JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

EMERGING TRENDS AND LEGAL RESPONSES TO CYBER FRAUDS IN INDIA: A DOCTRINAL ANALYSIS

Dr. Ajay Dayalji Patel
Assistant Professor
V.T. Choksi Sarvajanik Law College, Surat, (Gujarat) India
Email: ajay.patel873@gmail.com | Contact: +91 9904932093

Abstract

India's transition to a digital financial ecosystem has profoundly transformed patterns of commercial engagement and criminal opportunity. The proliferation of Unified Payments Interface (UPI) applications, e-commerce platforms, and mobile banking has streamlined financial transactions while simultaneously expanding avenues for cyber-enabled fraud. Adopting a doctrinal–analytical research approach, this paper investigates emerging typologies of cyber fraud and examines India's legal and institutional frameworks under the Information Technology Act (2000), Bharatiya Nyaya Sanhita (2023), and Digital Personal Data Protection Act (2023). Findings reveal that although statutory modernization has enhanced definitional precision and regulatory scope, enforcement deficits, limited technical capacity, and insufficient public awareness continue to facilitate cybercrime proliferation. The study concludes with recommendations for preventive education, institutional capacity building, and artificial-intelligence-driven fraud detection mechanisms.

Keywords: Cyber fraud, digital finance, UPI, data protection, India

1. Introduction

India's economic digitisation, propelled by the Digital India initiative and Jan Dhan Yojana, has reconfigured the modes of banking, commerce, and governance. Between 2017 and 2023, Unified Payments Interface (UPI) transactions rose from less than one billion per year to over 120 billion annually, positioning India as the world's highest-volume digital-payment market. While this transformation enhances financial inclusion, it simultaneously exposes systemic vulnerabilities within the digital ecosystem. According to the NCRB Crime in India Report (2023), India recorded 86,420 cybercrime cases—representing a 31 percent year-on-year increase—of which nearly 69 percent were financial in nature. Fraud now transcends urban–rural divides as low-digital-literacy users increasingly participate in electronic commerce.

This escalating trend raises two central questions for legal and policy scholarship. First, does India's modernised penal architecture adequately capture technology-mediated criminality? Second, are enforcement institutions sufficiently equipped to translate legislative innovation into practical deterrence? Addressing these questions requires a synthesis of statutory evolution, empirical trend analysis, and an evaluation of inter-institutional coordination mechanisms.

2. Literature Review

Global and Domestic Scholarship

Multidisciplinary research indicates that digitisation creates both economic opportunities and systemic vulnerabilities. For example, the Data Security Council of India (DSCI) reports that around 84 % of Indian organisations identify

phishing as their greatest cyber threat.[1] Similarly, the Indian Computer Emergency Response Team (CERT-In) documented more than 1.32 million cyber-security incidents by October 2023, including phishing, unauthorised network scanning, and ransomware.[2]

From a legal-scholarly perspective in India, Gupta & Taneja (2022) argue that fraud victimisation results from a "structural asymmetry" between fast-paced technology adoption and slow development of cyber-literacy among citizens.[3] Chaudhary (2021) critiques Indian law-enforcement responses as largely reactive, citing limited cyber-forensic training.[4] Nair (2022) emphasises that preventive education and community outreach (especially in regional languages) are key to reducing fraud victimisation.[5]

Internationally, the Organisation for Economic Co-operation and Development (OECD) frames cyber risks as "digital security risks" — emphasising economic and social impacts of digital incidents beyond just technical breaches.[6] The United Nations Office on Drugs and Crime (UNODC) report (2024) highlights the challenge of cyberfraud in emerging economies and calls attention to enforcement gaps and jurisdictional complexity.[7]

Indian legal commentaries recognise that the Bharatiya Nyaya Sanhita 2023 (BNS) modernises offences of cheating and personation via Sections 318 and 319, thereby aligning criminal law with digital realities.[8] Collectively, these analyses suggest that India's principal bottleneck lies not in the statute-book but in institutional execution and inter-agency synchronisation.

3. Research Objectives and Hypotheses

3.1 Objectives

1. To map the evolving patterns, typologies, and operational mechanisms of cyber frauds in India during the period 2020–2025.
2. To evaluate the adequacy and responsiveness of India's existing legal statutes—particularly the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023—in addressing electronic deception and digital impersonation.
3. To analyse the institutional frameworks and enforcement mechanisms of key agencies, including CERT-In, Reserve Bank of India (RBI), and the Indian Cyber Crime Coordination Centre (I4C), in managing and mitigating cybercrime.
4. To recommend comprehensive policy measures for strengthening prevention, detection, investigation, and prosecution of cyber frauds through legal and technological reform.

3.2 Hypotheses

1. Rapid digitalisation without a proportional increase in cyber awareness and education significantly amplifies citizens' susceptibility to fraud.
2. The Bharatiya Nyaya Sanhita (2023) represents a substantive advancement in India's cyber law framework by integrating digital fraud offences into the mainstream penal structure.
3. Institutional and forensic capacity deficits within investigative agencies reduce the overall efficiency and deterrent effect of cyber law enforcement.
4. Nationwide cyber awareness initiatives—if systematically implemented and evaluated—can lead to measurable reductions in the incidence and severity of cyber fraud.

---

1. Data Security Council of India (DSCI), India Cybersecurity Domestic Market 2023 Report (2023).
2. Indian Computer Emergency Response Team (CERT-In), Annual Report 2023: Cyber-Security Incidents in India (Ministry of Electronics & IT, New Delhi).
3. N. Gupta & P. Taneja, "Cyber Fraud and Digital Vulnerability in India" (2022) 14 Indian Journal of Law & Technology 34.
4. A. Chaudhary, "Cyber Crime and Legal Challenges in India" (2021) 12 Journal of Indian Law Review 45.
5. S. Nair, "Citizen Awareness and Digital Fraud Prevention" (2022) 8 Asian Law & Society Review 112.
6. Organisation for Economic Co-operation & Development (OECD), Digital Security Risk Management: Policy Insight (2023) https://www.oecd.org/digital-security/
7. United Nations Office on Drugs & Crime (UNODC), Transnational Organised Crime & Convergence of Cybercrime & Corruption (2024).
8. Bharatiya Nyaya Sanhita 2023 (Act No 45 of 2023) ss 318–319; Legal Bites, "Cheating under Section 318 of BNS: Explained" (2025).

4. Research Methodology

This study employs a qualitative doctrinal–analytical approach grounded in secondary data to examine the legal and institutional dimensions of cyber fraud in India. It analyses primary legal sources, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, alongside supplementary materials such as Reserve Bank of India circulars, NCRB Crime in India Report 2023, and the India Cyber Threat Report 2025 by the Data Security Council of India. The research also adopts a comparative perspective, contrasting India's cyber governance framework with international models such as the EU's GDPR and the US CCPA, to identify best practices and policy gaps. As official data on victims and enforcement outcomes remain limited, the analysis relies on authenticated government publications and peer-reviewed literature available up to October 2025.

5. Emerging Trends in Cyber Frauds in India

India's cybercrime landscape has evolved dramatically over the last five years, with the most recent data from CERT-In, NCRB, and the Data Security Council of India (DSCI) (2025) revealing sophisticated, multi-dimensional fraud patterns that transcend geography and class. The following analysis highlights key emerging trends that define the present phase of cyber fraud in India, particularly between 2021 and 2025.

5.1. Technological Sophistication and AI-Driven Deception:

Artificial intelligence and deepfake technologies have transformed the contours of identity fraud in India's digital ecosystem. Corporate executives have reported incidents of voice and facial replication leading to unauthorised fund transfers. According to the CERT-In Annual Report 2025, AI-generated impersonation and synthetic identity crimes increased by nearly 230 per cent compared to 2023.[9] These developments blur evidentiary boundaries between human and algorithmic actors, posing complex challenges to establishing mens rea in digital jurisprudence.

5.2. Digital Arrest and Law-Enforcement Impersonation:

A rising trend known as the "digital arrest" scam involves perpetrators posing as officers from central investigative agencies such as the Central Bureau of Investigation (CBI) or Enforcement Directorate (ED). Victims are coerced during video calls and threatened with money-laundering charges unless they transfer funds for verification. The Indian Cyber Crime Coordination Centre (I4C) documented over 100,000 such complaints between 2024 and 2025.[10] Under the Bharatiya Nyaya Sanhita, 2023, these acts constitute coercive extortion and criminal intimidation under Sections 319 and 326, punishable as offences committed through digital means.[11]

5.3. Investment and Cryptocurrency Frauds:

Fraudulent "investment communities" on messaging platforms like Telegram and WhatsApp continue to lure citizens with the promise of high returns from crypto-trading applications. A 2025 India Today investigation reported cumulative losses exceeding ₹1,500 crore, affecting around 30,000 individuals.[12] Weak oversight of virtual assets and data storage on offshore servers impede domestic regulatory intervention. The Reserve Bank of India (RBI) and Ministry of Finance have since initiated consultations on extending financial surveillance mechanisms to cryptocurrency exchanges operating within India.[13]

5.4. Remote-Access Application Manipulation:

Fraudsters now deploy remote-access applications (RAAs) disguised as customer-service interfaces, harvesting permissions to control victims' banking applications. CERT-In data indicate a 34 per cent year-

[9] . Computer Emergency Response Team of India (CERT-In), Annual Report 2025: Cyber-Security Incidents in India (Ministry of Electronics & IT, New Delhi).

[10] . Indian Cyber Crime Coordination Centre (I4C), National Cyber Crime Reporting Portal Data 2024–2025 (Ministry of Home Affairs, 2025).

[11] . Bharatiya Nyaya Sanhita 2023 (Act No 45 of 2023), ss 319–326.

[12] . India Today, "Crypto Scam: ₹1,500 Crore Lost by 30,000 Indians in Telegram Fraud Ring" (June 2025).

[13] . Reserve Bank of India, Consultation Paper on Virtual Asset Regulation (2025).

over-year increase in such cases in 2024–2025.[14] These attacks depend more on social engineering than technical exploitation, exposing the critical role of consumer awareness in fraud prevention.

5.5. Rural Penetration and Socio-Economic Vulnerability:

Between 2021 and 2024, the National Crime Records Bureau (NCRB) recorded a 600–800 per cent surge in cybercrime complaints from rural districts.[15] Rapid smartphone adoption and mobile-based microfinance have expanded the reach of digital services but simultaneously exposed low-literacy populations to phishing scams disguised as Know Your Customer (KYC) verifications. The linkage between financial inclusion and cyber vulnerability underscores the necessity of regional language awareness campaigns and rural digital training initiatives.

5.6. Cross-Border Fraud Networks:

Collaborative reports between Interpol and I4C in 2025 reveal that several organised cybercrime networks operate from servers located in Cambodia, Myanmar, and the Philippines.[16] These transnational operations exploit weak jurisdictional coordination, prompting India to reinforce Mutual Legal Assistance Treaties (MLATs) and expedite extradition procedures for cyber offenders.[17]

5.7. Demographic Shift Toward Educated Victims:

The Data Security Council of India (DSCI) Cyber Threat Report 2025 identifies a notable shift in victim demographics: 74 per cent of reported cyber fraud victims now belong to the 30–55 age group, comprising professionals, small business owners, and entrepreneurs.[18] This trend dispels the notion that digital literacy guarantees cyber resilience, highlighting the universality of susceptibility in a hyper-connected economy.

5.8. Synthesis and Implications:

Collectively, these data illustrate that cyber fraud in India has evolved into an industrialised and borderless enterprise. The convergence of artificial intelligence, cryptocurrency markets, and cross-border data flows has transformed cybercrime from isolated incidents into a systemic threat to national security and economic stability.[19] Addressing these risks requires institutional interoperability among law-enforcement bodies, regulators, and technology intermediaries, as well as sustained investment in cyber-forensic capacity, international cooperation, and public digital awareness.[20]

6. Legal and Institutional Framework

6.1. Legal Framework

- **Information Technology Act, 2000 and CERT-In Directions:**

The Information Technology Act, 2000 continues to serve as India's foundational cyber law. Sections 43, 66C, and 66D impose liability for unauthorised access, identity theft, and cheating by personation through electronic means.[21] The Indian Computer Emergency Response Team (CERT-In), exercising powers under Section 70B, issued the Cyber Security Directions 2022, mandating that all organisations report cyber incidents within six hours of detection.[22] This regulatory mechanism strengthens early incident response and evidentiary integrity in cyber-fraud investigations.

- **Bharatiya Nyaya Sanhita, 2023:**

The Bharatiya Nyaya Sanhita, 2023 (BNS), which replaces the Indian Penal Code, introduces technology-neutral language to address electronic frauds. Sections 316 and 317 criminalise cheating and personation

[14]. CERT-In (n 1).
[15]. National Crime Records Bureau (NCRB), Crime in India Report 2025: Cyber Crime Statistics (Ministry of Home Affairs, New Delhi).
[16]. Interpol–I4C Joint Report, Transnational Cyber Fraud Operations in South and Southeast Asia (2025).
[17]. Ministry of External Affairs, India's Mutual Legal Assistance Treaties and Cybercrime Cooperation Framework (2025).
[18]. Data Security Council of India (DSCI), India Cyber Threat Report 2025.
[19]. Organisation for Economic Co-operation and Development (OECD), Digital Security Risk Management Policy Insights (2023).
[20]. Gupta N. & Taneja P., "Cyber Fraud and Digital Vulnerability in India" (2022) 14 Indian Journal of Law & Technology 34.
[21]. Information Technology Act, 2000 (Act No 21 of 2000), ss 43, 66C, 66D
[22]. CERT-In Cyber Security Directions (28 April 2022) — Government of India, Ministry of Electronics & IT,

through any means, thereby encompassing digital impersonation and online fraud.[23] This reform bridges traditional offences with cyber contexts, ensuring that fraudulent activities committed through electronic media are prosecutable under general criminal law.

- **Digital Personal Data Protection Act, 2023:**

The Digital Personal Data Protection Act (DPDPA), 2023 establishes a rights-based privacy framework governing data processing and breach accountability.[24] It empowers the Data Protection Board of India to impose penalties of up to ₹250 crore for violations and authorises the Board to define timelines for breach notification.[25] While it does not prescribe a specific "72-hour" window, compliance with CERT-In's 6-hour reporting rule ensures convergence between privacy and cybersecurity governance. The DPDPA thus plays a preventive role in mitigating identity-linked cyber frauds.

6.2. Institutional Mechanisms

- **Indian Cyber Crime Coordination Centre (I4C):** Operates the National Cyber Crime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), which, according to the Press Information Bureau (2025), has helped block or recover hundreds of crores in fraudulent transactions.[26]
- **Computer Emergency Response Team (CERT-In):** Functions as the national nodal agency for cybersecurity incident management. In 2024, it recorded over 2.2 million incidents, coordinating with international CERTs to issue phishing and malware alerts.[27]
- **Reserve Bank of India (RBI):** The RBI's Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions Circular (2017) remains the benchmark framework, granting zero liability to customers who promptly report fraud.[28] The Master Direction on Digital Payment Security Controls (2021) further mandates multi-factor authentication and robust transaction monitoring for banks and payment intermediaries.[29]
- **Cyber Appellate Jurisdiction:** Following the merger of the Cyber Appellate Tribunal with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) in 2017, the appellate function under the IT Act continues before TDSAT.[30] This ensures continuity in adjudicating appeals arising from electronic fraud and intermediary liability cases.

7. Judicial Developments

Indian courts have reinforced the interpretation of cyber law provisions through key judgments. In Shreya Singhal v. Union of India (2015), the Supreme Court invalidated Section 66A of the IT Act as unconstitutional, but upheld other penal provisions, preserving the deterrent effect of Sections 66C and 66D.[31] In C.B.I. v. Arif Azim (2008), India secured its first conviction for email-based cheating, setting precedent for the admissibility of electronic evidence.[32] Recent cases have extended evidentiary acceptance to blockchain-based records under the Indian Evidence Act, 1872, strengthening digital integrity in judicial proceedings.

8. Critical Discussion

8.1. Enforcement and Capacity Challenges:

Despite comprehensive legislation, cyber-law enforcement in India continues to lag behind technological evolution. Conviction rates remain below 3 per cent, highlighting deficiencies in digital forensics and cross-

[23]. Bharatiya Nyaya Sanhita, 2023 (Act No 45 of 2023), ss 316–317
[24]. Digital Personal Data Protection Act, 2023 (Act No 22 of 2023)
[25]. International Association of Privacy Professionals (IAPP), "Operational Impacts of India's DPDPA" (2023).
[26]. Press Information Bureau, "National Cyber Crime Reporting Portal and Financial Fraud Recovery Statistics" (2025),
[27]. CERT-In Annual Report 2024, Ministry of Electronics & IT
[28]. Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" (6 July 2017), RBI Notification No. DBR.No.Leg.BC.78/09.07.005/2017-18
[29]. RBI Master Direction on Digital Payment Security Controls (18 February 2021)
[30]. Sansad Parliamentary Document, "Merger of Cyber Appellate Tribunal with TDSAT" (11 August 2023)
[31]. Shreya Singhal v. Union of India (2015) 5 SCC 1.
[32]. C.B.I. v. Arif Azim (2008) Cr LJ 1139 (Delhi).

jurisdictional coordination.[33] Many state-level cyber-crime units remain under-resourced and lack the forensic tools needed to trace digital trails or preserve chain-of-custody standards essential for prosecution.

8.2. Public Awareness and Digital Literacy:

Studies indicate substantial under-reporting of cyber-frauds, with only 20 per cent of victims lodging complaints within 24 hours. [34]Delayed reporting sharply reduces fund recovery, as proceeds move swiftly through multiple banks and wallets. The National Crime Records Bureau (NCRB) 2023 Report stresses that public awareness and digital-literacy programmes in regional languages are crucial for timely reporting and prevention.[35]

8.3. Inter-Agency Coordination:

Institutional overlap among the Ministry of Electronics and Information Technology (MeitY), the Ministry of Home Affairs (MHA), and the Reserve Bank of India (RBI) often fragments fraud-response efforts.[36] In contrast, Singapore's Cyber Security Agency (CSA) operates under a unified command model that integrates investigation, regulation, and threat analytics[37]. Establishing a comparable "Digital Safety Authority of India" could streamline coordination and strengthen evidence-driven enforcement.

8.4. Comparative International Perspective:

The European Union's General Data Protection Regulation (GDPR) requires breach notification within 72 hours and imposes heavy penalties, creating a culture of compliance.[38] The United States Federal Trade Commission (FTC) uses sector-specific oversight and consent decrees to enforce data-security standards.[39] India's hybrid system—anchored in the Information Technology Act 2000, Bharatiya Nyaya Sanhita 2023, and Digital Personal Data Protection Act 2023—should integrate these global lessons while maintaining constitutional freedoms and a federal balance of powers.

9. Policy Recommendations

1. National Cyber Awareness Mission: Institutionalise annual, multilingual awareness campaigns on cyber hygiene and fraud reporting through MeitY and I4C.[40]
2. Specialised Cyber Forensic Infrastructure: Establish regional forensic labs under CERT-In with expertise in AI and blockchain analytics.[41]
3. AI-Driven Fraud Detection: Deploy machine-learning models within UPI and banking systems for real-time anomaly detection.[42]
4. Comprehensive Cyber Crimes Code: Consolidate the IT Act 2000, DPDPA 2023, and BNS 2023 into a unified legislative framework.[43]
5. Cross-Border Enforcement: Deepen cooperation under the Budapest Convention on Cybercrime and bilateral MLATs.[44]
6. Dedicated Cyber Courts: Constitute specialised benches with technically trained judges to fast-track cyber-crime trials.[45]

---

33. National Crime Records Bureau, Crime in India Report 2023, Ministry of Home Affairs (Government of India).
34. Data Security Council of India (DSCI), India Cyber Threat Report 2024.
35. NCRB (n 1).
36. Press Information Bureau, "Government Launches Indian Cyber Crime Coordination Centre (I4C) to Strengthen Law Enforcement Capacity" (28 January 2024), PIB Release ID 1997769
37. Cyber Security Agency of Singapore (CSA), Annual Cybersecurity Report 2023 (Government of Singapore).
38. European Union, General Data Protection Regulation (GDPR) (Reg (EU) 2016/679).
39. Federal Trade Commission (FTC), Data Security and Privacy Enforcement Report 2023, United States Government.
40. Indian Cyber Crime Coordination Centre (I4C), National Cyber Safety Awareness Campaign 2023, MHA Press Release.
41. Computer Emergency Response Team of India (CERT-In), Annual Report 2024, Ministry of Electronics & IT.
42. Reserve Bank of India, Master Direction on Digital Payment Security Controls (18 February 2021).
43. Information Technology Act 2000 (Act No 21 of 2000); Digital Personal Data Protection Act 2023 (Act No 22 of 2023) Bharatiya Nyaya Sanhita 2023 (Act No 45 of 2023).
44. Council of Europe, Budapest Convention on Cybercrime (2001).
45. Department of Justice (India), "Judicial Infrastructure and Reforms Initiative 2023"

7. Public–Private Partnerships (PPP): Formalise data-sharing protocols between fintech platforms, telecoms, and law-enforcement agencies.[46]
8. Periodic Statutory Review: Mandate triennial legislative reviews through parliamentary standing committees to maintain technological alignment.[47]

10. Conclusion

Cyber fraud continues to pose a complex and evolving challenge to India's digital transformation. The country's rapid adoption of digital banking, e-commerce, and online communication platforms—while instrumental in promoting financial inclusion—has also expanded the attack surface for technologically advanced fraudsters. The analysis in this study demonstrates that cybercrime in India has moved beyond isolated acts of deception to form a structured, transnational, and data-driven industry. This industrialisation of cyber fraud highlights the urgent need for robust coordination between law, technology, and policy.

Legislative developments such as the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023 signify a conscious effort to modernise India's penal and privacy regimes. Yet, the effectiveness of these statutes depends less on their textual precision and more on the operational capacity of institutions like CERT-In, I4C, and RBI to detect, prevent, and prosecute fraud. Similarly, judicial interpretations, notably Shreya Singhal v. Union of India (2015) and C.B.I. v. Arif Azim (2008), continue to guide the evolving jurisprudence of digital accountability.

However, the true battle against cyber fraud lies beyond mere enforcement—it rests in cultivating a digitally aware and ethically informed citizenry. Embedding cyber ethics and data responsibility into formal education curricula, professional training, and corporate compliance frameworks can create a culture of proactive vigilance. Simultaneously, investment in AI-enabled forensics, cyber-policing infrastructure, and cross-border cooperation will determine India's capacity to keep pace with the velocity of technological change.

In sum, the path forward must integrate Prevention, Protection, and Prosecution within a coherent, multi-stakeholder governance framework. As India aspires to become a global leader in digital innovation, safeguarding its citizens from cyber fraud is not merely a technical or legal imperative—it is a moral and constitutional duty central to the vision of a secure, inclusive, and trustworthy digital Bharat.

References

1. National Crime Records Bureau. (2023). Crime in India Report 2023. Ministry of Home Affairs, Government of India.
2. Data Security Council of India (DSCI). (2024). India Cyber Threat Report 2024. DSCI Publications.
3. Computer Emergency Response Team–India (CERT-In). (2024). Annual Cyber Security Report 2024. Ministry of Electronics and Information Technology (MeitY), Government of India.
4. Reserve Bank of India. (2023). Customer Protection Guidelines for Digital Transactions. RBI.
5. Reserve Bank of India. (2021). Master Direction on Digital Payment Security Controls. RBI Circular DBR.No.Leg.BC.78/09.07.005/2017-18.
6. Gupta, N., & Taneja, P. (2022). Cyber fraud and digital vulnerability in India. Indian Journal of Law and Technology, 18(2), 112–124.
7. Chaudhary, A. (2021). Cyber crime and legal challenges in India. Journal of Indian Law Review, 12(3), 45–59.
8. Nair, S. (2022). Citizen awareness and digital fraud prevention. Asian Law and Society Review, 8(4), 88–104.
9. Ministry of Electronics and Information Technology (MeitY). (2023). Draft Amendments to the Information Technology Rules, 2021. Government of India.
10. Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023). The Gazette of India.
11. Information Technology Act, 2000 (Act No. 21 of 2000). India Code.
12. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Ministry of Electronics and Information Technology, Government of India.
13. Press Information Bureau. (2025). Government Launches Indian Cyber Crime Coordination Centre (I4C) to Strengthen Law Enforcement Capacity. PIB Release ID 1997769.

[46] . Reserve Bank of India, Cyber Security Framework in Banks (Circular DBR.No.BP.BC.79/21.07.018/2015-16, 2 June 2016, updated 2023).

[47] . Parliament of India, Standing Committee on Home Affairs, "Review of Cyber Security and Cyber Crime Management 2023-24," Lok Sabha Secretariat Report No. 247 (December 2024).

14. Cyber Security Agency of Singapore (CSA). (2023). Annual Cybersecurity Report 2023. Government of Singapore.
15. European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Official Journal of the European Union.
16. Federal Trade Commission (FTC). (2023). Data Security and Privacy Enforcement Report 2023. United States Government.
17. Council of Europe. (2001). Budapest Convention on Cybercrime. Strasbourg.
18. Legal Bites. (2024). Cheating under Section 318 of the Bharatiya Nyaya Sanhita: Explained. Retrieved from https://www.legalbites.in
19. C.B.I. v. Arif Azim, (2008) Cr LJ 1139 (Delhi).
20. Shreya Singhal v. Union of India, (2015) 5 SCC 1.