Page: 718-748 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.181

AI, FAIRNESS AND FINANCIAL DATA: A LEGAL STUDY OF INDIA'S UPDATED DATA PROTECTION RULES FOR BANKS

Pranav Kumar Saxena[1]

I. ABSTRACT

Artificial Intelligence (AI) now plays a central role in India's banking sector. Banks depend on AI systems for scoring credit risk, detecting fraud, monitoring transactions, automating customer interactions and supporting compliance processes. These systems promise efficiency and scale, but they also rely on continuous processing of personal and financial data. This increases concerns about fairness, transparency, accuracy and privacy. The Digital Personal Data Protection Act 2023 (DPDP) and the Digital Personal Data Protection Rules notified in 2025 have introduced a detailed and structured framework to govern the processing of such data. These Rules include strict standards for consent, retention, deletion, breach reporting, cross-border transfers and automated decision making. They also create new classifications, Significant Data Fiduciaries, under which most banks are likely to fall. This paper examines how these updated Rules affect AI enabled banking in India. It studies how the Rules shape responsibilities related to fairness, accountability and transparency in automated decision making. It also compares India's approach with global models such as the GDPR, China's PIPL and the United States' sector specific system. While the new Rules mark a major step forward for data governance, the paper argues that India still needs clearer standards on algorithmic fairness, explainability, vendor management and audit requirements. The aim is to support a regulatory environment that encourages innovation while protecting financial data and strengthening trust in AI driven banking.

II. KEYWORDS

Artificial Intelligence, Data Protection, Digital Personal Data Protection Act, 2023, Algorithmic Fairness, Banking Regulation.

[1] B.A. LL.B. (H), LL.M., Associate Vice President (Legal), Kotak Mahindra Bank Ltd. (India).
Email:pranavsaxena19@gmail.com

 (ISSN: 2583-7753)

III. INTRODUCTION

Artificial Intelligence (AI) has become a key part of India's banking ecosystem. Banks use AI to assess creditworthiness, detect unusual transactions, automate customer service, evaluate risk and support compliance functions. These systems help reduce operational costs and improve the speed of decision making. However, they also depend on the large-scale processing of personal and financial data. Because AI systems often operate as "black boxes", concerns around fairness, accuracy, privacy and accountability have grown. Financial data is highly sensitive, and AI models process it at a scale and speed that earlier systems never required. Strong data governance rules have therefore become essential for AI enabled banking.[2]

The Digital Personal Data Protection Act 2023 (DPDPA) is India's first comprehensive personal data law. It regulates the collection, processing, storage, sharing and deletion of personal data by Data Fiduciaries and Data Processors.[3] Many operational requirements under the Act, such as procedures for consent, mechanisms for reporting breaches and cross-border transfer conditions, were left to be clarified through delegated legislation. These have now been detailed in the Digital Personal Data Protection Rules 2025.[4] The Rules form the practical foundation of India's data protection framework and have major implications for how banks develop and deploy AI systems.

The Rules set out strict requirements for valid consent, including standardised notice formats, clear withdrawal procedures and machine readable consent receipts.[5] They impose a seventy-two hour deadline for reporting data breaches.[6] The Rules also introduce conditions for cross-border transfers of personal data, including the possibility of country specific restrictions for financial information.[7] New duties relating to retention and deletion require banks to justify the continued storage of personal data, even though AI models often depend on large historical datasets to

[2] World Bank, *Responsible AI for Financial Services* (2023).
[3] Digital Personal Data Protection Act, 2023 (India).
[4] Digital Personal Data Protection Rules, 2025 (India) r 3, 4, 7, 15.
[5] Digital Personal Data Protection Rules, 2025 (India) r 3.
[6] Digital Personal Data Protection Rules, 2025 (India) r 7.
[7] Digital Personal Data Protection Rules, 2025 (India) r 15.

maintain accuracy.[8] Importantly, the Rules include safeguards for automated decision making, such as the right to human review and transparency obligations when decisions impact a person's legal or financial interests.[9]

A major development in the 2025 Rules is the introduction of categories such as Significant Data Fiduciaries and Systemic Data Fiduciaries. Banks are expected to fall within these categories because of the volume and sensitivity of the financial data they process and the economic importance of their services. These categories involve heightened duties, including independent audits, enhanced documentation, algorithmic transparency measures and periodic compliance reporting.[9] Alongside these developments, the Reserve Bank of India (RBI) continues to impose technology related standards, such as the Cyber Security Framework for Banks,[10] the Digital Lending Guidelines[11] and the Master Direction on IT Governance.[12] Although these instruments help regulate financial technology risks, they were drafted before the DPDPA existed. Banks must now harmonise RBI expectations with the new legal duties under the 2025 Rules.

Scholarly work has also noted that AI enabled banking raises challenges for privacy, fairness and explainability unless regulators provide detailed guidance.[13] This research builds on those concerns but focuses specifically on the legal effects of the updated 2025 Rules, the fairness implications of automated banking systems and the compliance burdens created for the financial sector.

The argument developed in this paper is that while the DPDPA and its 2025 Rules provide an important legal foundation, additional clarity is still required. Banks need clearer regulatory standards on algorithmic fairness, explainability, vendor accountability and audit mechanisms for AI systems. The goal is to propose a regulatory pathway that supports innovation while preserving the privacy and fairness necessary to maintain trust in AI enabled banking.

---

[8] Digital Personal Data Protection Rules, 2025 (India) rr 3, 6, 8 and 13.
[9] Digital Personal Data Protection Rules, 2025 (India) r 13.
[10] RBI, *Cyber Security Framework in Banks* (2016).
[11] RBI, *Guidelines on Digital Lending* (2022).
[12] RBI, *Master Direction on Information Technology Governance* (2023).
[13] Pranav Kumar Saxena, *AI Driven Banking and Compliance with the Digital Personal Data Protection Act 2023* (LLM Dissertation, Jindal Global Law School 2025) 42-48 .

A. Research Objectives

This paper aims to critically examine the adequacy of the Digital Personal Data Protection Act, 2023 and the 2025 Rules in regulating the use of artificial intelligence in the banking sector, with particular emphasis on ensuring algorithmic fairness and data protection compliance.

B. Research Questions

1. Do the 2025 Rules under the Digital Personal Data Protection Act, 2023 provide sufficient safeguards to ensure algorithmic fairness in banking systems?
2. To what extent do existing data protection norms address risks arising from automated decision-making in financial services?
3. What regulatory gaps persist in balancing innovation with accountability in AI-driven banking?

C. Research Methodology

The study adopts a doctrinal legal research methodology, relying on statutory analysis of the Digital Personal Data Protection Act, 2023 and relevant Rules, supplemented by comparative evaluation of international data protection and AI governance frameworks. Secondary sources, including academic literature, policy reports, and regulatory guidelines, are also examined to assess emerging standards on algorithmic accountability.

IV. AI IN INDIAN BANKING: FUNCTIONS, BENEFITS AND RISKS

Artificial Intelligence is no longer experimental in Indian banking. It is embedded in routine operations across public and private sector institutions. Banks use AI systems for customer onboarding, fraud monitoring, credit scoring, anti-money laundering (AML) alerts, chatbot assistance, predictive risk modelling and internal compliance review.[14] These systems analyse transaction histories, behavioural patterns,

[14] Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices* (2023).

repayment records, device metadata and other financial indicators to generate risk assessments in real time.

One of the most visible uses of AI in banking is credit scoring. Traditional credit assessment relied heavily on static financial indicators such as income, collateral and repayment history. AI-driven models, however, incorporate alternative data sources and predictive analytics to generate dynamic risk profiles.[15] This improves speed and can expand access to credit. However, it also raises fairness concerns, especially when model inputs indirectly correlate with protected characteristics such as gender, geography or socio-economic background.

AI is also widely deployed in fraud detection and AML systems. Machine learning models monitor transaction flows and flag suspicious patterns that deviate from historical behaviour.[16] These systems are capable of processing millions of transactions per second, something impossible through manual oversight. While this enhances financial security, automated flagging may result in false positives, account freezes or denial of services without immediate human review. Such outcomes directly affect financial rights and may raise concerns under automated decision-making safeguards.

Another major area of AI deployment is customer interaction. Chatbots and virtual assistants now handle account queries, grievance registration and basic service requests.[17] These systems rely on natural language processing and continuous data training. Although these tools increase convenience, they depend on the storage and processing of conversational data, which may include sensitive financial information.

AI is further used in regulatory compliance and risk forecasting. Banks employ predictive analytics to anticipate non-performing assets, liquidity stress and systemic risk exposure.[18] This strengthens internal governance but increases dependence on large historical datasets. The accuracy of such systems improves with data volume, creating tension with data minimisation principles under privacy law.

---

[15] World Bank, *Responsible AI for Financial Services* (2023).
[16] RBI, *Cyber Security Framework in Banks* (2016).
[17] See industry analysis in NITI Aayog, *Responsible AI for All* (2021).
[18] Bank for International Settlements, *Artificial Intelligence in Banking: Implications for Risk Management* (2021).

The benefits of AI in banking are clear. It improves efficiency, reduces operational costs, enhances fraud detection accuracy and supports financial inclusion.[19] From a macro-economic perspective, reliable AI systems can strengthen the stability of the financial system. However, the same features that make AI powerful, scale, automation and predictive capability, also create structural risks.

First, AI systems are often opaque. Complex machine learning models may not provide clear explanations for their outputs. This creates challenges when individuals seek reasons for adverse financial decisions. Second, AI models can reflect or amplify existing social biases if trained on historically skewed datasets.[20] In the context of credit scoring, this may result in unequal access to financial services. Third, AI systems depend heavily on continuous data collection and retention. The more data available, the better the predictive performance. This creates friction with legal principles of purpose limitation and storage limitation under the DPDPA.[21]

Vendor dependence presents an additional risk. Many banks rely on third-party technology providers or cloud service platforms for AI deployment.[22] This creates layered accountability issues, especially when automated decisions are generated by outsourced systems. Determining responsibility between the bank and the vendor becomes complex in cases of algorithmic error or data breach.

Fairness therefore becomes central to AI driven banking. In financial systems, unfairness does not merely produce inconvenience, it can affect economic opportunity, credit access and livelihood. The legitimacy of AI in banking depends not only on technical accuracy but also on procedural transparency and accountability. The regulatory question is not whether AI should be used, but how it should be governed to prevent discriminatory or opaque outcomes.

The DPDPA 2023 and the Digital Personal Data Protection Rules 2025 must therefore be examined against this technological background. Without understanding how AI systems operate in practice, the legal obligations under the Rules cannot be

[19] International Monetary Fund, *AI and Financial Stability* (2022).
[20] OECD, *Artificial Intelligence, Machine Learning and Bias in Financial Services* (2021).
[21] Digital Personal Data Protection Act 2023, s 4; Digital Personal Data Protection Rules 2025, rr 13-16.
[22] RBI, *Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services* (2015).

meaningfully assessed. This section establishes the operational context within which fairness and compliance challenges arise.

V. INDIA'S DATA PROTECTION FRAMEWORK: THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act 2023 DPDPA represents India's first comprehensive statutory framework governing personal data.[23] It establishes a legal structure that regulates how personal data may be collected processed stored shared and erased. While the Act is technology neutral in language its implications are especially significant for AI systems that rely on large scale data processing.

A. Core Principles of the DPDPA

The DPDPA is built around a consent-based processing model. Personal data may be processed only for a lawful purpose and primarily on the basis of valid consent from the Data Principal.[24] Consent must be free specific informed unconditional and unambiguous.[25] The Act also recognises certain legitimate uses where consent may not be required such as compliance with legal obligations or employment related purposes.[26]

The principle of purpose limitation requires that data be collected only for specified purposes and not processed beyond those purposes.[27] Closely related is the principle of data minimisation which restricts collection to what is necessary for the stated purpose. Although the Act does not use the term data minimisation in the same manner as the GDPR the structure of section 4 reflects this idea by limiting processing to lawful and specified purposes.[28]

The Act also imposes a storage limitation requirement mandating that personal data be erased once the purpose for which it was collected is fulfilled and retention is no

[23] Digital Personal Data Protection Act 2023 (India).
[24] ibid s 4.
[25] ibid s 6.
[26] ibid s 7.
[27] ibid s 4(1).
[28] ibid.

longer necessary.[29] For AI systems which often rely on long term historical datasets for model training and refinement this requirement creates operational tension.

B. Duties of Data Fiduciaries and Data Processors

The DPDPA introduces the concept of a Data Fiduciary defined as any person who determines the purpose and means of processing personal data.[30] Banks clearly fall within this definition when they deploy AI systems to assess customers or monitor transactions. The Act also recognises Data Processors who process data on behalf of a Data Fiduciary.[31] This distinction becomes important in outsourced AI arrangements. Section 8 outlines the general duties of Data Fiduciaries. These include ensuring accuracy of personal data implementing reasonable security safeguards preventing unauthorised processing and notifying the Data Protection Board and affected individuals in the event of a breach.[32] The obligation to maintain reasonable security safeguards is particularly relevant for AI systems which rely on interconnected digital infrastructure.

The Act further provides for the designation of Significant Data Fiduciaries based on factors such as the volume and sensitivity of personal data processed and the risk to the rights of individuals.[33] Such entities may be required to appoint a Data Protection Officer conduct periodic audits and undertake additional compliance measures. Although the Act sets out the framework the operational details of these obligations are elaborated in the 2025 Rules.

C. Rights of Data Principals

The DPDPA provides Data Principals with several statutory rights. These include the right to obtain information about the processing of their data the right to correction and erasure and the right to grievance redressal.[34] These rights aim to promote transparency and individual control over personal data.

[29] ibid s 8(7).
[30] ibid s 2(i).
[31] ibid s 2(k).
[32] ibid s 8.
[33] ibid s 10.
[34] Digital Personal Data Protection Act, 2023 (India) ss 11–14.

However, the Act does not expressly provide a standalone right to explanation for automated decision making in the manner of Article 22 of the GDPR. Instead, safeguards relating to automated processing emerge more clearly in the 2025 Rules. This structural feature of the DPDPA indicates that Parliament intended the Act to function as a broad framework with operational depth supplied through subordinate legislation.

D. Enforcement and Penalties

The DPDPA establishes the Data Protection Board of India as the adjudicatory authority responsible for determining non-compliance and imposing penalties.[35] The Act authorises significant monetary penalties depending on the nature and gravity of the breach.[36] The enforcement structure is administrative rather than judicial in the first instance reflecting a regulatory model designed for compliance oversight rather than purely adversarial litigation.

For banks the possibility of substantial penalties reputational harm and regulatory overlap with RBI supervision creates a dual compliance environment. Financial institutions must therefore treat data governance as a board level issue rather than a purely technical matter.

E. Structural Limits of the Parent Act

Although the DPDPA provides an essential statutory foundation it leaves several areas open ended. It does not define detailed procedures for obtaining consent does not elaborate on cross border data transfer conditions and does not fully address automated decision-making safeguards. These gaps are not accidental. They allow flexibility and regulatory evolution but also create uncertainty until clarified through Rules.

The 2025 Rules therefore play a critical role in transforming the DPDPA from a broad legislative framework into an operational compliance regime. To understand the fairness implications of AI driven banking one must move beyond the text of the Act and examine how these Rules specify and strengthen statutory obligations.

---

[35] Digital Personal Data Protection Act, 2023 (India) s 18.
[36] Digital Personal Data Protection Act, 2023 (India) s 33 and Schedule.

VI. THE DIGITAL PERSONAL DATA PROTECTION RULES 2025: OPERATIONAL OBLIGATIONS FOR BANKS

The Digital Personal Data Protection Act 2023 provides the statutory foundation for personal data governance in India. However, it is the Digital Personal Data Protection Rules 2025 that transform broad principles into enforceable operational duties.[37] The Rules define how consent must be obtained, how breaches must be reported, how cross border transfers may occur and how automated decision making must be regulated. For banks that rely heavily on AI systems, these Rules introduce significant structural change.

It is important to note that the Digital Personal Data Protection Rules, 2025 adopt a phased implementation framework. While Rules 1, 2, and 17–21 came into force upon notification on 14 November 2025, key operational provisions are not immediately enforceable. The provisions relating to Consent Managers (Rule 4) are scheduled to come into force 12 months from notification (November 2026). The remaining substantive obligations including notice and consent requirements, breach notification, data retention, cross-border data transfers, and obligations of Significant Data Fiduciaries are set to become enforceable 18 months from notification, i.e., from approximately May 2027. Accordingly, as of the present analysis, these obligations remain prospective in nature and must be understood within the context of a transitional compliance period.

A. Consent Architecture and Its Implications for AI

The 2025 Rules introduce detailed standards for obtaining valid consent.[38] Consent notices must be presented in clear language and must specify the purpose of processing. Data Fiduciaries are required to provide accessible mechanisms for withdrawal of consent.[39] The Rules also recognise the role of Consent Managers who facilitate consent tracking and communication between Data Principals and Data Fiduciaries.[40]

[37] Digital Personal Data Protection Rules, 2025 (India) r 4 read with the First Schedule.
[38] ibid rr 4-12.
[39] ibid r 6.
[40] Digital Personal Data Protection Rules, 2025 (India) r 4.

For AI systems, consent becomes complicated. AI models often rely on layered analytics where data collected for one purpose may later be used for refinement or retraining of models. The requirement of purpose specificity raises practical concerns. If a bank collects transaction data to process payments, can the same data be used to improve predictive credit scoring models without fresh consent? The Rules demand clarity of purpose and traceability of consent. This may require banks to redesign data pipelines to ensure that each processing purpose is legally defensible.

The withdrawal mechanism also introduces operational risk. If a customer withdraws consent, banks must evaluate whether previously trained models that used that customer's data must be retrained or whether deletion from active datasets is sufficient. The Rules do not explicitly answer this question, leaving banks to interpret the extent of compliance required.

B. Automated Decision Making and Human Review

The Digital Personal Data Protection framework does not provide a standalone right against solely automated decision-making or a general right to human review comparable to GDPR Article 22. Instead, the framework adopts a more limited approach. Section 8(3) of the Digital Personal Data Protection Act, 2023 requires Data Fiduciaries to ensure the accuracy of personal data where it is used to make decisions affecting Data Principals[41]. Additionally, Rule 13(3) of the Digital Personal Data Protection Rules, 2025 imposes an obligation on Significant Data Fiduciaries to undertake due diligence to ensure that algorithmic systems do not pose risks to the rights of Data Principals. These provisions, while relevant, do not amount to a comprehensive regulatory regime governing automated decision-making[42]. Where automated processing significantly affects the rights or interests of an individual, the Data Principal must be informed and must be provided the opportunity to seek human review.

In banking, automated decisions frequently determine credit eligibility, fraud flags and transaction restrictions. These outcomes can directly affect a person's financial

[41] Digital Personal Data Protection Act, 2023 (India) s 8(3).
[42] Digital Personal Data Protection Rules, 2025 (India) r 13(3).

life. The human review safeguard therefore becomes central. However, meaningful human review requires more than superficial validation. It requires access to the reasoning behind the algorithmic output. This creates tension when banks rely on complex machine learning models that do not easily produce explainable outputs.

Unlike the GDPR which expressly articulates a right not to be subject to solely automated decisions in certain contexts,[43] the Indian Rules focus more on procedural safeguards. The emphasis is on transparency and review rather than prohibition. Whether this approach sufficiently protects fairness in high impact financial decisions remains an open question.

C. Data Breach Notification and Incident Reporting

The 2025 Rules impose a strict seventy-two-hour deadline for reporting personal data breaches to the appropriate authority.[44] Data Fiduciaries must also inform affected individuals where harm is likely.[45]

Banks operate interconnected AI systems that integrate transaction monitoring, fraud detection and customer profiling. A breach affecting one system may cascade across others. The reporting timeline therefore requires banks to maintain rapid incident detection and response mechanisms. Delayed discovery may itself become a compliance failure.

In addition to obligations under the DPDPA framework, banks remain subject to RBI cyber security reporting requirements.[46] This creates overlapping compliance structures that must be harmonised. Effective governance requires integrated incident management rather than parallel reporting silos.

D. Cross Border Data Transfers

The Rules establish conditions under which personal data may be transferred outside India.[47] The Central Government may notify jurisdictions to which transfers are restricted. Financial institutions often rely on global cloud infrastructure or

[43] Regulation (EU) 2016/679 General Data Protection Regulation art 22.
[44] Digital Personal Data Protection Rules, 2025 (India) r 7.
[45] ibid.
[46] RBI, Cyber Security Framework in Banks (2016).
[47] Digital Personal Data Protection Rules, 2025 (India) r 15.

multinational analytics vendors. This makes cross border compliance a practical concern.

If financial data is processed or stored in overseas data centres, banks must ensure that such transfers comply with notified restrictions. Contractual safeguards and vendor due diligence therefore become central to compliance strategy. The Rules signal a controlled transfer regime rather than complete localisation. However, uncertainty regarding future government notifications may create planning challenges for institutions that operate across jurisdictions.

E. Data Retention and Deletion

The Rules reinforce the requirement that personal data must not be retained longer than necessary.[48] Data Fiduciaries must erase data once the purpose is achieved unless retention is required by law. For AI systems, historical data often enhances model accuracy. Fraud detection models in particular benefit from long term behavioural datasets.

The tension is clear. Legal compliance encourages minimisation and deletion. Technological optimisation encourages retention and aggregation. Banks must therefore create internal retention schedules that align legal requirements with model development needs. Failure to do so may expose institutions to penalties and reputational harm.

F. Significant Data Fiduciaries

A major innovation of the 2025 Rules is the elaboration of obligations for Significant Data Fiduciaries.[49] These categories apply to entities that process large volumes of sensitive personal data or whose operations have significant impact on the rights of individuals or on economic stability.

Banks are likely to fall within these categories due to the scale of financial data processing and the potential systemic consequences of algorithmic failure. Entities classified under these categories may be required to appoint Data Protection Officers,

[48] Digital Personal Data Protection Rules, 2025 (India) rr 6, 8 and 13.
[49] Digital Personal Data Protection Rules, 2025 (India) r 13.

conduct periodic audits and maintain detailed documentation of data processing practices.[50]

For AI driven banking systems this implies structured internal governance. Algorithmic documentation, fairness assessment and independent audit processes may become regular compliance expectations rather than optional best practices.

This demonstrates that the 2025 Rules significantly deepen regulatory oversight of AI in banking. The next logical step is to examine fairness more directly and assess whether the current framework adequately addresses algorithmic bias and financial discrimination.

VII. FAIRNESS IN AI DRIVEN BANKING

Fairness in financial systems is not merely a moral aspiration. It is a structural requirement for economic stability and social legitimacy. When banks make decisions about credit access account suspension fraud investigation or risk categorisation those decisions directly affect a person's financial life. In an AI enabled environment these decisions are increasingly shaped by algorithmic systems rather than individual officers. This shift requires a careful examination of what fairness means and how it can be protected within a data protection framework.

A. Understanding Fairness in Financial Decision Making

In the banking context fairness includes non-discrimination transparency consistency and procedural accountability. A credit decision must not be based on irrelevant or discriminatory factors. A fraud alert must not disproportionately target specific communities. A risk score must not be influenced by hidden proxies that indirectly reflect protected characteristics.

AI systems are trained on historical datasets. These datasets often reflect existing economic and social patterns. If past lending behaviour favoured certain demographics an AI model trained on such data may reproduce similar outcomes.[51] The system may not explicitly use gender religion or caste as inputs. However, it may rely on correlated variables such as residential location purchasing behaviour or

[50] Digital Personal Data Protection Rules, 2025 (India) r 13.
[51] OECD, Artificial Intelligence and Bias in Financial Services (2021).

employment history. This phenomenon is commonly described as proxy discrimination.[52]

Fairness therefore requires more than absence of explicit bias. It requires active testing and validation of model outputs. In high impact sectors such as banking the consequences of unfair outcomes are not temporary. They may restrict long term access to credit or financial mobility.

B. Algorithmic Bias in Credit Scoring and Fraud Detection

Credit scoring models are particularly sensitive to fairness concerns. AI driven credit systems often incorporate alternative data such as transaction patterns repayment behaviour and digital footprints.[53] While this can expand financial inclusion it may also introduce structural bias if not carefully monitored.

Fraud detection systems present a different challenge. These systems identify unusual behaviour based on deviation from established patterns. If historical enforcement data is skewed towards certain regions or demographic groups, the model may generate higher risk scores for similar profiles. False positives can result in account freezes transaction delays or denial of service. Such outcomes may not always be easily reversible.

The absence of transparent reasoning further complicates the issue. Complex machine learning models including neural networks do not always produce easily interpretable explanations. Without explainability it becomes difficult to assess whether the system is operating fairly.

C. Fairness within the DPDP Framework

The DPDPA 2023 does not explicitly use the term fairness in the same way as the European General Data Protection Regulation.[54] However elements of fairness are embedded within its structure. The requirement of lawful purpose consent-based processing accuracy and grievance redressal indirectly promote fair treatment.[55]

---

[52] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.
[53] World Bank, Responsible AI for Financial Services (2023).
[54] Regulation (EU) 2016/679 General Data Protection Regulation art 5.
[55] Digital Personal Data Protection Act 2023 ss 4-8.

The Digital Personal Data Protection Rules 2025 further strengthen procedural safeguards. They introduce obligations relating to automated decision making and human review.[56] When automated processing significantly affects an individual the person must be informed and allowed to seek review. This procedural protection is important, but it does not automatically ensure substantive fairness.

Unlike the GDPR which recognises a right not to be subject to solely automated decision making in certain circumstances[57] the Indian framework focuses more on transparency and corrective review. The burden therefore shifts to institutions to ensure that AI systems are tested for bias before deployment.

D. Constitutional Dimensions of Fairness

Financial decision making by banks particularly public sector banks can raise constitutional concerns under Article 14 and Article 21 of the Constitution of India. Article 14 guarantees equality before law and prohibits arbitrary state action. Article 21 protects life and personal liberty which the Supreme Court has interpreted to include aspects of dignity and privacy.[58]

If AI systems used by public financial institutions produce discriminatory outcomes without adequate safeguards such decisions may attract constitutional scrutiny. Even private banks may be indirectly influenced by constitutional values given the regulatory environment and public function they perform. The intersection between data protection and constitutional equality therefore cannot be ignored.

E. The Need for Structured Fairness Audits

Given these risks fairness cannot be left to internal discretion. Structured testing procedures bias audits and model validation frameworks are necessary. Several international regulatory bodies have emphasised the importance of model risk management and fairness evaluation in financial AI systems.[59]

---

[56] Digital Personal Data Protection Rules, 2025 (India) rr 3, 6, 8 and 13.
[57] Regulation (EU) 2016/679 art 22.
[58] *Justice KS Puttaswamy v Union of India* (2017) 10 SCC 1.
[59] Bank for International Settlements, *Sound Practices Implications of FinTech Developments for Banks and Bank Supervisors* (2018).

The 2025 Rules create a foundation for accountability by imposing audit obligations on Significant Data Fiduciaries.[60] However the Rules do not specify detailed fairness metrics or testing methodologies. Without clear guidance institutions may adopt inconsistent practices.

For India to develop a credible AI governance framework in banking fairness must be treated as a measurable compliance requirement rather than an aspirational principle. Transparency human review and consent are important. Yet fairness ultimately depends on continuous evaluation of model outcomes and proactive correction of bias.

VIII. COMPLIANCE CHALLENGES UNDER THE 2025 RULES

The Digital Personal Data Protection Rules 2025 create a structured compliance regime for entities processing personal data. For banks that rely on AI systems this regime introduces operational and governance challenges. While the Rules clarify legal duties, they also reveal tensions between technological design and regulatory expectations. Compliance in this context requires institutional restructuring rather than minor procedural adjustments.

A. Data Minimisation versus Data Intensive AI

AI systems function through pattern recognition across large datasets. The predictive accuracy of credit scoring fraud detection and risk models generally improves with volume and diversity of data. Historical data enhances reliability. From a technical perspective data accumulation strengthens model performance.

The data protection framework however emphasises purpose limitation and storage limitation.[61] Personal data must be collected for specified purposes and erased when no longer necessary.[62] Banks therefore face a structural dilemma. If they delete historical data too quickly model accuracy may decline. If they retain data extensively, they risk non-compliance.

[60] Digital Personal Data Protection Rules, 2025 (India) r 13.
[61] Digital Personal Data Protection Act 2023 s 4.
[62] Digital Personal Data Protection Rules 2025 rr 13-16.

The Rules do not clearly define what constitutes necessary retention for model training. Institutions must therefore interpret proportionality standards internally. This creates uncertainty and increases compliance risk.

B. Consent Traceability in Layered AI Systems

Modern AI systems often operate through multiple layers of data processing. Data collected for payment processing may later be analysed to refine credit models or behavioural analytics. The 2025 Rules require purpose specificity and traceable consent.[63]

Ensuring that each dataset used for AI training is covered by valid consent can be administratively complex. If processing purposes evolve over time fresh consent may be required. Tracking consent status across dynamic AI systems demands strong internal data mapping architecture. Many legacy banking systems were not designed for this level of granular consent management.

The withdrawal of consent adds further complexity. When a customer withdraws consent the institution must determine whether that individual's data must be removed from active datasets historical archives or trained models. The Rules do not provide detailed technical guidance on this issue.

C. Explainability and Human Review Limitations

The Rules introduce safeguards for automated decision making including the opportunity for human review.[64] In theory this enhances procedural fairness. In practice meaningful human review requires access to understandable explanations.

Complex machine learning models such as deep neural networks often produce probabilistic outputs without transparent reasoning chains. Generating explainable summaries may require additional technical layers. This increases cost and development time.

There is also a risk of superficial compliance. If human review merely confirms the algorithmic output without independent reasoning the safeguard becomes symbolic.

[63] Digital Personal Data Protection Rules, 2025 (India) rr 8 and 13.
[64] Digital Personal Data Protection Rules, 2025 (India) rr 6 and 13.

Banks must therefore invest in training compliance teams to critically evaluate algorithmic outcomes rather than defer to system recommendations.

D. Vendor Dependence and Outsourcing Risks

Many banks rely on external technology vendors and cloud service providers for AI deployment. Outsourcing increases efficiency but diffuses accountability. The DPDPA distinguishes between Data Fiduciaries and Data Processors.[65] However ultimate responsibility for compliance rests with the Data Fiduciary.

If a third-party AI vendor develops a biased model or suffers a data breach the bank may still face regulatory consequences. Vendor due diligence contractual safeguards and ongoing audits become essential compliance mechanisms. The RBI has separately issued outsourcing risk guidelines which must be harmonised with DPDPA obligations.[66] Cross border data flows complicate this further. If cloud infrastructure is located outside India banks must ensure that transfers comply with notified restrictions under the 2025 Rules.[67] Future changes in government notifications may require technical restructuring of data storage systems.

E. Audit Burdens for Significant Data Fiduciaries

The classification of certain entities as Significant or Systemic Data Fiduciaries introduces enhanced compliance obligations including periodic audits documentation and oversight.[68] For large banks this may require the establishment of dedicated AI governance committees. Audits of AI systems are technically demanding. They may require evaluation of training datasets model performance bias metrics and data lineage documentation. Smaller financial institutions may face capacity constraints in meeting such standards.

While audits strengthen accountability, they also increase operational cost. Compliance therefore becomes not only a legal issue but a strategic resource allocation question.

---

[65] Digital Personal Data Protection Act 2023 ss 2(i), 2(k).
[66] RBI, *Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services* (2015).
[67] Digital Personal Data Protection Rules, 2025 (India) r 15.
[68] Digital Personal Data Protection Rules, 2025 (India) r 13.

F. Overlapping Regulatory Supervision

Banks operate under supervision of the Reserve Bank of India in addition to the data protection regime. RBI circulars on cyber security IT governance digital lending and outsourcing remain applicable.[69] The coexistence of sectoral regulation and horizontal data protection law creates overlapping obligations.

For example, breach reporting requirements under RBI cyber security frameworks may not align perfectly with DPDPA timelines. Institutions must therefore design integrated reporting structures to avoid duplication or inconsistency.

Regulatory overlap can also create interpretative ambiguity. Where guidance from different regulators appears to diverge institutions must adopt conservative compliance strategies. This may slow innovation and increase compliance expenditure. Compliance under the 2025 Rules is therefore not a narrow technical exercise. It requires rethinking data governance architecture internal accountability mechanisms vendor relationships and board level oversight. The next section places these domestic challenges within a comparative international context to assess whether India's framework is aligned with global standards.

IX. COMPARATIVE ANALYSIS: INDIA AND GLOBAL MODELS

The governance of AI in financial systems is not unique to India. Across jurisdictions regulators are grappling with similar questions concerning fairness transparency accountability and systemic risk. A comparative examination helps situate India's Digital Personal Data Protection framework within global regulatory trends and reveals both strengths and areas of uncertainty.

A. European Union: GDPR and the AI Act

The European Union adopts a rights centred approach to data governance. The General Data Protection Regulation GDPR establishes clear principles including lawfulness fairness transparency purpose limitation and data minimisation.[70] Article 22 provides individuals with a right not to be subject to decisions based solely on

[69] RBI, *Cyber Security Framework in Banks (2016); RBI, Master Direction on Information Technology Governance* (2023).

[70] Regulation (EU) 2016/679 General Data Protection Regulation art 5.

automated processing in certain circumstances.[71] This provision is particularly relevant in financial contexts where automated credit decisions may significantly affect individuals.

In addition to the GDPR the European Union has introduced the Artificial Intelligence Act which adopts a risk-based classification system.[72] High risk AI systems including those used in credit scoring and access to essential services are subject to strict obligations. These include conformity assessments documentation requirements transparency standards and ongoing monitoring.

The European model therefore combines individual rights with proactive risk classification. Financial institutions must conduct data protection impact assessments where processing is likely to result in high risk to rights and freedoms.[73] The emphasis is not only on post decision remedies but also on preventive compliance.

Compared to India the EU framework is more explicit in linking automated decision making to fundamental rights protection. However, it also imposes heavier compliance burdens and detailed documentation obligations.

B. China: Personal Information Protection Law and Algorithm Governance

China's Personal Information Protection Law PIPL establishes consent-based data processing with additional state oversight mechanisms.[74] The law includes provisions addressing automated decision making and requires that decisions based on automated processing be fair transparent and not result in unreasonable discriminatory treatment.[75]

China has also introduced algorithm regulation rules that require certain recommendation algorithms to be filed with regulatory authorities.[76] This reflects a governance model where the state plays an active supervisory role in monitoring algorithmic systems.

---

[71] ibid art 22.
[72] Regulation (EU) 2024/1689 Artificial Intelligence Act.
[73] Regulation (EU) 2016/679 art 35.
[74] Personal Information Protection Law of the People's Republic of China (2021).
[75] ibid art 24.
[76] Provisions on the Administration of Algorithmic Recommendation of Internet Information Services (China, 2022).

In the financial sector Chinese regulators emphasise risk control systemic stability and state oversight. While individual rights are recognised the regulatory culture prioritises public order and economic security. This contrasts with the European rights-based model.

Compared to India China's framework is more interventionist in algorithm oversight. India currently relies more on compliance duties and audits rather than mandatory algorithm filing or centralised review.

C. United States: Sectoral Regulation and Model Risk Management

The United States does not have a single comprehensive federal data protection statute comparable to the GDPR or DPDPA. Instead, it follows a sectoral approach. In the financial domain laws such as the Fair Credit Reporting Act FCRA regulate fairness in credit reporting and access to consumer reports.[77] The Equal Credit Opportunity Act prohibits discrimination in lending.[78]

Regulatory agencies such as the Office of the Comptroller of the Currency Federal Reserve and Consumer Financial Protection Bureau issue supervisory guidance on model risk management and AI governance.[79] These frameworks focus on validation documentation and internal controls rather than broad data protection principles.

The US approach is therefore pragmatic and industry specific. It emphasises fairness in lending outcomes and institutional accountability but does not create comprehensive data subject rights comparable to the GDPR. This results in flexibility but also fragmentation.

Compared to India the US model provides clearer fairness standards in credit markets through anti-discrimination statutes. However, it lacks a unified privacy structure governing all personal data processing.

D. Comparative Synthesis: Convergences and Divergences

Across jurisdictions several common themes emerge. First there is increasing recognition that automated decision making in finance carries significant social and

[77] Fair Credit Reporting Act 1970.
[78] Equal Credit Opportunity Act 1974.
[79] Board of Governors of the Federal Reserve System, SR 11-7 Guidance on Model Risk Management (2011).

economic impact. Second transparency and accountability are recurring regulatory priorities. Third human review or corrective mechanisms are widely adopted safeguards.

However, the regulatory philosophies differ. The European Union adopts a rights based preventive model grounded in fundamental rights. China combines consent requirements with strong state supervision of algorithms. The United States relies on sector specific fairness laws and supervisory guidance rather than comprehensive privacy legislation. India's framework occupies a middle position. It establishes broad data protection principles and introduces procedural safeguards for automated decision making but does not yet articulate detailed fairness metrics or explicit anti-discrimination standards for AI systems.

India's introduction of Significant and Systemic Data Fiduciary classifications resembles aspects of the EU risk-based approach. At the same time its reliance on sectoral regulators such as the RBI reflects elements of the US supervisory model. Unlike China India has not adopted centralised algorithm registration mechanisms.

This comparative landscape suggests that India has chosen a hybrid path. The framework is evolving and flexible but still developing its fairness architecture. Whether this hybrid approach will provide sufficient protection in high impact financial contexts depends on how the Rules are interpreted and enforced.

The next chapter draws lessons from this comparative analysis and identifies specific areas where India's framework can be strengthened.

X. LESSONS FOR INDIA

The comparative analysis demonstrates that while jurisdictions differ in regulatory philosophy, certain common principles emerge. These include fairness in automated financial decision making, structured oversight mechanisms, transparency obligations and institutional accountability. India's Digital Personal Data Protection framework reflects elements of these global approaches but remains in a transitional phase.

1. **Clarifying Fairness Standards:** India's framework promotes fairness indirectly through consent requirements transparency duties human review

mechanisms and audit obligations.[80] However unlike the European Union and the United States it does not expressly define algorithmic discrimination standards within financial decision making. Given the economic impact of credit scoring and fraud detection systems India may benefit from regulatory clarification on fairness testing. Supervisory guidance could specify minimum expectations for bias detection validation procedures and periodic model review. The US model risk management framework demonstrates how structured supervisory guidance can enhance accountability without overregulating technological innovation.[81]

2. **Moving Towards System Level Risk Classification:** The European Union's AI Act introduces system specific risk categorisation rather than only entity level classification.[82] India currently classifies Significant Data Fiduciaries at the organisational level.[83] This approach is important but incomplete. AI systems within the same bank do not pose equal levels of risk. A chatbot differs fundamentally from an automated loan rejection system. A calibrated system level risk assessment model would better align regulatory intensity with potential harm.
3. **Strengthening Documentation and Audit Standards:** Comparative frameworks emphasise documentation. The GDPR requires data protection impact assessments in high-risk scenarios.[84] US supervisory practice mandates model validation and documentation protocols.[85] India's Rules require audits for certain entities but do not define algorithm specific documentation standards. Clarifying expectations around training data lineage bias metrics explainability testing and version control would enhance transparency and reduce compliance uncertainty.

[80] Digital Personal Data Protection Rules, 2025 (India) r 13.
[81] Board of Governors of the Federal Reserve System, SR 11-7 Guidance on Model Risk Management (2011).
[82] Regulation (EU) 2024/1689 Artificial Intelligence Act.
[83] Digital Personal Data Protection Rules, 2025 (India) r 13.
[84] Regulation (EU) 2016/679 art 35.
[85] SR 11-7 Guidance on Model Risk Management (n 2).

4. **Coordinating Data Protection and Financial Regulation:** India's dual regulatory environment combines horizontal data protection oversight with sectoral supervision by the Reserve Bank of India. This structure offers strength but may generate duplication. Formal coordination between the Data Protection Board and RBI would improve coherence. Joint advisories on AI governance in banking could harmonise breach reporting retention standards and audit requirements.
5. **Balancing Innovation and Protection:** Comparative experience reveals a common dilemma. Strong rights-based systems enhance protection but increase compliance complexity. Flexible systems encourage innovation but risk inconsistency. India's hybrid framework can balance both objectives if regulatory clarity is progressively strengthened. Clear guidance phased compliance timelines and regulatory dialogue with industry stakeholders can preserve innovation while safeguarding fairness and privacy.

XI. POLICY RECOMMENDATIONS

The Digital Personal Data Protection Act 2023 and the Digital Personal Data Protection Rules 2025 establish a meaningful foundation for data governance in India. However, the rapid expansion of AI systems in banking requires further regulatory refinement. The following recommendations aim to strengthen fairness accountability and institutional clarity without stifling innovation.

1. **Issue Joint AI Governance Guidelines for the Financial Sector:** A coordinated framework between the Data Protection Board of India and the Reserve Bank of India would reduce interpretative uncertainty. Banks currently operate under horizontal data protection law and sector specific financial regulation.[86] Joint guidance could clarify how automated decision-making safeguards under the 2025 Rules interact with existing RBI expectations on model risk

[86] Digital Personal Data Protection Act 2023; Reserve Bank of India regulatory frameworks.

management digital lending and outsourcing.[87] A unified advisory document would promote consistent compliance practices across institutions.

2. **Mandate Structured Algorithmic Impact Assessments:** While the GDPR requires data protection impact assessments in high-risk scenarios[88] India's framework does not yet prescribe detailed AI specific impact assessments. For high impact systems such as automated credit approval fraud blocking and risk categorisation structured algorithmic impact assessments should be required. Such assessments should examine training data representativeness fairness metrics error rates and potential discriminatory outcomes. This would shift compliance from reactive grievance handling to preventive governance.
3. **Standardise Documentation and Model Registers:** Transparency requires documentation. Regulators may consider requiring Significant Data Fiduciaries to maintain internal AI model registers documenting purpose training data sources validation procedures performance benchmarks and version updates.[89] Standardised documentation templates would reduce ambiguity and promote comparability across institutions. This approach aligns with international supervisory practices in financial model governance.[90]
4. **Strengthen Vendor Accountability Mechanisms:** AI systems in banking are frequently developed or supported by third party vendors. The DPDPA places ultimate responsibility on the Data Fiduciary.[91] However practical enforcement requires detailed contractual and monitoring mechanisms. Regulators may consider minimum contractual clauses for AI outsourcing including audit access data localisation assurances security standards and bias testing obligations. RBI outsourcing guidelines provide a foundation but could be updated to explicitly address AI risk.[92]

[87] RBI, *Master Direction on Information Technology Governance* (2023); RBI, *Guidelines on Digital Lending* (2022).
[88] Regulation (EU) 2016/679 art 35.
[89] Digital Personal Data Protection Rules, 2025 (India) r 13.
[90] Board of Governors of the Federal Reserve System, SR 11-7 Guidance on Model Risk Management (2011).
[91] Digital Personal Data Protection Act 2023 ss 2(i), 8.
[92] RBI, *Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services* (2015).

5. **Clarify Retention Standards for AI Training Data:** One of the most complex compliance tensions concerns retention of historical data used for model training. The 2025 Rules require erasure when purpose is fulfilled.[93] However AI models benefit from long term datasets. Regulatory clarification on proportional retention for model improvement would reduce uncertainty. Clear guidance could specify circumstances under which anonymised or aggregated data may be retained without violating storage limitation principles.
6. **Develop Fairness Metrics for Financial AI:** India's framework currently embeds fairness through procedural safeguards. To make fairness measurable regulators could publish recommended fairness indicators for credit and fraud models. These may include disparate impact ratios error distribution analysis and outcome consistency testing. Such metrics need not be rigid thresholds but indicative benchmarks. This would align India with global trends while respecting contextual flexibility.
7. **Adopt a Phased Compliance Approach:** Large public and private banks may possess technical capacity to implement complex audit and documentation standards. Smaller banks non-banking financial companies and fintech entities may face resource constraints. A phased compliance approach based on institutional size systemic relevance and data volume would ensure proportional regulation. This aligns with risk-based governance principles reflected in global frameworks.[94] India stands at a transitional moment in AI governance. The 2025 Rules have moved the legal framework from abstraction to operation. The next step is refinement. Effective AI governance in banking will not emerge from prohibition but from structured oversight continuous monitoring and institutional coordination. If implemented carefully these recommendations can strengthen fairness transparency and trust without slowing digital transformation.

[93] Digital Personal Data Protection Rules, 2025 (India) r 13.
[94] Regulation (EU) 2024/1689 Artificial Intelligence Act.

XII. CONCLUSION

Artificial Intelligence has become deeply embedded in India's banking system. Credit decisions, fraud detection, transaction monitoring, customer service and internal compliance functions increasingly depend on algorithmic systems. These systems offer efficiency scale and predictive accuracy. At the same time, they rely on extensive processing of personal and financial data. This dependence creates structural tensions between technological optimisation and legal accountability.

The Digital Personal Data Protection Act 2023 established a foundational privacy framework. The Digital Personal Data Protection Rules 2025 have now given that framework operational depth. Through detailed consent standards, breach reporting requirements, automated decision-making safeguards, cross border transfer rules and enhanced duties for Significant Data Fiduciaries the Rules significantly reshape the regulatory environment for AI enabled banking.

However, compliance is not merely procedural. The central concern in AI driven finance is fairness. Financial algorithms influence access to credit liquidity and economic opportunity. Even unintentional bias can produce exclusionary effects. The current Indian framework promotes fairness indirectly through transparency human review audit duties and grievance mechanisms. While these safeguards are important they do not yet provide fully articulated fairness standards tailored to algorithmic financial systems.

Comparative analysis reveals that other jurisdictions have adopted varied approaches. The European Union emphasises rights based preventive regulation and risk classification. China combines consent-based governance with strong state oversight of algorithms. The United States relies on sector specific fairness statutes and supervisory guidance. India's model reflects elements of each but remains in a formative stage.

The paper has argued that India's framework provides a strong structural foundation but requires further clarification. Structured algorithmic impact assessments clearer documentation standards coordinated regulatory oversight and measurable fairness indicators would strengthen the system without undermining innovation. The

objective is not to restrain AI adoption but to ensure that its deployment in banking remains accountable transparent and consistent with constitutional values.

India's digital economy ambitions depend on public trust. Trust in AI driven banking will not emerge from technological sophistication alone. It will depend on credible safeguards demonstrable fairness and regulatory clarity. The Digital Personal Data Protection Rules 2025 mark an important step in that direction. Their success will ultimately depend on careful interpretation institutional coordination and continuous refinement as technology evolves.

XIII. BIBLIOGRAPHY

A. Cases

1. Justice KS Puttaswamy v Union of India (2017) 10 SCC 1

B. Legislation (India)

1. Digital Personal Data Protection Act 2023

C. Subordinate Legislation (India)

1. Digital Personal Data Protection Rules 2025

D. European Union Legislation

1. Regulation (EU) 2016/679 General Data Protection Regulation https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 27 February 2026
2. Regulation (EU) 2024/1689 Artificial Intelligence Act https://eur-lex.europa.eu/ accessed 27 February 2026

E. Chinese Legislation

1. Personal Information Protection Law of the People's Republic of China (2021) http://www.npc.gov.cn/ accessed 27 February 2026
2. Provisions on the Administration of Algorithmic Recommendation of Internet Information Services (China, 2022) http://www.cac.gov.cn/ accessed 27 February 2026

F. United States Legislation

1. Equal Credit Opportunity Act 1974 https://www.govinfo.gov/ accessed 27 February 2026
2. Fair Credit Reporting Act 1970 https://www.govinfo.gov/ accessed 27 February 2026

G. Books and Reports

1. Bank for International Settlements, *Artificial Intelligence in Banking: Implications for Risk Management* (2021) https://www.bis.org/ accessed 27 February 2026
2. Bank for International Settlements, *Sound Practices: Implications of FinTech Developments for Banks and Bank Supervisors* (2018) https://www.bis.org/ accessed 27 February 2026
3. International Monetary Fund, *AI and Financial Stability* (2022) https://www.imf.org/ accessed 27 February 2026
4. NITI Aayog, *Responsible AI for All* (2021) https://www.niti.gov.in/ accessed 27 February 2026
5. OECD, *Artificial Intelligence and Bias in Financial Services* (2021) https://www.oecd.org/ accessed 27 February 2026
6. World Bank, *Responsible AI for Financial Services* (2023) https://www.worldbank.org/ accessed 27 February 2026

H. Journal Articles

1. Barocas S and Selbst AD, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671 https://www.californialawreview.org/ accessed 27 February 2026

I. Official Publications and Regulatory Guidance

1. Board of Governors of the Federal Reserve System, *SR 11-7 Guidance on Model Risk Management* (2011) https://www.federalreserve.gov/ accessed 27 February 2026

2. Reserve Bank of India, *Cyber Security Framework in Banks* (2016) https://www.rbi.org.in/ accessed 27 February 2026
3. Reserve Bank of India, *Guidelines on Digital Lending* (2022) https://www.rbi.org.in/ accessed 27 February 2026
4. Reserve Bank of India, *Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services* (2015) https://www.rbi.org.in/ accessed 27 February 2026
5. Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices* (2023) https://www.rbi.org.in/ accessed 27 February 2026

J. Unpublished Academic Work

1. Saxena PK, 'AI Driven Banking and Compliance with the Digital Personal Data Protection Act 2023' (LLM dissertation, Jindal Global Law School, O P Jindal Global University 2025)