Kuwait Research Journal of
Education and Literature (KRJEL)

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

Toward A Duty of Algorithmic Care: Digital Fraud, Expert Systems, and Liability Shifts in Indian Banking Under the RBI Framework and the PMLA, 2002

Dr. Nikhil Kashyap

Dean, Delhi Global Institute of Management, Faridabad

Dr.NitanSharma
Assistant Professor, School of Law, SMVDU-Katra, J&K

*Corresponding Author

Dr. Nikhil Kashyap
Dean, Delhi Global Institute of Management, Faridabad

Article History
Received: 11.09.2026
Revise : 19.09.2026
Accepted: 8.10.2026
Published: 16.10.2026

DOI:10.61705/KRJEL.5.4.2026.1.7

Keywords: Digital Frauds, Expert Systems, Algorithmic Accountability, Liability Shifts, RBI, PMLA, Data Fiduciary

ABSTRACT
The integration of expert systems and artificial intelligence into Indian banking has fundamentally altered the traditional banker-customer relationship, creating a doctrinal vacuum where algorithmic opacity collides with established fiduciary obligations. While the Banking Regulation Act, 1949 and the Prevention of Money Laundering Act, 2002 established foundational governance structures predicated on human oversight, contemporary banking operations delegate critical decisions, from credit underwriting to suspicious transaction reporting, to proprietary algorithms whose internal logic remains shielded from regulatory scrutiny. This paper argues that traditional legal paradigms of negligence, contract, and vicarious liability are structurally inadequate to address the accountability deficits generated by algorithmic decision-making. Drawing upon the emerging framework of "algorithmic accountability" and the concept of "algorithmic hygiene" as articulated in comparative financial regulation scholarship, this research proposes a revised liability architecture grounded in a "Duty of Algorithmic Care." This duty would impose non-delegable obligations upon banking institutions to ensure that deployed expert systems are technically audited, functionally explainable, and subject to meaningful human oversight before autonomous decisions affect customer rights. Analyzing recent regulatory interventions including the RBI's FREE-AI framework, the India AI Governance Guidelines 2025, and the amendments to the digital fraud compensation regime in 2026 alongside enforcement actions against Bank of Baroda and Paytm Payments Bank, the paper demonstrates that Indian banking law is converging toward strict institutional liability for algorithmic failure. The paper concludes that statutory recognition of a Duty of Algorithmic Care is necessary to reconcile the efficiency imperatives of digital banking with the constitutional and statutory guarantees of privacy, due process, and consumer protection.

INTRODUCTION

The historical development of Indian banking institutions has been defined by a fiduciary relationship predicated on trust, transparency, and manual human oversight. From the Reserve

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

Bank of India Act, 1934 to the Banking Regulation Act, 1949, legislative intent has consistently focused on regulating the tangible and financial assets of banking companies.[1] However, the contemporary financial landscape has undergone an unprecedented digital metamorphosis, driven by scale, speed, and algorithmic automation.

The sheer volume of digital transactions in India necessitates the use of automated systems. The Unified Payments Interface (UPI) alone processed over 131 billion transactions in FY 2023-24, transferring value exceeding ₹199 trillion.[2] To manage this staggering volume, the introduction of New Technology, e-Banking, and 'expert systems' – artificial intelligence and machine learning software that emulates human expert decision-making- has automated core banking functions ranging from credit risk assessment to real-time remittance processing.[3] Expert systems now serve as the primary, and often sole, gatekeepers of financial transactions. Banks employ these systems to categorize 'Special classes of Customers', authorize dynamic credit limits, and monitor for malicious activities at a millisecond latency.

This technological shift has generated a critical legal vacuum. When an autonomous system erroneously triggers an anti-money laundering (AML) alert, or fails to detect sophisticated cyber-fraud, traditional frameworks of tort and contract law struggle to allocate liability appropriately. The 'black box' nature of neural networks means that even the developers often cannot explain how a specific automated decision was reached. This opacity stands in direct contradiction to the legal requirements of auditability and transparency embedded in Indian banking laws.

The scale of algorithmic governance challenges is matched by empirical evidence of its failures. The RBI's Annual Report 2024-25 documented 23,953 fraud cases involving ₹36,014 crore, with digital payments accounting for 56.5% of all cases.[4] More fundamentally, the RBI Governor's 2026 address acknowledges that AI adoption introduces what he terms the "black box" problem—where sophisticated models "do not readily explain their own reasoning," striking "at the heart of accountability".[5]

However, recent regulatory developments signal a decisive shift toward institutional accountability. The India AI Governance Guidelines, 2025 mandate sectoral regulators to enforce risk-based safeguards, while the RBI's own FREE-AI framework proposes strict algorithmic audits for credit scoring and fraud detection.[6] Simultaneously, the RBI's 2026 amendments to the digital fraud compensation regime, effective from January 1, 2027, establish statutory liability for banks that fail to prevent coerced transactions, redefining "fraudulent transactions" to include payments induced through deception.[7]

This paper critically analyzes this paradigm shift. It traverses the foundational principles of banking secrecy, reporting obligations under the PMLA, 2002, and the shifting locus of liability in digital bank frauds. By integrating statistical evidence from RBI's Annual Reports and Financial Intelligence Unit (FIU) publications, alongside concrete examples of Expert System implementations by major Indian commercial banks, this paper offers a comprehensive legal

[1] The Banking Regulation Act, 1949 (Act No. 10 of 1949), s. 5(b) defines 'banking' as the accepting, for the purpose of lending or investment, of deposits of money from the public.

[2] National Payments Corporation of India (NPCI), UPI Product Statistics (FY 2023-24); see also Reserve Bank of India, Annual Report 2023-24, detailing digital payment volumes.

[3] Reserve Bank of India, Report of the Working Group on FinTech and Digital Banking, (2018), highlighting the structural transition towards automated banking systems

[4] Reserve Bank of India, Annual Report 2024-25, Chapter on 'Consumer Protection and Grievance Redressal', detailing fraud statistics in the banking sector.

[5] Reserve Bank of India, 'Address by Shri Sanjay Malhotra, Governor, RBI at FIBAC 2026' (August 11, 2026), *available at:* https://www.rbi.org.in.

[6] Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines, 2025; Reserve Bank of India, Framework for Responsible and Ethical Enablement of AI (FREE-AI) Report, August 13, 2025.

[7] Reserve Bank of India, Draft Reserve Bank of India (Commercial Banks – Responsible Business Conduct) Third Amendment Directions, 2026.

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

critique grounded in recent regulatory directives and judicial pronouncements.

2. The Secrecy Paradigm vs. Algorithmic Inference: A Doctrinal Collision

The basic foundation of the banker-customer relationship is the implied contractual obligation of secrecy, codified in common law through the landmark English case of *Tournier v. National Provincial and Union Bank of England*,[8] which establishes that a bank may only disclose customer information under four specific exceptions: compulsion by law, duty to the public, the bank's own interest, or with the customer's express or implied consent. Indian courts have consistently affirmed this duty as a legal obligation arising from the banker-customer contract, rather than a mere moral duty, breach of which may give rise to claims for both nominal and substantial damages.[9]

In the era of algorithmic banking, the obligation to maintain secrecy is routinely tested, strained, and occasionally broken by the operational requirements of expert systems. Modern AI-driven credit scoring models ingest vast repositories of structured and unstructured data. For example, HDFC Bank's AI-driven chatbot 'EVA' (Electronic Virtual Assistant) and the State Bank of India's (SBI) 'YONO' (You Only Need One) platform utilize complex algorithms to process massive datasets of user behavior, geolocation, and transaction history to offer pre-approved personal loans (PAPL) and personalized financial products. While these systems offer immense consumer convenience, they fundamentally alter the nature of bank secrecy. Banks frequently utilize third-party FinTech vendors and cloud service providers (such as AWS or Microsoft Azure) to process this data, exposing customers financial footprints to external servers. The legal friction intensifies when predictive algorithms infer sensitive personal data from seemingly benign transaction histories.[10]

Consider a scenario where an expert system categorizes a user's late-night transactions at pharmacies and specific medical facilities to infer a chronic illness, subsequently adjusting their financial risk profile or cross-selling health insurance. This inferred data was never explicitly provided by the customer. Does the processing of this derived data violate *Tournier* principles? The Supreme Court's recognition of the right to privacy as an intrinsic facet of Article 21, as elaborated in *K.S. Puttaswamy v. Union of India*, establishes that privacy attaches to individuals, not places, and that documents or information voluntarily shared with a bank retain their confidential character.[11]

The Digital Personal Data Protection (DPDP) Act, 2023, imposes stringent obligations on Data Fiduciaries (banks) to ensure purpose limitation and data minimization.[12] The Act makes it mandatory for Data Fiduciaries to enter into valid contracts with Data Processors, ensuring that processing occurs only under documented instructions and that reasonable security safeguards are implemented. Critically, the DPDP Act holds the Data Fiduciary accountable for any personal data breach or contravention of the law, irrespective of any contractual arrangements to the contrary.[13] Section 8(1) explicitly states that a Data Fiduciary remains responsible for compliance "irrespective of any agreement to the contrary," even where actual processing was carried out by a Data Processor.[14] This creates an effectively *non-delegable, vicarious form of liability*.

This legislative architecture aligns with comparative regulatory frameworks. In the European Union, the GDPR's Article 24 places

---

[8] *Tournier v. National Provincial and Union Bank of England,* [1924] 1 KB 461.

[9] *Shankarlal Agarwalla v. State Bank of India,* 1987 Cal 29.

[10] Johan Schweigl, "From Internal Standards to the AI Act: Reshaping Financial Processes for the Era of Algorithmic Accountability" *Dyskurs Prawniczy i Administracyjny* 211-224 (2026).

[11] AIR 2017 SC 4161.

[12] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 4-8.

[13] Ministry of Electronics and Information Technology, Government of India, *Implementation of Digital Personal Data Protection Act, 2023*, Rajya Sabha Unstarred Question No. 2134 (Aug. 9, 2024), *available at:* https://sansad.in/getFile/annex/265/AU2134_DhfUx4.pdf?source=pqars.

[14] *Supra* note 12, s. 8(1).

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

the burden of proof on the controller to demonstrate compliance, while Article 26 establishes joint and several liability when a vendor's role exceeds simple processing.[15] The emerging scholarly consensus identifies a "tripartite liability matrix" across India, Uzbekistan, and the EU, wherein the financial institution—not the AI vendor—remains the primary custodian of customer data and bears full, non-delegable liability for algorithmic discrimination or privacy breaches.[16]

A notable mishappening in this domain occurred when digital lending applications (DLAs), acting as agents for regulated banking entities, excessively scraped user contact lists, photo galleries, and GPS data under the guise of algorithmic credit underwriting. This led to severe harassment of borrowers and a wave of suicides between 2020 and 2022, prompting the RBI to issue the stringent 'Guidelines on Digital Lending' in late 2022.[17] These guidelines explicitly outlawed the unrestrained algorithmic scraping of personal data, reasserting the primacy of customer secrecy over algorithmic convenience. The liability for data breaches in these algorithmic pipelines has consequently shifted from simple negligence to strict statutory liability.

3. Expert Systems and the Regulatory Perimeter of the Banking Regulation Act, 1949

Under Section 21 and Section 35A of the Banking Regulation Act, 1949, the RBI possesses broad powers to issue directives in the public interest or to prevent the affairs of any banking company from being conducted in a manner detrimental to depositors.[18] The deployment of expert systems complicates the traditional "control over management" envisioned by the Act.

Modern banks deploy platforms like ICICI Bank's 'iLens', which utilizes AI algorithms to replace traditional manual underwriting processes, independently assessing collateral value, validating legal documents, and issuing credit decisions.[19] However, when a bank's board of directors delegates critical operational decisions such as the suspension of accounts, the identification of non-performing assets (NPAs), or automated margin calls to proprietary algorithms, a severe 'black box' problem emerges. In the context of corporate law and banking regulations, this lack of transparency complicates statutory audit and inspection processes. If an algorithm systematically discriminates against a specific demographic in granting advances (algorithmic bias), who is legally liable -the data scientists, the proprietary software vendors, or the bank's executive management?[20]

While Indian courts are yet to adjudicate a major algorithmic bias case in banking, international precedents highlight this risk. The Goldman Sachs and Apple Card controversy in the United States involved allegations that the bank's credit-scoring algorithm systematically assigned lower credit limits to women compared to men with identical financial profiles.[21] While the New York State Department of Financial Services, after conducting an extensive investigation, reviewing underwriting data for nearly 400,000 applicants, ultimately found no evidence of unlawful discrimination, though it noted that deficiencies in transparency undermined consumer trust.[22]

---

[15] European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 24, 26.

[16] Shashank Sidharth, "Algorithmic Bias and Data Privacy in AML Transaction Monitoring: A Comparative Analysis of India, Uzbekistan and European Union" 14 *ILM-FAN XABARNOMASI SCIENCE BULLETIN* 92-98 (2026).

[17] Reserve Bank of India, Guidelines on Digital Lending, RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23 (Sept. 2, 2022).

[18] *Supra* note 1, s. 35A.

[19] ICICI Bank launches 'iLens' – powered by TCS lending platform, available at: https://www.business standard.com/article/news-cm/icici-bank-launches-ilens-powered-by-tcs-lending-platform122112900387_1.html

[20] Mugesh Kannan Reguraman, *et al.*, "Rethinking Responsibility: Corporate Liability Frameworks for AI-Driven Compliance and Risk Management in the Banking Sector", in Sriram Ananthan *et al.* (eds.), *Rethinking Responsibility at the Intersection of AI and Corporate Liability* (IGI Global 2026).

[21] Neil Vigdor, "Apple Card Investigated After Gender Discrimination Complaints" *The New York Times*, Nov. 10, 2019.

[22] Goldman cleared of bias claims in NYDFS's Apple Card probe, *available at:*

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

The Bank of Baroda's 'boB World' mobile banking application provides a stark Indian illustration. In an attempt to artificially inflate user onboarding numbers, business correspondents and bank agents exploited systemic vulnerabilities in the app's onboarding algorithm, linking unauthorized mobile numbers to customer accounts and facilitating fraud of roughly ₹2.2 million from innocent depositors' accounts. In October 2023, utilizing powers under Section 35A of the BR Act, the RBI directed the bank to suspend any further onboarding of customers onto the 'boB World' app.[23]

This case vividly illustrates the liability shift. The failure was not merely one of rogue employees, but a failure of the Expert System's authentication protocols to flag anomalous, bulk linkage of phone numbers. The RBI's Master Direction on Outsourcing of Financial Services mandates that the core management of a banking company cannot outsource its responsibilities. Therefore, even if a third-party AI fails or a technological loophole is exploited, the banking company remains wholly liable.

Recent scholarship proposes an "AI-adaptive corporate liability framework" grounded in four principles: *presumptive corporate responsibility* to prevent blame-shifting, *duty of algorithmic foresight* to anticipate foreseeable risks, a *shared accountability matrix* clarifying roles across organizational actors, and *ethical intent embedding* to institutionalize responsible AI governance.[24] Herein the "duty of algorithmic foresight" is particularly relevant as it imposes upon banks an obligation to anticipate and mitigate risks arising from algorithmic decision-making, irrespective of whether those risks originate in proprietary code the bank itself did not write.

4. The PMLA, 2002: Algorithmic Adjudication and FIU-IND Monitoring

Section 12 of the PMLA requires reporting entities (commercial banks) to maintain exhaustive transaction records and furnish information to the Director of the Financial Intelligence Unit-India (FIU-IND).[25] To manage millions of daily digital transactions, commercial banks employ Automated Transaction Monitoring Systems (TMS). These Expert Systems are programmed to flag 'Suspicious Transaction Reports' (STRs) based on pre-defined typologies of the offence of money laundering. The scale of this operation is immense; according to the FIU-IND Annual Report, reporting entities filed over 3.1 million STRs in a single reporting year.[26] Human review of this volume is impossible; thus, the FIU-IND itself utilizes a massive analytical platform called Project FINnet to parse these algorithmic reports. However, these algorithms are notoriously flawed. Traditional rules-based Expert Systems suffer from a false-positive rate often exceeding 85% to 90%, generating an overwhelming volume of 'noise' that obscures actual illicit activity.[27] Conversely, false negatives allow highly structured, sophisticated money laundering networks to operate undetected. Empirical research identifies an inverted U-shaped relationship between AI reliance and AML effectiveness: moderate automation assists, but excessive reliance on complex, outsourced models without local oversight render systems easier to defeat as criminal groups study predictable algorithmic behavior.[28]

The most prominent recent enforcement action concerning algorithmic AML compliance is the

https://www.bankingdive.com/news/goldman-sachs-gender-bias-claims-apple-card-women-new-york-dfs/597273/.

[23] Action against Bank of Baroda under section 35A of the Banking Regulation Act, 1949, *available at:* https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=56533.

[24] S*upra* note 20.

[25] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), s. 12.

[26] Financial Intelligence Unit - India (FIU-IND), Annual Report (recent reporting cycle), outlining the volume of Suspicious Transaction Reports (STRs).

[27] See generally, FATF (Financial Action Task Force) reports on Opportunities and Challenges of New Technologies for AML/CFT, discussing the high false-positive rates of traditional TMS.

[28] S.Lyeonov, L. Hrytsenko, *et. al.*, "Who benefits from AI in money laundering in Europe: The organised criminals or the AML services?" 21(1) *Human Technology* 222-245 (2025).

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

regulatory intervention against Paytm Payments Bank Ltd. (PPBL). In January 2024, the RBI imposed severe business restrictions on PPBL under Section 35A of the BR Act, effectively halting its core operations.[29] Subsequent investigations revealed that PPBL's automated KYC and AML monitoring systems completely failed to identify the systemic creation of thousands of accounts linked to single, identical PAN cards. These algorithmic blind spots allowed crores of rupees to flow through the system unchecked, raising massive money laundering concerns. In March 2024, the FIU-IND imposed a penalty of ₹5.49 crore on PPBL for severe violations of its PMLA obligations.[30] This landmark case underscores the shifting liability landscape: a failure of the expert system to perform its statutory monitoring role translates directly into punitive corporate liability for the banking entity. The bank cannot attribute failure to the algorithm; the algorithm's failure is the bank's failure.

Furthermore, algorithmic adjudication poses a direct threat to civil liberties. When an expert system flags a transaction, it can lead to automatic account freezing without human application of mind or due process. The evolving jurisprudence suggests that while algorithmic flagging is permissible to initiate scrutiny, actual attachment, adjudication, and confiscation of assets must be preceded by substantive human review to satisfy the principles of natural justice and Article 14 of the Constitution.

5. Bank Frauds, Cyber Thefts, and the Shift to Strict Institutional Liability

Historically, banking frauds were physical and localized. Today, the vector of fraud has migrated almost entirely to the digital realm, scaling globally through cyber channels. The quantitative scale of the problem is alarming. The RBI's Annual Report 2023-24 documented 36,075 fraud cases involving an aggregate amount of ₹13,930 crore.[31] A massive proportion of these incidents occurred in the digital payments and internet banking domains, specifically targeting fraud-prone areas like remittances and online credit card transactions. However, modern digital frauds have evolved beyond simple stolen passwords. Cybercriminals now utilize malicious AI including deepfake voice cloning to bypass biometric voice-authentication expert systems to circumvent bank security.[32]

The legal response has been decisive. In *Umashankar Sivasubramanian v. HDFC Bank,* the State Consumer Disputes Redressal Commission held the bank strictly liable for an unauthorized electronic withdrawal, articulating a vital principle: if a bank aggressively promotes digital services to reduce its own operational costs, it is legally bound to ensure the systemic, impenetrable security of those services.[33] The *caveat emptor* model has been legally discarded.

Building upon this jurisprudence, the RBI's amendments in 2026 to its customer protection framework establish a comprehensive shared-risk compensation model. Effective from January 1, 2027, banks must investigate and resolve domestic fraud claims within 45 calendar days.[34] A bona fide victim suffering fraud losses up to ₹50,000 may receive compensation of 85% of the net loss or ₹25,000, whichever is less, with the RBI contributing 65% and the customer's bank contributing 10% (with the beneficiary bank contributing the remaining 10% in domestic cases).[35] Crucially, the framework recognizes *coercion-based fraud*, transactions induced through deception or psychological

[29] Action against Paytm Payments Bank Ltd under Section 35A of the Banking Regulation Act, 1949, *available at:* https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=57345.

[30] Finance Ministry's Financial Intelligence Unit imposes Rs. 5.49 crore fine on Paytm Payments Bank for PMLA lapses, *available at:* https://www.thehindu.com/business/Industry/finance-ministrys-financial-intelligence-unit-imposes-549-crore-fine-on-paytm-payments-bank-for-pmla-lapses/article67904457.ece.

[31] Reserve Bank of India, Annual Report 2023-24, Chapter on Consumer Protection and Grievance Redressal, detailing fraud statistics in the banking sector.

[32] Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, advisories on AI-generated deepfakes and advanced phishing in the financial sector.

[33] *Umashankar Sivasubramanian v. HDFC Bank,* State Consumer Disputes Redressal Commission.

[34] S*upra* note 7.

[35] *Ibid.*

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

manipulation, as legally distinct from unauthorized transactions, acknowledging that consent obtained through fraud is defective under the Indian Contract Act.[36]

Even in complex cases where the customer's negligence is alleged (e.g., sharing an OTP), the burden of proof rests entirely on the bank. Section 76K of the amended directions explicitly states that "the burden of proving customer liability in complaints involving fraudulent electronic banking transactions shall lie on the bank."[37] The bank must deploy forensic technology to conclusively prove customer complicity. This regulatory stance coerces commercial banks to invest heavily in predictive, machine-learning-based anti-fraud algorithms that analyze user behavior, device telemetry, and keystroke dynamics to prevent fraud in real-time. Preventive measures now require active, dynamic expert systems, fundamentally pushing the boundaries of what constitutes 'reasonable care' in contemporary banking operations.

The recent observations by Supreme Court regarding "digital arrest" scams reinforce this trajectory. The Court emphasized that banks cannot remain passive bystanders and that "KYC isn't just about opening an account; it should be about active, real-time monitoring of how that account is used."[38] This judicial articulation of an expanded duty of care—from onboarding verification to continuous algorithmic surveillance—represents the clearest judicial endorsement of what this paper terms the Duty of Algorithmic Care.

6. Toward a Duty of Algorithmic Care

The foregoing discussion converge upon a single doctrinal necessity i.e., the recognition of a *Duty of Algorithmic Care* as a legally enforceable obligation incumbent upon banking institutions.

The concept of "algorithmic accountability" has emerged as a successor to traditional duty of care in financial regulation. Schweigl argues that as *Agentic AI* takes over cognitive workflows such as AML monitoring and risk management, the traditional focus on human behavior becomes less relevant; institutional stability now depends on "Algorithmic Hygiene", a continuous process of keeping software configurations clean, transparent, and compliant.[39] This requires moving beyond formal "tick-the-box" compliance toward real technical audit of an institution's "algorithmic DNA."

The RBI Governor's declaration that "the 'model decided' can never be an acceptable answer to a customer, an auditor, or the Reserve Bank" represents the clearest articulation of this liability principle.[40] Meaningful human oversight, "the ability to explain, to intervene, and, where necessary, to override", must transition from regulatory aspiration to legally enforceable obligation.

The India AI Governance Guidelines, 2025 explicitly reject "unrestricted deployment of high-risk AI systems" and mandate that sectoral regulators remain responsible for enforcement within their legal mandates.[41] Within banking, this responsibility translates directly into the Duty of Algorithmic Care. The RBI's FREE-AI framework and the deployment of AI-based detection tools like MuleHunter.AI, currently identifying approximately 20,000 mule accounts monthly with 85-90% accuracy, demonstrate that algorithmic solutions to algorithmic problems are feasible.[42]

The Duty of Algorithmic Care can be operationalized through four interconnected pillars:

---

[36] ForumIAS, *Analyze the significance of shifting from unauthorized to coercion-based digital fraud frameworks* (2026).

[37] S*upra* note 7.

[38] The Supreme Court in its *suo motu* cognizance of digital arrest scams observed that banks are trustees of public money and must move from one-time KYC to continuous real-time monitoring, while warning of accountability for mule accounts and directing RBI to issue SOPs on debit freeze and cooling periods. *See In Re: Victims of Digital Arrest Related to Forged Documents,* SMW (Crl.) No. 3/2025. Orders dated 17.10.2025, 01.12.2025 & Aug. 2026 (S.C., India)

[39] S*upra* note 10.

[40] *Supra* note 3.

[41] Ministry of Electronics and Information Technology, India AI Governance Guidelines, 2025.

[42] Reserve Bank of India, Framework for Responsible and Ethical Enablement of AI (FREE-AI) Report, August 13, 2025; see also Reserve Bank of India, 'MuleHunter.AI: A New Tool for Combating Mule Accounts' (2024).

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access

First, a Duty of Algorithmic Foresight. Banks must anticipate foreseeable risks arising from algorithmic decision-making, irrespective of whether those risks originate in code the bank did not write. This extends the traditional duty of care to encompass algorithmic risk assessment as a core management obligation.[43]

Second, Non-Delegable Institutional Liability. Vendor contracts cannot transfer statutory obligations. The DPDP Act's Section 8(1) already establishes that a Data Fiduciary remains responsible "irrespective of any agreement to the contrary." The RBI's outsourcing guidelines mandate that core management functions cannot be outsourced.[44] The logical extension is that algorithmic compliance obligations are similarly non-delegable—the bank that deploys the algorithm bears the liability.

Third, Algorithmic Hygiene as Continuous Obligation. Compliance is not a one-time audit but a continuous process of monitoring software health, testing agents through non-standard scenarios, and evaluating error statistics in real-time. This requires redefining the Three Lines of Defence model to focus on software integrity rather than merely human behavior.[45]

Fourth, Explainability and Meaningful Human Review. Black-box opacity cannot be a defense. Article 14 of the EU AI Act requires meaningful human oversight with the competence and authority to intervene or override.[46] India's emerging framework should mandate similar requirements—compliance officers must genuinely understand algorithmic outputs before confirming decisions that restrict customer access to funds.

Despite regulatory convergence, a coherent legal doctrine translating these principles into enforceable standards remains absent. The RBI's FREE-AI framework and the India AI Governance Guidelines are principle-based and non-prescriptive. Judicial pronouncements have expanded the duty of care without articulating its precise contours. Until statutory recognition of a Duty of Algorithmic Care is achieved, the banking sector will continue to navigate between algorithmic efficiency and opacity without adequate legal compass.

7. Conclusion

The empirical evidence is unambiguous: Indian banking sector processes hundreds of billions of digital transactions annually, governed by millions of algorithmic decisions made every second. As banking companies increasingly function as vast data-processing behemoths driven by Expert Systems, traditional legal doctrines are being fundamentally re-engineered. The implied obligation of secrecy must be strictly balanced against the insatiable data requirements of AI analytics, governed by the heavy penalties of the DPDP Act. The statutory mandate of corporate management must now encompass rigorous algorithmic auditing to prevent systemic disasters akin to the boB World or Paytm Payments Bank incidents.

Furthermore, the prevention of money laundering must transcend automated, high-false-positive STRs to include substantive human adjudication, ensuring that the heavy machinery of the State is not deployed erroneously by a flawed line of code. Liability for digital fraud has decisively shifted from the consumer to the institution, demanding faultless technological architecture.

For legal practitioners, corporate advisors, and regulatory authorities, the future lies not in resisting new technology, but in drafting robust, proactive statutory frameworks that enforce strict algorithmic accountability. By establishing non-delegable liability for systemic tech failures, demanding explainability in automated decision-making, and enforcing a 'Duty of Algorithmic Care', the Indian banking sector can reconcile the rapid pace of digital innovation with the immutable principles of consumer protection, data privacy, and national financial integrity.

[43] *Supra* note 20.

[44] Reserve Bank of India, Master Direction on Outsourcing of Financial Services.

[45] *Supra* note 10.

[46] European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act), art. 14.

Kuwait Research Journal of
Education and Literature (KRJEL)

ISSN Print: 2790-6469 | ISSN Online : 2790-6450 Open Access