

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

***Dr. Rajesh Kumar Verma**

****Deepak Chand**

Abstract

The emergence of “digital arrest” scams represents a new and rapidly evolving dimension of cybercrime and online harassment in India. In such schemes, cybercriminals impersonate police officers, judges, government officials, or other authorities and threaten victims with arrest or criminal prosecution through video calls, telephone communications, and digital platforms. By exploiting fear, trust, and lack of cyber-awareness, offenders often coerce victims into transferring money or disclosing sensitive personal and financial information.

This paper critically examines digital arrest as an emerging form of cybercrime from an Indian legal perspective. It analyses the existing constitutional, statutory, and regulatory framework applicable to such offences, including provisions relating to cheating, criminal intimidation, impersonation, extortion, identity theft, and misuse of electronic communication. The study further examines the challenges faced by law-enforcement agencies in investigating cross-border cyber offences, tracing digital evidence, protecting victims, and ensuring effective prosecution. The paper adopts a doctrinal and analytical approach, examining relevant legislation, judicial developments, regulatory measures, and emerging cybercrime trends. It argues that although existing criminal and cyber laws provide several mechanisms to address digital arrest scams, the rapidly changing nature of technology requires stronger institutional coordination, specialised cybercrime investigation, digital literacy, public awareness, and effective mechanisms for prevention and victim assistance.

Keywords: Digital Arrest, Cybercrime, Cyber Harassment, Online Fraud, Cyber Fraud, Digital Impersonation, Identity Theft, Criminal Intimidation, Online Extortion

Introduction:

The rapid expansion of digital technology, online communication, and electronic financial services has transformed the manner in which individuals interact with government institutions, businesses, and society. Alongside these developments, cybercriminals have adopted increasingly sophisticated methods to exploit digital platforms for financial fraud, identity theft, intimidation, and harassment. One of the most alarming recent developments in India is the emergence of so-called “digital arrest” scams, which represent a new and sophisticated form of cyber-enabled fraud and psychological

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

harassment.

The term “digital arrest” does not represent any legally recognized form of arrest under Indian law. Instead, it refers to a fraudulent technique in which criminals impersonate police officers, judges, officials of investigative agencies, or other government authorities and falsely inform victims that they are involved in a criminal case. Victims may be contacted through telephone calls, video conferencing platforms, messaging applications, or other digital means and are threatened with arrest, investigation, or imprisonment. The perpetrators frequently create an atmosphere of official authority and urgency to compel victims to transfer money or disclose confidential personal and financial information.

The emergence of digital arrest scams demonstrates how traditional forms of cheating and intimidation are being transformed through technology. Cybercriminals exploit personal information, social engineering, artificial intelligence, manipulated documents, fake identification, and video communication to create convincing fraudulent scenarios. The psychological pressure generated by the apparent involvement of law-enforcement authorities often causes victims to comply with unlawful demands without independently verifying the authenticity of the communication. From a legal perspective, digital arrest scams may involve several offences, including cheating, criminal intimidation, impersonation, extortion, identity-related offences, unauthorized use of electronic communication, and fraudulent financial transactions. The existing Indian legal framework, including the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, provides various provisions that may be invoked depending upon the facts and circumstances of a particular case. However, the technology-driven and often cross-border nature of such offences creates significant challenges relating to jurisdiction, identification of offenders, preservation of electronic evidence, recovery of stolen funds, and international cooperation.

The problem is further aggravated by limited public awareness regarding legitimate arrest and investigation procedures. Criminals exploit this lack of awareness by using official-looking documents, uniforms, video calls, fabricated case numbers, and threats of immediate arrest. Consequently, victims may experience not only financial losses but also severe psychological distress, reputational harm, invasion of privacy, and prolonged harassment. Against this background, the present study examines digital arrest as a new dimension of cybercrime and online harassment from an Indian legal perspective. It analyses the existing legal framework, the nature and modus operandi of digital arrest scams, emerging investigative challenges, and the role of law-enforcement and regulatory institutions. The study also considers the need for stronger cyber-awareness programmes, effective digital evidence mechanisms, inter-agency coordination, rapid financial-fraud response systems, and victim-centred legal remedies.

The study argues that combating digital arrest requires more than conventional criminal-law enforcement. It demands a coordinated approach combining legal reform, technological capability, cybersecurity awareness, institutional accountability, digital literacy, and international cooperation. Strengthening these mechanisms is essential for protecting individuals from emerging forms of

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

cybercrime and maintaining public confidence in India's rapidly expanding digital ecosystem.

Historical Background

The historical development of cybercrime in India is closely linked with the rapid growth of computers, telecommunications, the internet, digital banking, and social media. As India moved towards a digital economy, criminal activities also evolved from conventional forms of fraud and impersonation to technologically enabled offences. The emergence of "digital arrest" scams represents the latest stage in this continuing transformation, in which criminals use digital communication and false official identities to intimidate and financially exploit victims.

Early Development of Cybercrime in India

During the early stages of computerization, cyber offences were relatively limited and primarily involved unauthorized access, data manipulation, computer-related fraud, and misuse of electronic systems. The absence of a comprehensive cyber-specific legislation created difficulties in dealing with emerging technological offences through traditional criminal law.

The increasing use of the internet during the 1990s created new forms of cybercrime, including hacking, online fraud, identity theft, cyberstalking, and unauthorized access to computer systems. These developments demonstrated the need for a specialized legal framework capable of regulating electronic transactions and addressing technology-related offences.

Enactment of the Information Technology Act, 2000

A major milestone in India's cyber-law development was the enactment of the Information Technology Act, 2000. The legislation provided legal recognition to electronic records and electronic transactions and established a statutory framework for addressing several forms of computer-related offences.

The Information Technology Act subsequently became an important instrument for dealing with offences involving unauthorized access, identity-related misuse, computer resources, and electronic communication. The 2008 amendment significantly expanded its scope in response to the rapid development of internet-based activities and emerging cyber threats.

Expansion of Digital Technology

The growth of smartphones, social networking platforms, digital payments, online banking, e-commerce, and video-conferencing services substantially increased India's digital connectivity. At the same time, cybercriminals developed sophisticated techniques based on social engineering, phishing, impersonation, identity theft, malware, and online financial fraud. Traditional criminal methods such as cheating, intimidation, and impersonation began to operate through digital platforms. This transformation created a new category of cyber-enabled offences in which technology became not merely a means of communication but a tool for psychological manipulation and financial exploitation.

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

Emergence of Digital Arrest Scams

The concept of “digital arrest” emerged as a particularly sophisticated form of cyber-enabled fraud in which offenders impersonate police officers, judges, government officials, or personnel of investigative agencies. Victims are falsely informed that they are connected with serious criminal activities and are threatened with immediate arrest or legal action.

The offenders frequently use video calls, fabricated documents, fake identification cards, uniforms, official logos, manipulated case records, and continuous digital surveillance to create the appearance of a genuine investigation. Victims are then pressured to transfer money or provide sensitive information. Unlike conventional cyber fraud, digital arrest scams combine impersonation, intimidation, social engineering, and financial fraud. The technique exploits public trust in law-enforcement institutions and the fear associated with criminal proceedings.

Development of the Contemporary Legal Framework

The Indian legal framework has continued to evolve alongside these technological developments. The enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS) and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) marked an important modernization of India's criminal and procedural laws. Depending on the circumstances, conduct associated with digital arrest scams may attract provisions relating to cheating, criminal intimidation, personation, extortion, forgery, and other offences, in addition to applicable provisions of the Information Technology Act, 2000. Institutional mechanisms have also expanded through specialized cybercrime police stations, cybercrime reporting systems, financial-fraud response mechanisms, and greater coordination among law-enforcement and financial institutions.

Contemporary Challenges

The increasing sophistication of digital arrest scams demonstrates that cybercrime has moved beyond technical attacks against computer systems towards psychological and socially engineered forms of victimization. Criminals increasingly exploit personal data, artificial intelligence, digital communication, and publicly available information to create highly convincing fraudulent scenarios. Consequently, the historical development of cybercrime in India reveals a clear transition from relatively simple computer-related offences to sophisticated, technology-enabled crimes involving manipulation, impersonation, and psychological coercion. Digital arrest scams represent an important contemporary manifestation of this evolution and highlight the continuing need for dynamic legislation, effective cybercrime investigation, digital literacy, rapid financial-fraud response, and stronger protection of victims.

Legal Aspects

“Digital arrest” is not a legally recognized form of arrest in India. It is a term used to describe a fraudulent cybercrime technique in which offenders impersonate police officers, judges, or government officials and threaten victims with arrest or prosecution through digital platforms. The

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

legal response therefore depends on the specific acts committed by the offenders.

1. Constitutional Protection

The Constitution of India provides fundamental safeguards against arbitrary deprivation of liberty.

- Article 14 guarantees equality before law.
- Article 19 protects relevant freedoms subject to constitutional restrictions.
- Article 21 protects life and personal liberty and requires any deprivation of liberty to follow a lawful procedure.
- Article 22 provides safeguards relating to arrest and detention, including information regarding grounds of arrest and access to legal representation.

A person cannot be placed under “digital arrest” merely through a telephone call, video call, or online instruction from an unknown person.

2. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) provides the principal substantive criminal-law framework applicable to conduct involved in digital-arrest scams. Depending on the facts, offences may include:

- Cheating and dishonest inducement;
- Cheating by personation;
- Criminal intimidation;
- Extortion, where threats are used to obtain property;
- Forgery and use of forged documents, where fabricated official documents are employed; and
- Other offences arising from the particular method used by the perpetrators.

Thus, a digital-arrest scam may involve multiple offences rather than constituting one independent offence.

3. Information Technology Act, 2000

The Information Technology Act, 2000, remains an important statute for dealing with technology-related offences. Depending upon the circumstances, provisions concerning identity theft, cheating by personation using computer resources, unauthorized access, and misuse of electronic communication may become relevant.

The Act is particularly significant where offenders use digital identities, electronic records, computer resources, or online platforms to facilitate the fraud.

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

4. Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) governs criminal procedure, including arrest, investigation, search, seizure, and judicial proceedings. The procedural framework reinforces the principle that arrest must have a lawful basis and must be carried out by competent authorities in accordance with law.

Consequently, a private individual cannot legally place another person under “digital arrest” through a video call or demand money to prevent a purported arrest.

5. Electronic Evidence

Digital arrest cases generally involve substantial electronic evidence, such as:

- Telephone numbers and call records;
- Video-call recordings;
- WhatsApp or other messaging communications;
- Emails and electronic documents;
- Bank-account and transaction records;
- IP addresses and device information;
- Screenshots and recordings; and
- Digital payment records.

The Bharatiya Sakshya Adhiniyam, 2023 provides the contemporary evidentiary framework for electronic and digital records, making the proper collection, preservation, and authentication of digital evidence particularly important.

6. Data Protection and Privacy

Digital arrest offenders frequently exploit personal information obtained through data leaks, social media, phishing, or other unlawful means. The Digital Personal Data Protection Act, 2023 is therefore relevant to the broader privacy and data-security environment, although it does not itself create a specific offence called “digital arrest.”

Protection of personal data is important because criminals may use names, addresses, identification details, financial information, photographs, and other personal information to make fraudulent communications appear authentic.

7. Financial Fraud and Digital Payments

Where victims are induced to transfer money through bank accounts, UPI, wallets, or other digital payment systems, the matter may involve both criminal offences and financial-fraud mechanisms. Prompt reporting is important because rapid coordination with banks and payment intermediaries may increase the possibility of freezing or tracing fraudulent transactions.

8. Role of Cybercrime Authorities

India has developed institutional mechanisms for reporting and responding to cybercrime, including

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

the National Cyber Crime Reporting Portal and dedicated cybercrime investigation units. Effective investigation requires coordination among police authorities, banks, payment platforms, telecommunications providers, and other relevant institutions.

9. Legal Position on “Digital Arrest”

The central legal principle is that there is no provision under Indian law permitting a person to remain under arrest through a video call or telephone communication. Genuine arrest is a legal act performed by competent law-enforcement authorities in accordance with prescribed legal procedures. Demands for money to “release” a person from a supposed digital arrest are strong indicators of cyber fraud.

Judicial Trends :

The Indian judiciary has increasingly adopted a technology-sensitive and victim-oriented approach towards cybercrime and digital fraud. The recent judicial trend is particularly significant because courts are treating “digital arrest” not as a genuine legal process, but as a sophisticated form of cyber-enabled fraud involving impersonation, intimidation, forged documents, and financial exploitation.

1. State of Rajasthan – Suo Motu Digital Arrest Scam Case (2025)

The Rajasthan High Court took suo motu cognizance of the growing problem of digital-arrest scams in *In Re: Matter of Tackling the Issue of ‘Digital Arrest Scams’, Cyber Crimes and Saving the Innocent People from Losing Their Money and Lives* (22 January 2025). The Court expressed serious concern over the increasing number of victims and directed the Union and State authorities, RBI, NPCI and cybercrime authorities to report the measures being taken to control such offences.

This decision is important because it demonstrates that courts are treating digital arrest as a systemic cybercrime and public-interest issue, rather than merely an individual fraud.

2. Supreme Court’s In Re: Victims of Digital Arrest Related to Forged Documents (2025)

A particularly important development is the Supreme Court’s Suo Motu Writ Petition (Criminal) No. 3 of 2025, *In Re: Victims of Digital Arrest Related to Forged Documents*. The proceedings arose after a senior-citizen couple were allegedly defrauded of ₹1.05 crore by persons impersonating CBI, ED and judicial officials through telephone and video calls and by using forged Supreme Court documents.

The case reflects a significant judicial recognition that digital-arrest scams may involve organized criminal networks, impersonation of constitutional institutions, forged judicial documents and large-scale financial exploitation.

3. Emphasis on Financial Trail and Mule Accounts

Recent judicial developments have placed considerable emphasis on tracing the financial trail created through cyber fraud. Courts have recognized that mule bank accounts frequently facilitate the transfer and layering of fraudulently obtained funds. The Supreme Court has consequently sought stronger coordination between law-enforcement agencies, banks and financial regulators in dealing with such accounts.

4. Strict Approach towards Organized Cyber Fraud

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

Courts are increasingly recognizing that sophisticated cyber fraud can have consequences extending beyond individual financial loss. It may undermine public confidence in digital banking, online communication and government institutions. The judicial approach therefore increasingly considers the organized nature, financial magnitude, use of impersonation and technological sophistication of the offence while dealing with accused persons.

5. Protection of Victims and Senior Citizens

Recent cases demonstrate particular judicial concern for vulnerable victims, especially senior citizens who may be psychologically manipulated through threats of arrest and criminal prosecution. The Supreme Court proceedings described above originated from the alleged targeting of a senior-citizen couple, illustrating the importance of victim protection and rapid recovery of defrauded funds.

6. Importance of Digital Evidence

The judicial approach also highlights the importance of preserving and examining electronic evidence, including:

- Call records and telephone numbers;
- Video-call recordings;
- WhatsApp and other messaging communications;
- Forged electronic documents;
- Bank and UPI transaction trails;
- IP addresses and device information; and
- Digital identities used for impersonation.

Effective prosecution of digital-arrest cases increasingly depends upon the ability of investigating agencies to collect, preserve, authenticate and present such evidence before courts.

7. Judicial Recognition that “Digital Arrest” Is Not a Legal Arrest

An important underlying principle is that “digital arrest” has no independent legal status in Indian criminal procedure. Genuine arrest must be carried out by legally competent authorities according to the applicable criminal procedure. A demand made through a video call that a person remain connected online or transfer money to avoid arrest is therefore indicative of a fraudulent scheme rather than a lawful arrest.

Conclusion

The emergence of digital arrest scams represents a significant and evolving dimension of cybercrime and online harassment in India. Although “digital arrest” has no legal recognition under Indian law, cybercriminals exploit the fear of arrest and the authority associated with law-enforcement agencies to deceive, intimidate, and financially exploit victims. The growing use of video calls, forged documents, artificial intelligence, digital identities, and online payment systems has made such fraud increasingly sophisticated.

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

The existing legal framework, including the Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023, provides several provisions for dealing with cheating, impersonation, criminal intimidation, extortion, forgery, and electronic evidence. However, the rapidly changing nature of cybercrime presents continuing challenges relating to investigation, jurisdiction, digital evidence, financial recovery, and identification of offenders.

Recent judicial developments demonstrate an increasing emphasis on victim protection, financial-trail investigation, digital evidence, institutional coordination, and accountability. Courts have also recognized the need for stronger cooperation among law-enforcement agencies, banks, financial institutions, and cybercrime authorities.

Effective prevention of digital arrest scams requires a comprehensive strategy involving legal awareness, digital literacy, rapid reporting of financial fraud, specialized cybercrime investigation, protection of personal data, technological capacity-building, and international cooperation. Public awareness is particularly important because genuine government authorities do not conduct arrests through video calls or demand money to avoid arrest. Ultimately, addressing digital arrest requires more than strengthening criminal laws. It requires a coordinated legal, technological, institutional, and victim-centred approach capable of protecting citizens while maintaining trust in India's rapidly developing digital economy and criminal justice system.

***Professor**
****Research Scholar**
Department of Law
Lords University, Alwar (Raj.)

References

1. Pavan Duggal, *Cyber Law: The Indian Perspective*, Universal Law Publishing.
2. Apar Gupta, *Commentary on the Information Technology Act*, LexisNexis.
3. Rodney D. Ryder, *Guide to Cyber Laws*, Wadhwa & Company.
4. Vakul Sharma, *Information Technology: Law and Practice*, Universal Law Publishing.
5. Jonathan Clough, *Principles of Cybercrime*, Cambridge University Press.
6. David Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press.
7. Information Technology Act, 2000.
8. Bharatiya Nyaya Sanhita, 2023.
9. Bharatiya Nagarik Suraksha Sanhita, 2023.

Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian Legal Perspective

Dr. Rajesh Kumar Verma & Deepak Chand

10. Bharatiya Sakshya Adhiniyam, 2023.
11. Digital Personal Data Protection Act, 2023.
12. Prevention of Money Laundering Act, 2002.
13. Banking Regulation Act, 1949.
14. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
15. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
16. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
17. *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
18. *State of Rajasthan, In Re: Matter of Tackling the Issue of "Digital Arrest Scams", Cyber Crimes and Saving the Innocent People from Losing Their Money and Lives*, Rajasthan High Court, 2025.
19. *In Re: Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025, Supreme Court of India.

**Digital Arrest as a New Dimension of Cybercrime and Online Harassment: An Indian
Legal Perspective**

Dr. Rajesh Kumar Verma & Deepak Chand