VOLUME 6 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

THE MIRAGE OF DIGITAL TRUST - EXAMINING LEGAL INADEQUACIES IN INDIA'S FIGHT AGAINST SOPHISTICATED CYBER FRAUD NETWORKS

- Vimal Mahajan[1] & Prakriti Ambasht[2]

ABSTRACT

The accelerating digitization of India's economy has been accompanied by a parallel escalation in the sophistication of cyber fraud networks. While state discourse projects an image of secure and trustworthy digital infrastructures, through Aadhaar, Unified Payments Interface (UPI), and proliferating fintech platforms, the lived reality of citizens reveals a profound mismatch between perception and protection. This research interrogates the "mirage of digital trust" by situating India's cybercrime crisis within the inadequacies of its legal architecture. The Information Technology (IT) Act, 2000, once pioneering in recognizing electronic records and offences, now appears normatively stagnant and technologically obsolete. Its provisions fail to apprehend the fluid modalities of cyber fraud, AI-enabled impersonation, cryptocurrency laundering, and multi-jurisdictional scams that operate beyond territorial policing. Reliance on the Bharatiya Nyaya Sanhita, 2023 (BNS), designed for corporeal criminality, compounds doctrinal incongruities, as traditional notions of cheating and forgery inadequately capture the distributed and anonymous nature of cybercrime. Regulatory guidelines by the Reserve Bank of India and CERT-In offer procedural scaffolding, yet enforcement remains episodic, fragmented, and jurisdictionally contested. This research argues that these structural deficiencies not only hinder effective investigation and prosecution but also erode consumer confidence, undermining the very foundations of India's digital economy. Comparative insights from the European Union (EU), United States (US), and Singapore underscore the urgency of legislative overhaul, institutional specialization, and transnational cooperation.Hence, the analysis contends that India's digital

[1] Assistant Professor of Law, Chandigarh University
[2] Research Scholar, GNDU Regional Campus, Jalandhar

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

trust narrative is a juridical fiction sustained by symbolic regulation rather than substantive safeguards. To dismantle the mirage, legal reform must transcend incremental amendments and embrace a holistic recalibration, embedding cyber resilience, accountability of intermediaries, specialized adjudicatory mechanisms, and citizen-centric redressal. Absent such transformation, the promise of inclusive and secure digitization risks devolving into a terrain of unchecked predation by sophisticated fraud networks.

Keywords: Digital Trust, Cyber Fraud Networks, Legal Inadequacies, Consumer Protection, Cybercrime Enforcement.

BACKGROUND

The Indian digital economy has undergone a transformative expansion, propelled by state-led initiatives such as Digital India, the proliferation of the UPI, and the mass adoption of Aadhaar-based authentication.[3] This accelerated digitization, while designed to democratize access to financial and governmental services, has paradoxically engendered a new architecture of risk. The same technological vectors that enable rapid transactions and seamless integration have simultaneously facilitated complex, often transnational, modalities of cyber fraud. In effect, the narrative of "ease of access" has been shadowed by an equally pervasive narrative of "ease of exploitation". This paradox destabilizes the conceptual basis of digital trust, revealing it as a fragile construct contingent not merely upon technological innovation but upon the adequacy of legal and institutional safeguards.

The emergence of sophisticated cyber fraud networks demonstrates that cybercrime in India has evolved beyond isolated or opportunistic breaches into a systemic phenomenon orchestrated through coordinated, multi-layered operations. Fraudulent loan applications, phishing cartels, ransomware attacks, and cryptocurrency-based laundering illustrate that the operational strategies of these networks are increasingly indistinguishable from organized crime syndicates.[4] Their transnational dimension, often routed through jurisdictions with weak mutual legal assistance treaties, renders them resistant to traditional enforcement paradigms rooted in territoriality and rigid jurisdictional boundaries.[5] The victims of such

[3] *See* Ministry of Electronics & Information Technology, "Digital India Programme" (2015); Reserve Bank of India, *Vision Document on Payment and Settlement Systems in India, 2019–2021*; Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

[4] *See generally* CERT-In Annual Report 2022; National Crime Records Bureau, *Crime in India 2022: Cyber Crimes*.

[5] *See* Ministry of Home Affairs, "India's Position on Mutual Legal Assistance Treaties" (2021).

crimes, ranging from rural first-time digital users to large financial institutions, reveal the structural universality of vulnerability in the Indian digital ecosystem. Crucially, these networks thrive in a regulatory environment marked by legislative obsolescence, inadequate procedural tools, and fragmented enforcement capacity.

It is within this matrix that the inadequacies of India's cyber law framework must be interrogated. The IT Act, 2000, drafted at the dawn of India's digital transition, remains ill-suited to address crimes mediated through AI, encrypted technologies, or decentralized finance.[6]Supplementary reliance on the BNS (IPC)reveals a jurisprudential mismatch, provisions designed for corporeal fraud and forgery are awkwardly extended into the virtual realm, often producing interpretive ambiguities and enforcement paralysis. Further, institutional shortcomings, such as under-resourced cyber cells, lack of judicial expertise in digital evidence, and weak cross-border cooperation, exacerbate the gap between the sophistication of offenders and the capacity of the state.[7]

THE LANDSCAPE OF CYBER FRAUD IN INDIA

India's rapid transition to a digital-payments economy has produced a corresponding and measurable escalation in cyber-enabled fraud, such that macro-level crime statistics and incident-response reports now read as a catalogue of systemic vulnerability rather than episodic misfortune. Between the structural shock of demonetization and the exponential adoption of UPI and app-based banking, reported incidents and monetary loss attributed to digital fraud have surged, taxing law-enforcement capacity and consumer-redress mechanisms that were designed for a lower-volume, brick-and-mortar era.[8] Government and industry reporting corroborates that volume-driven exposure, CERT-In and the National Crime Records Bureau record year-on-year increases in cyber incident reporting while regulators and payments-industry analyses flag that fraud rates, even if small as a fraction of transaction volumes, translate into very large absolute losses as transaction throughput multiplies.[9]This quantitative reality is legally salient, it displaces any comfortable

[6] Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008.
[7] *See* Reserve Bank of India, Circular on Customer Protection in Unauthorized Electronic Banking Transactions, RBI/2017-18/15; CERT-In, Directions under §70B of the IT Act, 28 April 2022.
[8] Nat'l Crime Records Bureau, Crime in India 2022, Book 1 (tables and analysis on cybercrime trends), available at https://ncrb.gov.in (last visited Sept. 13, 2025).
[9] Indian Computer Emergency Response Team (CERT-In), Annual Report 2023; Press Information Bureau, Government of India, "Digital Payment Transactions Surge With Over …" (Mar. 11, 2025); see also PwC India, Combating Payments Fraud in India's Digital Payments Landscape (2025).

presumption that existing criminal statutes and administrative safeguards are merely "outdated" and instead demonstrates that the present statutory architecture routinely implodes under modern scale and modality of harm.[10]

Concomitant with this escalation is a qualitative shift from opportunistic, one-off phishing to organized, networked offending that exploits technological affordances and jurisdictional fragmentation. Contemporary threat actors operate as cartels, coordinating social-engineering campaigns, employing "service" ecosystems on encrypted platforms and the dark web, and weaponising emerging technologies (notably AI-synthesised deepfakes) to create credible personae and scripted narratives that materially facilitate extortion, impersonation and inducement to transfer funds.Parallelly, the telecommunications weak-link of SIM-swap and port-out attacks has become a primary vector for account-takeovers, undermining SMS-based two-factor authentication and thereby defeating a class of routine banking safeguards. The legal consequence is sharp, doctrinal treatments that parse culpability by reference to the isolated "act" of a single fraudster are ill-suited to a milieu where harm is produced by distributed, platform-mediated conspiracies; criminal law and regulatory liability must, therefore, be recalibrated to address jointness of action, intermediary facilitation and transnational evidence-gathering.

Against this backdrop, specific manifestations of sophisticated fraud have proliferated, AI-enabled deepfake impersonations used to coerce transfer of funds; coordinated SIM-swap campaigns for account takeovers; complex, multi-jurisdictional investment and "digital-loan" schemes that rely on shell companies, layered cryptocurrency flows and rapid cash-out rails; and dark-web marketplaces that commodify social-engineering tooling and stolen credentials.Recent investigative reporting and police disclosures reveal a string of high-value investment and "digital arrest" scams in which victims were induced via fabricated official identity and procedural theatre to remit life-savings, as well as an industry-wide hemorrhage of consumer funds through predatory digital-loan and job-offer scams.[11]These operational facts run up against core evidentiary and procedural law, Indian jurisprudence on electronic

[10] See Data Security Council of India (DSCI), India Cyber Threat Report 2023 (analysing threat-actor tactics and scale).

[11] See, e.g., Online fraudsters dupe IT professional of Rs 62 lakh in Belagavi, *Times of India* (Sept. 2025) (reporting a fake-investment Instagram-led scheme); "Digital arrest" scam: Retd BHEL supervisor loses Rs 68 lakh, *Times of India* (Sept. 2025); Digital Fraud — Cybercriminals Stole Rs 23,000 Crore From Indians In 2024, *NDTV* (Aug. 2025) (aggregating losses reported to banks and regulators).

evidence[12] and the Court's evolving privacy corpus materially shape prosecution strategy,[13] victim disclosures and lawful interception, but leave open acute lacunae in cross-border mutual assistance, intermediary takedown obligations and speedy restitution.

DIGITAL TRUST AS A MIRAGE

The perceived invulnerability of India's digital infrastructure, particularly payment rails and platform intermediaries, must be read against a rigorously skeptical legal register, what users experience as "security" is often a bundle of contractual warranties, algorithmic promises and regulatory soft law, not ironclad legal protection. Courts have reminded us that constitutional and statutory doctrines temper, but do not eliminate, these risks. The Supreme Court's affirmation of privacy as a fundamental right underscores the constitutional stakes of data-driven trust, but the holding does not itself translate into a remedial mechanism against third-party commercial exploitation or complex fraud chains; privacy protection, in the Court's schema, imposes limits on state action while leaving large swathes of private-market risk to ex post contractual and regulatory remediation.[14] Equally instructive is the judiciary's calibrated approach to intermediary regulation, while the Court read down overbroad takedown and intermediary liability provisions to protect speech and impose procedural safeguards, that doctrinal protection of intermediaries from summary liability simultaneously complicates victims' efforts to obtain rapid platform-level relief in fraud scenarios where time and actionability are the essence of loss mitigation.[15]

The public's reliance on institutional signifiers of digital identity and payment integrity, Aadhaar, UPI rails, and branded digital wallets, creates a latent risk calculus in which technological familiarity substitutes for legal sufficiency. This confidence is structurally fragile because Indian jurisprudence and regulatory instruments allocate burdens unevenly, regulators (notably the Reserve Bank of India) have issued customer-protection frameworks that speak of "zero liability" and procedural time-limits for remediation, but those norms are administrative and contingent, not the same as a private law cause of action that reliably compensates victims of socially engineered, deepfake, or SIM-swap conspiracies.[16] The

[12] *Anvar P.V. v. P.K. Basheer & Ors.*, (2014) 10 SCC 473.
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[14] *Ibid*.
[15] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[16] Reserve Bank of India, *Customer Protection—Limiting Liability of Customers in Unauthorized Electronic Banking Transactions* (RBI Circular DBR.No.Leg.BC./06.07.2017) (6 July 2017).

Supreme Court's recent disposition in *State Bank of India v. Pallabh Bhowmick*[17] illustrates the point, courts will enforce the RBI's customer-protection outer limits and expect banks to deploy available technology and chargeback mechanisms, yet they also preserve instances in which customer negligence may rebut relief, leaving open significant doctrinal uncertainty about when confidence in platform security yields to judicial imputations of contributory fault.

The cumulative consequence is an erosion of trust that is both normative and transactional, frequent reportage of "digital arrest" and impersonation scams, combined with documented instances of contested chargebacks and slow inter-bank remediation, has produced measurable consumer retreat from certain digital behaviors and intensified calls for stricter intermediary accountability. Regulatory actors such as NPCI have responded with iterative chargeback and dispute-TAT reforms intended to compress dispute windows and allocate on-the-spot liability, yet these technical fixes do not assuage the broader legal criticism, that piecemeal circulars and marketplace policing cannot substitute for integrated statutory doctrines addressing organized, cross-border fraud networks and platform economic incentives.From a critical legal perspective, then, the "mirage" is twofold, a descriptive misperception of safety & normative failure of legal architecture, India's courts and regulators have begun to plug holes, but judicial pronouncements and administrative circulars together show the system treating symptoms through adjudicative triage rather than reconstituting a durable, rights-based, and deterrence-oriented regime for sophisticated cyber-fraud.[18]

LEGAL INADEQUACIES AND ENFORCEMENT GAPS

Indian law currently lacks express statutory provisions to address many forms of fraud that are enabled by emerging technologies, such as AI-enhanced impersonation (deepfake), synthetic voice phishing, crypto-enabled laundering networks, and transnational shell company frauds. IT Act, 2000 does provide for extraterritorial jurisdiction u/s 75 for offences committed outside India if they involve a computer, network or data situated in India.[19] However, judicial interpretation of this section has been sparse, and courts have often been constrained by proof difficulties, especially with anonymized actors operating via VPNs,

[17] SLP (C) No. 30677/2024.
[18] Reporting on the 'digital arrest' and impersonation scams (illustrative of the social engineering vectors that erode public confidence), e.g., *Times of India*, "Digital arrest scam" reporting (2024–2025).
[19] Information Technology Act, No. 21 of 2000, § 75 (2000).

spoofed IPs, or intermediary jurisdictions. Furthermore, law does not yet adequately define or criminalize offences such as algorithmically generated fraudulent content, or liability of platform intermediaries for AI-produced misinformation or fraud. Absent clear amendment, these gaps mean many sophisticated cyberfraud networks operate in legally grey areas with little risk of substantive sanction.

Investigations and prosecutions in cyberfraud cases suffer from serious procedural infirmities.[20] For example, there is consistent judicial acknowledgement that investigative agencies lack standard-operating procedures for digital evidence seizure, chain of custody, forensic lab access, and timely cross-border legal cooperation, which leads to substantial delays and case collapse.In Karnataka, for instance, the conviction rate in cybercrime is recorded at only 0.23% since 2020, a figure indicative not only of weak substantive proof but of procedural breakdowns, delayed complaints, missing logs, or lack of ability to trace fraudsters across jurisdictions.[21] Such delays and procedural lacunae allow substantial erosion of evidence, loss of memory of witnesses, and multiple parked interlocutory applications that stall trials.[22]

The law places heavy burdens on victims for reporting, proving negligence, and falsity of the acts complained of. While regulatory instrumentsattempt to shift the burden of proof of customer liability to banks, courts have still required victims to show they did *not* act negligently, or that there was no deficiency in the bank's duty of care. In *Hare Ram Singh v. Reserve Bank of India*,[23]court held that upon detecting fraud, the bank has an implied duty to exercise reasonable care and take prompt action; further, that the burden of proving the customer's liability in unauthorized electronic banking lies on the bank. In *Suresh Chandra Singh Negi & Anr. v. Bank of Baroda & Ors.*,[24] the Court reaffirmed that, under 2017's Circular of RBI, the bank must prove customer liability in unauthorized transactions; but in that case, the petitioners' own actions (password change, beneficiary addition, etc.) were sufficient for the bank to satisfy that burden.Unless these principles are enforced uniformly and banks are held strictly to these standards of proof, and unless the mechanisms for

[20] *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004.
[21] Cybercrime Conviction Rate Dismal 0.23% in Karnataka, *DECCAN HERALD* (Jan. 12, 2024), https://www.deccanherald.com/india/karnataka/cybercrime-conviction-rate-dismal-023-in-karnataka-3691770.
[22] Why Most Cyber Crimes in India Don't End in Conviction, *LIVEMINT* (Apr. 19, 2018), https://www.livemint.com/HomePage/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html.
[23] W.P.(C) 6635/2023.
[24] W.P.(C) 1048/2025.

reporting, freezing suspicious transfers, and recovering funds are strengthened, victims will continue to bear an unfair share of the risk.

COMPARATIVE PERSPECTIVE

The EU represents perhaps the most mature legal response to the erosion of digital trust through its General Data Protection Regulation (GDPR) and the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation. The GDPR's articulation of individual rights, data minimisation, purpose limitation, and accountability, translates directly into enhanced consumer confidence in digital transactions. Coupled with the eIDAS framework, which establishes uniform standards for electronic identification and trust services across Member States, the EU has succeeded in embedding a comprehensive architecture where digital trust is both a legal entitlement and a regulatory guarantee. In decisions such as *Schrems II v. Facebook Ireland*,[25] the EU judiciary has reinforced that trust is not a matter of voluntary compliance by corporations but a legally enforceable obligation safeguarded by supranational judicial oversight. India's IT Act, by contrast, lacks this robust articulation of rights and judicially enforceable duties, rendering the promise of digital trust illusory.

The US adopts a more fragmented yet enforcement-driven approach. Federal statutes such as the Computer Fraud and Abuse Act (CFAA) & Electronic Communications Privacy Act (ECPA) establish criminal liability for unauthorised access and interception of communications, while the Federal Trade Commission (FTC) exercises wide discretion in prosecuting deceptive or unfair trade practices in the digital sphere. Notably, in *FTC v. Wyndham Worldwide Corp.*,[26] the Third Circuit confirmed the FTC's authority to hold corporations accountable for weak cybersecurity practices that facilitated consumer fraud. The jurisprudential emphasis is thus on corporate responsibility and deterrence through enforcement rather than harmonisation. India has no equivalent to the FTC, leaving consumers vulnerable in cases where digital service providers adopt negligent practices but cannot be effectively held accountable under the IT Act or general contract law.

Singapore's model reflects a hybrid approach, blending prescriptive statutory obligations with robust regulatory enforcement. The Personal Data Protection Act (PDPA) imposes mandatory

[25] *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, Case C-311/18.
[26] No. 14-3514.

data protection obligations, while the Cybersecurity Act (2018) designates Critical Information Infrastructure sectors and subjects them to stringent supervisory control. The Singaporean judiciary has been cautious but consistent in recognising these statutory duties as enforceable standards of digital governance. For instance, the *Re SingHealth Data Breach Inquiry* inquiry committee highlighted both organisational and technological lapses while reinforcing the principle that trust in digital infrastructures cannot be left to market self-regulation. India has often cited Singapore's model in parliamentary debates on data protection, but legislative inertia has stalled the enactment of comparable frameworks, leaving enforcement dependent on under-resourced agencies like CERT-In.

Taken together, these comparative experiences illustrate that India's primary inadequacy is not merely technological obsolescence but legal under-commitment to digital trust. Harmonisation of cybercrime and consumer protection statutes, akin to the EU's integrated approach, is necessary to avoid regulatory fragmentation. Stronger mechanisms of international cooperation, particularly mutual legal assistance in cross-border frauds, are critical given the transnational character of organized cybercrime. Most importantly, India must embed digital trust as a legal framework rather than a rhetorical aspiration, where service providers, regulators, and state actors are held to enforceable duties. Without such a recalibration, Indian jurisprudence will continue to lag behind global best practices, and judicial rulings, despite their growing sensitivity to cyber harms, will lack the statutory teeth to transform digital trust from a mirage into a legal reality.

CONCLUSION& SUGGESTIONS

The edifice of India's digital economy rests precariously on the construct of digital trust, yet this foundation reveals itself to be increasingly fragile in the face of sophisticated fraud networks. While statutory interventions, such as IT Act, 2000 and piecemeal regulatory guidelines from the RBI and CERT-In reflect a legislative intent to secure cyberspace, these instruments remain reactive, fragmented, and technologically outdated. They fail to adequately capture emergent modalities of cyber fraud that exploit artificial intelligence, deepfakes, cryptocurrency anonymity, and cross-jurisdictional data flows. In this sense, the legal architecture has become a static framework confronting a dynamic adversary, wherein the mismatch between regulatory pace and criminal innovation perpetuates systemic vulnerability. The result is a fragile legal response that burdens victims disproportionately and

fosters a climate of digital distrust, undermining both consumer confidence and the legitimacy of India's digital governance agenda.

Against this backdrop, urgent reforms are neither optional nor incremental but existential to India's digital future. The law must evolve from anachronistic statutes to a holistic framework that integrates cybercrime adjudication, data protection, consumer protection, and financial regulation into a seamless architecture of accountability. Such reform must be supported by institutional capacity-building, specialized cyber courts, technologically trained enforcement personnel, and cross-border legal cooperation agreements, so as to render the law both enforceable and resilient. Simultaneously, embedding technological safeguards such as blockchain verification and AI-driven fraud detection within statutory obligations can operationalize digital trust in practice. Hence, absence of comprehensive recalibration that marries law, technology, and consumer protection, India risks allowing digital trust to remain an elusive mirage, an aspirational concept proclaimed in policy but unattainable in lived experience. The credibility of India's digital transformation thus hinges on whether its legal system can decisively bridge this gap.

A reconfiguration of India's cyber law framework is imperative if digital trust is to be salvaged from the erosion caused by increasingly sophisticated fraud networks. The IT Act, 2000, conceived at a time when cybercrimes were largely rudimentary, fails to capture the legal nuances of AI-driven frauds, deepfake impersonations, and cryptocurrency-enabled scams. A modernized statute must explicitly recognize and criminalize emerging modalities of fraud, rather than relying on strained interpretations of outdated provisions. Furthermore, integration of data protection and consumer protection principles into the cybercrime regime is essential. A harmonized legal architecture, whereby consumer rights are protected through statutory redressal mechanisms and personal data misuse is criminally actionable, would ensure that victims of cyber fraud are not left to navigate fragmented remedies. Equally critical is the establishment of a clear liability framework for intermediaries and digital service providers. By defining the contours of due diligence and safe harbor more stringently, the law can prevent platforms from escaping accountability while balancing innovation and compliance.

Beyond statutory reform, institutional strengthening must occupy a central place in the reform discourse. The establishment of specialized cybercrime courts with judges trained in

digital forensics and technology law would mitigate the chronic delays and low conviction rates plaguing the current system. These forums could serve as fast-track tribunals, ensuring that technical evidentiary complexities do not translate into justice deficits. Parallelly, sustained capacity building for law enforcement and judicial officers is indispensable, given that sophisticated fraudsters exploit institutional ignorance as much as technological loopholes. Regulators, suchas RBI, SEBI, &MeITY, must adopt a more proactive role, not merely as rule-makers but as enforcers and coordinators across fragmented enforcement landscapes. Regulatory synergy, underpinned by statutory authority, could provide the institutional coherence presently missing in India's fight against cybercrime.