Page 314 - 326 **DOI:** *https://doi.org/10.63108/IJLMH.12884*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

Evaluating the Adequacy of Section 66D of the Information Technology Act, 2000 in Prosecuting Digital Arrest and Advanced Personation Scams

YALALA RAKESH[*] AND C. M. SRINIVAS RAO[**]

ABSTRACT

This paper critically evaluates the adequacy of Section 66D of the Information Technology Act, 2000 in addressing the emerging phenomenon of digital arrest scams and advanced forms of personation facilitated by contemporary digital technologies. Digital arrest constitutes a sophisticated social-engineering fraud in which offenders impersonate police officers, judicial authorities, or regulatory officials through video-conferencing platforms, fabricated electronic documents, and increasingly artificial-intelligence-generated voice and video content, thereby inducing victims to transfer substantial sums under threat of imminent arrest or prosecution. The study adopts a doctrinal research methodology supplemented by an interdisciplinary examination of cyber-forensics, electronic evidence rules under the Bharatiya Sakshya Adhiniyam, 2023, and the organised-crime provisions of the Bharatiya Nyaya Sanhita, 2023. The analysis demonstrates that while Section 66D is technologically neutral and doctrinally capable of covering the core elements of cheating by personation through a communication device, its maximum punishment of three years' imprisonment and fine of one lakh rupees is disproportionately low when measured against the gravity of organised digital-arrest operations that routinely involve mule-account networks, cross-border elements, and significant psychological and financial harm to victims, particularly senior citizens. The paper further identifies structural gaps relating to the absence of aggravated-personation categories, limited recovery mechanisms for defrauded funds, and persistent challenges of digital attribution and international cooperation. It concludes that Section 66D remains a necessary but insufficient instrument and recommends legislative recalibration through graded punishment structures, explicit recognition of aggravating factors including impersonation of public authorities and use of synthetic media, and the development of coordinated financial-freezing and victim-restoration protocols.

[*] Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: https://orcid.org/0009-0008-8076-9173

[**] Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: https://orcid.org/0009-0003-0342-4941

 [ISSN 2581-5369]

Keywords: *Section 66D IT Act, Digital Arrest, Cheating by Personation, Cybercrime, Bharatiya Nyaya Sanhita, Electronic Evidence, Organised Cyber Fraud, Artificial Intelligence Personation*

I. INTRODUCTION

The rapid digitisation of communication, identity verification, and financial transactions has fundamentally altered the architecture of criminal deception. Traditional forms of cheating depended upon physical proximity, forged paper documents, or face-to-face impersonation. Contemporary cyber-enabled fraud, by contrast, permits offenders to construct highly credible official identities through mobile applications, video-conferencing platforms, social-media accounts, synthetic media, and instantaneous electronic payment systems. Among the most socially disruptive manifestations of this transformation is the phenomenon popularly described as "digital arrest."

In a typical digital-arrest operation, fraudsters contact the victim through a telephone call or messaging application and represent themselves as officers of the police, the Central Bureau of Investigation, the Enforcement Directorate, or even judicial authorities. The victim is informed that a criminal case has been registered against him or her, often linked to a parcel containing illegal substances, a compromised bank account, or an identity document associated with money-laundering or terrorism-related activity. Through a combination of urgency, fear of immediate arrest, and the display of fabricated warrants, identity cards, and institutional backgrounds during video calls, the offender induces the victim to remain continuously online and to transfer large sums of money into designated accounts for purported "verification," "security deposit," or "release from digital custody." The Ministry of Home Affairs has issued repeated public advisories warning citizens against such impersonation-based scams.[1]

The Rajasthan High Court has characterised digital arrest as an emerging cybercrime technique rather than any legally recognised form of custody.[2] The Supreme Court of India has taken *suo motu* cognisance of the issue after receiving complaints from senior-citizen victims who were induced to part with sums exceeding one crore rupees through forged judicial documents and

[1] MINISTRY OF HOME AFFAIRS, Government of India, *Alert against Incidents of "Blackmail" and "Digital Arrest" by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and Other Law Enforcement Agencies*, Press Information Bureau (14 May 2024), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2020570.

[2] *Suo Motu: In the Matter of Tackling the Issue of "Digital Arrest Scams," Cyber Crimes and Saving the Innocent People from Losing Their Money and Lives v. Union of India*, Rajasthan High Court, Jaipur Bench, Order dated 22 January 2025, https://indiankanoon.org/doc/152104806/.

 [ISSN 2581-5369]

continuous digital coercion.[3] These judicial interventions underscore both the scale of the problem and the institutional recognition that existing legal tools require careful scrutiny.

Section 66D of the Information Technology Act, 2000 was enacted to address the specific offence of cheating by personation committed through a computer resource or communication device.[4] At the time of its introduction, the provision represented a progressive legislative response to the technological dimension of personation. More than two decades later, however, the digital environment has evolved dramatically. Artificial-intelligence-generated voice cloning, deepfake video, sophisticated mule-account networks, and cross-border criminal organisations have raised the question whether a provision carrying a maximum sentence of three years' imprisonment remains adequate either as a deterrent or as a vehicle for proportionate punishment.

Existing academic literature has examined cybercrime, identity theft, electronic evidence, and intermediary liability in relative isolation. The specific convergence of social engineering, institutional impersonation, synthetic media, and organised financial architecture that characterises digital-arrest scams has received comparatively limited doctrinal attention. The simultaneous enactment of the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 further necessitates a fresh assessment of the continued utility and limitations of Section 66D within the broader criminal-law framework. This paper seeks to fill that gap through a systematic doctrinal evaluation.

The manuscript proceeds as follows. Section 2 examines the nature of digital-arrest scams, the role of artificial intelligence in advanced personation, and the financial architecture that sustains these operations. Section 3 analyses the relevant statutory framework under the Information Technology Act, the Bharatiya Nyaya Sanhita, and the Bharatiya Sakshya Adhiniyam. Section 4 undertakes a detailed doctrinal evaluation of Section 66D, focusing on the ingredients of the offence, the electronic-nexus requirement, and questions of punishment and proportionality. Section 5 addresses evidentiary challenges arising from forged digital documents, synthetic media, and cross-border investigation. Section 6 reviews the judicial and institutional response, particularly the Supreme Court's continuing *suo motu* proceedings. Section 7 offers a critical assessment of the strengths and limitations of Section 66D, and Section 8 formulates concrete legislative and institutional recommendations. Section 9 concludes.

---

[3] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025, Supreme Court of India, Order dated 17 October 2025.

[4] Information Technology Act, 2000 (Act No. 21 of 2000), s. 66D.

 [ISSN 2581-5369]

II. Digital Arrest and the Architecture of Advanced Personation

A. Nature and *Modus Operandi* of Digital Arrest Scams

Digital-arrest scams are distinguished from ordinary online fraud by their deliberate exploitation of the victim's respect for state authority and fear of criminal process. The offender does not merely solicit money under a false commercial pretext; rather, the offender constructs a complete institutional narrative in which the victim is positioned as a suspect or accused person whose liberty is under immediate threat. This narrative is sustained through continuous video presence, prohibition on contacting family members or legal counsel, and the repeated display of fabricated official documents.[5]

The psychological mechanism employed is classic social engineering amplified by technology. By creating an artificial emergency and isolating the victim from external verification, the offender converts ordinary caution into compliance. The technological interface itself becomes an instrument of control: the victim is instructed to keep the video call active for hours or days, thereby preventing independent inquiry and reinforcing the illusion of official custody.[6]

B. Impersonation of Public Authorities

The effectiveness of digital arrest rests substantially on the impersonation of police officers, investigating agencies, judges, and financial regulators. The use of uniforms, institutional logos, official-sounding designations, and fabricated warrants creates an expectation of legal obedience that ordinary commercial fraud cannot generate. This form of personation is therefore more culpable than generic online deception because it undermines public confidence in the institutions of the state itself.[7]

---

[5] *Suo Motu: In the Matter of Tackling the Issue of "Digital Arrest Scams"*, *supra* note 2 (victims are instructed to keep camera and microphone on throughout the interaction, which makes it difficult for them to seek assistance or discuss the situation with anyone, and fraudsters employ phony uniforms, counterfeit identification cards, forged documents and simulated government office environments); Ministry of Home Affairs, *supra* note 1 (victims are made to undergo "Digital Arrest" and to remain visually available over Skype or another video-conferencing platform until the demands are met, the fraudsters using studios modelled on police stations and government offices).

[6] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024* (October 2024), ch. 5 (Social Engineering), https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[7] The Sanhita treats personation of public office as a distinct wrong in itself: Bharatiya Nyaya Sanhita, 2023, s. 204 (pretending to hold any particular office as a public servant, or falsely personating a person holding such office, and in that assumed character doing or attempting any act under colour of the office, punishable with imprisonment of not less than six months and up to three years, and fine), which stands apart from the general personation offence in s. 319. On the institutional harm specifically, the Supreme Court in the digital-arrest proceedings observed that the fabrication of judicial orders bearing forged signatures of judges strikes at the very foundation of public trust in the judicial system and in the rule of law: *In re Victims of Digital Arrest Related to Forged Documents*, *supra* note 3.

When such impersonation is combined with continuous digital surveillance of the victim and the threat of immediate physical arrest, the conduct acquires a coercive character that ordinary cheating provisions may not fully capture. The law must therefore distinguish between routine online personation and the aggravated impersonation of constitutional and statutory authorities.

C. Artificial Intelligence and Synthetic Media

Artificial intelligence has introduced a qualitatively new dimension to personation. Voice-cloning systems can now replicate the speech patterns, accent, and vocal characteristics of a genuine official with a high degree of fidelity. Synthetic-video technologies, commonly described as deepfakes, can generate realistic audiovisual representations of authority figures. When these tools are combined with conventional social-engineering scripts, the resulting deception becomes extraordinarily difficult for an ordinary citizen to detect in real time.[8]

Section 66D is technologically neutral and therefore capable, in principle, of covering AI-enabled personation. The provision does not require the personation to be accomplished through any particular medium; it is sufficient that a communication device or computer resource is used. Nevertheless, the increased sophistication and reduced detectability of synthetic media raise important questions of culpability and sentencing. Treating AI-generated personation as indistinguishable from a simple false telephone claim risks under-penalising conduct that demonstrates higher levels of planning, technical skill, and potential for widespread harm.[9]

D. Financial Architecture and Networked Criminality

Successful digital-arrest operations depend upon a supporting financial infrastructure. Funds obtained from victims are typically received into mule accounts, that is, accounts belonging either to knowing participants or to individuals whose credentials have been compromised or purchased. The proceeds are then layered through multiple accounts, often across jurisdictions, rendering rapid recovery extremely difficult.[10]

The operational structure is frequently networked rather than individual. One participant may specialise in obtaining SIM cards and creating online identities; another may prepare forged

---

[8] ORIN S. KERR, COMPUTER CRIME LAW (5th edn, West Academic Publishing 2021).

[9] CHRIS REED, MAKING LAWS FOR CYBERSPACE (Oxford University Press 2012).

[10] RESERVE BANK OF INDIA, *Customer Protection: Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, Circular DBR.No.Leg.BC.78/09.07.005/2017-18 (6 July 2017, as amended), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11040. On mule accounts specifically, see RESERVE BANK OF INDIA, *RBI Invites Comments on the Draft "Reserve Bank of India (Know Your Customer) Amendment Directions, 2026"*, Press Release (11 September 2026), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=63587, issued to give effect to the Supreme Court's direction of 4 August 2026 that the Reserve Bank adopt and circulate a standard operating procedure for temporary debit holds on amounts or accounts linked to money-mule activity and cyber-enabled fraud.

documents and institutional templates; a third may handle real-time communication with the victim; and a fourth may control the movement of funds. This division of labour means that the person who appears on the video call may have only limited knowledge of, or control over, the ultimate beneficiaries. Effective legal response therefore requires tools capable of addressing organised cybercrime rather than isolated acts of deception.[11]

III. Statutory Framework Governing Digital Personation

A. Section 66D of the Information Technology Act, 2000

Section 66D provides that whoever, by means of any communication device or computer resource, cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to one lakh rupees.[12] The provision incorporates three essential elements: (a) cheating, (b) personation, and (c) the use of a communication device or computer resource as the means of committing the offence.

The electronic-nexus requirement is significant. Section 66D does not criminalise every act of personation; the personation must be accomplished through the specified technological medium and must be connected with cheating. This specialised character distinguishes the provision from the general personation offences found in the traditional penal code and later in the Bharatiya Nyaya Sanhita.[13]

B. Relationship with Identity Theft under Section 66C

Section 66C addresses the fraudulent or dishonest use of another person's electronic signature, password, or any other unique identification feature.[14] Although digital-arrest cases may simultaneously engage both provisions, the two offences remain conceptually distinct. Personation concerns the false representation of identity, whereas identity theft concerns the misuse of specified identifying credentials belonging to another. Conflation of the two provisions risks analytical imprecision in charging decisions and judicial reasoning.

C. Complementary Provisions under the Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita introduces several provisions of direct relevance. Section 318(4) prescribes imprisonment that may extend to seven years where cheating dishonestly induces the delivery of property.[15] Section 319 separately criminalises cheating by personation and provides

[11] Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 111.
[12] Information Technology Act, 2000, s. 66D. See *supra* note 4.
[13] N.S. Nappinai, Technology Laws Decoded (1st edn, LexisNexis 2017).
[14] Information Technology Act, 2000, s. 66C.
[15] Bharatiya Nyaya Sanhita, 2023, s. 318(4).

 [ISSN 2581-5369]

for imprisonment that may extend to five years, or fine, or both.[16] Section 111 creates a statutory framework for organised crime and expressly includes certain cybercrime and economic-offence activities within its scope, subject to the remaining statutory conditions.[17]

These provisions are capable of operating alongside Section 66D. In cases involving substantial financial loss or organised networks, prosecutors may prefer the higher sentencing ceilings available under the Bharatiya Nyaya Sanhita. The continued utility of Section 66D therefore lies primarily in its specific recognition of the technological medium rather than in its punitive severity.

D. Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam expressly recognises electronic and digital records and establishes rules governing their admissibility.[18] Sections 61 to 63 provide the contemporary framework that has replaced the earlier regime under the Indian Evidence Act. Digital-arrest prosecutions will ordinarily rely upon call-detail records, messaging logs, video recordings, electronic documents, bank statements, and device extraction reports.

The principal evidentiary difficulty is not the existence of electronic material but its reliable attribution to the accused. Screenshots and recordings may establish what the victim received; they do not, by themselves, establish who generated or transmitted the communication. Investigators must therefore construct a chain of digital attribution that combines subscriber information, device identifiers, internet-protocol logs, financial trails, and other corroborative evidence.[19]

IV. Doctrinal Evaluation of Section 66D

A. The Ingredients of Cheating and Personation

The prosecution must establish the classic elements of cheating: deception and dishonest inducement resulting in the delivery of property or the alteration of a valuable security. In digital-arrest cases, the fraudulent claim of governmental authority and the threat of imminent arrest ordinarily supply the deception that causes the victim to part with money. The personation element is satisfied when the accused represents himself, or causes himself to be represented,

[16] Bharatiya Nyaya Sanhita, 2023, s. 319(2).
[17] Bharatiya Nyaya Sanhita, 2023, s. 111. See *supra* note 11.
[18] Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), ss. 61–63.
[19] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

 [ISSN 2581-5369]

as a person whom he is not, most commonly a police officer, investigating-agency official, or judicial authority.[20]

These elements are capable of being established on the facts of a typical digital-arrest prosecution. The doctrinal reach of Section 66D is therefore not the primary source of difficulty.

B. The Electronic-Nexus Requirement and Attribution Challenges

Section 66D requires that the personation be accomplished by means of a communication device or computer resource. This requirement serves as an important safeguard against over-criminalisation; mere possession or incidental use of a mobile telephone does not attract liability.[21] In organised cybercrime, however, the requirement generates practical difficulties. A SIM card may be registered in one name, controlled by another person, and used from a third jurisdiction. Online accounts may be operated through multiple devices and proxy servers. Establishing a legally sufficient chain of attribution therefore demands sophisticated cyber-forensic capacity.[22]

C. Punishment and Proportionality

The most significant limitation of Section 66D lies in its sentencing ceiling. A maximum term of three years' imprisonment and a fine of one lakh rupees does not differentiate between a minor act of online impersonation and a sophisticated, multi-victim digital-arrest operation that causes substantial financial loss and prolonged psychological trauma.[23] By contrast, Section 318(4) of the Bharatiya Nyaya Sanhita permits imprisonment up to seven years where cheating induces delivery of property, and Section 319(2) permits up to five years for cheating by personation.[24]

This disparity does not render Section 66D redundant. It does, however, indicate that the specialised cyber provision is no longer calibrated to the gravity of the most serious forms of digital personation. A graded statutory framework capable of recognising aggravating circumstances (impersonation of public authorities, use of synthetic media, targeting of

[20] *R.K. Vijayasarathy v. Sudha Seetharam*, (2019) 16 SCC 739.

[21] *C. Vaishnavi v. C.B. Krishnan*, C.C. No. 19511 of 2016, XLV Additional Chief Metropolitan Magistrate, Bengaluru, judgment dated 27 February 2026. See also *Dr Madhukar G. Angur v. State*, Criminal Petition No. 11024 of 2023, Karnataka High Court, judgment dated 22 April 2025, https://indiankanoon.org/doc/162564262/ (proceedings registered under ss. 66 and 66D of the Information Technology Act, 2000 quashed in what was in substance a civil domain-name dispute, none of the ingredients of those offences being made out).

[22] PAVAN DUGGAL, CYBERLAW: THE INDIAN PERSPECTIVE (2nd edn, Saakshar Law Publications 2004); see also PAVAN DUGGAL, TEXTBOOK ON CYBER LAW (2nd edn, LexisNexis 2016).

[23] Information Technology Act, 2000, s. 66D. See *supra* note 4.

[24] Bharatiya Nyaya Sanhita, 2023, ss. 318(4) and 319(2). See *supra* notes 15 and 16.

 [ISSN 2581-5369]

vulnerable victims, or participation in organised networks) would restore proportionality without sacrificing the technological specificity of Section 66D.

V. Evidentiary and Investigative Challenges

A. Forged Digital Documents

Digital-arrest offenders routinely reinforce their impersonation through fabricated warrants, notices, identity cards, and judicial orders. Such documents may independently attract offences relating to forgery and the use of forged documents under the Bharatiya Nyaya Sanhita.[25] Their presence demonstrates that digital-arrest scams typically involve a constellation of interconnected offences rather than a single statutory violation.

From an evidentiary standpoint, investigators must establish the origin, transmission pathway, and authenticity of each digital document. A screenshot or forwarded file is rarely sufficient to attribute authorship. Device extraction, metadata analysis, account-access logs, and communications records become essential.

B. Synthetic Audio and Deepfake Video

Synthetic audio presents a particular forensic challenge because a recording may sound identical to the voice of a genuine official. Where the accused disputes the authenticity of a recording or alleges manipulation, expert examination becomes necessary. Deepfake video raises analogous difficulties: the content of the recording may be accurate, yet its provenance and integrity remain contested. The evidentiary focus must therefore shift from mere content to the complete chain of creation, storage, and transmission.

C. Cross-Border Dimensions

Section 75 of the Information Technology Act extends the legislation to offences committed outside India that involve a computer, computer system, or computer network located in India.[26] While this provision establishes legal reach, it does not resolve the practical obstacles of identifying foreign offenders, obtaining subscriber data from overseas platforms, or securing extradition. Effective investigation of digital-arrest networks frequently requires mutual legal assistance, cooperation with foreign financial-intelligence units, and rapid preservation of electronic evidence across jurisdictions.[27]

---

[25] Bharatiya Nyaya Sanhita, 2023, ss. 335–340 (forgery and related offences).
[26] Information Technology Act, 2000, s. 75.
[27] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (Draft, February 2013), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

 [ISSN 2581-5369]

VI. Judicial and Institutional Response

A. Supreme Court Intervention

The Supreme Court's continuing *suo motu* proceedings in *In re Victims of Digital Arrest Related to Forged Documents* represent the most significant institutional response to date.[28] The proceedings originated from complaints involving impersonation of CBI, Enforcement Directorate, and judicial authorities and substantial financial loss to victims. Subsequent orders have expanded beyond the individual facts to address systemic issues, including the role of mule accounts, temporary debit holds, delayed transaction mechanisms, grievance-redressal pathways, and restoration of defrauded funds.[29]

This judicial approach recognises that effective control of digital-arrest fraud cannot be achieved solely through post-hoc criminal prosecution. Preventive financial measures and rapid inter-agency coordination are equally essential.

B. Governmental and Regulatory Measures

The National Cyber Crime Reporting Portal and the 1930 financial cyber-fraud helpline provide important channels for early reporting. Timely reporting is critical because the probability of fund recovery declines as money moves through successive accounts.[30] The Indian Cyber Crime Coordination Centre, together with financial institutions, telecommunications service providers, and law-enforcement agencies, must function as an integrated ecosystem; no single institution controls the complete evidence or financial trail.

VII. Critical Assessment of Section 66D

A. Strengths

Section 66D possesses two enduring strengths. First, its reference to communication devices and computer resources is technologically neutral; the provision can accommodate new applications and platforms without legislative amendment. Second, it expressly recognises that personation conducted through digital technology warrants specialised legal treatment. This recognition remains valuable even after the enactment of the Bharatiya Nyaya Sanhita.

---

[28] *In re Victims of Digital Arrest Related to Forged Documents*, *supra* note 3.

[29] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025, Order dated 9 February 2026, https://api.sci.gov.in/supremecourt/2025/59769/59769_2025_1_39_68501_Order_09-Feb-2026.pdf.

[30] Ministry of Home Affairs, Government of India, *Cyber Awareness*, Press Information Bureau (17 March 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241336 (the Citizen Financial Cyber Fraud Reporting and Management System was launched for immediate reporting of financial frauds and to stop siphoning off of funds by the fraudsters; more than Rs. 8,690 crore saved in more than 24.65 lakh complaints up to 31 January 2026; the release annexes the National Crime Records Bureau State-wise cyber-crime figures from *Crime in India*).

B. Limitations

The limitations are equally clear. The three-year maximum punishment is inadequate for aggravated digital-arrest fraud involving substantial loss and organised networks.[31] The provision contains no statutory recognition of aggravating circumstances such as impersonation of judges or police officers, use of artificial-intelligence-generated material, or targeting of vulnerable victims. It also provides no direct mechanism for freezing or restoring victim funds; judicial directions have had to fill this institutional gap.[32]

C. Overall Evaluation

Section 66D is doctrinally adequate to cover the core conduct involved in digital-arrest scams. Where an offender uses a digital communication device to impersonate another person and thereby cheats a victim, the ingredients of the offence may be satisfied. Its practical inadequacy arises from insufficient punishment, difficulties of digital attribution, the networked character of contemporary cybercrime, and the absence of integrated recovery mechanisms. Consequently, Section 66D should be understood as one necessary component of a broader legal and institutional architecture rather than a comprehensive solution in itself.

VIII. RECOMMENDATIONS

A. Legislative Recalibration

The law should recognise an aggravated form of digital personation encompassing impersonation of law-enforcement or judicial authorities, substantial financial loss, vulnerable victims, deployment of AI-generated synthetic media, or participation in organised criminal activity. Such circumstances justify enhanced punishment through a graded sentencing structure that distinguishes minor online impersonation from sophisticated, multi-victim operations.

B. Institutional and Financial Safeguards

Banks and payment-system operators should maintain clear, time-bound procedures for placing temporary holds on transactions reported through recognised cybercrime channels. These procedures must incorporate safeguards against wrongful freezing and mechanisms for rapid review. A structured victim-restoration framework should complement criminal prosecution, maximising recovery where funds remain traceable and providing appropriate compensatory pathways where recovery proves impossible.

---

[31] Information Technology Act, 2000, s. 66D. See *supra* note 4.

[32] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025, Order dated 4 August 2026.

 [ISSN 2581-5369]

C. Investigative Capacity

Cybercrime investigators require continuous specialised training in device extraction, metadata preservation, cloud-evidence acquisition, account attribution, and the forensic examination of AI-generated content. Investigations should be designed to map the entire criminal network rather than terminating with the individual who communicated with the victim. Financial investigators, cyber-forensic specialists, and conventional police officers must operate as integrated teams.

IX. Conclusion

Digital-arrest scams represent a significant evolution in cyber-enabled personation. Their effectiveness derives from the convergence of technological deception, psychological coercion, fabricated institutional authority, and rapid electronic fund transfers. Artificial intelligence has further elevated the sophistication of these schemes by rendering synthetic voice and video increasingly convincing to ordinary citizens.

Section 66D of the Information Technology Act, 2000 remains relevant because it directly addresses cheating by personation accomplished through communication devices and computer resources. Its technologically neutral formulation confers continuing utility in a rapidly changing digital environment. Nevertheless, its existing maximum punishment and limited statutory architecture render it inadequate as a standalone response to sophisticated, organised digital-arrest operations.

The principal conclusion of this study is that Section 66D is doctrinally adequate yet institutionally and punitively inadequate when applied to advanced digital-arrest networks. The Bharatiya Nyaya Sanhita supplies complementary provisions of greater punitive severity concerning cheating, personation, and organised crime, while the Bharatiya Sakshya Adhiniyam furnishes the contemporary evidentiary foundation for electronic records. These instruments must operate in concert.

The appropriate reform path is not the repeal of Section 66D but its careful recalibration. Aggravated digital personation, particularly where public authorities are impersonated, vulnerable persons are targeted, synthetic media are employed, substantial loss is caused, or organised networks are involved, should attract enhanced punishment. Simultaneously, financial institutions, telecommunications providers, intermediaries, cybercrime agencies, and police authorities must be integrated into a coordinated framework capable of preventing further transfers, preserving electronic evidence, identifying entire criminal networks, and restoring

 [ISSN 2581-5369]

victims' property. Only through such a comprehensive, technologically informed, and victim-centred architecture can the law respond adequately to the contemporary reality of digital arrest.

*****

 [ISSN 2581-5369]