DIGITAL ARREST IN INDIA: LEGAL FRAMEWORK, JUDICIAL RESPONSE, AND PROPOSALS FOR REGULATORY REFORM

Manan Jhamb, UILS, Chandigarh University, Mohali

Sanya Mutneja, UILS, Chandigarh University, Mohali

ABSTRACT

Digital Arrest An emerging type of cyber-enabled coercive criminality where wouldn't players pose as law enforcement agents, judges, or regulators via video conferencing software (WhatsApp, Skype, or Zoom) to simulate a virtual arrest, take money off victims by threat of so-called criminal charges, and then laundering the money through layered financial services. Though the reported cases have exponentially increased, reaching 39,925 cases in 2022 and 1,23,672 cases in 2024, and the financial losses have been on the increase to reach ₹91.14 crore to 1,935.51 crore in the past two years, Indian law does not include a statutory definition of what is considered as a digital arrest, no specific criminal offence provision, and no centralized institutionalized mechanism used to investigate and prosecute such offence.

The paper is a systematic study of the doctrines applicable to digital arrest in current laws on the subject of digital arrest of Section 204, 205, 308, 318, 319, 336-340 and 111 of the Bharatiya Nyaya Sanhita, 2023; These provisions of the Information Technology Act, 2000, Section 66C, 66D and 69; and the evidentiary provisions of Bharatiya Sakshya Adhiniyam, 2023. It follows the developing judicial pronouncements, such as the Suo Motu action of the Supreme Court, addressed in In Re: Victims of Digital Arrest Related to Forged Documents (2025), and the judgment of the Delhi High Court, which was issued in Ashok Kumar v. State (NCT of Delhi) (2026), that have started to formulate a conceptualization of digital arrest as a type of organized, cyber-enabled fraud as opposed to outright cheating.

Based on comparative examples, the paper reveals three gaps in the Indian regulatory approach: the lack of a visible offence of digital confinement; the lack of effective co-ordination of enforcement by multiple agencies; and the lack of platform-level responsibility carried by duty-of-care. The paper involves concludes with concrete legislative, institutional, and technical reform suggestions, such as BNS amendments, passing of an Online Safety

and Anti-Fraud Act, requirement of caller-ID authentication, and creation of a National Digital Fraud Authority, tuned to the special harms of digital arrest without violating constitutional protections of privacy and due process.

Keywords: Digital Arrest, Cybercrime, Bharatiya Nyaya Sanhita, Information Technology Act, Impersonation Fraud, Virtual Detention, Organized Cybercrime, Regulatory Reform, Online Safety, Deepfakes.

I.DEFINING "DIGITAL ARREST": CONCEPTUAL AND LEGAL DEMARCATION

A. Ordinary Meaning and Conceptual Origin.

An informal term which has been coined in India lacks legal meaning in any statute yet has been used as a colloquialism, Digital Arrest. Digital arrest, in other words, is comprised of three parts:

1. Impersonation: The offender poses as a police officer, a quasi-judicial figure or a regulatory officer.

2. Virtual Detention: The person who is under threat of being arrested in reality is instructed to stay on a video call hour or days at a time, ironically limiting their actions and interactions with the external world.

3. Blackmail: Money has to pass hands as a way of settling fabricated legal troubles.

In contrast to other cyber frauds like phishing, SIM swap, or telephone impersonation, digital arrest involves ongoing communication using video calls and the active imitation of sovereign law power.

B. Victim Profiles and Targeting Rationales.

According to empirical research by the National Cybercrime Reporting Portal (NCRP), offenders choose the victims using: (a) lack of awareness about the limitations in which law enforcement acts under video conferencing procedures; (b) the recent use of cross-border money transfer or other internet activities that can be subjected to fabricated suspicion; or (c) old age, social isolation, or previous financial difficulties. Official virtual backdrops, fake identity cards appearing on the screen and use of legalese are all factors that induce fear in the victims.

C. Difference with Cognate Offences.

There is not as yet any clause of the Indian law which would correct the equivalence of long-term video-mediated coercion with any kind of known "arrest" or "wrongful confinement." One of the main regulatory issues tackled in this paper is this definitional vacuum. Section 319 (hurt), 339-340 (wrongful restraint and wrongful confinement), 383 (extortion) and 420 (cheating) of the Indian Penal Code, 1860, now rewritten under the Bharatiya Nyaya Sanhita (BNS), 2023, can be applied to attackers, but none of them anticipated the digital medium. Lacking a definition of the concept of digital confinement, the fact that the psychological and functional similarity of captivity on a physical level and captivity in the realm of virtual space is unacknowledged legally.

II. MODUS OPERANDI: TECHNICAL AND PSYCHOLOGICAL ARCHITECTURE

A. The Typical Attack Chain

The attack chain that was built based on FIR analyses and press reports comprises a number of stages that are always the same:

- Stage 1 – First Contact: The victim is called via a robocall or WhatsApp notification claiming that the parcels directed to him or her abroad were intercepted because it allegedly contained narcotics, fake money, or sensitive papers.

- Stage 2 - Authority Ramp-Up: The call is passed on to an alleged high-ranking official, a CBI Director, ED Joint Director, or Registrar of the Supreme Court, who talks in an authoritative manner and uses legal terminologies.

- Stage 3 - This stage is referred to as Video Captivity: at this step, the victim is instructed to connect a Skype, WhatsApp, or Zoom meeting, during which the fraudster shows up with a digital backdrop of governmental symbols and proclaims the victim to be under digital arrest.

- Stage 4 Document Terror: Faked warrants of arrest, Supreme Court orders and so-called case files associated with Aadhaar appear onscreen, to simulate appearance.

- Stage 5: Financial Exploitation at this stage, the victim is lured into sending money to

an "escrow account" that is supposedly operated at the Supreme Court or the Reserve Bank of India - where email accounts are actually run by money mules.

- Stage 6 - Layering and Laundering: money moves rapidly in through layered bank accounts, cryptocurrency exchanges or the hawala pathway.

B. Technology Enablers

VoIP Spoofing: Callers Spoof call id To show official government helpline numbers (i.e., 100, 1930) using foreign VoIP networks, and making it harder to track the call.

- Deepfakes with Artificial Intelligence: The faces and voices of the IPS or IAS officials are synthetically recreated so as to defeat the verification of suspicious victims.

- Encrypted Applications: Not only can legal interception be limited because of End-to-end encrypted messaging services like WhatsApp and Signal, but it is also forbidden under Section 69 of the IT Act.

- Cryptocurrency Off-Ramp: Due topseudonymity of blockchain, extorted money is often transferred to USDT or BTC via peer-to-peer trading systems, then repatriated to the US.

Offshore Syndicate Harbours: According to intelligence reports, some of the large syndicates are based in Myanmar (Myawaddy), Cambodia, as well as in Dubai, territories mostly outside the reach of Indian investigators.

C. Psychological Mechanisms

Digital arrest is a singularly impactful weaponization of two potent psychological mechanisms: authority bias, or the innate human propensity to adhere to perceived authorities, especially those related to law enforcement, and forced social isolation. The perpetrators remain undetected because they cut off the victim contact with the family and advisors to the victim during the arson session that controls the fraud by societal verification checks. The long period in the course of the call- as long as 72 hours- causes sleep deprivation and decision fatigue, which further negatively affects the victim and limits his critical thinking abilities.

III. EMPIRICAL TRENDS AND STATISTICS

Official data present a stark picture of the digital arrest surge in India. The Ministry of Home Affairs (MHA) reports that incidents "almost tripled" between 2022 and 2024.[1] In the NCRP portal, 39 925 arrest-related cases were reported in 2022 (with 91.14 crore defrauded) and in 2024 (₹1,935.51 crore lost), reported 123672 cases (a twenty-one-fold increase in the losses) is twenty-one times more than the increase in incidents, indicating that the average loss-per-case increased significantly, as well.

These worrisome numbers notwithstanding, there is limited quality aggregate statistics on the topic. National Crime Records Bureau (NCRB) does not presently classify digital arrest as such; they are reported under the larger provisions of fraud or BNS. Some reports of the incidents are compiled by CERT-In and not publicly released. Although there are several agencies such as MHA, RBI, I4C monitoring these crimes internally, there is not much available in terms of official breakdowns. Overall, digital arrest has emerged as a growing type of cybercrime, showing authorities reporting in the hundreds of thousands each year and loss in the thousands of crores each year, highlighting the significance of the current research.

IV. LACK OF LEGAL STATUS

A doctrinal problem needs to be defined before examining specific provisions: there is no provision known as "Digital Arrest" under the Bharatiya Nyaya Sanhita, 2023; the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Information Technology Act, 2000. The Ministry of Home Affairs, cybercrime and courts have spurred on occasion to clarify that there is no legal framework that allows arrest using WhatsApp, Skype, Zoom, Telegram, Signal or any other video conferencing application. Any allegation that someone has been digitally arrested is thus fraudulent in nature. The significance of this doctrinal reality is that, the prosecution of digital arrest is based upon a group of offences instead of a specific statutory statute.

V. LEGAL FRAMEWORK

A. Section 204 BNS: Personating a Public Servant

Section 204 BNS criminalizes the act of falsely pretending to hold a public office or falsely

[1]Ministry of Home Affairs, Annual Report on Cybercrime (2024); National Cybercrime Reporting Portal, Statistical Data (2024).

representing oneself as a public servant. The provision seeks to preserve public confidence in governmental authority and prevent abuse of official status for unlawful purposes. In reported digital arrest cases, offenders commonly impersonate police officers, CBI officers, Enforcement Directorate officers, NCB officials, Customs officers, RBI representatives, and judicial officers.[2]

It is not just an act of deception and it constitutes an assault on the legitimacy of the administration of the people itself. Classical impersonation instances tend to be the acquisition of a benefit of false representation. Digital arrest, though, implies simulation of the sovereign authority: the criminal steals the coercion power of the State and uses it against the victim. This makes Section 204, no longer a peripheral offence, but one of the major provisions that are applied to digital arrest. The main limitation, though, is that Section 204 is only dealing with impersonation but not with the resultant psychological imprisonment, monitoring and blackmail.

B. Section 205 BNS: Wearing Garb or Carrying Token Used by Public Servants

Section 205 penalises any person who fraudulently wears official uniforms, insignia, badges, or carries symbols associated with public office with intent to deceive. Many digital arrest syndicates conduct video calls while wearing police uniforms and displaying official logos against fabricated police station backgrounds.[3] Section 205 is especially important since digital arrest will be a visual crime: a victim will not be convinced solely by the words, but by the specific visual imagery of the power of the government. Nonetheless, the clause was initially written to cover instances of physical impersonation and lacks any specific consideration of deepfakes, artificial intelligence generated uniforms, AI generated video simulators or virtual police stations, which is a clear interpretative challenge.

C. Section 318 BNS: Cheating

Section 318 BNS criminalizes cheating and dishonest inducement resulting in the delivery of property. Every digital arrest ultimately seeks a financial outcome: victims are instructed to transfer money for "verification," deposit funds for "clearance," move savings to "safe accounts," or transfer funds to avoid arrest. Reported losses frequently range from several lakh

[2]ASV Legal LLP, "Digital Arrest: Legal Framework and Emerging Jurisprudence" (2024).
[3]Live Law, "AI and Deepfakes in Digital Arrest Scams: Evidentiary Challenges" (2024).

rupees to multiple crores; recent cases have involved losses exceeding ₹30 crore by individual victims.[4]

There is a digital rear bone called cheating that is the economic backbone of arrest. But a digital arrest is not like a common case of cheating as victims are not sending money as a result of an offer of profit but rather as a result of fear. This distinction is doctrinally significant as it brings the crime nearer to extortion as opposed to the traditional fraud. The coercive environment in which the transfer takes place is not sufficiently guarded under section 318 since the section under consideration is concerned with deception, not domination.

D. Section 319 BNS: Cheating by Personation

Section 319 is frequently invoked alongside Section 204. Where Section 204 protects public authority, Section 319 protects individuals from deception arising from false identities. Digital arrest typically satisfies every element of this offence because the fraudster: (i) assumes a false identity; (ii) induces reliance upon that identity; and (iii) secures wrongful gain through that deception.[5] There is still a gap in the doctrine though: the provision regards a digital arrest as a sort of cheating in personation and fails to acknowledge the offence as a type of simulation of coercive governance, which poses a significant conceptual weakness of the current legal framework.

E. Section 308 BNS: Extortion

Most academic and policy discussions incorrectly classify digital arrest exclusively as cyber fraud. In reality, many digital arrest schemes satisfy the legal ingredients of extortion: victims are threatened with arrest, imprisonment, asset seizure, reputational destruction, and criminal prosecution—and money is transferred not because the victim trusts the fraudster but because the victim fears the threatened consequence.[6] Criminologically, the term extortion would offer a more suitable definition of digital arrest as compared to cheating- a situation that is mostly deficient in the literature.

[4]The Indian Express, "Digital Arrest Victim Loses Over ₹30 Crore" (2024).
[5]SCC Online, "Digital Arrest: Cheating by Personation and Extortion under BNS" (2024).
[6]Live Law, "Digital Arrest and Extortion: A Doctrinal Distinction" (2024).

F. Section 351 BNS: Criminal Intimidation

Digital arrest relies upon sustained psychological pressure. Victims are routinely informed that police teams are en route, warrants have been issued, bank accounts will be frozen, and family members will be implicated. These threats generate the fear necessary for compliance.[7] Cheating and extortion are the leading to actions in the digital arrest process where intimidation (intended to enable these illegal acts) happens beforehand thus fulfilling the conceptual base of criminal intimidation under the law of 351.

G. Sections 336–340 BNS: Forgery and Use of Forged Electronic Records

Investigations consistently reveal use of forged arrest warrants, fabricated Supreme Court orders, forged ED notices, fake RBI communications, and counterfeit police documentation.[8] Provision of forgery is thus inevitable. However, the increasing use of AI-generated documents and deepfake technology raises novel evidentiary questions regarding authenticity and attribution.[9]

H. Section 111 BNS: Organized Crime

A particularly neglected provision in digital arrest scholarship is Section 111 BNS, dealing with organized crime. Investigative reports increasingly indicate that digital arrest operations are not isolated acts by individual offenders but coordinated networks involving call-centre operators, data brokers, mule account holders, cryptocurrency channels, and foreign-based criminal syndicates.[10] This could be one of the most significant legal means of prosecuting digital arrest syndicates on a large scale in the future.

I. Concluding Finding

The most significant finding from the Bharatiya Nyaya Sanhita is that digital arrest is already partially criminalized, but only through a fragmented collection of offences. Sections 204, 205, 308, 318, 319, 351, 336–340, and 111 collectively address impersonation, extortion, cheating, intimidation, forgery, and organized criminal activity. However, no provision recognizes the

[7]SCC Online, "Criminal Intimidation and Digital Arrest" (2024).
[8]Lawful Legal, "Forgery Provisions in Digital Arrest Cases" (2024).
[9]Live Law, "AI-Generated Documents and Attribution Challenges in Digital Arrest" (2024).
[10]SCC Online, "Section 111 BNS and Organized Cybercrime Networks" (2024).

distinctive harm caused by the fraudulent simulation of state authority. Consequently, Indian criminal law punishes the individual components of digital arrest while failing to conceptualize the offence as a unified form of cyber-enabled coercive criminality.[11]

VI. THE INFORMATION TECHNOLOGY ACT, 2000: APPLICABLE PROVISIONS AND LACUNAE

A. Section 66C-- Identity Theft.

Section 66C criminalizes the fraudulent or dishonest use of the electronic signatures, passwords, or any other special identification characteristics. Although the aspect of impersonating the identity of an official during a video call might be constrained to the practice of the section due to the particularity of identifiers, the framing of the section around the element of unique identification requires is smaller than persona impersonation which the concept of digital arrest demands. Three years of imprisonment and a fine amounting to 1 lakh is generally seen as very mild as per the magnitude of damage.

B. 66D cheating using computer resource and personation.

The most relevant section of the IT Act is section 66D, which explicitly punishes cheating by personation through a communication device or a computer resource, thus arguably the most relevant section. That portion however needs evidence of cheating, a mens rea, which brings about greater difficulties when extortion is occurred by way of intimidation at lawful procedure instead of a traditional false promise of an upcoming advantage.

C. Section 69 -Interception and Monitoring.

Section 69 allows the government to intercept, monitor, or decrypt information under the interests of national security or even the peace of the people. But encrypted platform operators have opposed going all the way, on the basis of end-to-end encryption architecture, and no particular amendment has imposed the revelation of metadata in online arrest cases.

D. Lack of a “Digital Confinement” Provisions.

There is no analogous provision, i.e. the wrongful confinement, (Sections 339–340 IPC/BNS)

[11]Live Law, "Digital Arrest as Unified Cyber-Enabled Coercive Criminality" (2024).

modified so as to be applied to the digital medium. The concept that it is coercion (sustained using video-call) could qualify as a type of unlawful restraint fails to appear anywhere in the statute.

VII. RECORD-SAFEEGUARDING, EVIDENTIAL FRAMEWORK.

A. Procedural Protections of Lawful Arrest.

The Bharatiya Nagarik Suraksha Sanhita includes numerous safeguards to avert unreasonable arrest: (A) notice of arrest grounds; (B) right to notify relatives or known persons; (C) appearance before the nearest Magistrate within twenty-four hours; and (D) the preparation of arrest memoranda and keeping of required procedural records.

Online arrest fraud flouts each of these protections. Victims are often told not to call family members, not to seek legal counsel, not to vacate the premises, not to talk with banks and not to talk to anybody about the situation. Through this, the fraudsters do exactly the reverse of what is required by law and that is to prove that working in digital arrest, the coercive force is not based on the law but on the wrong perception of the legal authority as was done by the victim.

B. Admissibility of the Electronic Evidence.

Digital arrest investigations near wholly rely on electronic evidence, such as WhatsApp messages, video records, VoIP call records, screenshots, bank account transaction records, IP logs, and e-mail communications. According to the Bharatiya Sakshya Adhiniyam, 2023, electronic and digital records shall be considered admissible evidence under the provisions of law.

Digital arrest investigation is characterized by serious attribution challenges even though it is statutorily recognized. The investigators need to find out who was in charge of the device, who started the communication, who managed the account, who minced the money, and whether more than one person had access to the digital infrastructure. This becomes especially challenging in situations whereby criminals use VPN solutions, spoofed phone numbers, overseas servers, (encrypted) communications solutions, and cryptocurrency networks.

C. Deepfakes and Synthetic Evidence.

New digital arrest procedures are using artificial voices on AI, fake identities, and altered video clips and counterfeit government records. The Bharatiya Sakshya Adhiniyam does not include any specific structure addressing the problem of deepfake evidence, artificial impersonation projected by the AI, or synthesized messages by the government, one of the most critically evidentiary issues that Indian criminal justice agencies will struggle with in the future.

VIII. JUDICIAL INTERPRETATION AND EMERGING JURISPRUDENCE

A. In Re: Victims of Digital Arrest Related to Forged Documents (Suo Motu Proceedings, Supreme Court of India, 2025)

The proceedings originated after a senior citizen from Ambala, Haryana, alleged that fraudsters impersonating public officials subjected her to a "digital arrest" and induced the transfer of more than ₹1 crore using forged Supreme Court documents and fabricated legal proceedings.[12] The Supreme Court described the matter as one of grave national concern, observing that the forgery of judicial documents and misuse of the Court's authority strike at the foundation of public trust in the judicial system.[13]

This is arguably the first time the digital arrest phenomenon has been a legal issue with an explicit mention by the Supreme Court. What is important is not just the financial fraud at play in it, but the finding of the Court that digital arrest itself is a scam of sovereign power a subversion to the citizens trust in the police and the judiciary itself, the sanctity of the judicial materials and the very bona fides of the administration of justice.

B. Ashok Kumar v. State (NCT of Delhi), Delhi High Court (2026)

The case arose from a large-scale digital arrest fraud in which a retired banker allegedly lost approximately ₹22.92 crore after being subjected to a prolonged digital arrest operation involving fabricated criminal proceedings. The Delhi High Court refused bail and observed that digital arrest fraud is not an ordinary cheating offence; Justice Manoj Jain noted that every participant in the scheme appeared to be an "important cog of the conspirational wheel" and

[12]The Times of India, "Supreme Court Initiates Suo Motu Proceedings on Digital Arrest Scams" (2025).
[13]Verdictum, "In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Proceedings, Supreme Court of India (2025).

that such offences have serious societal consequences.[14]

What was significant about this decision is that it treated digital arrest operations as organised, no more part of the conventional views of cyber fraud as a simple transaction, and recognised the existence of coordinated criminal networks which engaged several actors. The decision reinforces the contention that it is appropriate to invoke the Section 111 BNS (Organised Crime), criminal conspiracy and money-laundering investigations..

C. Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273

This Supreme Court decision established that arrest must remain an exception rather than the norm, emphasising that police officers must justify the necessity of arrest.[15] In the surrounding of a digital arrest, the case also depicts how huge disparities exist between lawful arrest authority and the malicious authority asserted by the offenders of digital arrest.

D. Rajasthan high court Suo Motu Decree.

On the state level, the High Court of Judicature of Rajasthan (at Jaipur Bench), under Justice Anoop Kumar Dhand, undertook Suo motu proceedings, reiterating the fact that in regards to the Indian law, there is no concept of digital arrest which has a basis in law and that no police agency is authorized to proceed with an arrest through video conferencing. The Court served notice to the Union of India, the National Cyber Forensic Laboratory, RBI and the National Helpdesk, and asked the Chief Secretary of Rajasthan, and the Secretary of MHA, to provide detailed reports on what has been done regarding the issue of digital arrest scams. The Court also requested the RBI to put in place measures that threatened the immediate suspension of the funds transfer as soon as a victim lodged a complaint.

IX. CONSTITUTIONAL BACKDROP

Article 21 of the Constitution guarantees life, liberty, and personal security. Digital arrest infringes these values by undermining the sense of security and due process: victims experience a form of virtual "detention." The Supreme Court in Puttaswamy v. Union of India affirmed informational privacy as intrinsic to Article 21.[16] The loopholes in data protection are

[14]Ashok Kumar v. State (NCT of Delhi), Delhi High Court (2026), as reported in The Times of India.
[15]Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273.
[16]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

characteristics of digital arrest scams, which use personal information, such as Aadhaar numbers, financial information. The Digital Personal Data Protection Act, 2023 codifies the principles of lawful processing, although is in its staged implementation (core data-processing provisions to be enforced only in 2027), and victims are not sufficiently safeguarded in the meantime.

Article 14 (arbitrariness) and Article 22 (protection against illegal arrest) are also involved in digital arrest. The very idea of the scam is the unlawful, capricious warrantless arrest without any statutory process. Even though it is perpetrated by the private actors, they falsely represent state force, thus degrading the belief of people in the legality of authority and the legitimacy of institutions.

X. THE PRE-EXISTING LEGAL AND REGULATORY FRAMEWORK: A REVIEW

A. Bharatiya Nyaya Sanhita, 2023.

Even though the BNS, which will take effect on 1 July 2024, limits the digital methods to be used in instantiating cheating, as was done with the IPC, Section 318 of the former has now included digital means in extortion, with Section 308 of the former incorporating extortion. Nevertheless, a gap that is equally important has been identified; the inability to consider virtual detention as an independent crime. The drafting committee failed to discuss the issue of digital arrest expressly.

B. The DoT Framework and TRAI.

TRAI has already developed regulations toward unsolicited commercial communication by creating the Telecom Commercial Communications Customer Preference Regulations, 2018. The DoT has established the Sanchar Saathi program of reporting and blocking fraudulent calls. However, spoofing of caller ID is still possible because the principles of CLI verification are not mandatory with all service providers; voice calls over OTT (WhatsApp, Skype) are not subject to regulation by TRAI; and and cross-border voice calls through transit service providers are not subject to local regulation.

C. Prevention Money Laundering Act, 2002.

Digital arrest is a financial crime that is based on a financial foundation. Amended in 2023, the

PMLA allows the Enforcement Directorate, among other proceeds, to attach and confiscate scheduled offences, such as cheating and criminal breach of trust. Nevertheless, the overlay money-mule economy, quick conversion to and among cryptocurrencies, cross-border transfers of cash significantly deteriorate tracking and recovery. The Financial Intelligence Unit (FIU-IND) has raised several of suspicious transaction reports concerning digital arrest proceeds, yet there are slow attachments proceedings.

D. Jurisdictional Fragmentation

Online arrest prosecutions have to push their way through a maze of jurisdictional competency. The state police cyber cells, the CBI, the ED, the DoT, the RBI (via its ombudsman in payment fraud), and SEBI (where the fraud is encompassed by investment fraud) have a partial jurisdiction, and have no overall nodal agency with end-to-end investigative and prosecutorial accountability. This discontinuity leads to duplication of proceedings, duplication of evidence and accused individuals taking advantage to play with jurisdictions.

XI. CYBERSECURITY AND INSTITUTIONAL RESPONSE- CYBERSPACE INFRASTRUCTURE.

The ministry of home affairs setup the Indian Cybercrime Coordination Centre (I4C) to coordinate the response to cyber threats and started as an Attached Office of the MHA on 1 July 2024. The I4C uses a number of tools that enhance coordination and response times:

- Samanvaya Platform: It is a data repository and coordination platform to enable law enforcement agencies in various states to share and analyze cybercrime data.
- Pratibimb Module: Logs the physical position of active cybercriminals and charts the online infrastructure employed in scams.

-Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS): It is working with the 1930 helpline enabling an individual to report financial fraud so that the bank could intervene as quickly as possible.

In its own proceedings, WhatsApp, in January 2026, acting upon the prompt of I4C, MeitY and the DoT, banned more than 9,400 accounts that were engaging in digital arrest fraud, in response, deploying new enforcement mechanisms such as logo-detecting systems to safeguard

users and curb the emergence of digital arrest fraud.

XII. COMPARATIVE REGULATORY ANALYSIS

A. United Kingdom

The strategy of the United Kingdom with regard to its fight against technology-assisted fraud provides a number of lessons. Within the Online Safety Act, 2023, the large social media platforms are obliged to do the option of policing the content of the posts allowing impersonation fraud. The Fraud Act, 2006 protects against fraud by false representation which includes all of the technological materials of the simulation of arrest without any particular category. Moreover, the reports of such crimes are received by a central body- Action Fraud/NFIB- and telecommunications companies in the UK must implement STIR/SHAKEN caller-ID authentication measures.

B. Singapore

The Protection from Scams Act, 2024, of Singapore, gives police a right to order financial institutions to cease payments to anyone who has been determined as a victim of a scam even without the victim's consent and terminate the monetization at the decisive point. In the Online Criminal Harms Act, 2023, it is obligatory to block an account of a scammer within twenty-four hours of a police request. ScamShield app is a machine learning-based application that ensures that scam messages are identified at the device level in Singapore.

C. European Union

The Digital Services Act of EU, 2022 obliges the Very Large Online Platforms to have systems to reduce risks of illegal content, such as impersonation and fraud. The AI Act, 2024 specifically addresses the deep-synthesis (deepfake) technologies, obligating the labelling of AI-generated content, which is directly applicable to the deepfake aspect of digital arrest. The NIS2 Directive requires telecom operators to report incidents, which forms a data trail that can support cross-border fraud investigations via the Europol.

D. Important lessons to India.

There are three overarching lessons which can be drawn through the comparative analysis: (i)

proactive platforms liability frameworks are more effective than reactive criminal law alone; (ii) network level caller-ID authentication is an underlying technical requirement that needs to be used in addition to legal reform; and (iii) single nodal coordinating agencies with cross-sectoral authorities are more successful in rapid, coordinated responses than fragmented multi-agency models.

XIII. REFORM PROPOSALS

A. Legislative Reforms

An amendment should be added to the Information Technology Act or a new Digital India Act to specify and punish the phenomenon of digital confinement: the practice of applying any electronic communication medium to make a person think that they are being lawfully restrained and thus to make them give money or property. It should come with at least five years imprisonment with fine that increases to ten years in case, the victim is either a senior citizen or person with disability. The mens rea must be defined to embrace wilful blindness which will embrace the organizers of digital arrest syndicates who shield themselves by not engaging in direct perpetration.

Section 308 BNS (Extortion) is to be revised with more specific wording that does include a reference to the extension of digital communication under duress which would have to be categorized as a means of extortion. The Section 127 BNS (Wrongful Confinement) ought to be modified and reworded to cover virtual confinement by any form of electronic communications where free movement or communications are significantly limited because the victim is afraid being charged.

B. Environmentally Online Safety and Anti-fraud Act.

Based on the model of Online Safety Act of the UK and Online Criminal Harms Act of Singapore, India ought to enact a wholesome action Online Safety and Anti-Fraud Act that: (i) deposes a duty-of-care on the part of the OTTs to spot and shut down accounts being used to perpetrate impersonation fraud; (ii) bestows jurisdiction to the I4C Director to commence an emergency take-down order that will be enforceable against non-compliant platforms at the risk of having to pay a pecuniary penalty; and (iii) creates a statutory framework of law-enforcement access to metadata of accounts under investigation subject to judicial control.

C. Technical Reforms, Telecom Levels.

DoT is to require, within a specified time frame, the implementation of a STIR/SHAKEN, or similar caller-ID authentication protocol, by all licensed telecom service providers. International calls made over Indian gateways should have outgoing network authentication. TRAI must be given the authority to oversee OTT-based communication services to be used as a means of preventing fraud, and must demand that the platforms put in place real-time detection of call fraud by using AI to identify patterns in call rooms.

D. Institutional Reforms

This would form a statutory National Digital Fraud Authority (NDFA) with a mandate that includes: (i) central pleased to all digital fraud cases, overturning the current jurisdictional division between NCRP, TRAI, RBI Ombudsman and the appropriate state police unit; (ii) binding orders on banks, payment aggregators and crypto exchanges to freeze accounts and its nullification in a so-called golden hour; (iii) coordinated cross-border Mutual Legal Assistance Treaty (MLAT) investigation requests, alongside MEA and Interpol; (iv) establishing a centralized Fraud Intelligence database, available to all investigative authorities.

E. Financial System Safeguards.

The Reserve Bank of India would instruct the scheduled commercial banks to provide a compulsory cooling-off period of 30 minutes, to first-time large transactions in the form of transfers made through the use of a device that the customer has not been using before. Machine learning algorithm for real-time tracking of transactions must be implemented to identify transfers being transferred to familiar money mules accounts. RBI needs to extend the positive pay scheme established on cheque transactions exceeding ₹50,000 to online transactions exceeding ₹1 lakh.

F. Public knowledge and Digital literacy.

The criminal act based on the inequality of information and psychological manipulation cannot be resolved by regulatory reform only. India needs an ongoing, government-funded Digital Awareness and Literacy Programmed that: (i) requires the inclusion of those modules of cyber-safety into the school and university education plans, which states that it is impossible to perform an arrest via a video call, and (ii) should hold multilingual awareness campaigns on

the level of DD National, All India Radio, and community radio, targeting the rural population and the elderly citizens in particular, (iii) must ensure that all banks actively include digital arrest warnings on their account statements, UPI application splash screens, and ATM receipts, and (iv) should provide police forces with training on how to detect, record, and act against cases of digital arrest.

XIV. AFGHANISTAN LACKS SECURITY AGENCY FUNCTIONALITIES: CHALLENGES IN IMPLEMENTATION AND COUNTER-ARGUMENTS

A. Privacy Trade-offs and Encryption.

The inherent privacy right as was identified in Justice K.S. Puttaswamy v. Union of India (2017) is implicated by whatever it takes to provide such communication content to law enforcement via the OTT platforms. Taking a judicial checkpoint and proportionality checkpoint and sunset provisions to ensure the access to platform data is court-monitored and has proportionality checks and balances - lest the anti-fraud architecture turn into a surveillance architecture - must be considered Pareto tuned.

B. Cross-Border Jurisdiction

Digital arrest syndicates which are the operationally most advanced are based in those jurisdictions which have either weak or non-existent extradition treaties with India -Myanmar, Cambodia and the UAE. These actors cannot be directly subject to domestic legislative reform. Nonetheless, financial sanctions/blacklisting of cryptocurrency exchanges, which is organized by the Financial Action Task Force (FATF), and diplomatic pressure in the form of Project ENFAST within the frames of the INTERPOL can be used to supplement domestic reform.

C. Regulatory Capacity

To make the proposed changes effective, it will be impossible without proper investment into the capacity building of the postulated NDFA and state police cyber cells. Adequate funding should be channelled towards training programmes and inter-agencies data exchange systems.

XV. CONCLUSION

Digital arrest is a qualitatively new type of coercive criminal activity, which is based on the

architecture of modern communication technology, control advantage of the specifically targeted members and the fragmentation of legal and institutional reaction in India. It is not just mere cheating or the act of impersonation on a smaller scale, but the pretentious imitation of the king of court jurisdiction on a large scale.

The current legal sphere, though not completely silent, is basically inferior. Sections 204, 205, 308, 318,319,336-340 of the Bharat Nyaya Sanhita, and, Parts 66C, 66D, 69 of the Information Technology Act, and the Bharatiya Sakshaya Adhiniyam all offer a partial arsenal, albeit not intended to this threat, nor acknowledging the combined damage of virtual coercive detention. Some new judicial statements are indicative of the potential emergence of a jurisprudential understanding of digital arrest as a special and serious form of organized cyber criminality, in the Supreme Court suo motu proceedings of 2025 and the Delhi High Court of 2026 in the case of Ashok Kumar.

The way ahead involves a convergential response: a specific statutory definition of digital confinement; revision of the extortion and wrongful confinement law; an Online Safety and Anti-Fraud Act that imposes liability on platforms; widespread use of STIR/SHAKEN authentication; a National Digital Fraud Authority that has cross-sectoral jurisdiction; specific protection of the financial system; and long-term public awareness campaign. All of this would place the Indian response to digital arrest at the same level with global best practices but still maintain the constitutional rights to privacy and due process which establish the legal order respectful to rights.

APPENDIX: STEP BY STEP FOR VICTIMS.

Should someone call you and inform you that you are being digitally arrested:

1. Do Not Comply: Immediately disconnect the call. No government agent will intimidate you by arresting you live on the phone or video call.

2. Check: In case you are suspecting that an official investigation is underway; you may address your case to the contact department on the official verified website or visit the police station of your area.

3. Report: Immediately call the National Cyber Crime Helpline at 1930; report the incident at the web site www.cybercrime.gov.in; and inform your bank to freeze your accounts or otherwise block additional transactions in case funds were transferred.