DIGITAL ARREST FRAUD IN INDIA: PSYCHOLOGICAL MANIPULATION, CYBER-FORENSIC CHALLENGES, AND THE NEED FOR A COORDINATED LEGAL RESPONSE

Dr. Surinder Kalyan, Associate Professor, School of Law, NIILM University, Kaithal (Haryana)

ABSTRACT

The rise of digital communication technology has revolutionized way in which economic activities, governmental governance systems social engagements take place. On flip side, rise in these technologies provides grounds for cybercriminals to come up with highly complex schemes of deception. Digital arrest is one of latest examples of fraudsters exploiting cyber space to defraud victims out of their assets through coercion and manipulation. Digital arrest scams involve individuals posing as policemen, customs personnel, officers from Central Bureau of Investigation or Enforcement Directorate and other regulatory authorities and accusing victims of committing illegal acts. They threaten victims of arrest, prosecution, confiscation of their property and ruin their reputation until latter transfers hefty sums of money purportedly to prove their innocence. The rise of digital arrest scam is an indication of how cybercrime, coercion manipulation have become a reality of modern era. This study aims to critically examine conceptual underpinnings of digital arrest scam, process by which victims are psychologically manipulated, evidentiary challenge involved in investigating such cases and legal adequacy of laws of cybercrime in India.

Keywords: Digital Arrest, Cybercrime, Cyber Forensics, Digital Evidence, Financial Fraud, Cyber Law, Psychological Manipulation, Online Scams.

1. CONCEPTUAL FOUNDATIONS AND EVOLUTION OF DIGITAL ARREST FRAUD

1.1 Introduction to Digital Arrest Fraud

With advent of digital transformation in modern world, new avenues of communications, commercial transactions even governing became possible. At same time, technological advancements gave rise to a variety of cyber criminal organizations whose goal is to take advantage of human vulnerabilities using digital means of communication. Among them stands digital arrest fraud, a type of deceitful cyber activity whereby criminals pretend to be police officers or other representatives of government and make claims of their legal authority over victims of scam. The aim of scammers is not just money extortion but psychological dominance that is gained via fear, urgency, threats of legal action intimidation. Contrary to traditional phishing scams where hackers main motive is theft of personal information or credentials, digital arrests are based on people's trust in governmental bodies and lack of understanding of legal matters. Individuals are told that they have committed crimes related to money laundering, drug dealing, computer crime financial scams threat is imposed to be arrested if they do not follow orders given by scammers. The latter use fake warrants, videos with faked badge.[1]

The rise in frequency of these frauds can be attributed to changing approaches to committing cybercrimes. Earlier forms of cybercrime took advantage of technological vulnerabilities, but modern day digital arrest scam is also based on psychological weaknesses. Scammers have successfully used techniques that influence perception of legitimacy and authority, turning everyday communication tools into tools of intimidation. This example showcases how cybercrime has transcended from being purely a technical issue to a behavioral one as well. Digital arrest, therefore involves multiple disciplines including criminology, psychology, cyber law public policy.[2]

1.2 Evolution of Cyber-Enabled Fraud and Emergence of Digital Arrest

It is necessary to note that digital arrest scams emerged as a logical consequence of progression

[1] S. James Robert et al., *Digital Arrest in Cyber Age: A Psychological Perspective on Fear, Authority and Consciousness*, 17 Frontiers Psychol. 1726740 (2026).
[2] Shailesh Kumar Pandey & Ansh Parashar, *Navigating Digital Arrest Under India's Cyber-Forensics Framework: Complexities, Legal Gaps and Pathways Forward*, 4 J. Forensic Just. 80 (2025).

of other types of cyber crime that involved deceiving people. Initially, cyber fraud included phishing emails, lottery scams, ID theft scams, online purchasing scams romance scams. Most of these crimes were based on deceiving victims to make them voluntarily disclose some pieces of information or transfer money. Later on, however criminals have started to use various social engineering approaches and authority impersonation. This transition to more complex methods is another important feature of cyber criminal activities.

According to studies, cybercriminals tend to evolve their strategies in order to keep up with changing technologies and anti-fraud campaigns. The fact that victims became aware of standard scamming methods has forced criminals to devise new strategies that could prevent them from getting suspicious. Digital arrest scams can be considered an example of such evolution since they involve several different types of cybercrimes such as ID theft, impersonation, extortion, psychological manipulation financial scams. Contrary to romance scams which usually take months to build emotional connection between scammers and their victims, digital arrest scams use coercion within a few hours.[3]

The growth of digital payment systems has further fueled their success. Digital banking apps, quick cash transfers, electronic wallets other online financial products make it possible for perpetrators of these crimes to collect and send illegal money in record time. At same time modern digital communication platforms provide criminals with opportunities to impersonate, remain anonymous operate internationally. The result is that digital arrest scams are a truly modern crime.[4]

1.3 Characteristics and Operational Structure of Digital Arrest Scams

Specific features characterize digital arrest scams that distinguish them from other types of cybercrimes. First, they are associated with impersonating authority figures who have legitimate powers. For instance, person contacting victim pretends to work for police force, investigations agency, customs service, financial regulator, or even judiciary. Secondly, criminals strive to instill a sense of urgency and fear by accusing individual of being involved in a grave crime. The third characteristic is isolation of victim from relatives, legal counsel, or any external confirmation services. Lastly, compliance is guaranteed by constant

[3] Muhammad Zahid & Muskan Rasool, *Online Romance Scams and Financial Crime: The Migration of Cybercriminals Across Borders* (Mar. 2025).
[4] Fakhar Zaman & Wasif Shah, *Law Enforcement and Fight Against Online Scams: Lessons from Convicted Fraudsters* (Mar. 2025).

communications using video calls, fake documents fabricated investigation. The victim is also required to make different transfers under guise of verification, security deposit or settlement.[5]

One may easily notice highly sophisticated approach that scammers use while implementing their schemes. Firstly, offenders often rely on spoofed phone numbers, forged IDs, manipulated videos official logos. It is noteworthy that several people can be used to complete one scam, each of them having a specific function such as an investigator, supervisor, prosecutor, or financial officer. Therefore offenders use ordinary means of communication to coerce victims psychologically.[6]

2. PSYCHOLOGICAL MANIPULATION, FEAR, AUTHORITY, AND VICTIM COMPLIANCE IN DIGITAL ARREST FRAUD

2.1 The Psychology of Digital Arrest: Beyond Traditional Cybercrime

Though digital arrest frauds are considered a type of cybercrime, success of such activities lies in psychology and not technology. The conventional cybercrime includes hacking into system, deploying malware, or exploiting software bugs. Unlike in traditional cybercrimes digital arrest depends on psychological manipulation for success. It is not necessary for a scammer to have expertise in hacking into a system to defraud victim, all fraudster needs is to get victim into scam willingly by playing with his emotions. This makes digital arrest distinct from former cybercrime. Some researchers suggest that this activity be referred to as cyber-enabled coercion since it blends technology and psychological tricks in cybercrime.[7]

The psychological design of such con games is very well thought out in order to hinder any sort of rational thinking. This is achieved through quick succession of statements, intimidations, legalese even false evidence, meant to instill confusion and fear. Once there is sufficient emotion aroused within victim, he or she becomes less capable of logical thought. People in this state turn more often to those in authority for help and advice, exactly what con man is trying to induce. Hence scammer plays two parts, part of menace and then that of

[5] *Digital Arrest: The Modern-Day Cyber Scam* (2025).
[6] Shashank Shekhar & Divya Sridhar, *Rewind: Arrested on a Screen—Inside India's Digital Arrest Fraud*, Telangana Today (Feb. 7, 2026).
[7] S. James Robert et al., *Digital Arrest in Cyber Age: A Psychological Perspective on Fear, Authority and Consciousness*, 17 Frontiers Psychol. 1726740 (2026).

solution to problem.[8]

2.2 Fear as an Instrument of Psychological Coercion

The role played by fear is still at heart of how digital arrest scams work. While other types of scams involve offers for gain, digital arrest scams involve threats of dire legal actions. The potential victim is told that their Aadhaar number, bank account, cell phone, passport, or delivery package is associated with a crime. They are usually charged with taking part in criminal acts that carry social disgrace, such as money laundering, drug trafficking, terrorist activities, or cybercrimes. The goal here is not only to convey fear but to convey a feeling of looming disaster.[9]

Studies have shown that psychological experience of fear causes people to narrow down their focus and concentrate on actions meant to reduce their perceived threat. In such cases there is little likelihood of critical assessment of information provided as well as compliance with demands that seem to be necessary to protect one's life from harm. Digital arrest scammers take advantage of this phenomenon by introducing urgency into situation while urging people to act before it is too late.[10]

Threats based on fear work effectively since they affect several aspects of life of a person at once. Apart from incarceration there is a fear of social shame, career repercussions, problems with one's family financial ruin. In numerous cases, it is enough just to imply a link between someone and a crime in order for a victim to agree to blackmailers demands.[11]

2.3 Authority, Legitimacy and Obedience

A distinct feature of digital arrest scams involves clever manipulation of authority. The fabric of society revolves around entities that exert lawful power such as law enforcement bodies, courts, regulatory bodies government agencies. Individuals have been brought up to recognize and comply with authority. Scammers take advantage of people's inclination by posing as

[8] *Id.*
[9] Shashank Shekhar & Divya Sridhar, *Rewind: Arrested on a Screen—Inside India's Digital Arrest Fraud*, Telangana Today (Feb. 7, 2026).
[10] *Id.*
[11] Robert et al., supra note 7.

officials and using symbols of lawful power.[12]

Victims usually receive calls from scammers who claim to be representatives of Central Bureau of Investigation, Enforcement Directorate, Customs Department, Reserve Bank of India, Narcotics Control Bureau, or any other local authority. Scammers try to establish their credibility through use of formal language, spoof phone numbers, fake ID cards even fake warrants. Through video calling applications, fraudsters can present their uniforms and working environment to make themselves look more credible. Thus scam appears like an official process to victim.[13]

Authority is significant from a psychological perspective due to its capacity to mitigate uncertainties. In cases where one encounters novel circumstances tendency is often to listen to people regarded as experts or legal authorities. Digital arrests scammers take advantage of this by posing as experts who can solve legal problems that one faces. One might then follow orders not out of any true belief in legitimacy of person but out of danger of defying authority figures.[14]

2.4 Social Isolation and Information Control

Another consistent aspect of these types of scams is that victims are isolated from other sources of information. Scammers usually warn victims about confidential nature of process and prevent them from discussing case with their relatives, lawyers, colleagues other people. These precautions are explained as necessary due to confidential nature of investigation or its relation to national security, ongoing research or legal processes. It is difficult to deny such explanations because many real investigations require confidentiality.[15]

Such isolation plays an important psychological role. Most of these stories are unlikely to survive when examined externally. A lawyer will be able to find numerous contradictions and prove absurdity of claims made by scammer. The fraudster does not want victim to get any feedback from third parties because then latter would have another information source that could undermine his/her authority.

[12] *Id.*
[13] *Digital Arrest: The Modern-Day Cyber Scam* (2025).
[14] Robert et al., supra note 7.
[15] Shekhar & Sridhar, supra note 9.

In many real cases victims are warned to stay online for several hours or even days in case of prolonged interaction. During such periods of time it is impossible for person to think about anything else. The scammer thus remains main character in victim's mental universe.[16]

2.5 Cognitive Overload and Decision-Making Under Stress

The digital arrest scam hinges on cognitive overload in a big way. The individual is presented with many complicated accusations, legalese, procedural advice demands for money at once. Meanwhile they have to deal with emotions triggered by threat of their being arrested. This overload hampers their analytical reasoning skills and makes it easier for them to make intuitive decisions.[17]

As far as psychological aspects of fraud victimization go studies show that people who are under stress tend to simplify their decision making processes. Instead of analyzing all data available to them, they concentrate solely on eliminating pain. The scammers play into their hands by convincing them that making a financial transfer will be quickest and easiest way to resolve situation. For victims complying means making a move to return to normalcy instead of losing any of their resources.[18]

The combination of factors such as fear, power, isolation information overload produces an atmosphere in which even rational people can act irrationally upon hindsight. It is clear that digital arrest scams take advantage of human psychology in general and do not involve gullible people only. Digital arrest scams succeed due to manipulation of psychological aspects of decision making.[19]

2.6 Vulnerable Populations and Differential Risk

While digital arrest scams can affect anyone research reveals that some social groups are at a greater risk than others. Seniors are one of most vulnerable targets. In terms of their cyber knowledge, many seniors are found not to be familiar with new cyber threats even though they rely on technology to communicate and conduct financial and governmental affairs.[20]

---

[16] *Id.*
[17] Fakhar Zaman & Wasif Shah, *Law Enforcement and Fight Against Online Scams: Lessons from Convicted Fraudsters* (Mar. 2025).
[18] *Id.*
[19] Robert et al., supra note 7.
[20] Nireekshan Singh Gowgi S.K., *Navigating Digital Age: Digital Literacy, Fear of Scams and Self-Protection*

In addition, being socially isolated makes people more vulnerable. For example living alone means that seniors have less access to advisors who might help verify messages sent to them. Individuals lacking legal expertise may also fail to differentiate between true demands and fake information provided by fraudsters. Frauds make use of such vulnerabilities by customizing their messages according to personal specifics of each potential victim.

It is essential to stress that vulnerability is not same thing as ignorance. Victims of digital scams range from professionals, businessmen, government officials to highly educated individuals. This shows that even those who are well educated can fall into traps if they do not apply enough critical thinking.[21]

2.7 Psychological Consequences and Long-Term Harm

Financial costs are not only consequences of digital arrest. Most victims suffer from severe psychological effects such as anxiety, depression, shame, guilt diminished self worth. It is hard for many people to feel proud in light of their inability to identify fraud and avoid being arrested. These factors hinder reporting of cybercrime cases and make extent of problem less obvious.[22]

The aftermath of digital arrest may comprise mistrust toward modern technologies, reluctance to conduct business transactions via Internet damage to personal relationships. Financial harm to victim can lead to domestic tension and financial instability. At same time, psychological damage can leave a lasting negative impact on victim even long after financial damages are recovered. In some cases, psychological trauma caused by digital arrest resulted in suicidal attempts on part of victims.[23]

3. CYBER-FORENSICS, DIGITAL EVIDENCE, INVESTIGATIVE MECHANISMS, AND JURISDICTIONAL CHALLENGES IN PROSECUTING DIGITAL ARREST FRAUD

3.1 The Investigative Complexity of Digital Arrest Fraud

Research into digital arrest scam fraud faces unique difficulties that set them apart from other

Measures Among Senior Citizens, Nat'l Res. J. Soc. Scis., Vol. 10, Issue 2 (2025).
[21] Robert et al., supra note 7.
[22] Gowgi S.K., supra note 20.
[23] Robert et al., supra note 7.

criminal activities. In traditional crime, it is easy to see that perpetrators and their victims are both from same physical jurisdiction but in digital arrest scams, criminals use technology to conduct themselves in a completely anonymous manner while using trans-national communication lines. For this reason detectives have to create chains of technological interaction, which include cell phone data, telecommunications logs, financial transaction data computer logs, amongst others. These cases become even more complicated because of fact that perpetrators of such crimes always work together with members of an organized crime ring.[24]

Digital scams frequently include a number of offenders posing as several governmental agencies in course of scam. The victim is first contacted by someone claiming to be representing telecommunications company then comes contact with people pretending to be members of law enforcement, investigations, prosecution, custom officers, or even banking regulatory officials. Such a complex scheme makes it exceedingly difficult to trace down individuals responsible for particular acts in this scheme of criminal activity. In addition, encryption technologies, spoofing caller ID software, virtual private network technology disposable Internet identity tools provide offenders with anonymity which complicates work of law enforcements further. Consequently an efficient investigation will have to include not only traditional approaches but also cyber-forensics tools.[25]

3.2 Digital Evidence and Its Evidentiary Significance

Digital evidence plays an important role in process of investigating and prosecuting digital arrest frauds. Unlike traditional forms of evidence, digital evidence refers to any information existing in electronic form and encompasses a wide range of information including emails, telephone records, text messages, financial transaction history, video conference logs, Internet history, metadata, information from cloud services other electronically stored documents. Due to fact that digital arrest frauds take place mainly through electronic means of communication, prosecution of offenders often relies on ability of investigators to prove accuracy and credibility of digital evidence.[26]

[24] Shailesh Kumar Pandey & Ansh Parashar, *Navigating Digital Arrest Under India's Cyber-Forensics Framework: Complexities, Legal Gaps and Pathways Forward*, 4 J. Forensic Just. 80 (2025).
[25] *Id.*
[26] Somkanae Akkarakantrakorn, *Guidelines for Management of Digital Evidence Gathering Concerning Online Shopping Fraud*, 23 Thammasat Rev. 138 (2020).

As digital communication and financial transactions have been increasingly developing and becoming more popular role of digital evidence in investigations of digital crimes has been becoming more important. Any interaction between victim and criminal leaves traces which may help in proving guilt of latter. At same time collecting this evidence is complicated due to rapid speed at which digital information is transferred, changed, deleted or encrypted. Therefore prompt actions must be taken by investigator in order to preserve evidence in time for use during proceedings.[27]

Increasing dependence on digital evidence means that cyber forensics has become one of most vital aspects of modern investigations. The successful prosecution of cases requires not only identification of culprits but also making sure that evidence collected meets certain criteria for legality.[28]

3.3 Cyber-Forensic Tools and Investigative Technologies

Today, any investigation of cyber crimes involves employment of advanced forensic tools capable of recovering digital data and preserving evidence related to crime under study. The research carried out with regard to cyber-forensics infrastructure in India indicates that such tools as Cellebrite UFED, Forensic Tool Kit (FTK), EnCase some native forensic tools developed by Indian governmental institutions are currently employed. These tools allow investigators to retrieve deleted data, analyze communications, trace events link users actions to criminal behavior.[29]

The use of forensic tools is especially critical when it comes to investigating digital arrests due to efforts made by offenders to delete all traces of their actions. Smartphones, computers, cloud storage services online payment websites can become sources of evidence related to fraud, which can connect a suspect to criminal activity. Modern forensic analysis can help investigators to detect networks of offenders, identify financial transactions involved link communications to offender and time period they were made. In this way victims claims can be backed up by actual facts.[30]

Advances made in artificial intelligence and machine learning have increased effectiveness of

[27] *Id.*
[28] Pandey & Parashar, supra note 24.
[29] *Id.*
[30] *Id.*

process of cyber-forensics even more. Various analytical models help in detecting unusual transaction patterns, mule accounts behavioral patterns of organized cybercrimes. This is necessary owing to huge amount of digital data created in course of investigating any case of digital arrest frauds. Therefore it is evident that technological innovations are now a key aspect of combating such crimes.[31]

3.4 Financial Trail Analysis and Problem of Mule Accounts

One of most important tools used when conducting investigations on digital arrests is financial trail analysis. Due to fact that money is always primary motive behind all of these crimes, tracking flow of money can help identify perpetrator of an offense in best way possible. Nevertheless cybercriminals have become very skillful in disguising any financial transactions and creating a distance from illegal activities. One of greatest difficulties includes employment of mules' accounts.[32]

Mules accounts refer to bank account where criminals deposit their illegal gains for subsequent transfers. Mules accounts can be established with help of stolen identities or with help of persons hired for participation in illegal schemes in return for some financial reward. Once money has been deposited by victim in bank it is quickly distributed among several different accounts in order to disguise origin of funds and make any tracebacks impossible. In many cases money is further transferred abroad or into digital space.[33]

Financial investigations thus require considerable effort in tracing financial streams and determining account holders involved in such transactions. Collaboration between law enforcement bodies, financial institutions, payment processing facilities regulators is critical in conducting financial investigations. Prompt reporting from victims will improve chances of stopping fraudulent transactions early enough before any of proceeds can be dispersed irretrievably. However, fast paced nature of current financial systems continues to pose considerable challenges.[34]

[31] Pandey & Parashar, supra note 24.
[32] *Id.*
[33] *Id.*
[34] Fakhar Zaman & Wasif Shah, *Law Enforcement and Fight Against Online Scams: Lessons from Convicted Fraudsters* (Mar. 2025).

3.5 Legislative Framework Governing Digital Evidence in India

Digital arrest fraud in India is investigated and prosecuted through laws related to substantive and procedural rules. The Information Technology Act, 2000 provides essential legislative framework on electronic record-keeping, cyber crimes, intermediaries duties digital communications systems. Despite fact that this act preceded occurrence of digital arrest frauds, certain provisions in Act are pertinent to issue at hand in terms of accessing systems, misusing identities, electronic fraud role of intermediaries.[35]

The passage into law of Bharatiya Sakshya Adhiniyam, 2023 has also improved legal process surrounding establishment of electronic record evidence. This law reflects growing need for digital evidence in judicial processes and offers means for proving admissibility and authentication of such electronic evidence. Likewise Bharatiya Nagarik Suraksha Sanhita, 2023 addresses procedural issues related to investigation, search, seizure collection of electronic evidence.[36]

Nevertheless having up-to-date legislation alone will not ensure effective enforcement of new laws. The success of these efforts depends on factors such as availability of appropriate technology, professional training, coordination among institutions knowledge of judicial authorities about cyberspace and cyber forensics.[37]

3.6 Cross-Border Operations and Jurisdictional Challenges

The most crucial challenge facing investigators is perhaps international nature of today's cybercrime. Online fraud schemes usually employ offenders who conduct their activities in jurisdictions completely unrelated to countries where their victims are located. The message could have been communicated from one country, payments could have passed through several countries infrastructure could be scattered across continents. In such a scenario there are jurisdictional challenges with regards to investigation, evidence collection, prosecution law enforcement.[38]

Most conventional laws governing crimes are based on territorial principle. Cybercrimes do

[35] Information Technology Act, No. 21 of 2000, India Code (2000).
[36] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023); Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (2023).
[37] Pandey & Parashar, supra note 24.
[38] *Challenges in Prosecuting Digital Arrest Crimes Across Jurisdictions* (2025).

not always respect geographical boundaries and take advantage of gaps existing among nations legal frameworks. Cyber criminals may consciously opt to conduct their operations in countries that do not have effective laws against cyber crimes or do not cooperate internationally to apprehend suspects. As such investigators face delays when seeking to obtain evidence from other countries through their service providers, financial institutions, or telecommunication companies.[39]

Moreover this issue becomes even more complex due to variance in levels of evidentiary proof required and policies on privacy across different jurisdictions. Evidence that is accepted as valid in one legal jurisdiction may face challenges in others. This means that any solution to this issue should be characterized by better international cooperation and harmonization of cyber crime laws among others.[40]

3.7 Institutional Capacity and Future of Cybercrime Investigation

As digital arrest fraud becomes increasingly common, necessity to bolster institutional capacity at law enforcement agencies emerges with utmost urgency. Cybercrime units, forensics labs, digital evidence databases technology related training programs have emerged as key factors in modern investigative practice. The ever growing intricacy of cybercriminal practices implies that investigators should be equipped with skills that go beyond conventional police work.[41]

Furthermore there is an evident need to develop standardized methods of evidence collection and analysis. Standardized protocols increase validity of evidence and eliminate risks associated with its use in trial process. Partnerships between state and private entities such as financial institutions, technology firms, telecommunication operators cybersecurity specialists can significantly contribute to efficiency of investigative process. Collaboration with external partners fosters information exchange and accelerates threat identification and response.[42]

Consequently success of digital arrest investigations in future will largely hinge on how effectively legal institutions respond to emerging technological realities. In context of cybercriminals constantly inventing new methods of deceit it becomes imperative that

[39] Muhammad Zahid & Muskan Rasool, *Online Romance Scams and Financial Crime: The Migration of Cybercriminals Across Borders* (Mar. 2025).
[40] *Challenges in Prosecuting Digital Arrest Crimes Across Jurisdictions*, supra note 38.
[41] Zaman & Shah, supra note 34.
[42] Pandey & Parashar, supra note 24.

investigators keep up with evolving technological trends. In turn effective cyber-forensic capabilities cease being a matter of operational convenience and become a crucial prerequisite for ensuring justice.[43]

4. LEGISLATIVE EVALUATION, REGULATORY REFORMS, PREVENTIVE STRATEGIES

4.1 Evaluating Adequacy of India's Existing Legal Framework

With rising trend in digital arrest scam cases, there emerges need to determine whether current legal measures employed to counter cyber deception and fraud, including that of false impersonation and electronic evidence are adequate. However despite Indian law not recognizing arrests carried out using video conferencing, electronic warrant through messages, or paying money to prevent criminal charges, digital arrest scams pose a clear indication of shortcomings in public awareness and preparations for such scenarios. The response to digital arrest fraud from legal angle involves use of provisions in Bharatiya Nyaya Sanhita, 2023 (BNS), Information Technology Act, 2000 (IT Act), Bharatiya Sakshya Adhiniyam, 2023 (BSA) Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS).[44]

The substantive criminal law regime touches upon many aspects which are normally found in connection with digital arrest scams. The offender may face legal consequences due to his cheating, personation, forgery, criminal intimidation, misuse of identities participation in conspiracy. Moreover if electronic communication networks are employed by fraudsters for carrying out such activity, provisions of IT Act can be used. However since current legislative acts were not created with intention of regulating issues related to digital arrest scams, problems may arise in their application. The failure to legislate explicitly on digital arrest fraud as a type of cybercrime may cause certain discrepancies in investigation, prosecution and data collection. Thus even though current legal system possesses tools for dealing with constituent parts of offense, need to introduce legislation on subject is evident.[45]

[43] *Id.*
[44] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023); Information Technology Act, No. 21 of 2000, India Code (2000).
[45] Shailesh Kumar Pandey & Ansh Parashar, *Navigating Digital Arrest Under India's Cyber-Forensics Framework: Complexities, Legal Gaps and Pathways Forward*, 4 J. Forensic Just. 80 (2025).

4.2 Intermediary Liability and Role of Digital Platforms

The effectiveness of such fraud as that involving digital arrest scams depends directly on communication network employed by perpetrators. Telecom operators, social networking sites, messaging apps, video conferencing applications financial technology companies form ecosystem that enables cybercrime. Therefore legislation on reforming process is increasingly concentrated on role played by intermediaries and their involvement in prevention of crimes.[46]

Certain duties of intermediaries are imposed by Information Technology Act. Nevertheless increasing complexity of cybercrime requires a discussion on whether it is enough to deal with problem effectively. Scammers often use anonymous messaging, anonymous accounts, identity manipulation encryption to remain hidden. Indeed most technologies used to enable effective communication become tools for criminal activity. Thus there emerges issue of finding a balance between strict regulations and allowing technological progress and right to privacy of users.

A comprehensive regulation regime should thus promote detection of any potential criminal activities while respecting privacy rights. Such technology-assisted monitoring processes, detection of suspicious communication patterns, improved identity verification tools prompt reporting systems can substantially minimize opportunities for engaging in cybercriminal activities. Most importantly such efforts should be undertaken within an open legal process under judicial control. It is possible to achieve active participation of intermediaries in cybercrime prevention without sacrificing privacy rights.[47]

4.3 Public Awareness and Digital Literacy as Preventive Mechanisms

However alongside importance of reforming legal measures and developing technologies, literature shows that prevention is key tool for combatting issue of digital arrest fraud. Indeed as scheme is based on psychological tricks, awareness campaigns as well as programs aimed at increasing one's level of digital literacy will greatly contribute to addressing problem. Studies on vulnerability of scam victims among elderly people and individuals who lack experience in using digital media indicate that raising awareness of main tricks helps

[46] Information Technology Act, No. 21 of 2000, India Code (2000).
[47] Pandey & Parashar, supra note 45.

considerably resist deceptive messages.[48]

It is important to note that digital literacy means not only mastering use of digital tools but also having an understanding of cybersecurity principles, risks associated with digital communication, prevention of financial scams procedures of contacting authorities. Regarding problem of online arrests, citizens need to know that arrests cannot take place via video calls, law enforcement agencies do not ask for money to save their clients from going to prison, all information about being charged should be double checked.

Such campaigns need to address various groups and use several means for communicating with them, including schools, colleges, banks, government departments, community based organizations, traditional media channels social networking websites. Senior people especially need to be addressed since they are more often faced with increased threats because of their reduced awareness about emerging online dangers. Educational efforts need not merely include general advice but also provide specific information on how to protect oneself from particular methods of cheating used by online criminals.[49]

4.4 Strengthening Institutional Responses and Inter-Agency Coordination

One of persistent issues that have emerged in literature regarding management of digital crime is institutional coordination. Digital arrest scams involve various sectors such as law enforcement agencies, banking institutions, telecommunications companies, cybersecurity experts, digital intermediaries regulatory authorities. Responses thus need to be coordinated because isolated institutional actions will not help.[50]

The creation of cybercrime units can be viewed as a positive development in dealing with digital threats in India. However advancement of techniques employed by cybercriminals requires more investment in forensics, technology intelligence to enhance investigation and prosecution. There is a need for uniformity in incident reporting, evidence collection, financial transaction monitoring victim protection.

Equally important is development of fast action mechanisms able to freeze transactions until

[48] Nireekshan Singh Gowgi S.K., *Navigating Digital Age: Digital Literacy, Fear of Scams and Self-Protection Measures Among Senior Citizens*, Nat'l Res. J. Soc. Scis., Vol. 10, Issue 2 (2025).
[49] *Id.*
[50] Fakhar Zaman & Wasif Shah, *Law Enforcement and Fight Against Online Scams: Lessons from Convicted Fraudsters* (Mar. 2025).

money cannot be transferred to mule accounts. Due to rapid nature of cybercrimes, it may take only several hours for criminals to transfer money outside, significantly decreasing opportunities for recovery. Increased coordination efforts on part of banking organizations, payment services companies law enforcement organizations are required in this case. The implementation of artificial intelligence solutions designed to recognize any anomalies in transaction flows may prove highly beneficial in matter. Finally, solving problem of digital arrest fraud requires an ecosystem approach.[51]

4.5 International Cooperation and Future of Cybercrime Governance

However transnational character of digital arrest scams requires an increased framework of cooperation among states. Transnational criminal organizations tend to engage in activities that span across different jurisdictions, taking advantage of variations in legislation, investigative capacities regulation systems. It may happen that although internal reforms are introduced these may not be enough without cooperation among countries.[52]

There are several goals that should be pursued through international cooperation. First, process of exchanging digital evidence should be streamlined in order to decrease any possible delays caused by mutual legal assistance. Second, legislative harmonization efforts should aim at reducing differences between cybercrime laws and evidence standards. Third, financial intelligence sharing can be enhanced in order to trace and recover ill-gotten gains. Finally, capacity building can be facilitated through international cooperation programs.

Cyber crime governance in future will require a delicate balancing act between issues of state sovereignty and need for international cooperation. This is due to continuing erosion of geography brought on by technological advances. However, problem will require much more than technology, new frameworks of cooperation are required to combat crimes that cross many borders at once.[53]

5. CONCLUSION

Digital arrest fraud is one of most technologically advanced forms of cyber-enabled crimes in

[51] Pandey & Parashar, supra note 45.
[52] Muhammad Zahid & Muskan Rasool, *Online Romance Scams and Financial Crime: The Migration of Cybercriminals Across Borders* (Mar. 2025).
[53] *Challenges in Prosecuting Digital Arrest Crimes Across Jurisdictions*, supra note 38.

modern era. Whereas traditional fraud tends to depend on victim's trust in promises regarding finances or personal connections, psychological impact of digital arrest fraud is rooted in much deeper reactions based on concepts of fear, authority, urgency obedience. This form of crime capitalizes on an individual's trust in public officials and authority by threatening their freedom through legal consequences. As such, it exemplifies ways in which technological advancement may augment established methods of psychological manipulation.[54]

This research paper has shown that digital arrest fraud is far more complicated than a mere combination of technological developments and legal loopholes. It depends on interplay of several factors such as vulnerable human psyche, digital communication technology, public trust, institutional mechanisms transnational organized criminal activity. As a result, fight against this crime calls for multi-dimensional strategies that will combine all of these aspects into a coherent whole. Legislation offers a valuable foundation for legal prosecution, although adjustments to current approaches remain necessary in light of changing conditions.[55]

Ultimately battle against arrest scamming through digital means is not only an issue of law enforcement but also a wider effort aimed at preserving trust of increasingly digital societies. In an era where dependency on digital means of communication, administration finances continues to increase, ensuring safety of citizens from cyber manipulation is crucial for building trust in digital revolution itself. In this sense, future efficacy of governance in cybercrime issues depends on ability of law, technology society to collaborate against an adversary that is both psychological, technological, legal international in its essence.[56]

[54] S. James Robert et al., *Digital Arrest in Cyber Age: A Psychological Perspective on Fear, Authority and Consciousness*, 17 Frontiers Psychol. 1726740 (2026).
[55] Robert et al., supra note 54.
[56] Pandey & Parashar, supra note 45.

REFERENCES

- Akkarakantrakorn, Somkanae, Guidelines for Management of Digital Evidence Gathering Concerning Online Shopping Fraud, 23 THAMMASAT REV. 138 (2020).
- Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, INDIA CODE (2023).
- Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).
- Bharatiya Sakshya Adhiniyam, No. 47 of 2023, INDIA CODE (2023).
- Challenges in Prosecuting Digital Arrest Crimes Across Jurisdictions (2025).
- Digital Arrest: The Modern-Day Cyber Scam (2025).
- Fakhar Zaman & Wasif Shah, Law Enforcement and Fight Against Online Scams: Lessons from Convicted Fraudsters (Mar. 2025).
- Gowgi S.K., Nireekshan Singh, Navigating Digital Age: Digital Literacy, Fear of Scams and Self-Protection Measures Among Senior Citizens, NAT'L RES. J. SOC. SCIS., Vol. 10, Issue 2 (2025).
- Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
- Pandey, Shailesh Kumar & Ansh Parashar, Navigating Digital Arrest Under India's Cyber-Forensics Framework: Complexities, Legal Gaps and Pathways Forward, 4 J. FORENSIC JUST. 80 (2025).
- Robert, S. James et al., Digital Arrest in Cyber Age: A Psychological Perspective on Fear, Authority and Consciousness, 17 FRONTIERS IN PSYCHOL. 1726740 (2026).
- Shekhar, Shashank & Divya Sridhar, Rewind: Arrested on a Screen—Inside India's Digital Arrest Fraud, TELANGANA TODAY (Feb. 7, 2026).