

Digital Arrest Scams in India: Doctrinal Analysis of the Legal Framework, Enforcement Challenges and Regulatory Reforms

Meena Shree G S*

* Student, LL.M., (Cyber Law), School of Law, Joy University, Tirunelveli, Tamil Nadu, India

Research Article History

Received: 24-Sep-2026
Revised: 27-Sep-2026
Accepted: 29-Sep-2026
Published: 01-Oct-2026

Keywords

*Cheating by Personation
Criminal Law
Cyber Fraud
Cybercrime
Digital Arrest
Electronic Evidence
Regulatory Reform*

Abstract

The quick proliferation of technologies of digital communication, online banking services and digitized public services has given rise to new ways of cyber criminals to make use of technological mechanisms and people's trust. Digital arrest scams are one of the new types of cyber enabled financial scams, which are known as "digital arrests". In the case of digital arrest, the offenders take the identity of any of the investigating agencies, police, court or any public official and make the individuals believe that they have any involvement in the crime. Through phone calls, video conferencing, false documents, the threat of being arrested and psychological manipulations, the victims are convinced into transferring the amount to bank accounts maintained by the offenders. Notably, there is no concept of digital arrest in the laws of India and any process that does not allow an individual to be arrested or detained via phone call or video call. This paper will carry out a doctrinal analysis of the current Indian legal system in regard to digital arrest scams. In this context, the paper will review the relevant sections of Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, in addition to the institutional measures involved in reporting and investigation of cyber frauds. The paper posits that the criminal law can be utilized in dealing with constituent crimes like cheating, cheating by personation, criminal intimidation and forgery. Nevertheless, challenges still exist in terms of identifying offenders, preservation of electronic evidence, tracing and freeze of the fraudulent money, jurisdiction and inter-agency cooperation.

Corresponding Author:

Meena Shree G S

Student, LL.M., (Cyber Law), School of Law, Joy University, Tirunelveli, Tamil Nadu, India
smeena2001sree@gmail.com

This article is under the [CC BY- NC-ND](#) licenses

Copyright @ Journal of Law and Legal Research

Development, available at www.jllrd.com



1. INTRODUCTION

Digital revolution in the Indian society has radically altered the way people communicate, pay for services and deal with government offices. Mobile phones, internet banking, digital payments, social networks and video conferencing tools made these activities easier and more convenient. However, the increasing reliance on digital technology has opened new possibilities for committing crimes without personal communication between the offenders and their victims. Cybercrime of today often proves that technology can be used not only to attack computers and gain unauthorised access to information. It can be also used to manipulate people's behaviour. Such a kind of cyber-enabled crime usually involves

social engineering, in which the offender uses human traits like trust, fear, urgency and authority to convince the victim to do something that is against their interests. Digital arrest scams can be considered a vivid example of such deception. The term "digital arrest" creates an illusion that one can be legally arrested or detained using a telephone or video call. However, there is no such legal procedure under Indian laws. The fraudsters take advantage of this misperception, pretending to be a police officer, an investigator, a customs officer or any other representative of the judicial system. Victims are told that their bank account, identity papers, mobile phone number or packages are somehow involved into a crime and may be arrested, jailed or seized. Deception is usually achieved

through fake government notices and documents along with prolonged phone or video conversations. They might be asked not to reach out to their families and independently investigate the claims. Under constant mental pressure, they end up transferring money for purposes of investigating, verifying, securing, and other legal requirements, which are entirely false. This issue is gaining judicial recognition even in the landmark case of *In Re: Victims of Digital Arrest Related to Forged Documents*, where cases of impersonation, forged government documents, and use of digital communication technology to make the victims transfer large amounts of money were brought before the court. This shows how cyber technology, social engineering, impersonation, and monetary gain have come together in one scam. Digital arrest scams thus go beyond online payment scams because here, State authority is deliberately simulated. Even though existing laws in India may cover individual elements like cheating, impersonation, intimidation, forgery, and abuse of electronic communications, many issues still persist. In light of the above context, the present research involves a doctrinal study of the legal regime related to digital arrest scams in India. It involves a discussion on the relevance and practical application of the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023, while also focusing on the issues related to the enforcement and reform of the regulatory framework to address this new form of cybercrime.

2. LITERATURE REVIEW

Previous literature on cybercrimes is quite significant in providing a theoretical base for discussing the topic of digital arrest scams. However, the topic of digital arrest scams itself has not yet been addressed by many researchers so far. The earlier studies on cybercrimes mainly focus on phishing, vishing, identity theft, online financial frauds and social engineering. One important thing that has been established in these studies is that cybercrimes require not only the technological vulnerability but also the manipulation of human behaviour. Research on fraud victimisation also questions the simple belief that victims are negligent and technologically ignorant. The process of decision-making in the course of fraud could be affected by psychological stress, emotional manipulation and legitimacy of the perpetrator. Research in internet fraud shows how the fraudsters build their legitimacy and employ specific wording to influence their victims' decisions. Such an approach is especially applicable to the phenomenon of digital arrest scam because this type of deception is based on the fear of being involved in criminal prosecution and legitimate status of the individual communicating with the victim. It has become evident from the recent researches that digital arrest scam is a special category of cyber frauds. In contrast to traditional phishing or vishing, aimed at obtaining login credentials, personal information and/or access to bank accounts, digital arrest scams mimic legitimate procedures and institutions. The fraudsters impersonate police officers, investigating authorities and judicial authorities in order to make the victim believe that he/she is under the investigation. In the Indian context, the available literature has concentrated on the modus operandi of such frauds, public awareness, victim vulnerability, and the overall development of cyber-based financial crime. The existing body of knowledge acknowledges the usage of impersonation, fraudulent documentation, and digital communications technology. Institutional responses to such crimes have also concentrated on awareness, reporting and

coordination of efforts to combat cybercrime. However, legal scholarship concerning digital arrest is scant. The existing body of literature discusses cheating, impersonation, forgery and cybercrime, but doctrinal scholarship on substantive criminal law, criminal procedures, electronic evidence and institution-based enforcement is relatively scant. This deficiency is critical because a digital arrest scam would involve forgery of electronic documentation, impersonation of official authorities, psychological persuasion, and the fast transfer of funds through various accounts. The current research seeks to fill this gap through a doctrinal analysis of the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023, as well as the practical problems of offender identification, electronic evidence and financial tracking. Therefore, this study seeks to contribute to the emergent body of legal literature on digital arrest by bringing together the psychological and technological aspects of digital arrest into an Indian legal framework.

3. METHODOLOGY

The study employs doctrinal methodology for conducting legal research on the legal and regulatory framework surrounding digital arrest scams in India. This is a suitable research approach since the study is focused on the examination of the legal interpretation, scope and adequacy of rules governing the acts comprising the crime of digital arrest scams. Accordingly, the research will involve the analysis of relevant statutes, judicial rulings and mechanisms without necessarily conducting empirical studies or interviews. The main sources of the research include the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. Further, the judicial rulings and proceedings with regard to cyber-enabled fraud, impersonation, digital evidence and offenses associated with digital arrest will be analyzed. Also, documents from government and institutional bodies in relation to reporting and investigating cyber-enabled financial scams will be included in the study. Secondary sources like scholarly books, journal articles and other relevant academic materials on cybercrimes, social engineering, cyber fraud, impersonation and digital evidence will also be referred to for theoretical understanding of digital arrest scams and challenges posed by the use of technology in deceitful practices. This research will take an analytic and critical perspective. Not only will it identify legal provisions that could be used to address digital arrest scams; but it will examine whether the present legal framework is effective enough to respond to the entire nature of the crime. Special focus will be paid to the interconnections of criminal law, criminal procedure, electronic evidence and institutional enforcement. In addition to the doctrinal analysis, practical issues related to offender detection, jurisdiction, preservation and authentication of electronic evidence, tracking and freezing of illicit funds, and cooperation of law enforcement, banks, telecommunications companies and digital intermediaries will be assessed. On the basis of such analysis, the research identifies legal and enforcement gaps and proposes reform recommendations in terms of regulations and institutions in order to improve the Indian response to digital arrest scams.

4. THEORETICAL FRAMEWORK

Digital arrest scams could be studied with the help of theoretical models, which would clarify offenders' behaviour in exploiting human weaknesses and creating opportunities in

digital environment. Because digital arrest scams are not mere technical attacks, their analysis should cover not only psychological aspects but also conditions for victimization. Thus, in this research Social Engineering Theory and Routine Activity Theory are employed.

4.1 Social Engineering and Control of Human Behaviour

Social engineering is an important theoretical approach which helps to understand the psychological aspect of digital arrest scams. From the point of view of cybercrime, it can be defined as certain techniques according to which offenders force people to reveal some information, make some payments or take some actions beneficial to the offenders themselves. In the case under consideration, the offender does not overcome security measures but uses psychological factors of human behaviour (e.g. fear, obedience to authority). Digital arrest scams represent an excellent example of social engineering in a structured manner. Offenders create a situation of investigation which looks legitimate as they pretend to be police officers, investigating agencies or courts. The victims are forced to believe that their bank account, mobile phone, passport, identity papers or other personal data are linked with any criminal activities. Then they are threatened to be arrested, prosecuted or to lose their property. In general, the main idea of the fraud lies in the victim's perception of the authority of the one who pretends to be the investigator or the law enforcer. The official titles, uniforms, logos, fictitious notifications or video conferences may give the appearance of legitimacy. Thus, the victims can believe the information and act immediately because the message comes from a legitimate agency which has legal authority.

4.2 Routine Activity Theory and Digital Crime Environments

An additional perspective provided by the Routine Activity Theory could be used for understanding the circumstances conducive to digital arrest scams. As a theory explaining the conditions leading to crime, the Routine Activity Theory assumes the convergence of three factors, such as motivated offender, appropriate target and lack of effective guardianship. Within the context of digital crimes, motivated offenders apply information technologies to contact potential victims and to convince them to make transactions. In case of digital arrest scams, individuals can easily access a variety of potential targets because mobile phones, Internet banking and other electronic payment systems have become increasingly popular nowadays. Those people who cannot verify their communication in time may become especially vulnerable when being informed about their involvement in criminal activities. Lack of effective guardianship can also be seen as important for explaining the crime. The concept of guardianship can include such factors as public awareness, reliable tools for verification of official communications, fast reaction of banks and the law enforcement agencies, quick response procedures. In cases where there is lack of such guardianship or the measures are undertaken late enough, offenders can maintain the control over victims and conduct the money through different bank accounts. Thus, the Routine Activity Theory focuses on the aspects of the crime, which go beyond the offender's actions and victim's vulnerabilities. It shows that the broader technological and institutional environment contributes to commission of organized cybercrimes.

4.3 Relevance of the Theoretical Framework

Social Engineering Theory and Routine Activity Theory, when put together, make a very good theoretical framework for analyzing digital arrest scams. The former explains offender psychology, and the latter explains the conditions which give rise to and sustain these kinds of offenses. The above theoretical framework indicates that digital arrest scams cannot be tackled merely by the application of criminal offences. It needs to take into account the psychological techniques used by the offenders, and weaknesses of institutions which make the fraud possible. Therefore, the above theoretical framework justifies the below analysis of the legal framework, enforcement difficulties, electronic evidence, institutional coordination and reform measures.

5. DISCUSSION

5.1 Concept and Modus Operandi of Digital Arrest Scams

Digital arrest scams are unique impersonation and financial scams in which the offender impersonates a government official, an investigative agency, or judiciary personnel in order to acquire money from the victim. The term "digital arrest" itself is misleading since it does not have any independent legal meaning under Indian law. The fraud works by giving an impression that a legal investigation or coercive action is being carried out by way of digital communication. Its basic components may be summarized as follows. The scam is usually initiated through an unsolicited phone call, video call or any other form of electronic communication. The fraudster will pose as a law enforcement agent or any other individual from an investigating authority, customs or a judicial entity. The victim is then made to believe that there is some criminal activity associated with the victim's Aadhaar number, mobile number, bank account, parcel or financial transactions. Such claims serve as the starting point for the entire manipulation. An increase in the perception of legitimacy is achieved through the use of various government officials who claim to be investigating an issue on behalf of a department or a ministry. Fraudsters also show some fake documents which resemble notices, warrants, identity cards or any court order. It is important to note that these documents do not stand the test of law; however, they are useful for convincing the victims that an investigation is being carried out. Threats form a crucial part of the scam process since they are used to scare the victims from conducting an investigation. Victims are usually asked to keep the connection active via video call without consulting anyone else including their families, attorneys or anyone else. The continuous contact helps the perpetrators to gain control over the situation and prevent any third party from interfering. The scam ends with the transfer of money through fictitious reasons like investigation, verification, protection or bail. The legal significance of digital arrest scams comes from this blend of both conventional criminal behaviour and digital technologies. This is because the fraud is not just one particular activity but is instead a set of deceptions, personations, intimidations, electronic communications, and fraudulent inducements by financial means. Hence, there is a crucial doctrinal issue that arises from this situation, i.e., whether the current legal system can deal with not only the crimes themselves but also the technological structure behind them.

5.2 Legal Framework Governing Digital Arrest Scams in India

It must be noted that the legal approach to the issue of digital arrest scams in India is not focused on one specialised legislation. The different acts associated with fraud can fall

under various legal documents. The BNS of 2023 is the primary document that is used in order to deal with the criminal activities associated with these acts. The ITA of 2000 is responsible for regulating certain aspects of fraud that involve electronic communication. BNSS of 2023 regulates criminal investigations and procedures, and BSA of 2023 is responsible for regulating the use of electronic evidence. According to the BNS, the offences of cheating under this statute can be committed when one deceives and induces the other party dishonestly to give away their money or property. In particular, the offence of cheating by personation will be applicable since the crime is associated with impersonation of police or investigating authorities. In certain situations, criminal intimidation, extortion, forgery, use of forged documents and impersonation of public servants might become pertinent to the case. The Information Technology Act, 2000 will complement this framework in case of the use of electronic communication, computer resources or other digital means. Both statutes should work in tandem rather than being mutually exclusive. While the BNS will deal with the criminal element of the crime, the IT Act will cover the technical aspects. This complex legal scheme demonstrates that there are no shortages of criminal offences in the Indian legal system which could be employed against digital arrest scams. The problem is that the application of these criminal offences will depend on the proper investigation. It will be necessary to combine all evidence about impersonation, electronic communication, forgery of documents and money transfer along with identification of multiple criminals.

5.3 Electronic and Digital Evidence and Procedure Issues

Electronic and digital evidence forms the crux of digital scam investigations. The relevant types of evidence could include call detail reports, messages, video call recordings, screen shots, electronic documents, bank transactions and other electronically stored data. The evidence could establish a sequence of events and statements made by the fraudster. However, merely the existence of an electronic record cannot determine the origin and the individual behind it. The Bharatiya Sakshya Adhiniyam, 2023 outlines the law and procedure for using electronic and digital records. The process requires investigators to establish the authenticity, provenance, integrity and relevance of the evidence and connect digital identifiers to the suspect. While a fake court order shown on a video call is likely to show the fraud attempt, additional evidence may be required to trace the maker or user of that order. Likewise, a phone number will not necessarily identify the user. It thus becomes important to coordinate between the law enforcement procedures and technical procedures. A delay in the acquisition of subscribers' data, records from platforms or banking information may undermine investigations. Since digital evidence is subject to deletion, alteration or loss, its timely preservation and coordination between various investigating authorities, banks and telecommunication companies, etc., become imperative.

5.4 Role of Banking, Telecommunications and Digital Intermediaries

The cases of digital arrest scams make it clear that there is more to cybercrime prevention than leaving the matter to be handled by police services alone. This is because the final goal of the scam is usually monetary gain and transfer of money. The swiftness with which these transactions are reported, identified and dealt with can determine whether the money is stopped from being transferred through a chain of accounts. It is equally

important to include telecommunication providers as part of the institutional response because the telephone and digital communication infrastructure has been used to perpetrate the scam. Information in the digital intermediaries may also help in identifying accounts, communicating and tracking the fraudulent network. Therefore, the institutional response should not be limited to crime investigation alone but should involve law enforcement authorities, banks, telecommunication service providers and digital intermediaries. Recent judicial decisions have shown how important the broader institutional response is when dealing with digital arrest scams. Cases related to digital arrest fraud have taken into account the role of telecommunication authorities, service providers, banking institutions and other intermediaries. It shows that the problem is also related to criminal justice, financial regulation and telecommunication governance.

5.5 Judicial and Institutional Response

The rise of the phenomenon of digital arrest scams has led to more and more attention being paid to the issue both institutionally and judicially. It is especially significant to look at the Supreme Court case *In Re: Victims of Digital Arrest Related to Forged Documents* since it shows how impersonation, forged documents, digital communications and blackmailing can be utilized as part of one single fraud scheme. The case concerned accusations made that fraudsters engaged in impersonating officials and judicial authorities, presented forged documents and threatened with arrest using digital communication. The victims of such actions were coerced into sending large sums of money. The case illustrates the fact that the digital arrest is not a legal process but rather a fraudulent one aimed at mimicking the State's exercise of power. It also demonstrates that the crime may encompass several criminal elements and cannot be dealt with through a narrow view on the online fraud problem. In terms of institutional response, the focus has now shifted to a broader prevention approach. Proper protection entails raising public awareness, reporting, financial action, telecommunications control and investigation. It is vital since prosecution after the fraud will not help when the funds have been moved around several accounts or even sent out of reach of the investigators.

5.6 Enforcement and Investigation Difficulties

Though there are adequate legal provisions on how digital arrest scams should be enforced, enforcement of the scam is fraught with many difficulties. One such difficulty is jurisdictional complications arising from the fact that both victims and perpetrators of the fraud may be in different States or countries. This means that there is need for effective inter-jurisdictional cooperation in dealing with digital arrest scam enforcement. Secondly, it is difficult to identify fraudsters because these people use many telephone numbers, false identities, intermediary accounts and money transactions. As a result of this, technical attribution should be complemented by subscriber information, financial information, device information and other forms of corroborative evidence. Thirdly, the rapid flow of fraudulent money becomes a challenge to recovery of the money because the money flows through many accounts before the victims know of the fraud committed against them. In this case, reporting should be prompt and there is need for cooperation between banks and law enforcement agencies in order to freeze or recover the money. Finally, victim vulnerability makes enforcement

difficult. Fear of arrest, shame and mental torture may cause victims to fail to report the crime promptly.

5.7 Doctrine Evaluation of the Current Legal System

It appears that there are no issues with the availability of the law in the context of the current legal system in India, at least when evaluated doctrinally. The existing legal framework includes provisions necessary to combat deceit and personation cheating and other elements of the criminal scheme. The laws concerning the procedure and evidence can be used to investigate such crimes and to use electronic records as evidence. What appears to be more problematic is the fragmented nature of the current legal system. Elements of one scam can be within different legal and institutional systems. Criminal liability will be covered by the BNS, the technology elements will be covered by the IT Act, the use of electronic records will be regulated by the BSA, criminal procedure will be governed by the BNSS and cooperation of the bank and regulatory institutions is necessary for the financial tracing. Thus, although the criminal scheme is integrated, the response might be fragmented. It means that there is no coordination between the systems. The introduction of the new statutory crime of digital arrest could help with classification, collecting data and increasing awareness, but the problems related to financial tracing, electronic evidence, jurisdiction and institutional coordination could not be solved with the introduction of the new crime. The more urgent task appears to be the introduction of coordination mechanisms.

5.8 Regulatory Gaps

A number of regulatory gaps have been observed in dealing with digital arrest frauds. Despite common use of the term 'digital arrest', there is no specific legal or statistical category of digital arrest frauds. The development of a better mechanism of classification would help law enforcement agencies track trends, gather proper data and implement targeted prevention. The limited ability of citizens to confirm the legitimacy of alleged governmental notifications is another regulatory gap, as such scams depend largely on the officialness of the document and authentication methods could help in reducing the number of victims of the crime. The delay of financial measures could also result in movement of funds to other accounts, which cannot be returned. Moreover, the rise in the level of sophistication of the falsified documents creates evidentiary and forensic challenges and requires the investigation to be carried out by an experienced person. Another issue to be mentioned is the lack of the knowledge of the criminal procedure among the citizens and the belief in the legitimacy of 'digital arrest'. Therefore, digital arrest frauds can be considered as the convergence of social engineering, impersonation, technical and financial aspects of the crime. Although there is sufficient legal base for addressing the described problems, there are evidentiary and jurisdictional issues and other gaps in the implementation of these regulations.

6. RECOMMENDATIONS

The foregoing analysis shows that digital arrest scams cannot be combated successfully via criminal prosecution alone. While there exist laws to cover the constituent actions, effective prevention needs a coordinated effort by the government, the police, financial institutions, telecommunication companies and digital platform providers. The following recommendations are intended to bolster

preventive measures, investigations, protection of victims, and coordination among the stakeholders.

6.1 Public Awareness about the Non-Existence of "Digital Arrest"

The public should be made aware that "digital arrest" is not a legal procedure in India. Through government agencies, there should be a sustained campaign to explain to people that the police, investigating agencies, and courts do not make arrests just through telephone or video calls. People should be made aware of some of the red flags such as immediate payment requirements, threats of arrest and requests for money transfers to verify the legitimacy of the transaction.

6.2 Government Verification Mechanism

A simple and reliable verification mechanism should be put in place to enable citizens to verify the veracity of any government communication. When an individual receives any electronic notification or calls from an individual representing the public authority, then he or she should be able to verify whether the person really represents a government authority.

6.3 Quick Financial Action

As money transfers under fraudulent pretences take place very fast, then there should be quick action from financial institutions in case of cyber fraud. Procedures for quick identification, temporary restriction and tracing of suspicious transactions can enhance chances of money recovery. This is particularly important since the prospects of recovering funds reduce with each transaction through other accounts.

6.4 Specialised Investigation for Cybercrime

Investigating agencies should have special knowledge about technology-facilitated financial scams. This training should be related to social engineering, electronic evidences, digital attribution, financial traces and organized cybercriminal networks. Due to the combination of psychological tactics along with technology and finance in digital arrest scams, an interdisciplinary approach is needed for investigation.

6.5 Integrated Inter-Agency Coordination

An integrated and coordinated response is required for successful enforcement of any measure that involves prompt information exchange between the police forces, the Indian Cybercrime Coordination Centre, banking institutions, telecommunication companies and other digital platforms. The authorized information sharing systems will enable quick exchange of information about fraudulent accounts, phone numbers and communications.

6.6 Improving Coordination Between States

Digital arrest scams usually take place across the state lines because of their victims, offenders, phones, and bank accounts being present in different states. The system should be developed for identifying inter-related complaints and patterns. This integration will help to find common accounts and modes of communication.

6.7 Improving Capacities for Handling Electronic Evidence

Investigating agencies need to enhance capacities in relation to preserving and analyzing electronic evidence such as video call logs, messages, electronic documents, device data and other records that may help in establishing chronology and identifying offenders. Proper protocols for preservation,

collection and authentication of electronic evidence would make investigation and prosecution more effective.

6.8 Victim-Oriented Response Mechanisms

Victims need prompt assistance in reporting the scam, collecting evidence and recovering their finances. As the crimes take advantage of fear and mental pressures, victims cannot be made responsible merely for having followed the fraudulent instructions. A victim-oriented mechanism will encourage prompt reporting and facilitate freezing of money and evidence collection.

6.9 Introduction of a Distinct Classification Under the Law

Legislature needs to consider whether a specific classification of fraudulent digital impersonation of authorities under the law would improve reporting of crimes, data gathering and prevention efforts. However, such reform would be undertaken only where there is evidence of gaps in law, but not where it may create overlap with the offences of cheating, personation, forgery and others.

6.10 Regular Review of Regulations

Scamming by digital impersonation constantly changes as offenders learn from technological and other advances. This means that legal and regulatory frameworks need periodic review in order to respond to the latest techniques of impersonation, manipulation and extortion. Periodic regulatory review would allow proactive response and not just reliance on the legal framework.

7. CONCLUSION

Digital arrest scams are an important kind of technology-enabled financial crimes where the offenders make use of digital communication to pretend as State authorities and deceive the victims using fear, urgency, and the pretends of legal proceedings against them. It shows how cybercrimes in the modern era have become about exploiting the human element and the psychological weakness of individuals along with technology-based systems. According to the study, Indian laws already offer a strong foundation for dealing with the components of the scam. The Bharatiya Nyaya Sanhita, 2023 deals with issues of cheating, personation, intimidation, and forgery whereas the Information Technology Act, 2000

continues to hold relevance regarding technology-enabled activities. The fundamental issue in this context is not necessarily one that involves the existence of legislation on this matter, but rather one of effective enforcement and coordination of technological capabilities. This is because cross-border operations, anonymity of communication, creation of fake documentation, quick movement of money and dispersed digital evidence make the job of investigation and retrieval harder. The current judicial and institutional response to this situation also highlights the importance of acting before losses become irreparable. Authenticating government correspondence, financial intervention, cyber-crime investigation, preservation of electronic evidence, inter-state cooperation and victim support measures thus need to be part of any comprehensive plan. It is just as important that people are legally aware of this because these scams rely fundamentally on people's trust of the government. Ultimately, this problem brings to light the larger problem of digital trust. In order to protect people from such situations, we need effective prosecution along with mechanisms to distinguish between true government authority and digital counterfeit.

Author Contribution

The author conceptualized the research, conducted the literature review and doctrinal analysis, drafted the manuscript, and finalised the article for submission.

Conflict of Interest

Conflict of interest declared none.

Funding

The review presented in the article did not receive any external financial support.

Acknowledgements

The authors would like to acknowledge that no external funding or assistance was received for this research, and therefore, no acknowledgements are necessary.

AI Declaration

The authors declare that no artificial intelligence (AI) tools were used in the preparation, writing, or development of this manuscript.

REFERENCES

- Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
- Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
- Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
- Constitution of India, 1950.
- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- *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 October 17, 2025).
- *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 December 16, 2025).
- Government of India, Ministry of Home Affairs. (n.d.). *New criminal laws*.
- Indian Cyber Crime Coordination Centre. (n.d.). *Cybercrime awareness and prevention materials*.
- National Crime Records Bureau. (n.d.). *Crime in India*. Government of India.
- Reserve Bank of India. (n.d.). *Customer protection and awareness measures relating to digital payment fraud*.
- Sansad. (n.d.). *Parliamentary material concerning measures against cybercrime and digital arrest scams*.
- Council of Europe. (2001). *Convention on Cybercrime*. Council of Europe.
- Financial Action Task Force. (n.d.). *Reports and guidance on cyber-enabled financial crime and fraud*.
- United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. United Nations.