INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 2 Art. 42

2025

Navigating the Digital Frontier: Strengthening Cyber Law to Combat the Surge in Digital Arrest Crimes

Pragya Agrahari and Jyotsna Singh

Recommended Citation
Pragya Agrahari and Jyotsna Singh, *Navigating the Digital Frontier: Strengthening Cyber Law to Combat the Surge in Digital Arrest Crimes*, 4 IJHRLR 618-627 (2025).
Available at www.humanrightlawreview.in/archives/.

Navigating the Digital Frontier: Strengthening Cyber Law to Combat the Surge in Digital Arrest Crimes

Pragya Agrahari and Jyotsna Singh

Law student, 5th year, B.A.LL.B.(Hons.), Amity Law School, Amity University, Lucknow
Assistant Professor, Amity Law School, Amity University, Lucknow

Manuscript Received	Manuscript Accepted	Manuscript Published
14 Apr. 2025	16 Apr. 2025	18 Apr. 2025

ABSTRACT

The digital revolution in India has connected millions, but it has also fueled a surge in cybercrimes, particularly digital arrest scams. In these frauds, criminals impersonate law enforcement or government officials, using fear tactics to extort money from victims for fabricated crimes. In 2024, these scams led to losses of ₹2,140.99 crore across 92,323 reported cases (Indian Cybercrime Coordination Centre, 2024). This paper explores the mechanics of digital arrest scams, their devastating societal impacts, and the effectiveness of India's legal frameworks, such as the Information Technology (IT) Act, 2000. Through case studies, legal analysis, and data from credible sources, we identify critical gaps in legislation, including lenient penalties, cross-border enforcement issues, and the lag in addressing advanced technologies like AI. Recommendations include stricter laws, enhanced technological interventions, and widespread public awareness campaigns to secure India's digital ecosystem.

KEYWORDS

Cybercrime, Digital Arrest, Cyber Law, Information Technology Act, Cybersecurity, India.

INTRODUCTION

India's digital landscape, with over 900 million internet users, is a global powerhouse, driving economic growth and connectivity (National Crime Records Bureau, 2023). However, this progress has a shadow: the rise of cybercrimes, with digital arrest scams

emerging as a particularly menacing threat. These scams involve fraudsters posing as police, tax officials, or other authorities, claiming victims are under "digital arrest" for fictitious offenses like money laundering or tax evasion. Using fear and deception, they coerce payments, often in untraceable forms [1]. The Indian Cybercrime Coordination Centre (I4C) reported 92,323 digital arrest cases in 2024, with losses totaling ₹2,140.99 crore (Indian Cybercrime Coordination Centre, 2024).

This paper investigates digital arrest scams in India, analyzing their operations, societal impacts, and the adequacy of laws like the IT Act, 2000 [2], and Bharatiya Nyaya Sanhita (BNS), 2023 [3] in this digital era.

BACKGROUND

The Evolution of Cybercrime in India

Cybercrime, encompassing illegal activities via digital platforms, has evolved with India's internet boom. The widespread adoption of smartphones and affordable data since the 2010s has made digital services accessible but also vulnerable to exploitation [4]. Digital arrest scams, a form of social engineering fraud, exploit trust by impersonating authorities. Scammers use fake calls, emails, or video chats, often backed by forged documents or AI-generated voices, to convince victims of their "arrest" [5, 6].

Unlike earlier cybercrimes targeting institutions, digital arrest scams prey on individuals, particularly the elderly, rural populations, and those unfamiliar with technology [7]. Payments are demanded in cash, bank transfers, cryptocurrencies, or gift cards, which are nearly impossible to trace.

India's Legal Frameworks

The IT Act, 2000, amended in 2008, is India's cornerstone cyber law, addressing fraud, identity theft, and unauthorized access. The BNS, 2023, complements it by criminalizing cheating and fraud, applicable to digital scams. India engages with the Budapest Convention for global cybercrime cooperation, though it remains a non-signatory, limiting its role (Ministry of External Affairs, 2019). Despite these measures, enforcing laws against digital arrest scams is challenging due to international perpetrators and rapidly evolving scam techniques [8].

METHODOLOGY

This study adopts a qualitative approach, analyzing India's legal frameworks, including the IT Act and BNS, alongside real-world

cases and data from authoritative sources like the NCRB, I4C, and Indian Cyber Squad. In this paper, we have examined scam operations, their socio-economic impacts, and legislative gaps, synthesizing recommendations to enhance India's cyber defences.

DIGITAL ARREST SCAMS: MECHANICS AND IMPACTS

How scammers operate?

Digital arrest scams typically start with an unsolicited call, message, or email accusing the victim of crimes like tax evasion, drug trafficking, or money laundering [9]. Scammers pose as officials from agencies like the CBI, Enforcement Directorate, or Income Tax Department, using spoofed phone numbers, fake logos, and forged warrants to seem authentic. Advanced scams employ AI-driven tools, such as deepfake videos or voice cloning, to enhance credibility.

Victims are pressured into immediate payments to "resolve" their case, often under threats of arrest or public shaming. Scammers may isolate victims for hours or days via continuous calls or virtual "interrogations," preventing them from seeking help. For instance, a Coonoor IT professional was confined to her home for eight days under a fake "digital arrest" in 2024, losing ₹16 lakh [1].

Socio-Economic Consequences

The financial toll is staggering, with ₹2,140.99 crore lost in 2024 alone (Indian Cybercrime Coordination Centre, 2024). Beyond money, victims suffer emotional trauma, including anxiety, shame, and distrust in institutions. A tragic case in Madhya Pradesh saw a teacher commit suicide after losing savings to a digital arrest scam (Indian Cyber Squad, 2024). Small businesses and rural households, often less equipped to detect fraud, face severe disruptions (Rao, 2017). At a macro level, these scams undermine confidence in digital banking and e-governance, slowing India's digital economy.

INDIA'S LEGAL RESPONSE AND CHALLENGES

Legal Frameworks

The IT Act, 2000, serves as India's primary legislation for cybercrimes, with Sections 66C (identity theft) and 66D (cheating by personation) directly applicable to digital arrest scams. These provisions carry penalties of up to three years' imprisonment or fines up to ₹1 lakh. The BNS, 2023, under Section 318, addresses

cheating with up to seven years' imprisonment, offering a broader framework for prosecuting fraud (BNS, 2023). However, the term "digital arrest" is not explicitly defined in either statute, forcing reliance on general provisions, which complicates case classification and sentencing (Mehta et al., 2025).

The Indian Penal Code (IPC), replaced by the BNS in 2023, previously applied Sections 419 (cheating by personation) and 420 (cheating) to such scams, but the BNS consolidates these into a unified framework, aiming for clarity (Indian Cyber Squad, 2024). The I4C, established under the Ministry of Home Affairs, coordinates cybercrime responses, integrating state police, banks, and tech firms. Its Citizen Financial Cyber Fraud Reporting System and helpline 1930 have recovered ₹3,431 crore by enabling rapid fraud reporting (Mehta et al., 2025). The National Cyber Crime Reporting Portal (cybercrime.gov.in) further streamlines complaints, with over 66,000 daily reports in 2024 (Indian Cybercrime Coordination Centre, 2024).

India's alignment with the Budapest Convention facilitates international cooperation, though its non-signatory status restricts access to formal mechanisms like mutual legal assistance treaties. The Ministry of Home Affairs has also introduced specialized cyber police stations in every state, with 53 units operational by 2024, handling digital arrest cases under the IT Act and BNS. Additionally, the Reserve Bank of India (RBI) mandates banks to implement fraud detection systems, which have blocked ₹11,269 crore in suspicious transactions, though only ₹11.97 crore was returned to victims.

Recent amendments to the IT Act, proposed in 2024, aim to address emerging threats by introducing provisions for AI-driven fraud and increasing penalties for repeat offenders (Indian Cyber Squad, 2024). The government's Cyber Fraud Mitigation Centre collaborates with platforms like Microsoft and Meta to block scam accounts, as seen in Maharashtra's blocking of 1,000 Skype IDs in 2024. These efforts reflect a multi-pronged approach, combining legislative, institutional, and technological measures. Since "digital arrest" isn't a defined offence, prosecutions rely on these broader provisions. For example, in *State v. Kumar* (2022), a scammer was convicted under the IT Act for a digital arrest fraud, receiving a five-year sentence [10].

Initiatives like the Citizen Financial Cyber Fraud Reporting System and helpline 1930 have recovered ₹3,431 crore by enabling swift reporting (Mehta et al., 2025). The I4C coordinates national efforts, integrating police and banks to freeze fraudulent accounts.

Key Challenges

1. **Cross-Border Operations**: Many scammers operate from countries like Cambodia, Myanmar, or Nigeria, complicating arrests.

2. **Lenient Penalties**: IT Act fines and jail terms are insufficient to deter organized syndicates [11].

3. **Technological Lag**: Laws don't explicitly cover AI-driven scams, leaving prosecutors to stretch existing statutes and making it difficult to interpret those laws to match with the severity of the present case.

4. **Underreporting**: Stigma and distrust discourage victims from reporting, with only 20-30% of cases documented (Rao, 2017).

5. **Enforcement gaps:** Though there are ways to report the cases to Cybercrime Police and sufficient laws to prosecute the criminal, but delayed actions and lack of enforcement make them deterrent to such crimes. Maharashtra's cyber police reported recovering just ₹11.97 crore of ₹11,269 crore blocked in 2024, highlighting this enforcement gap [12]**.**

CASE STUDIES

The 2023 Mumbai Scam Ring

In 2023, Mumbai Police dismantled a digital arrest syndicate defrauding victims of ₹10 crore. The group used fake call centers and posed as CBI officers, targeting seniors with AI-enhanced video calls. Many perpetrators fled abroad, evading justice [13]. This case underscores the need for international cooperation.

The 2024 S.P. Oswal Case

Padma Bhushan recipient S.P. Oswal lost ₹7 crore in 2024 to scammers posing as CBI officers. They staged a fake Skype "Supreme Court hearing" with forged documents, keeping him under "digital arrest" for two days. The case gained attention for targeting a high-profile figure, exposing scam sophistication [14].

The Coonoor IT Professional Case

In 2024, a Coonoor IT professional lost ₹16 lakh after scammers, posing as Mumbai cyber police, held her under "digital arrest" for eight days. They used video calls with police-like backdrops,

barring her from contacting others. This case highlights the psychological manipulation involved [15].

The 2024 Hyderabad Fraud

A Hyderabad tech worker was defrauded of ₹2 lakh in 2024 after receiving a call from a fake "Delhi Police" officer alleging involvement in a money laundering case. The scammer used a cloned voice to mimic a senior official, keeping the victim on a call for six hours [16]. This illustrates the role of emerging technologies.

ANALYSIS OF LEGAL AND TECHNOLOGICAL GAPS

Legal Shortcomings

The IT Act's broad definitions of fraud and impersonation struggle to address the nuances of digital arrest scams. For instance, Section 66D doesn't explicitly cover psychological coercion or AI-enabled deception, forcing reliance on general fraud laws. The BNS's seven-year maximum for cheating is often reduced in practice, with convicts serving minimal time [17]. The absence of a specific "digital arrest" offense complicates data tracking and sentencing.

Cross-border enforcement is a major hurdle. While Interpol and bilateral agreements aid investigations, non-signatory nations hosting scam hubs limit extraditions. The Budapest Convention's frameworks, like mutual legal assistance, are underutilized due to India's observer status [18].

Technological Challenges

Scammers' use of AI—deepfakes, voice cloning, and automated scripts—outpaces current detection systems. While banks employ fraud detection algorithms, these are less effective against social engineering. Police lack real-time tools to trace spoofed calls or cryptocurrency transactions, delaying responses. Victim education also lags, with many unaware of basic scam indicators like unsolicited calls.

RECOMMENDATIONS

1. **Global Cooperation**: The government should take steps to fully ratify the Budapest Convention to streamline cross-border investigations and extraditions.

2. **Tougher Penalties**: New amendments must be done in the IT Act to impose higher fines (e.g., ₹10 lakh) and minimum sentences of five years for digital arrest scams.

3. **AI-Powered Detection**: Police should be equipped with AI tools to detect deepfakes and spoofed calls, as trialled in Maharashtra's collaboration with Microsoft [19].

4. **Public Awareness Campaigns**: Expand initiatives like Union Bank's workshops and I4C's social media alerts to educate vulnerable groups [20].

5. **Streamlined Reporting**: Enhance cybercrime.gov.in and helpline 1930 with multilingual support and anonymous options to boost reporting.

6. **Specialized Legislation**: A new specific offence named "digital arrest fraud" should be introduced under the IT Act to improve tracking and prosecution.

7. **Capacity Building**: Police and other law enforcement agencies should be trained in AI forensics and cybercrime trends to expedite cases.

CONCLUSION

Digital arrest scams are a pressing threat to India's digital aspirations, draining billions and eroding trust. The IT Act and BNS provide a foundation, but their limitations—lenient penalties, cross-border hurdles, and technological gaps—demand urgent reform. By adopting stricter laws, leveraging AI detection, and empowering citizens through education, India can transform its digital space into a secure, inclusive ecosystem. The fight against digital arrest scams is not just legal but societal, requiring collective action to protect the nation's future.

REFERENCES

1. Mehta, A., Navodia, S., & Phadke, A. (2025). From clicks to cuffs: Understanding digital arrest in the Indian legal landscapes. https://disputeresolution.cyrilamarchandblogs.com/2025/02/from-clicks-to-cuffs-understanding-digital-arrest-in-the-indian-legal-landscapes/
2. Information Technology Act, 2000 (Act 21 of 2000).
3. Bharatiya Nyaya Sanhita, 2023 (Act. 45 of 2023).
4. Kumar, S. (2018). The rise of cybercrime in India. *Indian Journal of Criminology, 40*(1), 22-35.

5. Union Bank of India. (2024). Digital arrest: Understanding modus operandi, current trends, and safety tips. https://www.unionbankofindia.co.in/en/blog/Digital-Arrest-Understanding-Modus-Operandi-Current-Trends-and-Safety-Tips
6. Indian Cyber Squad. (2024). Digital arrests: Understanding their legal framework, technology, and case studies in India. https://www.indiancybersquad.org/post/digital-arrests-understanding-their-legal-framework-technology-and-case-studies-in-india
7. Rao, P. (2017). Victimology of cybercrime in India. *Indian Journal of Victimology, 8*(1), 30-45.
8. Gupta, R. (2021). Cybercrime in India: Challenges and solutions. *Journal of Indian Legal Studies, 15*(2), 45-60.
9. Sharma, A., & Gupta, R. (2019). Social engineering and cyber frauds in India. *Journal of Cybersecurity Studies, 12*(3), 88-102.
10. *State v. Kumar*. CRL.A. 123/2022, Delhi High Court. (2022).
11. Singh, R., & Sharma, S. (2020). Strengthening India's cyber laws. *Indian Journal of Law and Technology, 16*(1), 55-70.
12. Mumbai Police. (2023). *Operation Cyber Shield: 2023 Report*. Mumbai: Mumbai Police.
13. Samiullah Khan (2023). Mumbai: Sakinaka cops bust international fraud ring. Mid-Day. https://www.mid-day.com/mumbai/mumbai-news/article/sakinaka-cops-bust-international-fraud-ring-23306837
14. The Economic Times. SP Oswal, Vardhman Group's chief, lost Rs 7 crore in online scam by fake CBI (2024). https://economictimes.indiatimes.com/news/india/ludhiana-how-padma-awardee-vardhman-groups-sp-oswal-lost-rs-7-crore-inonlinescam/articleshow/113813450.cms?from=mdr
15. The Hindu. IT professional kept under 'digital arrest' for over a week in Coonoor, defrauded of ₹16 lakhs (2024). https://www.thehindu.com/news/national/tamil-nadu/it-professional-kept-under-digital-arrest-for-over-a-week-in-coonoor-defrauded-of-16-lakhs/article68976757.ece
16. NDTV News. Placed Under 'Digital Arrest', Techie Escapes With Police's Help (2024). https://www.ndtv.com/hyderabad-news/placed-under-digital-arrest-techie-escapes-with-polices-help-6894099
17. Sharma, A., & Gupta, R. (2019). Social engineering and cyber frauds in India. *Journal of Cybersecurity Studies, 12*(3), 88-102.
18. Ministry of External Affairs. (2019). *India and the Budapest Convention*. New Delhi: Government of India.

19. NDTV Profit. (2024). Digital arrest scam: Maharashtra cyber fraud solutions. https://www.ndtvprofit.com/nation/digital-arrest-scam-maharashtra-cyber-fraud-solutions
20. Indian Cybercrime Coordination Centre. (2024). *Cybercrime Statistics 2024*. New Delhi: Ministry of Home Affairs.
21. National Crime Records Bureau. (2023). *Crime in India 2023*. New Delhi: Ministry of Home Affairs.
22. Sharma, A., & Gupta, R. (2019). Social engineering and cyber frauds in India. *Journal of Cybersecurity Studies, 12*(3), 88-102.