involving multiple platforms, the international transactional role of the Central Bureau of Investigation combined with the cross-border cybercrime module, while they do not replace evidence, are pertinent for the issue of obsolescence of evidence, i.e. preserving evidence before it is lost. In a digital arrest case, delay is an evidence loss as well as a loss from an investigative perspective.

1.5.2 Arrest Safeguards

The severity of the offence does not take away from the principle of procedural fairness. While the anti-money laundering framework has serious arrest powers, Section 19 of the Prevention of Money Laundering Act, 2002 states that an authorised officer has to record reasons to believe and has to inform the arrested person of the reasons for arrest. In practice, disputes arise not so much as to whether an arrest power exists, but about whether there has been clear, adequate and timely communication of this. Such disputes involve substantive constitutional issues as they implicate personal liberty and adversely affect the practical exercise of the right to legal recourse.[37]

In the case of *Pankaj Bansal v. Union of India*[38], the Supreme Court, while exercising real content to the safeguards, ruled that the reasons for arrest must be provided in writing so that the person arrested can constructively challenge the detention and seek the remedy. This case is significant not so much for what it does to the anti-money-laundering legislation, but for reaffirming the principle that procedural safeguards must be real, not illusory. There is always the risk of postponing concerns for personal liberty in the interest of investigative zeal in cases

[36] Yuvraj P. Narvankar, *Electronic Evidence in the Courtroom: A Lawyer's Manual* 155 (Lexis Nexis, Gurugram, 2nd edn., 2025).
[37] Anjali Rautela, "Constitutional Rights of the Accused and Analysis of Prison Administration", 4 *Journal of Legal Studies & Research* 18 (2018).
[38] [2023] INSC 866, (2024) 7 SCC 576.

of economic offences; Pankaj Bansal v. Union of India counters that tendency.[39]

Since the beginning of the online scam interactions, most suspects detain digitally for laundering crimes have not been originally identified. The digital trail is only analysed after the interactions. A person may only be identified as a beneficiary, account holder, or facilitator after the documents have been assembled. In cases of later arrests, justifications for the arrest become crucial. If an accused is farther removed from the coercive encounter with the victim, the state must describe in detail the crime comprise of proximate gap to the coercive crime and laundering activities.

1.5.3 Complaint Stage and Court Process

The Supreme Court's ruling on *Tarsem Lal v. Directorate of Enforcement Jalandhar Zonal Office*[40] is of recent but major significance. The Court examined the circumstances of accused individuals who have not been arrested during the investigation but were subsequently summoned after the complaint had been filed. The judgment refuses an automatic slide from complaint to custody and states that the ordinary criminal process still counts. This is important for the digital arrest prosecutions as many downstream participants in a financial trail are added without prior arrest.[41]

This decision is also consistent with the procedural framework constructed under the Bharatiya Nagarik Suraksha Sanhita, 2023. Relating to the court, when a complaint is filed, the provisions for the examination of the complainant, process delays, the issuance of process, and the dispensation of the complainant's personal attendance become relevant to the accused's presence in court. The gist of such a provision is procedural gradation. The issuance of a summons is the standard position, whereas a warrant would require additional justification.

That principle regulates the move from inquiry to prosecution.[42]

1.5.4 Victim Freezing and Restitution

Digital arrests compel legal analyses not simply on the cases of the prosecution side vis-à-vis

[39] Richa Kaur, "Preventive Detention Vis-À-Vis Rule of Law in India- A Critical Study", 10 *Journal of Legal Studies & Research* 123 (2024).
[40] [2024] INSC 434, (2024) 7 SCC 61.
[41] Filing a Complaint on National Cyber Crime Reporting Portal, *available at:* https://cybercrime.gov.in/Webform/Accept.aspx (last visited on March 25, 2026).
[42] Submit a Tip, *available at:* https://cbi.gov.in/submit-tip (last visited on March 24, 2026).

the 'restitution' side. The design of the Citizen Financial Cyber Fraud Reporting and Management System allows for the immediate reporting of a fraud, and the freezing of transactions. The Government claims significant loss has been prevented as a result of this. The Ministry of Home Affairs claims that as of 31 December 2025, saved losses for over 23.61 lakh fraud complaints amount to over ₹8,189 crore. For a crime that is defined by the rapidity of the transfers involved, this type of remedial architecture is not peripheral, it is central.[43]

The following figure 2 aids visual analysis by showing the concentration of reported fraud under cyber-crimes by the top States in 2023. It can be adapted to a bar chart to show concentration by region or a pie chart to show the top reporting States.

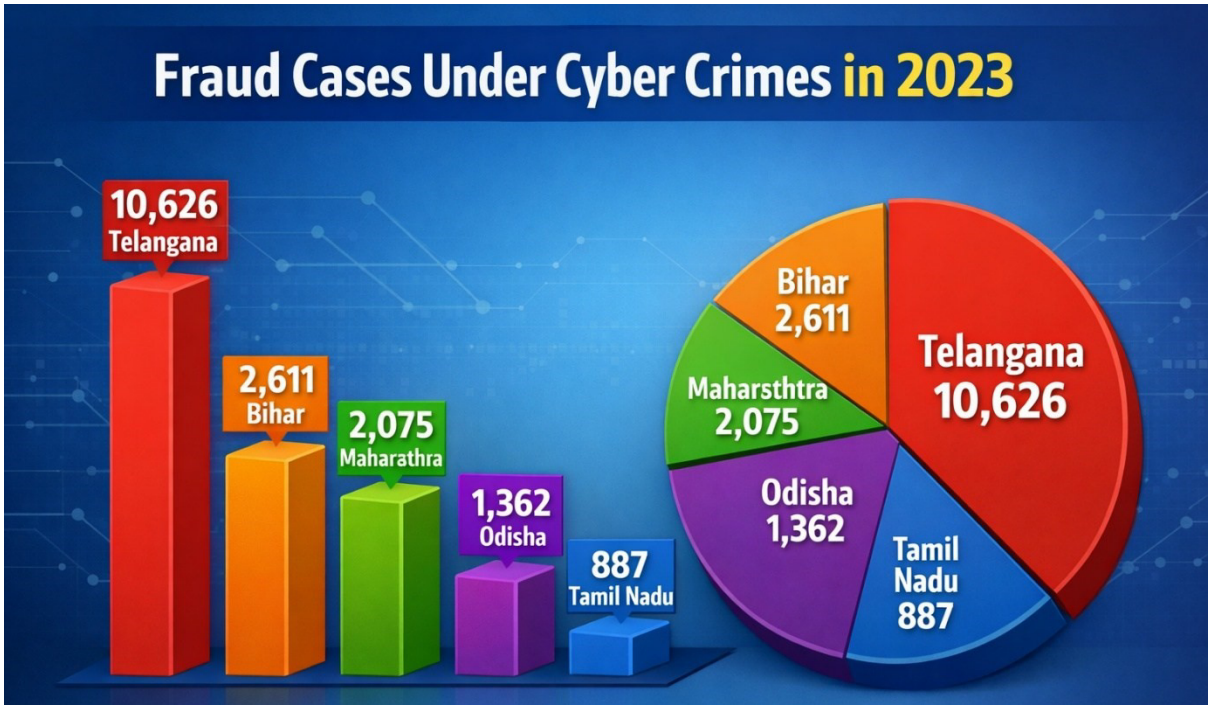

Figure 2. Top five States by fraud-for-cyber-crime cases, 2023.[44]

The figure 2 should not be analysed too simplistically as simply a map of victimization. In the cyber-financial crime, the place may reflect the strength of reporting, the focus of enforcement, operational hubs, account structures, and victim location. In the analysis of digital arrests, the figure supports a broader argument; that is, the jurisdictional fragmentation is part of the problem, which is why the rules on coordination are almost as important as the substantive

[43] Pavan Duggal, *Online Frauds and Law* 167 (Law & Justice Publishing Co., Delhi, 1st edn., 2026).
[44] Rajya Sabha Unstarred Question No. 553: Prevention of Cyber Financial Fraud, *available at:* https://www.mha.gov.in/MHA1/Par2017/pdfs/Par2026-pdfs/RS04022026/553.pdf (last visited on March 21, 2026).

crimes.

The victim must be central to the remedy and the offender must be punished. The ability of victims to file complaints quickly, banks to act and freeze accounts, to flag accounts as suspicious, and have clear and easy ways to escalate, is likely to be of more help in achieving actual justice than a post facto, punitive prosecution that is likely to be empty of any recovery. The inability of a legal system to describe an offence and to freeze or intercept the crime proceeds may appear to be sophisticated to some, but in practice it is profoundly unjust. In cases of digital arrest, the victim's perception of possible recovery is central to the legitimacy of the criminal process.

Recent drafts standard operating procedure for the National Cybercrime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System, indicates a more victim-centric approach. Officially, these drafts aim for a more uniform victim-centric approach with better coordination across States and Union Territories. Integrated with the suspect registry, platform analytics, and the 'Pratibimb' module, the emerging picture is of an anti-fraud framework that prioritises financial speed, interstate connections, and the need for operational responsiveness to detect laundering activity.[45]

1.6 CONCLUSION

The term digital arrest possesses some of the legal significance that comes with its newly coined public name. It is important legally because arrest digitization integrates the elements of coercion, fraud, transfer, concealment, and urgency in the event chain. Consequently, any legal response that remains inadequate must be moved from substantive offence to financial tracing, from tracing to statutory nexus, from nexus to due process, without omissions.[46]

The primary focus of this article is the conceptualization of digital arrest as a predicative financial crime, where the anti-money laundering ramifications operate on proof as opposed to narrative. The Supreme Court in respect to the rulings of *Vijay Madanlal Choudhary v. Union of India*,[47] Pavana Dibbur v. Directorate of Enforcement and *Yash Tuteja v. Union of*

[45] Kush Kalra, *Law Relating to Bank Frauds (Issues and Challenges)* 203 (Whitesmann Publishing, New Delhi, 1st edn., 2025).
[46] Harsh Mahaseth, "When Can Electronic Evidence Be Admitted in a Court of Law?", 8 *Commonwealth Law Review Journal* 599 (2022).
[47] *Supra* note 16.

India,[48] has made it clear that the crime of money laundering is not, and cannot be, a freestanding crime. There has to be a predicate crime as described in the schedule of the relevant piece of legislation. The Constitution does impose that kind of a requirement. It is the discipline that keeps the anti-money laundering legislation from becoming a law of general suspicion.

The institutional conclusion holds equal importance. While overlaps between the ED and CBI are real, they must remain principled. The CBI may be entering an ecosystem of digital arrests, and this may be warranted where issues of corruption, intricate economic crime, inter-state and international funding and involvement of terrorism crosses the border. However, the case of *State of West Bengal v. Committee for Protection of Democratic Rights*, *West Bengal*[49] cautions that the constitutional authority to centralise investigations is singular. It is not a routine matter. Coordination is the rule; displacement is the exception.[50]

Digital arrest cases uniquely suggest that legal scholarship should incorporate victims. While the arrest doctrine, the doctrine of electronic evidence, and the doctrine of attachments deserve attention, those areas of law are value-preserving only because the legal system has been and will continue to be measured by its ability to preserve a legal value before the opportunity is lost. Future advancement in this area will necessitate synthesis in three areas of law: arrest warrant doctrines, proceeds-of-crime law, and law on civil and criminal asset forfeiture. Absent the three, India will continue to prosecute digital arrest as a humour while failing to prosecute it as a financial crime.

1.7 SUGGESTIONS

Based on the analysis of the article regarding cyber-enabled coercion, laundering trails, and overlapping investigative mandates, the following suggestions are offered.[51]

1. Predicate-offence checklists as part of FIR registration: All digital-arrest complaints should be converted into a standardized intake form describing the impersonated authority, the particular threat employed, the channel of transfer, and the initial

[48] *Supra* note 18.
[49] *Supra* note 30.
[50] Rashi Shah, "Mode of Taking and Recording Evidences in India", 7 *Journal of Legal Studies & Research* 122 (2021).
[51] Customer Liability in Unauthorised Electronic Banking Transactions, *available at:* https://www.rbi.org.in/limitedliability/ (last visited on March 23, 2026).

beneficiary account. This would assist investigators in understanding the offence more substantively from the beginning and limiting later laundering allegations from becoming factually vague.

2. Establish a protocol to preserve funds on the same day. Complaints directed to 1930, NCRP, or CFCFRMS must automatically escalate to the banks, payment intermediaries, and police nodal officers. Scam models have speed as a defining factor, and value recovery is more likely if value is frozen in the initial hours as opposed to recovery being the focus later on through prosecution.

3. Standard kit for preservation of electronic evidence's for victims: Simplified checklists of evidence for claimants explaining how to save screenshots, call logs, transaction notifications, beneficiary information, and device details would improve evidence continuity, and minimize the number of disputes related to evidence authenticity, incompleteness, and evidence reconstruction.

4. Mule-account analysis is an early stage task. Focus on the first recipient account, linked UPI handles, most recent inward credits, device ID, and cash out pattern. These are all data points that should be analysed early and should not be postponed until after the primary scam story is done. Early analysis of these points will allow for better differentiation between organised routing and incidental receipt.

5. It is necessary to have a written proceeds-of-crime nexus note before escalating to ED: Before any attachments or complete PMLA actions are taken, there must be a case file short supervisory memorandum addressing the predicate offence, the traced property, and the subsequent process or activity related to that property. This would maintain statutory discipline and lower the likelihood of turning simple fraud complaints into excessively broad laundering stories.

6. Issue a joint deconfliction SOP for State police, ED, and CBI: Each agency should identify its lead on victim engagement, financial tracing, foreign preservation requests, and cross agency record sharing while maintaining the separate legal barriers and implicatures. A clear order will minimize overlap and maintain the legal separation between faux and laundering investigations.

7. Set up an automated trigger for cross-border evidence preservation: Whenever an account chain, platform record, server log, or communication service record trails outside India, investigators should trigger evidence preservation for the cross-border channels without waiting for the domestic file to mature. This is needed as cross-border records are highly volatile and the delay can destroy the evidence trail.

8. Create joint training programmes for police, prosecutors, and judges on the digital coercion, payment, and evidence and electronic patterns, and the statutory nexus as per anti-money laundering law. They will jointly enhance the police charge, the prosecutor's attachments, and the judge's courtroom consistency.

9. Integrating victim-recovery transparent tracking into case management: Complainants should have visibility into the status of funds at each stage. Each status (frozen, partially restored, withdrawn with reasons) should be documented. This will enhance victimcentrality and improve the measuring of how the system performs on restoring value, not just on arrests.

10. There needs to be a separate NCRB reporting category for digital arrests: No new substantive offence is required. Just the addition of a category would enhance trend analysis, hotspot mapping, and policy formulation. Greater classification would enable the State to assess the impact of awareness campaigns and coordinated efforts on the specific digital scam patterns.