International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Revolution of Digital Scams and Right to Privacy in India

Ms. Amrutha Bharathan Karamvalappil

Assistant Professor, Political Science, St.Mary's College Puthanangadi, Malappuram

Abstract

The integration of digital technologies has transformed the human interaction, commerce and information sharing, starting from shopping to instant messaging; people now rely on digital platforms for almost every aspect of daily life. With great convenience it has drastically increased efficiency and productivity, improved collaboration and communication leading to new innovation and opportunities to learning and adverse knowledge. But, like how the coin has two sides, the advance in technology has its pros and cons. It has led to the introduction of new threats, particularly digital scams. These scams target individuals by breaching personal information and invade their privacy. In India, the rise of digital platforms has expanded the scope of such scams, due to rapid adoption of smart phones and digital payment system, which encompasses activities like phishing, social engineering, and impersonation fraud. These scams exploit gaps in digital literacy and use sophisticated manipulation techniques to deceive users, posing severe risks to financial security and privacy. The right to privacy, established as a fundamental right, ensures every individual a control over their personal information and autonomy in making decisions without interference. The significance of the right to privacy has intensified, owing mostly to the growing influence of social media and the internet in this contemporary digital landscape. This right is frequently compromised by extensive data collection practices by both government and private entities, as well as by cybercriminals. The concept of digital arrest has also emerged and helped in serving as a tool for law enforcement to monitor or restrict online activity for various security purposes. However, the scammers often bypass the security firewalls, threatening individuals to extort money under the pretence of legal action. This paper explores the complex balance between safeguarding citizens from digital scams and upholding their right to privacy in this data-driven digital age.

Digital Revolution: An Introduction

Digital footprints are all over the place. Each time you visit a website, enter your personal information, credit or debit card information, sign up for an account, deliver your email, fill out online forms, post on social media, or store images or documents in cloud storage, you release personal information into cyberspace. India's digital revolution is a remarkable journey that has reshaped its socio-economic landscape. India has emerged as a global digital powerhouse. Recently, India has jubilee with 9 successful years in implementing the program of Digital India enabling 1.3 billion Indians a biometric, digital identity. Also, Digital India has complemented government programs such as Make in India, Startup India, and Atmanirbhar Bharat, enhancing the economy and rendering India as a centre for technological capital and industrial production. The nation attained status as one of the most advanced global fintech ecosystems. As a result, the ease of doing business has improved considerably, bringing it easy for business owners to start and expand their start-ups.

Key Milestones and Drivers

Smartphone Adoption: A significant percentage of the Indian population is now able to utilize digital services because to the widespread availability of inexpensive smartphones.

Digital India Initiative: Launched in 2015, the Digital India campaign has been a significant government push towards digital transformation. It aimed to improve digital infrastructure, increase digital literacy, and deliver government services electronically. Key projects under this initiative include BharatNet (to connect rural areas with broadband), DigiLocker (for digital document storage), and Aadhaar, the world's largest biometric identification program, which serves as a foundation for digital identity.

Rise of Digital Payments: The emergence of digital payments has been enabled by India's Unified Payments Interface (UPI), which has made it accessible to simple and fast bank transfers. India is currently a global leader in real-time digital payments because of UPI, which has accelerated the acceptance of digital payments even in rural and small towns, encouraging a cashless economy. According to the Reserve Bank of India's (RBI) latest annual report, the value of UPI transactions climbed 137% in the past two years, to INR200 trillion (USD199 billion) (Digital fraud: India's wild frontier, 2024).

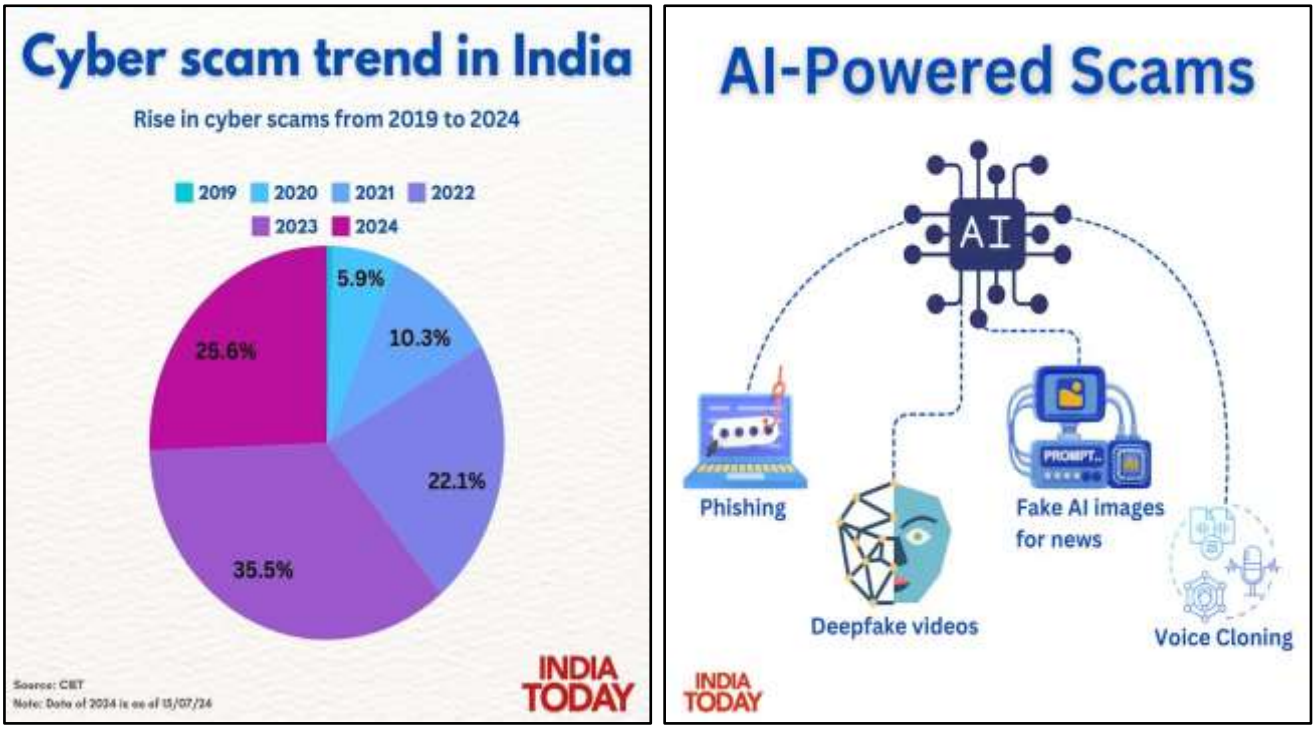
E-commerce and Social Media Growth: Social media sites like Facebook and WhatsApp, as well as e-commerce behemoths like Amazon and Flipkart, have become essential parts of Indian customers. Particularly during the COVID-19 epidemic, when online buying and digital engagement further increased, digital platforms have become crucial for both consumers and small enterprises.

Digital scams in India: Trends and Tactics

The rapid digitization of services and the growing dependence on technology in everyday life have contributed to an exponential rise in digital scams in India such as cyber security risks, data privacy issues, and gaps in digital literacy. Digital scams refer to a broad category of online frauds that target the assets of people or organizations, such as data, money, or personal information. Digital frauds, on the other hand, have also emerged as a serious hazard in this age of convenience and connectivity. These malevolent actions frequently jeopardize people's privacy and personal information by taking advantage of the weaknesses brought forth by massive data collection. Numerous sources launch cyberattacks with the goal of obtaining or abusing personal information.

The most prevalent cybercrimes include:

1. Phishing and Identity Theft: Cybercriminals use deceptive emails, fake websites, and social engineering techniques to steal sensitive information such as bank credentials and personal identification details.
2. Financial Frauds: Cases of UPI fraud, credit card fraud, and fake investment schemes have increased due to the proliferation of digital payment systems.
3. Social Media Scams: Cybercriminals exploit social media platforms to impersonate individuals, commit extortion, and engage in romance scams.
4. AI-Based Threats: The emergence of deepfake technology and AI-driven cyberattacks has further complicated digital security challenges



Source: (Sharma & Shah, 2024)

The Right to Privacy in the Indian Context: Legal Framework

The right to privacy in India has evolved through judicial interpretation and constitutional amendments, culminating in its recognition as a fundamental right. This legal framework comprises constitutional provisions, judicial pronouncements, and statutory laws. The Indian Constitution does not explicitly mention the right to privacy. However, the Supreme Court has interpreted it as an essential part of the Right to Life and Personal Liberty under Article 21. K.S. Puttaswamy v. Union of India (2017): This landmark judgment unanimously recognized privacy as a fundamental right under Article 21. The Supreme Court ruled that privacy is intrinsic to human dignity and individual autonomy. Article 19: Protects freedom of speech and expression, which includes the right to control personal information. Article 20(3): Provides protection against self-incrimination, reinforcing an individual's right against forced disclosure of personal data.

Digital Arrest: A new age threat

Digital arrest scams in India have emerged as a significant form of cybercrime, exploiting advancements in technology and the growing reliance on digital communication. The rise of such scams reflects a broader trend of escalating cybercrime in India, with losses from digital financial fraud alone reaching approximately 1.25 lakh crore over three years, including a staggering 66.66 crore reported in 2023 (Reddy, 2024). Digital arrest scams specifically gained notoriety as criminals adopted more sophisticated methods to instill fear and manipulate victims. Typically, these scams initiate with unsolicited phone or video calls from individuals impersonating law enforcement officials, such as representatives from the Central Bureau of Investigation (CBI) or local police departments. The scammers falsely accuse victims of serious crimes, such as financial fraud or drug trafficking, creating a panic situation that pressures victims into compliance. The development of these scams can be seen as a response to increased awareness and regulation around traditional financial scams. By leveraging technology and creating elaborate

stories that mimic official legal procedures, scammers have managed to bypass some of the safeguards that individuals might normally rely on when dealing with financial transactions. Following are the recent cases:

1. **Case 1: High-Profile Businessman Defrauded:** In September 2024, S.P. Oswal, chairman of Vardhman Group, was deceived by fraudsters posing as federal investigators. They orchestrated a fake online Supreme Court hearing, complete with an impersonator of former Chief Justice of India D.Y. Chandrachud, coercing Oswal into transferring approximately ₹6.9 crore ($830,000) under the threat of arrest. Authorities arrested two individuals and recovered $600,000, marking a significant recovery in such cases.
2. **Case 2: Senior Citizen Duped by Fake Law Enforcement:** A 72-year-old woman received a call from individuals claiming to be police officers, informing her of a legal case against her. Under the pretext of helping her avoid arrest, they coerced her into transferring a substantial amount of money.
3. **Case 3: Doctor Defrauded Through Video Call: Dr**. Anvitha, a renowned doctor, received a late-night call from someone posing as a CBI officer, claiming a money laundering warrant was issued against her. She was told she was under digital arrest and must participate in a video call. Terrified, Dr. Anvitha transferred ₹70 lakh to the scammer's account.
4. **Case 4: 70-year Old Retired Engineer Tricked To Losing His Life Savings:** A 70-year-old retired engineer from Delhi lost over Rs 10 crore to fraudsters who impersonated law enforcement officials. The scammers deceived him into transferring his life savings by fabricating a story about a drug parcel linked to his name and threatening him with arrest.

However, social media and online footprints have become crucial in legal actions, playing a role in both civil and criminal cases. Photos, videos, and status updates can be used as evidence in court, whether in divorce cases, personal injury claims, or criminal investigations. GPS tracking from posts can confirm or dispute alibis. Private communications can be subpoenaed as evidence. Online statements can lead to libel or slander lawsuits. Cyber bullying and harassment on social platforms can result in restraining orders or criminal charges. Unauthorized sharing of copyrighted material on social media can lead to legal action. Businesses monitor social media for trademark violations. Leaking private information or hacking into accounts can result in lawsuits or criminal charges. Some regions allow individuals to request removal of certain online data under privacy laws. The legal records and public interest matters however, may not be erasable.

Risk in Cyber security

Many users do not understand privacy settings, making them vulnerable to data exploitation. Misinformation and fake news spread rapidly, influencing public opinion and legal cases. People unknowingly share self-incriminating content, which can be used in legal actions. Businesses and employees may not follow cyber security best practices, leading to increased risks. India's IT laws, such as the Information Technology Act, 2000 and the Intermediary Guidelines, have been criticized for their potential misuse. Authorities have used IT regulations to curb dissent, remove content from social media, and prosecute individuals for online speech. The Digital Personal Data Protection Act, 2023 raises concerns about exemptions granted to government agencies for surveillance and data collection. The lack of judicial oversight in takedown requests and website bans threatens free expression and digital rights.

Policy Recommendations and Solutions

To address the growing challenges of digital scams and privacy concerns in India, a multi-faceted approach is required. Strengthening cybersecurity, implementing comprehensive data protection laws, increasing public awareness, and ensuring ethical surveillance practices are critical steps toward a safer digital ecosystem.

- The government must establish a well-defined, proactive cybersecurity strategy that includes real-time monitoring and response mechanisms for cyber threats.
- Encouraging businesses and public institutions to invest in cybersecurity technologies, such as AI-based threat detection, blockchain for secure transactions, and encryption tools.
- Sectors like banking, healthcare, and governance require robust cybersecurity frameworks to prevent large-scale data breaches.
- Collaboration between government agencies, private sector companies, and cybersecurity firms can enhance India's overall digital security.
- A specialized unit to handle emerging cyber threats, coordinate with law enforcement agencies, and assist victims of digital fraud.
- India's *Digital Personal Data Protection Act, 2023* needs effective enforcement mechanisms to protect user data from unauthorized access and misuse.
- Individuals should have clear rights over their personal data, with the ability to control its collection, storage, and deletion.
- Limiting data retention periods and ensuring businesses and government agencies comply with transparent data-handling practices.
- A regulatory body to monitor compliance, investigate data breaches, and impose penalties on violators.
- Launching awareness programs to educate citizens, especially in rural areas, about common digital scams and cybersecurity best practices.
- Teaching students about online safety, privacy risks, and responsible digital behavior.
- Given India's linguistic diversity, scam awareness campaigns should be available in multiple languages through TV, radio, social media, and local outreach programs.
- Banks and digital payment platforms should have clear fraud-reporting processes, quick grievance redressal mechanisms, and strong customer support.
- Authorities must provide accountability mechanisms to prevent the misuse of surveillance tools against citizens.
- Any government action related to online monitoring, content takedowns, or arrests based on digital activity should be subject to judicial scrutiny.
- While law enforcement agencies require access to digital data to combat crime, policies must prevent unwarranted mass surveillance and ensure civil liberties are protected.
- Encouraging ethical reporting of privacy violations and illegal data collection practices by both public and private entities.

Conclusion

India's rapid digital revolution has opened up a world of possibilities for technical innovation, financial inclusion, and economic prosperity. But technology has also brought about hitherto uncommon difficulties, such as cybersecurity threats, privacy invasions, and online frauds. Cybercriminals actively

take advantage of the vulnerabilities brought forth by the broad use of digital services, regulatory monitoring deficiencies, and digital literacy gaps. The pressing necessity for all-encompassing digital security measures is highlighted by instances of phishing, financial fraud, social engineering schemes, and the growing possibility of digital arrests. At the heart of these concerns lies the fundamental right to privacy. While judicial precedents, such as the *K.S. Puttaswamy v. Union of India* ruling, have recognized privacy as a fundamental right, existing data protection laws remain inadequate in addressing emerging threats. Moreover, the misuse of surveillance technologies and IT laws poses risks to democratic freedoms, requiring a delicate balance between national security and individual rights. To navigate these challenges, India must adopt a multi-pronged approach. Strengthening cybersecurity infrastructure, enforcing robust data protection legislation, enhancing public awareness, and ensuring ethical law enforcement practices are critical steps in safeguarding digital rights. A proactive legal and policy framework, backed by stringent implementation and judicial oversight, can help curb digital fraud while protecting citizens from privacy violations and unlawful surveillance. The future of India's digital ecosystem depends on the collective efforts of the government, private sector, and civil society. By fostering a culture of cybersecurity awareness, ethical digital governance, and strong legal protections, India can build a resilient digital economy—one that prioritizes both innovation and the fundamental rights of its citizens. The digital revolution should not come at the cost of individual freedoms, but rather empower every Indian to engage confidently and securely in the digital age.