Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 22s (2025)
https://www.jneonatalsurg.com

The Evolution of Digital Arrest Scams and Their Impact on Privacy Rights Guaranteed Under Constitution of India

Anuprash Rajat[1], Upendra Grewal[2]

[1]Research Scholar, School of Law, IFTM University, Moradabad

[2]Assistant Professor, School of Law, IFTM University, Moradabad

Cite this paper as: Anuprash Rajat, Upendra Grewal, (2025) The Evolution of Digital Arrest Scams and Their Impact on Privacy Rights Guaranteed Under Constitution of India. *Journal of Neonatal Surgery*, 14 (22s), 1329-1337.

ABSTRACT

In recent years, the emergence of “digital intrusion games” has put personal security and privacy at serious risk. What began as simple phishing emails has evolved into more sophisticated techniques, with scammers now using new technologies to circumvent the law and trick victims into giving up money or confidential information. This study looks at how these scams have evolved – from basic email scams to complex operations that involve data mining, social engineering and even artificial intelligence. The damage goes far beyond economic loss. These fraudulent practices violate privacy on a massive scale, leaving victims vulnerable and confused. Using social media and print media, criminals make claims that blur the line between law enforcement and freedom. The result? Growing distrust of law enforcement agencies and increasing concerns about privacy in the digital age.

Through case studies and current trends, the study also examines the psychology behind victimisation and the wider societal impact of these scams. It examines existing privacy laws and asks whether they are strong enough to deal with these constantly changing threats. Ultimately, the article calls for urgent action – better digitisation and stronger legal protections – to protect privacy in an age where technology is as easy to use as it is to obtain. By empowering citizens and building resilience, we can combat digital exploitation and protect the fundamental right to privacy.

Keywords: Right to Privacy, Data Protection, Digital Scams, Arrest Fraud, Identity Theft

1. INTRODUCTION

The rise of technological innovation in the digital age has increased the possibilities and incentives to commit crime. One of these threats is the “digital lockout” created by new technologies. Unlike traditional arrests, “digital arrests” are carried out by impersonating government officials online and making vague threats or false accusations against them. The victim is tied with puppet strings and does not realize it until it is too late. From pure phone scams to sophisticated fraud scams, the combination of different tactics and aggressive practices is proving to be a major issue for the public and law enforcement. By understanding digital access and its implications, education can effectively guard against the rapid expansion of these fraudulent methods, which are at the heart of today’s cybercrime landscape.

Here, we are using the term “digital hoarding” to mean online harassment under which a person can lodge a complaint with law enforcement agencies like the CBI or ED without any evidence. The threats include personal or video surveillance until the victim’s needs are met.

Digital fraud works like this: Scammers use caller ID spoofing to impersonate law enforcement officials, intimidate victims with fake documents and false accusations, discriminate through blackmail, and obtain stolen identity information to demand anonymous payments.

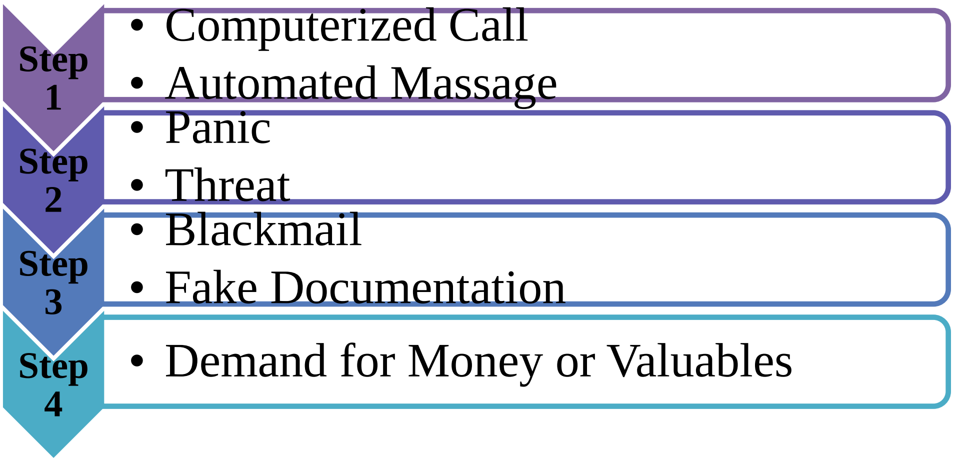

Fig.1 - Digital Arrest- Anatomy of the Fraud

2. DEFINITION OF DIGITAL ARREST SCAMS

A relatively new trend called "digital listening" is the intense interaction of audiences with digital audiences. Sometimes if a suspect gets arrested for a crime or misdemeanor and is in jail, they even inform their relatives. Fraudsters ask for money in exchange for money. Sometimes, a well-intentioned victim is forced to commit "digital crime". To put it simply, hackers wear costumes and use theatre to resemble government buildings or police stations. Cyber-Crimes can involve disrupting or interfering with communication or online access.

3. EARLY FORMS OF CYBER FRAUD IN INDIA

Digital arrest scams, which target victims by impersonating government or law enforcement personnel and threatening arrest unless immediate payments are made, have been on the rise since 2023. The severity and changing strategies of these scams are illustrated by a few recent cases:

1. On October 12, 2023, a 23-year-old woman from Faridabad contacted a trafficker from Lucknow and was asked to “login” via Skype call, along with some “fake” passports etc. Aadhaar number as per 10- physical verification is necessary. He stole her personal and financial information before she became suspicious and disappeared from social media.
2. In a "digital arrest" on November 13, 2023, a 50-year-old woman from Noida lost ₹11.11 lakh after fraudsters claimed a package in her name that was connected to narcotics smuggling. As in earlier instances, con artists were portrayed as police and customs officers. The victim said that she was approached via an Interactive Voice Response (IVR) call and informed that a mobile SIM card was purchased in Mumbai using her Aadhaar card. The SIM card was subsequently used for illegal purposes, such as harassing women.

A fraudster who claimed to be a Mumbai Police officer thereafter took over her conversation, did the ‘initial interrogation’ over the phone, and later on Skype VC. Subsequently, he sent phony documents through Skype that claimed she had been accused of money laundering once more in relation to (a fictional airline founder), for which the Supreme Court had issued an arrest order and a formal complaint had been filed against her. The woman has also told others not to publish this information since it pertains to "national security and will make her liable for further action."

3. A Noida-based IT engineer lost ₹3.75 lakh on March 4, 2024, when con artists impersonating customs officers said that a package in her name contained illegal drugs. In order to coerce her into divulging personal information and sending money to "clear her name," the con artists created a "digital arrest" during a Skype session.
4. An Associate Professor in the Neurology Department of the Sanjay Gandhi Postgraduate Institute of Medical Sciences (SGPIMS), Uttar Pradesh, Dr. Ruchika Tandon, filed a complaint on August 1, 2024, against anonymous con artists posing as representatives of the Telecom Regulatory Authority of India (TRAI). The con artist told her that a CBI official would be questioning her via Skype and that 22 complaints had been made against her mobile SIM card. She was informed by the "fake" CBI official that she was charged with money laundering and that her bank account was used to fund illegal operations, such as the trafficking of women and children. The victim paid scammers ₹2.81 Crore in order to avoid more legal repercussions.
5. On August 28 and 29, 2024, scammers impersonating representatives of the Supreme Court of India and other government bodies conned S P Oswal, 82, the Chairman and Managing Director of the well-known Vardhman Group, out of ₹7 crore. The strategy, which included phone documentation and a "fake" virtual courtroom, resulted in the victim, S P Oswal, being placed under "digital arrest" for two days. He was duped into thinking he was being investigated for financial infractions related to a case involving Naresh Goyal, the former chairman of Jet Airways. In addition, the con artists deceived Oswal into believing that his identity had been stolen and that he was under investigation for having a (fake) bank account, which was linked to the ongoing investigation into Goyal.

6. A 70-year-old retired engineer from Delhi lost all of his life wealth on November 10, 2024, after becoming a victim of a digital arrest fraud. The scammers deceived him into thinking that a package in his name had been seized by customs officers and contained illegal drugs. The con artists warned him that if the victim did not participate, there would be legal repercussions. Panicked and bewildered, the victim did what they said and lost 10 crores in the roughly eight-hour-long "digital arrest" scam. The money was moved to a number of bank accounts the scammers provided. The victim told authorities about the incident after realizing he had been tricked. Sixty lakhs of the stolen funds were frozen by the police's cybercrime unit. The remaining amount is being sought by the authorities.
7. These scammers are very sophisticated, using tactics such as video calls and fake documents to lend credibility to their threats. The fact that the police do not make arrests or demand money via video calls or emails makes it clear that the public needs to be aware and vigilant. If an employee receives such a request, they must be able to identify the caller and inform the appropriate authorities.

4. THE MECHANISMS OF DIGITAL ARREST FRAUD

Steps of a digital arrest fraud:

1. **Initiate by Contact:** Scammers contact you via phone, text, email or social media. They use fake government symbols or figures to appear legitimate.
2. **Threat Tactics:** Victims are told they are under investigation or being arrested. Attackers use scare tactics to create fear and anxiety.
3. **Video Conferencing:** Clients are requesting video conferencing. They create a fake police station setting using video footage to make it look real.
4. **Social Distancing:** Inmates are asked to maintain social distancing and bring their own cameras and microphones. They are forced to pay money to resolve the issue.
5. **Money Transfer:** Victims are instructed to send money. People are mistakenly told the money is part of a check or refund.
6. **After Receiving Payment**: Once the money is paid, the criminals will be run.

5. DIGITAL ARREST FRAUD: TACTICS & WARNING SIGNS

Some common tactics of the digital arrest fraud techniques:

1. **Account Deletion and Exploitation:** Account hacking and phishing are two ways attackers gain access to a victim's account. This results in restrictive and unauthorized behavior.
2. **Identity Theft:** Fraudsters swap victims' SIM cards to gain access to one-time passwords or secure connections. They then access the account and make transactions using the victim's name.
3. **Ransomware:** Scammers encrypt or lock the victim's files and demands money to open or decrypt them.
4. **Watch out for fake accounts:** Scammers are often financial institutions or law enforcement agencies. Using bogus emails and phone calls to threaten retaliation or legal action.

6. OVERVIEW OF PRIVACY RIGHTS IN THE DIGITAL AGE

The ability and right to control how personal information is collected, used, and shared online is known as “DIGITAL PRIVACY.” People want to live freely in the digital world without having to worry about their data being collected, used, or shared without their consent. This is cybersecurity. The importance of cybersecurity is evident in many areas. Its primary benefit is that it empowers users to manage their data and interact with the digital community. Secondly, it helps prevent cybercrimes such as identity theft, phishing, and harassment. Thirdly, protection from excessive governmental and societal surveillance is essential to maintaining an open and free society. The concept of privacy has changed dramatically with the advancement of digital technology. Privacy has evolved from a simple concept to a complex and multifaceted one, as personal information is readily available, created, and shared. As individuals evolve, privacy extends beyond the physical environment to online relationships, habits, and activities. People face many challenges when it comes to protecting their privacy online.

First, online data collection methods are abundant and often classified, making it difficult for citizens to know what is collected and how it is used. Second, managing the distribution of personal data across a large network is a daunting task. Finally, many people lack the knowledge and skills needed to properly protect their online information. It is important to have policies and regulations in place to address the challenge of cybersecurity. These regulations, such as the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States, are designed to give individuals control over their personal data and prevent it from being collected and to require them to accept it when it is collected. However, these laws vary significantly across countries, creating challenges for individuals and online businesses around the world.

The rise of smart city technology is a serious threat to cyber privacy. Although these initiatives aim to improve the quality of life by applying digital and analytical technologies in government, they actually result in the collection of more and more personal data. If this information is misused, people can become targets of targeted advertising, biased advertising, and unwanted surveillance. The complex web of the digital age makes digital privacy a complex and multifaceted issue. All users of digital technology care about this fundamental principle, which forms the foundation of trust in the digital world. This means finding a balance between the benefits of the digital age and the potential risks and harms of misuse of personal data.

7. THREATS TO DIGITAL PRIVACY

- Many cyber threats take advantage of technological and human capabilities to gain unauthorized access to or misuse personal data, making it difficult to protect and preserve personal data in a rapidly changing world
- Cybercrime is one of the biggest threats on the Internet. These types of attacks aim to compromise user data security. For this purpose, the latest technologies are used to overcome security loopholes. Cyberattacks and combating them are an important part of cybersecurity.
- In this context, data breaches - a type of cyberattack - pose a significant risk. An unauthorized person has gained access to a private network. Identity theft and financial loss are the two most common types of data breaches that can occur during an attack. These tools are extremely dangerous because they can lead to unauthorized disclosure of information.
- Another common threat is social attacks, which exploit human behavior rather than malice. These attacks force people to reveal their personal information or commit cyberattacks. Examples of social engineering include phishing emails posing as trusted organizations and scam agencies, where attackers devise ways to lure their victims
- In addition, tracking technologies pose a serious threat to their cyber activities. These technologies, which include cookies, tracking tools, and ads, provide a comprehensive view of a customer's online activity. Companies use these cookies to store a variety of information, from the website you visit to your device, for various reasons, including improving performance and showing you relevant ads, but because they are using tools that not everyone knows or trusts, they can put privacy at risk.
- Although cybersecurity measures have been implemented to mitigate threats, it is still difficult to provide comprehensive protection against the spread of these threats. In an increasingly digitally fragmented world, where threats are becoming more complex and dangerous, people need to be vigilant, aware, and proactive to protect their privacy.
- Therefore, not only do organizations need to properly secure their systems and data; in addition, it is the responsibility of every citizen to stay informed of developments in the digital world and be aware of threats and security measures. Therefore, balancing the many benefits of the digital age with the need to protect and respect computer data is a constant struggle, requiring continuous, intensive and highly visible learning.
- With so many concerns, managing your digital assets can seem like a daunting and confusing task. However, by understanding the risks and using secure technologies such as authentication and privacy protection, people can take proactive digital steps to protect their privacy

8. SOCIAL MEDIA AND PRIVACY

In today's digital world, social media has fundamentally changed the way people communicate and has shaped complex aspects of human life, each of which has its own challenges and complexities. The use of social media has a significant impact on people's lives. Since users share information about their lives on these platforms, such as photos, updates, location information and other things they are interested in, they often serve as a repository of personal information. The amount of data collected provides in-depth information about users' lifestyles and behavior, making them prime targets for privacy threats such as identity theft, cyberstalking or intrusive advertising.

Websites collect a lot of personal information. Users' personal information, such as name, gender, age and interests, is combined with data collected from activities on the platform, such as "likes", follows and shares. To improve content, many platforms collect data about devices and locations. The user experience depends on the privacy policy that applies to all communication channels. If used correctly, this method can also protect your privacy by preventing unauthorized access to your data and government information. However, it is likely that users provide more information than expected, as this data is often complex, changes rapidly, and can vary widely across different platforms.

In addition, there are some risks involved in sharing personal information on social media. If this data falls into the wrong hands, it can be used for fraud or identity theft, but it can also be misused by the platform itself. For example, some services have begun sharing user data with outside parties without the user's consent. In addition, excessive distribution can lead to "scam" business or unsolicited, unwanted advertising. Properly managing your online presence and implementing security measures such as multi-factor authentication are simple ways to reduce this risk. Employees can take more control of their online privacy by understanding each platform's policies and procedures, as well as how employee data is protected. The relationship between privacy and social media is complex and multifaceted. Despite the many benefits of this technology, it also raises privacy issues. Therefore, you need to be careful when using social media, maintaining a balance between ensuring positive content and being aware of negative content, and sharing content responsibly.

9. DATA COLLECTION AND CONSENT

- With the advent of the digital age, data collection has become a necessity in companies and organizations. With so much data available – which typically includes online activity, purchases, reviews, and more – consumer consent and the use of that data is a hot topic of discussion.
- Companies collect and use your personal information in a variety of ways. This information is often used to help customers better understand their needs, improve their products or services, or market their products. Data collection methods include cookies, information provided by users, and even information collected by third parties. Improper management and processing of personal data can lead to identity theft, unwanted information requests or fraud, and other serious privacy issues.
- If the purpose of raising funds is to improve user experience and business performance, it should be legally binding. Before obtaining consent, the individual should be aware of the type of data collected, its intended use, and the purpose for which it is being collected. However, due to lack of information and understanding, consumers often do not know how to express consent, which can lead to data loss.
- Transparency is important in data sharing decisions. Users should be fully informed about what information is collected, how it is stored, with whom it is shared, and how it is used. Users can be empowered to make decisions by giving them clear instructions about their data.
- Unfortunately, due to the complexity of electronic data management, keeping data open is a difficult task. Companies may store sensitive information for long periods of time and also in a state where consumers are unable to read it discreetly. Due to the variety of data storage technologies, such as cookies and other technologies, it can be difficult for users to control when and how their personal information is collected and used.
- In short, data storage can improve customer service, but it also raises important questions that go beyond ethics and customer data protection. People must be very careful when sharing personal information to protect their privacy. At the same time, in the pursuit of digital innovation, companies and regulators must work together to ensure that users are accountable, transparent, and respectful of all their data.

10. FUTURISTIC TRENDS IN DIGITAL PRIVACY

As technology advances, the challenges and challenges in this industry increase. The status of the digital economy is changing rapidly and often unpredictably due to rapidly developing and emerging technologies, regulatory processes and shifts in public opinion New technologies such as Artificial Intelligence (AI), Internet of Things (IoT) and others have the ability to store, process and manipulate vast amounts of data Exacerbating further challenges are posed by IoT, which can connect multiple devices and share information across multiple platforms, and AI, which can mimic human behavior and on the other hand, abuse can breach data protection laws.

As technology advances, privacy laws can change as lawyers encounter them. As evidenced by the CCPA in California and the EU GDPR, the importance of clear regulation and robust protection of personal data continues to grow but the challenge remains to create a solid regulatory framework to preserve independence and keep pace with technological developments. There are many things you can do to prepare for the digital age. First, accept the new rules and restrictions that apply to your online casino. Second, people can control their privacy by being aware of their unique information and tracking it consistently. Finally, additional layers of security can be added with technologies such as Virtual Private Networks (VPNs), firewalls, and antivirus software.

It is important to note that AI can not only create better solutions but also play an important role in shaping the future of cybersecurity. The enhancement of artificial intelligence systems to learn more about the capabilities of organizations and individuals is one example of how AI can be used to identify and address security risks in addition to how it can be used to solve problems. Widespread use of social media gives organizations greater access to public information, putting data protection issues at the forefront of discussions. Policies and research organizations should develop and implement appropriate procedures to protect the confidentiality of the use of data collected.

11. THE IMPORTANCE OF RESEARCHING DIGITAL ARRESTS IN THE CONTEXT OF INDIA

Cybercrime known as ‘digital fraud’ occurs when fraudsters pretend to be legal entities (such as Bank of India, Central Resources Corporation or Department of Information Technology, etc.) to circumvent law enforcement and extract huge amounts of money or fines. This is a threat. Fake emails and fake numbers. Websites that promote well-known companies. According to the Cyber Crime Intelligence Unit (“IC4”) of the Ministry of External Affairs, the first quarter of FY24 itself saw the maximum number of incidents of revenue loss of Rs. 120.30 crore due to cyber~attacks. There are some areas that affect people and the entire society.

12. PRIVACY RIGHTS IN INDIA: LEGAL AND CONSTITUTIONAL FRAMEWORK ADDRESSING DIGITAL ARRESTS

Although "Digital~Arrest" is not currently a recognized offense under the Information Technology Act of 2000 ("IT Act") or the Bharatiya Nyaya Sanhita of 2023 ("BNS"), several provisions of both laws apply when such crimes are carried out. The elements of a digital arrest include the use of technology to pose as an authoritative figure and the manipulation of victims into disclosing private information and other valuables under the pretense of intimidation and menace.

Consequently, a person who makes a "digital arrest" could face charges for the following offenses, among others:

- Impersonating a public servant [Section 204 of BNS] (which carries a fine and a six-month to three-year jail sentence);
- Cheating [Section 318 of BNS], which carries a maximum sentence of seven years in jail and a fine;
- Forgery [BNS, Section 336] (liable to a maximum sentence of seven years in prison and may incur a fine [Section 336(3) of BNS]) under the BNS;
- Extortion [Section 308 of BNS] (can be fined and imprisoned for a maximum of 10 years) under the BNS; and
- Identity theft [Section 66(C) and Section 66(D) of IT Act] (subject to a fine of up to INR 1 lakh and a maximum sentence of three years in prison) under the IT Act.

The severe increase in digital arrests in India has prompted the Rajasthan High Court to take suo moto attention of the matter. According to Justice Anoop Kumar Dhand, the Bharatiya Nagrik Suraksha Sanhita, 2023 (BNSS) does not include the idea of "digital arrest." The Reserve Bank of India has been ordered to take action to stop payments to these scammers, and the government has been instructed by the High Court to increase awareness. Since there is currently no statute that permits law enforcement to make arrests through online communication, the ruling emphasizes the need for citizens to be informed about the proper procedures for making arrests, including their rights during such proceedings.

Section 63 of the BNSS permits the electronic serving of summonses; nevertheless, each summons must be encrypted, bear the Court's image and seal, and have a digital signature. The BNSS describes the due process for making an arrest in a number of situations, all of which call for physical confinement. Along with making sure that the person being arrested is properly identified, the arresting police officer is also required to prepare an arrest memo at the moment of the arrest.

Additionally, if an arrest is not required under Section 35(1) of the BNSS, a notice under Section 35(3) of the BNSS requires people suspected of committing a cognizable offence to appear before the police for the necessary questioning. Recently, a Supreme Court division bench issued directives with the goal of creating consistency in the procedural framework. Among other things, the directives reiterated the rules established in Satender Kumar Antil v. CBI and Others and Rakesh Kumar v. Vijayanta Arya (DCP) and Others. The Supreme Court has ruled that although Section 63 of the BNSS permits summonses to be served electronically, notices requiring an individual to appear under Section 35(3) of the BNSS or Section 41A of the Code of Criminal Procedure, 1973 ("CrPC"), cannot be issued electronically.

This ruling also makes it clear that notices that could result in an arrest should be given in accordance with the BNSS's rigorous guidelines. Additionally, it issued guidelines prohibiting police officers from using WhatsApp to deliver notices in accordance with Sections 160 or 175 of the CrPC (now Sections 179 or 195 of the BNSS) in order to summon witnesses or other individuals for their inquiry.

13. REASONS FOR RISE IN DIGITAL ARRESTS IN INDIA

- **Surge in Digital Transactions:** Fraudsters now have additional options to target victims due to the rise in internet transactions.
- **Lack of Digital Security Awareness:** Many people are still ignorant of the fundamentals of online security, which leaves them open to fraud.
- **Advancement in Fraud Techniques:** Fraud detection has become more difficult for victims and authorities because to the use of artificial intelligence (AI)-generated voices, professional logos, and simulated video calls.
- **Southeast Asia as a Hub for Digital Arrest Fraud:** Many of the offenders operate out of Myanmar, Laos, and Cambodia, where it is difficult to investigate and bring them to justice due to a lack of effective law enforcement and little international collaboration.

14. RECOMMENDATIONS AND SOLUTIONS TO PREVENT DIGITAL ARREST SCAMS AND RELATED FRAUDS

A. Check the Identity of the Caller

- Never answer a call that seems to be from law enforcement without asking. A legitimate police officer will never ask for personal information over the phone or demand money right away.
- If in doubt, end the conversation and make another call using the national helpline or the local police station's official number, never the one the caller gives.

B. Safeguard Financial and Personal Data

- Aadhaar or PAN numbers, bank account or credit card information, OTPs, PINs, or scanned copies of identification documents should never be shared in response to unwanted requests.

- All high-risk and financial accounts should have two-factor authentication (2FA) enabled to provide an additional degree of security.

C. Make use of Spam-Filtering and Call-Blocking Tools.

- To cut down on spam calls, sign up for the National Do Not Disturb (DND) register.
- Install trustworthy programs that automatically identify and block known scam numbers, such as call filters or mobile security.

D. Update Your Firmware and Software.

- Update the operating system and apps on your smartphone on a regular basis to fix security holes that scammers could use to launch malware or SIM-swap attacks.
- Apps from unreliable third-party marketplaces should not be installed.

E. Report Any Questionable Activities Right Away

- To report digital arrest calls or other cyber frauds, use the National Cyber Crime Reporting Portal (https://cybercrime.gov.in).
- To report and monitor financial scams, you can also contact the Citizen Financial Cyber Fraud Reporting & Management System at toll-free 1930.

F. Make Yourself and Your Community Educated

- Participate in or host awareness campaigns about the strategies used by fraudsters (social engineering, caller-ID spoofing) in community centers, workplaces, and educational institutions.
- Give friends and family access to reliable internet sources and official government advisories.

G. Boost Defenses within the Organization

- Firm call-verification procedures should be put in place, and staff members should be trained to spot impersonation efforts.
- Use real-time fraud monitoring technologies and work with telecom companies to identify widespread SIM-swap or spoofing schemes.

H. Promote Strict Regulation and Supervision

- Urge lawmakers to impose sanctions on telecom companies that fail to block compromised numbers promptly and to require expedited "SIM deactivation" procedures.
- Encourage the creation of clear procedures that will enable customers who have been mistakenly blocked by fraud-prevention technologies to have their services back.

We can significantly limit the scope of digital arrest frauds and secure the financial information and privacy of potential victims by integrating individual awareness with technology protections, timely reporting, and policy-level changes.

15. CONCLUSION

Digital fraud schemes have evolved over the past decade from phone-based scams to highly targeted, technology-driven schemes that exploit technical errors and public trust in law enforcement. Unlike previous versions that used the threat of arrest, new operators use fake caller IDs, cloned SIM cards, dark analysis of compromised messaging platforms, and social engineering to trick people into publishing a lucrative story or monetize information victimized by those they do. This growth will have a significant impact on the right to privacy. In addition to committing fraud, scammers also blur the line between government agencies and individual privacy by obtaining personal information such as banking credentials and identity credentials. Victims frequently feel helpless because the police, who are supposed to protect them, are impersonated to violate their privacy and weaponize their private correspondence. In addition, the widespread barring of millions of internet accounts, SIM cards, and IMEIs raises concerns about potential due-process violations and collateral privacy breaches for legal users who are caught in the whirlpool, even while it is important to dismantle criminal networks. Indian authorities have taken important steps to interrupt the lifecycle of digital arrest scams with the introduction of regulatory and technological countermeasures, including the National Cyber Crime Reporting Portal, financial-fraud helplines, and cooperation with platform providers. However, in order to avoid going too far, they must be weighed against strict protections. To make sure that initiatives to stop cyber-fraud do not turn into tools of privacy violation themselves, it is crucial to have strong data-protection regulations, transparent blocking decisions, and explicit redress procedures for people who have been wrongfully blacklisted. A multimodal approach will ultimately be needed to combat digital arrest scams, including persistent public awareness efforts, closer public-private cooperation in digital forensics, and continuous legislative improvement to cement responsibilities for protecting privacy. The only way for nations to successfully combat these lies without compromising the democratic liberties they jeopardize is to balance security requirements with the unalienable right to individual privacy.

REFERENCES

[1] Kamalanathan, Sharade and Wadhwani, Rakhi R., All You Need to Know About Digital Arrest: A Novel Cybercrime Trend, National Cyber Security Consulting, available at https://nationalcybersecurity.com/all youneed-to-know-about-digital-arrest-a-novel-cybercrime-trend-cybercrime-infosec/ (last visited Nov. 14, 2024). 2 Kamalanathan, Sharade and Wadhwani, Rakhi R., All You Need to Know About Digital Arrest: A Novel Cybercrime Trend, National Cyber Security Consulting, available at https://nationalcybersecurity.com/all-youneed-to-know-about-digital-arrest-a-novel-cybercrime-trend cybercrime-infosec/ (last visited Nov. 14, 2024).

[2] https://digitalprivacy.ieee.org/publications/topics/understanding-privacy-in-the-digital-age

[3] Dixit, Pranav. “Cybercriminals ‘digitally arrest’ Faridabad woman, duper her of ₹ 2.5 lakh”, Business Today, 03 November 2023, available from: https://www.businesstoday.in/technology/news/story/cybercriminals-digitally-arrest-faridabad-woman-dupe-her-of-rs-25-lakh-404429-2023-11-03

[4] PTI. “New Scam: Noida Woman ‘Digitally Arrested’, Duped of ₹ 11 Lakh”, NDTV, 02 December 2023, available from: https://www.ndtv.com/india-news/new-scam-noida-woman-digitally-arrested-duped-of-rs-11-lakh-4627048

[5] Bhati, Divya. “Woman in Noida falls prey to digital arrest scam, was forced to pay ₹ 3.75 lakh for release”, India Today, 04 March 2024, available from: https://www.indiatoday.in/technology/news/story/woman-in-noida-falls-prey-to-digital-arrest-scam-was-forced-to-pay-rs-37-lakh-for-release-2510317-2024-03-04

[6] TNN. “PGI doc duped of ₹2.81 Crore in ‘digi arrest’ scam”, Times of India, 15 August 2024, available from: https://timesofindia.indiatimes.com/city/lucknow/pgi-doctor-scammed-of-281-crore-in-digital-arrest-fraud/articleshow/112536972.cms

[7] Singh, Nandini. “Digital arrest and ₹7 Crore heist: how Vardhman Group head was tricked”, Business Standard, 01 October 2024, available from: https://www.business-standard.com/companies/news/digital-arrest-and-rs-7-crore-heist-how-vardhman-group-head-was-tricked-124100100832_1.html

[8] Ojha, Arvind and Himanshu Mishra. “70-year-old retired Delhi engineer duped of Rs 10 crore in digital arrest scam”, India Today, 15 November 2024, available from: https://www.indiatoday.in/cities/delhi/story/delhi-man-retired-engineer-duped-crore-digital-arrest-scam-2633687-2024-11-15

[9] https://www.digitalsamba.com/blog/data-privacy-trends

[10] https://www.osano.com/articles/data-privacy-trends

[11] https://www.lexology.com/library/detail.aspx?g=6d91378b-7080-4b73-bba2-063a961b2a16

[12] https://www.zendata.dev/post/consent-management-101-navigating-user-consent-for-data-collection-and-use

[13] https://gdpr-info.eu/issues/consent/

[14] https://www.informationgovernanceservices.com/articles/ethics-and-consent-for-data-collection-and-use/

[15] https://disputeresolution.cyrilamarchandblogs.com/2025/02/from-clicks-to-cuffs-understanding-digital-arrest-in-the-indian-legal-landscapes/#_ftn1

[16] https://disputeresolution.cyrilamarchandblogs.com/2025/02/from-clicks-to-cuffs-understanding-digital-arrest-in-the-indian-legal-landscapes/#_ftn2

[17] https://indianexpress.com/article/india/indians-lost-rs-120-crore-in-digital-arrest-frauds-in-january-april-2024-9641952/

[18] In Re: In the 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] Satender Kumar Antil v. CBI, Miscellaneous Application No. 2034/2022 in MA 1849/2021 in SLP (Crl) No. 5191/2021.

[20] PIB Delhi, Digital Arrest Scam (December 10, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2082761.

[21] Digital Arrests: The New Frontier of Cybercrime https://www.msspalert.com/native/digital-arrests-the-new-frontier-ofcybercrime

[22] https://www.digit.in/news/general/digital-arrest-scam-mumbai-woman-forced-to-strip-loses-rs-17-lakh.html/amp/?merchant=all

[23] https://www.hdfcbank.com/personal/resources/learning-centre/vigil-aunty/how-digital-arrest-fraud-works

[24] https://www.vifindia.org/article/2024/november/26/The-Growing-Problem-of-Digital-Arrest-Scams-in-Bharat

[25] https://www.pmfias.com/digital-arrest/