THE SCIENTIFIC TEMPER (2026) Vol. 17 (4): 6184-6190

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2026.17.4.28

https://scientifictemper.com/

RESEARCH ARTICLE

India's Digital Banking Era: Cyber Fraud Targeting Women and Senior Citizens from Legal and Socio-Economic Perspectives

Kuku Ram Kanojia[1*], Rajesh Kumar Singh[2]

Abstract

The evolution of digital banking in India can be traced back to the early 2000s, particularly following the global concerns surrounding the Y2K crisis, which accelerated advancements in information technology and cybersecurity. Over time, experts have worked extensively to counter threats such as phishing, vishing, data breaches, and SQL-based attacks. While technological systems have become more stable and secure, cybercriminals have simultaneously developed increasingly sophisticated techniques to exploit financial systems.

In recent years, digital payment platforms—especially Unified Payments Interface (UPI) and Aadhaar-enabled payment systems (AePS)—have significantly enhanced financial inclusion across India. Spearheaded by institutions such as the Government of India, the Reserve Bank of India (RBI), and the National Payments Corporation of India (NPCI), these systems have made financial services accessible to millions. However, this rapid digital expansion has also led to a surge in cyber fraud, disproportionately affecting vulnerable groups, particularly women and senior citizens.

These groups are often targeted through deceptive practices such as phishing messages disguised as official communications, impersonation scams, and coercive tactics like "digital arrest" frauds. Such crimes exploit not only technological gaps but also socio-cultural vulnerabilities, including limited digital literacy and trust-based social behavior.

Recent data highlights the severity of the issue. In 2025 alone, the National Cybercrime Reporting Portal recorded over 76,000 cybercrime incidents involving women. Similarly, senior citizens—especially those living in isolation—have suffered significant financial losses. Studies indicate that nearly half of individuals in these categories struggle to identify fraudulent schemes due to limited awareness and digital skills.

This study adopts a doctrinal and socio-legal approach, examining statutory frameworks such as the Information Technology Act, 2000, along with recent reforms under the Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023. It identifies critical gaps in existing legal mechanisms and highlights the need for adaptive and responsive regulatory structures.

To address these challenges, the paper proposes targeted interventions, including real-time fraud alerts within banking interfaces, enhanced cybercrime investigation infrastructure, improved coordination among enforcement agencies, and the introduction of compensation mechanisms for victims. These measures aim to shift the focus from reactive enforcement to proactive prevention.

Additionally, the study draws upon ethical principles from Buddhist philosophy, emphasizing values such as non-violence (ahimsa) and mindfulness (sati), to frame cyber fraud not merely as a legal violation but as a broader moral concern.

Keywords: Cyber Fraud in India, Digital Banking Security, UPI Fraud Prevention, IT Act 2000, Bharatiya Nyaya Sanhita, Women Victims of Cybercrime, Senior Citizen Fraud, Digital Arrest Scams, Digital Literacy, Cybersecurity Policy

Introduction

India's banking sector has experienced a profound digital transformation, largely driven by innovations such as the Unified Payments Interface (UPI) and Aadhaar-based authentication systems. By 2025, UPI had become a cornerstone of everyday financial transactions, processing billions of transactions monthly and reshaping the financial ecosystem. These developments have significantly advanced financial inclusion by enabling access for rural populations, informal workers, and previously unbanked individuals.

Digital platforms—including mobile banking applications, internet banking services, and instant payment systems—have created a highly interconnected financial environment aligned with the broader vision of Digital India. Despite these advancements, the rapid expansion of digital infrastructure has also given rise to a parallel increase in cyber fraud, resulting in substantial financial losses and declining public trust.

Within this evolving landscape, women and senior citizens have emerged as particularly vulnerable groups.

Received: 10/04/2026 **Accepted:** 23/04/2026 **Published:** 25/04/2026

[1]PhD Scholar, Parul Institute of Law, Parul University, Vadodara, India

[2]PhD, Associate Professor of Law, Parul University, Vadodara, India

***Corresponding Author:** Kuku Ram Kanojia, PhD Scholar, Parul Institute of Law, Parul University, Vadodara, India, E-Mail: kr.kanojia@gmail.com

How to cite this article: Kanojia, K.R., Singh, R.K. (2026). India's Digital Banking Era: Cyber Fraud Targeting Women and Senior Citizens from Legal and Socio-Economic Perspectives. The Scientific Temper, **17**(4):6185-6190.

Doi: 10.58414/SCIENTIFICTEMPER.2026.17.4.28

Source of support: Nil

Conflict of interest: None.

Women, despite comprising nearly half of India's population, continue to face barriers in digital access and literacy. Socio-economic constraints such as limited education, restricted mobility, and domestic responsibilities often reduce their exposure to digital technologies. As a result, they are more susceptible to fraudulent schemes that exploit trust and lack of technical awareness.

Similarly, senior citizens encounter distinct challenges, including limited familiarity with digital tools, physical isolation, and a tendency to trust authoritative figures. Fraudulent practices such as impersonation by officials and coercive "digital arrest" scams have led to severe financial losses among this demographic, often affecting their life savings.

The disproportionate targeting of these groups reflects a combination of structural inequalities, behavioral vulnerabilities, and technological gaps. Lower levels of digital literacy among women and cognitive or social vulnerabilities among elderly individuals create opportunities for cybercriminals to exploit.

Although India has established a legal framework to address cybercrime—including the Information Technology Act, 2000, and recent criminal law reforms—implementation challenges remain significant. Low conviction rates, delays in investigation, and limited victim compensation mechanisms undermine the effectiveness of these laws. Additionally, existing cybersecurity measures often struggle to keep pace with emerging threats such as AI-driven fraud and deepfake technologies.

This paper argues for the development of a comprehensive and protective legal framework that integrates both preventive and punitive approaches. It emphasizes the need for stronger legal enforcement, enhanced digital literacy initiatives, and proactive risk mitigation strategies.

Drawing from socio-legal theory and ethical perspectives, including principles derived from Buddhist philosophy, the study advocates a balanced approach that combines legal accountability with moral responsibility. Such an approach not only addresses the consequences of cyber fraud but also seeks to prevent its occurrence through awareness, education, and systemic safeguards.

The structure of the paper is as follows:

- Section 2 reviews existing literature on cyber fraud and vulnerable populations.
- Section 3 outlines the research methodology.
- Section 4 presents empirical findings based on official data.
- Section 5 critically examines the legal framework.
- Section 6 provides comparative international perspectives.
- Section 7 offers policy recommendations.
- Section 8 concludes with future directions and ethical considerations.

By integrating legal analysis, technological insights, and ethical reflection, this study aims to contribute to a more inclusive and secure digital financial ecosystem. Ensuring the protection of vulnerable groups is essential not only for justice but also for sustaining trust in India's digital growth trajectory.

Literature Review

The rapid expansion of digital banking in India has generated extensive academic discussion, particularly in relation to cyber fraud and its uneven impact on vulnerable populations such as women and older adults. Existing research highlights a complex situation in which technological progress intersects with socio-economic inequalities, thereby increasing exposure to cyber risks.

Scholars have emphasized the psychological dimension of cyber fraud. For instance, recent studies point out that fraudsters frequently exploit behavioral tendencies such as trust in authority, urgency, and reciprocity to manipulate victims. These tactics are especially effective when directed at individuals with limited digital awareness. Industry reports further indicate a significant rise in cyber incidents affecting senior citizens over the past few years, attributing this increase to social isolation, reduced digital familiarity, and inadequacies in user-friendly banking interfaces.

Gender-based disparities in digital access have also been widely documented. Empirical research demonstrates a persistent gap between men and women in terms of digital literacy and secure financial practices, particularly in rural areas. This divide increases women's susceptibility to online fraud, especially phishing attacks and identity-related crimes. Scholars examining socio-legal dimensions argue that such vulnerabilities are reinforced by structural inequalities, including restricted access to education and technology, as well as social norms that limit independent digital engagement.

Recent statistical evidence further illustrates the severity of the issue. Data from official cybercrime reporting platforms show a consistent rise in complaints involving women, including cases of online harassment, impersonation, and financial fraud. These trends are exacerbated by emerging technologies such as deepfakes and social media manipulation. In the case of senior citizens, research highlights a pattern of fraud driven by emotional manipulation—often described as a combination of fear, greed, and lack of awareness—which significantly impairs their ability to recognize fraudulent schemes.

Legal scholarship has critically examined the adequacy of India's cyber law framework. Many authors argue that existing legislation, particularly the Information Technology Act, 2000, is largely reactive and does not sufficiently address preventive mechanisms. Although newer legal frameworks, such as the Bharatiya Nyaya Sanhita, introduce stricter punitive provisions, concerns remain regarding low conviction rates and limited mechanisms for victim compensation. Regulatory guidelines issued by financial authorities have improved compliance requirements, but they still lack targeted safeguards for vulnerable groups based on age or gender.

Interdisciplinary perspectives further enrich the literature. Surveys and reports indicate that elderly individuals are highly vulnerable to emotionally manipulative fraud, often due to cognitive decline and poorly designed digital interfaces. At the same time, studies focusing on women highlight issues such as underreporting of cybercrime due to social stigma and fear of reputational harm. Comparative analyses with international systems reveal that countries employing coordinated, multi-agency approaches have achieved better outcomes in fraud prevention.

Despite these contributions, several research gaps remain. There is limited longitudinal data on repeat victimization and the long-term psychological impact of cyber fraud. Additionally, behavioral economic approaches—such as the use of "nudges" to guide safer digital behavior—are not sufficiently integrated into current system designs. Ethical perspectives, though occasionally referenced, remain underdeveloped as a framework for policy formulation.

Recent policy developments indicate gradual progress. Proposals for victim compensation and improvements in cyber forensic infrastructure suggest a shift toward more responsive governance. However, critics argue that these measures remain inadequate in addressing large-scale financial losses and systemic vulnerabilities.

Overall, the literature points toward a clear need for integrated solutions that combine legal reform, technological innovation, and social awareness. This study builds upon existing scholarship by addressing overlooked areas such as intersectional vulnerability (e.g., elderly women), emerging payment technologies, and ethical approaches to cyber governance.

Materials and Methods

This research adopts a doctrinal legal methodology to examine the effectiveness of existing laws in addressing cyber fraud, particularly as it affects women and senior citizens. The study focuses on key legislative frameworks, including the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, with specific attention to provisions related to identity theft, impersonation, and digital fraud. Regulatory instruments such as guidelines issued by the Reserve Bank of India on digital payments and fraud risk management are also analyzed.

To support the legal analysis, the study incorporates empirical data from authoritative sources, including reports published by the National Crime Records Bureau, complaint data from the National Cybercrime Reporting Portal, and advisories issued by the Indian Cyber Crime Coordination Centre. These sources provide insights into trends, patterns, and typologies of cybercrime.

A socio-legal approach is further employed through qualitative analysis of judicial decisions and reported cases. A selection of court judgments and police reports has been examined to identify recurring themes such as delays in prosecution, challenges in evidence collection, and gaps in victim restitution. This thematic analysis allows for the identification of broader structural issues within the legal system.

Secondary sources, including research reports, policy documents, and institutional studies, are used to strengthen the analysis and ensure triangulation of findings. Analytical tools such as qualitative coding techniques are applied to organize and interpret data, enabling the identification of patterns across different sources.

An additional ethical perspective is incorporated to contextualize cyber fraud beyond its legal dimensions. Drawing on philosophical concepts related to harm, deception, and moral responsibility, the study frames cybercrime as not only a legal violation but also a broader societal concern requiring preventive and value-based approaches.

This combined methodology ensures a comprehensive evaluation of both the legal framework and its practical implementation, allowing the study to identify gaps and propose informed policy recommendations.

Empirical Observations

The current landscape of cyber fraud in India reflects a significant and continuing increase in incidents, particularly affecting vulnerable groups such as women and senior citizens. The expansion of digital banking and online financial services has created new opportunities for fraudsters, transforming routine financial transactions into potential points of exploitation.

Official data reveals a steady rise in reported cybercrime cases over recent years, with a substantial proportion

involving financial fraud. Women frequently encounter forms of cybercrime such as impersonation, phishing, and online harassment, while senior citizens are often targeted through schemes that exploit trust and emotional vulnerability.

The data also indicates that many victims lack the necessary digital awareness to identify and respond to fraudulent activities. In the case of elderly individuals, factors such as social isolation, limited technological familiarity, and reliance on others for digital transactions further increase susceptibility. For women, socio-economic constraints and limited access to digital education contribute to their vulnerability.

A notable trend is the growing sophistication of cyber fraud techniques. Fraudsters increasingly use advanced tools such as artificial intelligence, deepfake technology, and social engineering strategies to deceive victims. These methods make detection more difficult and increase the scale of financial losses.

Another important observation is the gap between reported incidents and actual enforcement outcomes. Despite the increase in complaints, conviction rates remain relatively low, and recovery of lost funds is often limited. This highlights challenges in investigation, evidence gathering, and legal processes.

Overall, the empirical evidence demonstrates that cyber fraud is not only increasing in frequency but also evolving in complexity. The disproportionate impact on vulnerable populations underscores the need for targeted interventions, improved digital literacy, and stronger legal and institutional responses.

Fraud Trends

Recent data indicates a sharp increase in cyber fraud cases across India, with women and senior citizens experiencing a disproportionate rise.

Group	2024 Cases	2025 Cases	% Increase	Common Methods
Women	48,335	76,657	58.7%	Stalking, impersonation
Seniors	~10,000	17,000+	70%	Digital arrest scams, phishing

National-level statistics suggest that financial cybercrimes increased by approximately 25% in 2025, largely driven by the widespread use of digital payment platforms such as UPI. Cases involving women rose significantly from 48,335 in 2024 to 76,657 in 2025. Similarly, reported incidents affecting senior citizens grew from around 10,000 to over 17,000 during the same period.

Among women, impersonation-based fraud constituted a substantial proportion of cases, often involving manipulated audio-visual content or fabricated emergency situations. Senior citizens, on the other hand, were heavily targeted through "digital arrest" scams, resulting in financial losses exceeding ₹3,000 crore. These schemes typically involve fraudsters posing as law enforcement officials and coercing victims into transferring money under threat.

Demographic Vulnerabilities

The vulnerability of women to cyber fraud is closely linked to limited digital access and literacy. Estimates suggest that only about one-third of women are able to independently and securely use digital financial applications. Rural women, who represent a significant share of victims, are particularly exposed to phishing attempts through misleading SMS messages related to government schemes or financial benefits.

Online harassment also remains a major concern. A large number of complaints relate to cyberstalking and misuse of personal information, often facilitated through social media platforms. These experiences not only result in financial harm but also have serious psychological consequences.

For senior citizens, vulnerability is shaped by different factors. With a population exceeding 150 million, many older individuals face challenges such as social isolation, reduced familiarity with digital technologies, and declining cognitive abilities. Studies indicate that a significant proportion of elderly users are unable to recognize fraudulent cues, making them more susceptible to deception. Trust in unsolicited phone calls and messages further increases their risk exposure.

Urban elderly populations have also reported higher financial losses, particularly in cases involving ATM fraud and mobile-based compromises. When gender and age intersect, risks become even more pronounced. Elderly women, for example, experience higher rates of victimization due to the combined effects of social stigma and age-related limitations.

Case Studies

Selected case examples provide insight into the operational patterns of cyber fraud:

Case 1: Digital Arrest Fraud (Delhi, 2025)

A 72-year-old woman was deceived into transferring ₹50 lakh after receiving a video call from an individual posing as a law enforcement officer. Although legal action was initiated under relevant cybercrime provisions, only a small portion of the funds could be recovered. This case highlights how fear-based tactics are particularly effective against elderly individuals.

Case 2: UPI Refund Scam (Mumbai, 2025)

A young woman lost ₹8 lakh in a fraudulent UPI refund scheme. The situation escalated when the perpetrator engaged in threats and harassment. Although the platform involved was eventually blocked, the victim continued to

face emotional distress. This illustrates the dual financial and psychological impact of cybercrime on women.

Case 3: Phishing Network (Bengaluru, 2025)

An elderly couple lost approximately ₹2 crore after responding to a fraudulent email disguised as a bank communication. Investigations revealed links to an international cybercrime network. The case demonstrates the complexity of cross-border fraud and the limitations of domestic enforcement mechanisms.

Analysis of multiple such cases indicates frequent delays in investigation and trial processes, along with low recovery rates of stolen funds.

Scam Typologies

Cyber fraud techniques have evolved significantly in recent years. Phishing attacks increasingly involve advanced tools such as AI-generated voice messages, making them more convincing and difficult to detect. "Digital arrest" scams have seen a substantial rise, emerging as one of the most financially damaging forms of fraud.

Impersonation tactics are often combined with voice-based fraud (vishing), particularly targeting senior citizens who are more likely to trust authority figures. In cases involving women, cyberstalking frequently extends beyond the digital space into real-world harassment.

Fraudulent schemes disguised as promotional offers or lottery winnings have also become widespread, with a large number of victims being women. These scams typically rely on urgency and misinformation to prompt immediate financial transactions.

Economic Impact

The financial impact of cyber fraud in India has reached alarming levels. Total reported losses in the financial year 2025 exceeded ₹1.37 lakh crore, with a notable portion linked to vulnerable groups.

Senior citizens alone accounted for losses of over ₹3,500 crore in specific scam categories such as "digital arrests." For women, the economic impact extends beyond direct financial loss to include indirect costs such as lost income, legal expenses, and psychological support.

Although regulatory authorities have taken steps to block fraudulent communication channels, cybercriminals continue to adapt their methods. A significant number of cybercrime complaints remain unreported or unresolved, further complicating the assessment of actual economic damage.

Reporting Gaps

Underreporting remains a major challenge in addressing cyber fraud. Women often hesitate to file complaints due to concerns about privacy, social stigma, or reputational harm. Senior citizens, meanwhile, may face difficulties navigating reporting mechanisms due to limited technological proficiency.

Institutional constraints further aggravate the problem. Many rural areas lack adequate cyber forensic infrastructure, while urban enforcement agencies are often overburdened with a high volume of cases. These gaps hinder timely investigation and effective resolution of complaints.

Legal Framework Analysis

India has developed a comprehensive legal framework to combat cybercrime. However, its effectiveness in protecting vulnerable groups remains limited due to gaps in implementation and design.

Existing Laws

The Information Technology Act, 2000, along with subsequent amendments and regulatory rules, forms the foundation of India's cyber law regime. Key provisions include penalties for identity theft, impersonation, and data breaches, along with provisions for compensation in cases of negligence by service providers.

The Bharatiya Nyaya Sanhita, 2023, which replaces the earlier penal code, incorporates cyber-related offenses into the broader criminal law framework. It addresses offenses such as cheating, fraud, and organized criminal activity, including those conducted through digital means.

In addition, the Reserve Bank of India has issued guidelines to strengthen fraud prevention and customer protection. These include requirements for timely reporting of fraud, classification of incidents, and limited liability for customers in unauthorized transactions.

Institutional mechanisms such as the Indian Cyber Crime Coordination Centre and cybercrime police units support enforcement through investigation, training, and coordination across jurisdictions.

Judicial decisions have also played an important role in shaping cyber law by clarifying issues such as intermediary liability and content regulation.

Key Gaps and Limitations

Despite these developments, several shortcomings persist:

- **Lack of targeted protections:** Existing laws do not provide specific safeguards or enhanced penalties for crimes against vulnerable groups such as women and senior citizens.
- **Inadequate penalties:** Monetary fines and punishments are often insufficient compared to the scale of financial losses involved.
- **Low conviction rates:** Enforcement remains weak, with relatively few cases resulting in successful prosecution.
- **Limited restitution mechanisms:** Victims often face difficulties in recovering lost funds, particularly when legal procedures are complex.
- **Infrastructure constraints:** Many regions lack adequate forensic facilities and trained personnel.

- **Cross-border challenges:** A large proportion of cyber fraud originates from outside India, complicating enforcement efforts.
- **Platform accountability issues:** Digital platforms are not always subject to strict regulatory obligations, leading to delays in action against fraudulent activities.

Normative Critique

From a doctrinal perspective, India's cyber law framework is largely reactive, focusing on punishment after the occurrence of crime rather than prevention. There is limited emphasis on proactive measures such as risk identification, user protection, and system design improvements.

An ethical perspective further highlights the need to treat cyber fraud as a broader societal issue rather than merely a legal violation. Preventive strategies—such as improving digital literacy, enhancing user awareness, and designing safer technological systems—are essential for reducing risk.

Reform Pathways (India-Centric)

To address these challenges, the following reforms are suggested:

- **Legislative reform:** Introduce specific provisions addressing exploitation of vulnerable groups, with wstricter penalties.
- **Procedural improvements:** Simplify reporting mechanisms and prioritize cybercrime cases involving high-risk groups.
- **Regulatory measures:** Implement real-time monitoring systems and provide compensation frameworks for victims.
- **Capacity building:** Expand cyber forensic infrastructure and training programs for law enforcement agencies.
- **Awareness initiatives:** Promote digital literacy programs tailored to women and senior citizens.

Scope and Future Research

While this study examines the impact of cyber fraud on women and senior citizens within India's digital banking ecosystem, several areas require deeper investigation to strengthen future policy and legal responses.

One important direction is the need for intersectional research, particularly focusing on elderly women. This group faces overlapping vulnerabilities arising from both gender-based digital exclusion and age-related limitations such as social isolation and reduced technological familiarity. Future empirical studies could involve field surveys across multiple semi-urban regions, combined with longitudinal tracking of digital payment usage. Such research would help measure not only financial losses but also broader consequences, including psychological stress and reduced economic independence.

Technological innovation also presents significant research opportunities. The potential integration of blockchain-based transaction systems within digital payment platforms could enhance transparency and traceability. Similarly, the development of advanced tools to detect manipulated audio and video content—especially those tailored to regional languages and accents—could play a crucial role in fraud prevention.

Comparative studies across Indian states may further reveal disparities in enforcement capacity and institutional preparedness. For example, differences between urban cybercrime units and under-resourced rural policing systems could be systematically analyzed to identify best practices and gaps. In addition, behavioral research grounded in nudge theory may offer insights into how digital interfaces can be redesigned to guide users toward safer financial decisions, particularly those with limited digital literacy.

From an ethical standpoint, future scholarship may explore how principles such as awareness, responsibility, and non-harm can be embedded into digital financial systems. Awareness-based interventions—such as interactive or gamified training modules—could be tested for effectiveness through controlled experimental methods, especially among populations newly introduced to digital banking.

There is also a need for more robust quantitative analysis. Economic modeling could help estimate the broader macroeconomic impact of cyber fraud, including its effect on national productivity and financial stability. Additionally, studies on underreporting—particularly among women and elderly individuals—could utilize anonymous or technology-enabled reporting mechanisms to generate more accurate data.

Overall, future research should adopt an interdisciplinary approach, combining legal analysis, technological innovation, behavioral science, and ethical inquiry to address the evolving nature of cyber fraud in India.

Conclusion

India's rapid transition toward digital banking has significantly expanded financial inclusion, but it has also created new opportunities for cybercrime. The findings of this study indicate that women and senior citizens are disproportionately affected, experiencing both financial losses and psychological harm as a result of increasingly sophisticated fraud schemes.

An analysis of existing legal frameworks reveals that, although India has established comprehensive laws and regulatory mechanisms, these systems remain largely reactive. Challenges such as low conviction rates, delays in investigation, and limited compensation for victims continue to undermine their effectiveness. At the same time, structural factors—including gaps in digital literacy and behavioral vulnerabilities—further increase the risk faced by these groups.

To address these issues, a shift toward a preventive and inclusive approach is essential. Legal reforms must incorporate specific protections for vulnerable populations, while regulatory bodies should promote stronger risk detection systems and user-centric safeguards. Technological solutions, including AI-based monitoring and real-time alerts, must be complemented by widespread awareness and education initiatives.

Ultimately, the goal should be to create a digital financial environment that is not only efficient but also equitable and secure. Protecting vulnerable users is not merely a policy requirement—it is fundamental to sustaining trust in India's digital economy. Without meaningful intervention, the benefits of digital inclusion may remain unevenly distributed. With appropriate reforms, however, India can move toward a more resilient and just financial ecosystem.

Acknowledgements

The author expresses sincere gratitude to Prof. Dr. Rajesh Kumar Singh for his valuable academic guidance and insightful contributions, which significantly enhanced the analytical depth of this research. Appreciation is also extended to the Reserve Bank of India for providing access to relevant reports and regulatory materials that informed the empirical analysis.

The author acknowledges the support of the legal and compliance professionals at Bank of Baroda for sharing practical perspectives on banking fraud and regulatory challenges. Special thanks are due to Parul University and the Institute of Law for providing essential research infrastructure, including library facilities and access to legal databases such as Manupatra and Indian Kanoon.

Constructive feedback from academic peers and supervisors has been instrumental in refining the socio-legal and ethical dimensions of this work.

Conflict of Interest

The author declares that there are no conflicts of interest that could have influenced the research or its findings. This study has not received funding from any commercial organization, financial institution, or advocacy group.

All data and materials used in this research are derived from publicly available sources, including statutory provisions, government reports, and academic literature. Any professional affiliations mentioned are purely academic in nature and have not affected the objectivity or independence of the research.

References

Basu, S. (2018). *Cyber Law in India*. LexisNexis.

Future Crime Research Foundation. (2023). *Cyber Fraud Trends in India*.

Indian Cybercrime Coordination Centre (I4C). (2025). *National Cybercrime Report*. Ministry of Electronics and Information Technology.

Khera, P., et al. (2021). Gender disparities in digital access in rural India. *Journal of Development Studies*, 57(4), 567–589.

Kumar, A. (2020). Challenges in enforcing cyber laws in India. *Indian Journal of Criminology*, 45(2), 112–130.

Mehta, R. (2021). Evolving cyber law reforms in India. *NUJS Law Review*, 14(3), 45–67.

National Crime Records Bureau (NCRB). (2023–2025). *Crime in India Reports*. Ministry of Home Affairs.

National Cybercrime Reporting Portal (NCRP). (2025). *Annual Statistics Dashboard*.

Quick Heal Technologies. (2025). *Elder Fraud and Cybersecurity Report*.

Reserve Bank of India (RBI). (2023–2025). *Master Directions on Fraud Risk Management*.

Reserve Bank of India (RBI). (2026). *Draft Guidelines on Cyber Resilience*.

Sharma, R., & Gupta, P. (2022). Legal challenges in banking-related cyber fraud. *Indian Journal of Law and Technology*, 18(1), 23–45.

Tripathy, S. S. (2025). Psychological strategies in cyber fraud. *Legal Review Quarterly*, 12(2), 78–95.