

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

AI Governance, Data Privacy and Financial Risk in the Indian FinTech Ecosystem: Recalibrating the Right to Privacy in AI-Driven Lending Markets

ARJUN* AND DR. KHALEEQ AHMAD**

ABSTRACT

Artificial intelligence now underpins credit assessment across India's FinTech ecosystem, yet the legal frameworks governing it still conceive privacy as an individual right and financial risk as a balance-sheet phenomenon. This paper argues that AI-driven credit-scoring systems in India's digital lending markets convert privacy failures into systemic financial risk. Drawing on the technical architecture of behavioural scoring and the economics of alternative data, it shows how algorithmic inference, automated decision-making and standardised model infrastructure transform localised privacy harms into market-wide instability that consent-based data protection and consumer-focused financial regulation cannot contain. Examining the Digital Personal Data Protection Act 2023 and the Reserve Bank of India's digital lending guidelines, it identifies the regulatory gaps through which such risk accumulates. The paper then reconceives privacy as a mechanism of credit-risk governance and sets out policy and technical recommendations, including integrated oversight, mandatory algorithmic impact assessments, algorithmic auditing and privacy-by-design, to align data protection with financial stability and constitutional values.

Keywords: *AI governance; digital lending; data privacy; algorithmic credit scoring; systemic financial risk; Digital Personal Data Protection Act 2023; RBI digital lending guidelines; algorithmic accountability; privacy-by-design; India*

I. INTRODUCTION: AI, DIGITAL LENDING AND THE RECONFIGURATION OF RISK IN INDIA

Artificial intelligence (AI) has become a foundational element of India's fast-growing FinTech ecosystem, particularly in digital lending. AI-driven credit-scoring systems increasingly determine whether individuals can obtain loans, the interest rates they are offered, and how risk

* Author is a Student at Law College Dehradun, Uttarakhand University, Dehradun, Uttarakhand, India.

** Author is an Assistant Professor at Law College Dehradun, Uttarakhand University, Dehradun, Uttarakhand, India.

is allocated to each prospective borrower. Trained on large volumes of personal and behavioural data, machine-learning models promise greater efficiency, scalability and financial inclusion. At the same time, these systems intensify data extraction, reduce transparency and rely on probabilistic reasoning, raising significant concerns for data privacy and fairness.¹ Unlike traditional banking models grounded in human judgment and verifiable financial indicators, AI-driven lending systems reach credit decisions through opaque correlations and proxy variables. In doing so, they unsettle legal and regulatory frameworks that conceptualised privacy as an individual right and financial risk as a balance-sheet phenomenon.²

This paper argues that AI-driven credit-scoring systems in India's digital lending ecosystem convert privacy failures into systemic financial risk. Although the Reserve Bank of India regulates the sector through oversight focused on consumer protection and disclosure, it does not govern the AI systems used to assess credit.³ The structure of the paper reflects this argument. Section 2 explains the technical and economic foundations of AI-driven credit scoring and data extraction. Section 3 examines privacy failures in digital lending and their implications for exclusion and accountability. Section 4 shows how these failures amplify financial risk through model fragility, feedback loops and aggregation effects. Section 5 critiques the regulatory gaps in India's data-protection and financial-oversight regimes. Section 6 offers a theoretical reconstruction of privacy as credit-risk governance, and Section 7 translates that framework into practical policy and technical recommendations. The conclusion addresses the broader implications for AI governance and digital finance in India and beyond.

II. AI CREDIT SCORING AND DATA EXTRACTION IN DIGITAL LENDING

AI-driven credit scoring marks a shift within India's digital lending system away from document-based, institutionally mediated credit assessment towards data-intensive, platform-mediated prediction of creditworthiness. This is more than a technical change: it establishes a new informational basis for credit markets and a new way in which risk is created, priced and distributed. Digital lenders increasingly treat data as both a predictive input and an economic asset, converting heterogeneous behavioural signals into machine-learning models that generate probabilistic judgments of creditworthiness. The resulting socio-technical framework

¹ Douglas W. Arner, János Barberis & Ross P. Buckley, *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 NW. J. INT'L L. & BUS. 371, 393–401 (2017).

² *Id.*

³ RESERVE BANK OF INDIA, *Guidelines on Digital Lending*, RBI Circular No. DOR.CRE.REC.66/21.07.001/2022-23, at 5–6 (Sept. 2, 2022), <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12382> (since superseded by the RESERVE BANK OF INDIA (Digital Lending) Directions, 2025, dated May 8, 2025).

encourages large-scale data collection, widens informational asymmetry and embeds model risk within routine lending decisions.⁴

A. From traditional credit assessment to predictive lending infrastructure

Conventional credit assessment relies on a small set of readily interpretable variables, such as documented income, credit history, collateral and credit-bureau records. These are processed within institutionalised settings subject to controls and regulatory oversight of discretionary decision-making. AI-based predictive lending systems operate differently and share three principal characteristics: they ingest a wide range of individual and behavioural data; they identify features that correlate with repayment probability; and they render decisions algorithmically on the basis of those predictions. Because such assessment rests on indirect or proxy measures of behaviour, the legitimacy and reliability of the resulting decisions depend on data quality, feature-selection methods, model stability and governance arrangements, all of which are typically opaque to both borrowers and regulators.⁵

B. Model architecture, feature engineering and the production of risk

Machine-learning credit-scoring systems in digital lending typically follow four stages: data collection and aggregation; feature engineering; model development and testing; and deployment with continuous performance monitoring. Feature engineering is especially significant, because the processes that convert raw data into predictive variables, such as mobile-usage patterns, device characteristics and communication or spending proxies, encode normative assumptions about which borrower behaviours count as “credit relevant.”⁶ These assumptions carry two implications. First, the choice of which behaviours are treated as relevant shapes how credit is distributed across classes of borrowers, so that those who do not display the behaviour patterns dominant in the training data may be disadvantaged. Second, the assumptions introduce fragility into risk estimation, because a model's reliance on correlations within the training data is liable to break down during periods of economic stress or when borrower behaviour changes.⁷ Moreover, given the emergence of requirements that lenders

⁴ Arner, Barberis & Buckley, *supra* note 1, at 393–401.

⁵ Brent D. Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter & Luciano Floridi, *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y 1, 8–10 (2016), <https://doi.org/10.1177/2053951716679679>.

⁶ WORLD BANK GROUP, *The Use of Alternative Data in Credit Risk Assessment: Opportunities, Risks, and Challenges* 24–35 (2025), <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031325132018527>.

⁷ Chong Huang, Arash Nourian & Kevin Griest, *Hidden Technical Debts for Fair Machine Learning in Financial Services*, in NEURIPS 2020 FAIR AI IN FINANCE WORKSHOP 2–6 (2021).

explain their credit decisions, the difficulty of interpreting complex models is likely to impair their ability to comply and to offer intelligible explanations.⁸

C. Alternative data and the logic of behavioural scoring

The defining operational feature of India's AI-driven digital lending industry is its reliance on alternative data. Mobile metadata, app-usage patterns, geolocation signals, social-graph proxies, browsing activity and transactions conducted through digital platforms are among the alternative data sources used. Such data has been presented as a solution for “thin-file” borrowers, that is, individuals without an established formal credit history. As alternative data is integrated into lending in India, however, it raises governance questions concerning necessity, proportionality and legitimacy.

Alternative data has enhanced the ability to predict borrower behaviour, but that gain has simultaneously created new risks to borrower privacy. Many of the alternative data sources used by lenders serve as proxies for individual characteristics such as socio-economic status, location and occupation. In many cases the predictive power of these variables derives from structural inequality rather than from a borrower's actual financial conduct. Behavioural scoring can therefore operationalise financial disadvantage as financial risk, producing exclusion under the guise of a neutral predictive model.⁹ A market-based view reveals a further effect: strategic opacity for borrowers and lenders alike. Borrowers cannot determine how the data they generate, such as social-media activity, contributes to their credit score, while lenders may be incentivised not to disclose the feature logic behind those scores, particularly where the models are proprietary. The resulting asymmetry makes it difficult for borrowers to contest decisions and increases the likelihood that errors, whether from biased data, spurious correlations or model drift, remain hidden until they surface as a default or reputational crisis for the lender.¹⁰

III. PRIVACY FAILURE IN DIGITAL LENDING APPLICATIONS

The use of AI in credit evaluation has accelerated the delivery of loans in India's digital lending market, but it has also exposed the limits of prevailing data-protection paradigms. Privacy regulation has traditionally defined harm as the loss of individual control over personal information. AI-enabled lending shows, however, that privacy failures occur systematically and

⁸ Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 35–47 (2017), <https://doi.org/10.2139/ssrn.2972855>.

⁹ Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 691–702 (2016).

¹⁰ Sandra Wachter, Brent Mittelstadt & Chris Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, 41 COMPUTER L. & SEC. REV. 105567, at 7–12 (2021), <https://doi.org/10.1016/j.clsr.2021.105567>.

produce collective, market-wide consequences. In this setting, privacy violations are no longer isolated infringements of individual autonomy; they are mechanisms through which algorithmic decision-making amplifies informational asymmetry, exclusionary outcomes and financial instability.¹¹

A. The structural limits of consent in AI-driven lending

Data-protection law relies heavily on consent, which assumes that individuals can make informed decisions about the use of their personal data. In AI-driven digital lending, that assumption largely collapses. A credit application typically requires the borrower to accept broad terms granting wide-ranging permission to collect device information, contact lists, location, behavioural patterns and other data extending well beyond what a conventional assessment would require.¹² Machine-learning models generate predictions by identifying associations across large datasets rather than by reference to defined variables, enabling further downstream inferences that the borrower may neither anticipate nor understand.¹³ Even where formal consent is given for discrete categories of data, the borrower has no realistic means of knowing how those categories will be combined, reused or inferred in reaching a credit decision. Consent therefore loses its force as a constraint on the algorithms used in that process.¹⁴ Because consent is obtained at a single point in time, it cannot reasonably be expected to govern all future uses of the borrower's data. In India's digital lending markets, consent functions largely as a procedural device for platforms rather than as substantive protection for borrowers.

B. Algorithmic inference and the erosion of informational boundaries

A defining feature of AI-based credit evaluation is algorithmic inference, which has become central to how creditworthiness is assessed. Traditional lending evaluates borrowers on the basis of explicit financial information and does not infer creditworthiness from proxy variables and behaviour. Those proxy variables often embody sensitive socio-economic information that is not collected directly from the borrower.¹⁵ Inferential capacity erodes the regulatory boundary between sensitive and non-sensitive data. Apparently innocuous data points, such as how often an applicant uses a mobile application, how their location changes over time or how frequently they communicate with others, can be used to infer whether a borrower has stable employment, is in financial difficulty or is socially vulnerable.¹⁶ The dispersion of knowledge about the logic

¹¹ Mittelstadt et al., *supra* note 5, at 10–14.

¹² RESERVE BANK OF INDIA, *supra* note 3, §§ 5–9.

¹³ Barocas & Selbst, *supra* note 9, at 691–702.

¹⁴ Paul De Hert & Vagelis Papakonstantinou, *The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?*, 32 COMPUTER L. & SEC. REV. 179, 182–86 (2016).

¹⁵ Barocas & Selbst, *supra* note 9, at 691–97.

¹⁶ WORLD BANK GROUP, *supra* note 6, at 24–33.

underlying AI-based credit models creates accountability gaps that undermine both the protection of individual privacy and the management of lending risk.¹⁷

C. Privacy failure, algorithmic bias and financial exclusion

Where a model uses proxy variables correlated with socio-economic status, geographic location or historical disadvantage, it is likely to reproduce and intensify existing structural inequality. This form of algorithmic exclusion is typically concealed beneath a veneer of technical objectivity and predictive accuracy, and so does not resemble the overt discrimination familiar from other areas of law. While such methods may extend credit to some individuals who lack a formal credit history, they also subject vulnerable populations to greater surveillance and less transparent evaluation. Biased datasets and erroneous inferences produce misclassifications and exclusions across large segments of the population, resulting in inefficient and risky allocation of credit. Such distortion undermines lenders' ability to hold diversified portfolios and increases their exposure to correlated defaults. Privacy violations are therefore not only infringements of privacy but also a source of financial instability.¹⁸

IV. FINANCIAL RISK AMPLIFICATION THROUGH AI

AI-enabled credit scoring reaches far beyond the individual lending decision, generating new risks across digital lending platforms. The automation of judgment, the embedded use of black-box inferential logic and the standardisation of decision architecture across lenders together create financial risks that traditional risk-management and regulatory tools cannot readily detect. Within India's expanding digital lending ecosystem, privacy failures and algorithmic bias thereby become systemic vulnerabilities capable of undermining the stability of credit markets.

A. Model risk and algorithmic fragility in credit markets

Digital lenders in the Indian FinTech market increasingly rely on similar models, third-party analytics providers and off-the-shelf machine-learning tools, creating conditions in which correlated model failures become likely. When many lenders build credit models with comparable structures and train them on comparable datasets, errors or biases propagate across lenders at the same time.¹⁹ Such correlated failures erode the diversity that ordinarily mitigates credit risk. Model fragility is also strongly influenced by the quality and provenance of the

¹⁷ Andrew D. Selbst, danah boyd, Sorelle A. Friedler, Suresh Venkatasubramanian & Janet Vertesi, *Fairness and Abstraction in Sociotechnical Systems*, in PROCEEDINGS OF THE 2019 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 59, 60–65 (2019).

¹⁸ Arner, Barberis & Buckley, *supra* note 1, at 398.

¹⁹ D. Sculley et al., *Hidden Technical Debt in Machine Learning Systems*, in 28 ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS 2503, 2504–07 (Corinna Cortes et al. eds., 2015).

training data. Although these weaknesses may remain dormant during periods of stable growth, they can become pronounced during downturns, when shifts in borrower behaviour cause previously stable relationships to break down. Excessive data extraction can thus reduce model resilience rather than improve the prediction of risk.

B. Feedback loops and the automation of credit risk

AI lending operates within feedback-driven environments: decisions are produced from past data, and those decisions in turn shape the data fed into future models. The approval or rejection of credit influences borrower behaviour, which then re-enters the training data for later models, creating a self-reinforcing loop that can magnify an initial error or bias.²⁰ Automation accelerates these dynamics. Unlike human decision-makers, whose judgments vary in consistency, AI systems apply uniform logic and reach instantaneous decisions at scale. When flawed assumptions are applied across thousands of credit decisions with little friction, the speed and scale of automation transform localised model defects into a market-wide risk vector.²¹

C. Opacity, explainability and supervisory blind spots

Most machine-learning models used in credit scoring, including deep-learning and ensemble methods, are highly opaque. Although such models may offer greater predictive accuracy than simpler ones, they yield little insight into their decision-making for borrowers, lenders or regulators.²² This opacity poses significant challenges for the supervision of financial institutions. Regulators depend on transparency and auditability to assess an institution's risk exposure, yet opaque AI models offer few opportunities for such analysis. Where lenders cannot adequately explain model behaviour, regulators struggle to determine whether a credit decision rested on prudent risk assessment or on unstable correlation. Opacity also creates internal risk-governance problems. Senior managers and compliance staff often lack the technical capacity to interrogate model outputs, which encourages greater reliance on automated decisions. This tendency, known as automation bias, reduces human oversight and increases the likelihood that model errors remain undetected until a loss is incurred.²³

D. Privacy failures as a catalyst of financial instability

Privacy violations in digital lending destabilise the financial environment by distorting the information on which lenders assess creditworthiness. When lenders extract excessive personal

²⁰ *Id.* at 2505–06.

²¹ *Id.*

²² Edwards & Veale, *supra* note 8, at 35–42.

²³ Sculley et al., *supra* note 19, at 2505–08.

information, they heighten their vulnerability to breaches, regulatory action and reputational loss. These harms impose financial burdens on lenders and erode consumer trust, further weakening confidence in the marketplace.²⁴ Crucially, the risks generated by privacy failures do not fall on the individual lender or borrower alone. A data breach, regulatory intervention or public backlash can trigger a sudden contraction of available credit and spill over into other parts of the economy. Privacy breaches thus operate as negative externalities that transmit risk across institutions and markets.

E. Aggregation effects and systemic credit risk

Systemic risk arises from an accumulation of vulnerabilities across connected actors rather than from any single event. AI-driven lending fosters such aggregation through shared infrastructure, common algorithms and common data sources.²⁵ In India, digital lending platforms partner with third parties such as banks and non-banking financial companies, multiplying the channels through which risk is shared. The failure of one entity, or a regulatory intervention against it, can propagate rapidly to others linked by contract and technology. Traditional prudential tools, designed for balance-sheet risk and human decision-making, cannot adequately manage these algorithmic risks. Pre-empting rather than merely reacting to privacy and AI-driven lending risks requires rethinking how they are governed as part of financial risk management.²⁶

V. REGULATORY GAPS IN INDIA: THE RBI AND THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

India's regulatory response to AI in digital lending is marked by fragmentation, sectoral silos and frameworks built on assumptions that predate algorithmic decision-making. The DPDP Act 2023 provides an overarching legal framework for the processing of personal data but does not address the systemic risks posed by AI-driven credit scoring, and neither do the RBI's sector-specific digital lending guidelines. The failure to align data-protection law with financial regulation produces regulatory blind spots through which privacy failures translate into credit-market instability rather than merely individual harm.²⁷

A. Consent without algorithmic accountability

The DPDP Act rests on established principles of consent, purpose limitation and data minimisation. Sound as these principles are, their application presupposes conditions that do

²⁴ De Hert & Papakonstantinou, *supra* note 14, at 183–87.

²⁵ WORLD BANK GROUP, *supra* note 6, at 37–43.

²⁶ FIN. STABILITY BD., *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* 31–39 (2017).

²⁷ *Id.*

not obtain when AI is used in lending.²⁸ As shown above, where borrowers cannot reasonably determine what will be inferred, combined or repurposed by a machine-learning system, consent becomes largely meaningless. The Act provides no mechanism to require explanations of how inferential analytics or proxy variables are used, or of how continuously trained models reach decisions. Compliance with consent requirements can therefore coexist with wholly opaque and discriminatory credit decision-making.

More significantly, the DPDP Act imposes no requirement of algorithmic transparency, explanation or impact assessment for high-risk automated decision-making. The fiduciary obligations it places on data fiduciaries are essentially procedural; nothing requires an entity to demonstrate how its use of AI affects market stability or access to finance.²⁹ This absence of algorithmic accountability has significant consequences for digital lending. Without such requirements, lenders can deploy complex credit-scoring models without demonstrating that they operate fairly, accurately or without adverse effects on the wider economy or on financial inclusion.

B. Regulatory silence and the problem of systemic risk

The most critical gap in the regulatory framework for AI in lending is the absence of systemic-risk assessment. Both the DPDP Act and the RBI guidelines assume that harms from AI lending can be contained through individual enforcement, an approach that fails in an algorithmic market characterised by scale, automation and interdependence. Privacy violations and model errors accumulate where many lenders deploy similar AI systems trained on similar datasets. Individual consent withdrawals may address particular privacy concerns, and post-incident grievance mechanisms may compensate consumers harmed by flawed models, but neither remedies the systemic distortion of credit allocation. Addressing that distortion requires a regulatory structure that prevents the accumulation of risk and ensures that models are diverse, robust and accountable.³⁰ Recognising privacy as a determinant of financial stability is essential to a complete regulatory response. Regulation of the AI lending market therefore demands a shift from procedural compliance towards substantive oversight of AI systems as determinants of systemic risk.

²⁸ Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 76, 81–86 (2017).

²⁹ Gillian K. Hadfield & Jack Clark, *The Role of Standards in the Governance of Artificial Intelligence*, 7 NATURE MACH. INTELLIGENCE 1, 6–10 (2023).

³⁰ EUR. BANKING AUTH., *Report on Machine Learning for Internal Ratings-Based Models* 39–49 (2021).

VI. RECALIBRATING PRIVACY AS CREDIT-RISK GOVERNANCE

Privacy violations in AI-based lending cannot be corrected effectively by consumers or by procedural compliance such as consent. Consent-based data protection and consumer-oriented financial regulation are alike unable to capture how algorithmic lending restructures risk at the market level. This section advances the paper's central conceptual proposition: privacy in AI-based lending should be reconceived as a means of governing credit risk within markets, rather than solely as a consumer right. So understood, it aligns the values embedded in the Indian Constitution with financial stability and supplies a normative basis for regulatory action in algorithmic markets.

A. From individual right to systemic safeguard

Privacy law has been grounded in protecting individual autonomy, dignity and control over personal information, on the assumption that privacy harms are individuated, traceable to an identifiable source and remediable through a claim for damages. AI-driven credit markets unsettle these assumptions. Automated credit decisions rely on aggregation, inference and automation, producing harms that are diffuse, probabilistic and collective.³¹ Privacy violations in digital lending arise not only from the misuse of data without consent but also from distortions of credit judgment that affect large numbers of consumers simultaneously. Such harms cannot be remedied effectively through individualised consent withdrawal or grievance resolution.

Recognising privacy as a safeguard against systemic harm acknowledges that data protection stabilises the financial marketplace. By limiting the data that may be collected and used to assess creditworthiness, constraining the opacity of AI systems and requiring transparency and accountability in system design, privacy regulation reduces the probability of correlated model failures and the mispricing of credit risk. Privacy protection thereby functions as a form of oversight analogous to prudential regulation, curbing negative externalities and preserving market integrity.

B. Privacy-by-design as a risk-control mechanism

Privacy-by-design is commonly treated as a risk-management or compliance strategy in AI-driven lending. It is better understood as a practical, technical approach to controlling the risks inherent in building accurate and reliable credit-scoring models. Embedding privacy controls in the architecture of such models can improve model stability, data quality and the reliability of

³¹ Tal Z. Zarsky, *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making*, 41 SCI., TECH. & HUM. VALUES 118, 124–33 (2016).

the decisions they produce.³² Constraints on inferential analytics, such as limiting the use of opaque proxy variables, reduce the likelihood that models embed bias or unstable correlations. These constraints do not restrict innovation; they promote responsible system development by aligning technical optimisation with regulatory objectives. From a governance perspective, privacy-by-design operates as an ex-ante risk-reduction strategy rather than an ex-post compliance exercise.

C. Explainable AI and the governance of credit risk

Explainability is the central mechanism through which privacy is recalibrated as credit-risk governance. The inability to explain the basis of algorithmic loan decisions erodes both the capacity of individuals to assert their rights and the capacity of systemically relevant actors to supervise lending activity. Borrowers cannot contest unfavourable decisions, lenders cannot confirm that a model is behaving appropriately, and regulators cannot assess the risk that AI-driven lending introduces into the system.³³ From a financial-governance standpoint, explainability enables auditing and accountability. It does not require full transparency of complex models; it requires a meaningful, context-specific account of how and why a model produces particular outcomes, sufficient for regulators and supervisors.³⁴ Incorporating explainability standards within privacy standards transforms the right to explanation from an individual entitlement into an instrument of risk management. Explainability strengthens institutional oversight of AI systems by enabling regulators to assess whether such systems generate correlated risk or market instability, thereby bridging the gap between data protection and prudential supervision.³⁵

D. Regulatory integration and the governance of algorithmic markets

Reconceiving privacy as credit-risk governance calls for an integrated regulatory response. Data-protection authorities and financial regulators must move from separate, individualised oversight towards integrated oversight of AI-based lending systems. Such integration is necessary because both the collection of personal data for AI-driven credit assessment and its use in credit decisions implicate personal-data rights and systemic financial stability at once. These requirements should be understood by developers as establishing predictability rather than stifling innovation; they are designed to provide certainty and to enhance trust in digital

³² Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy* 40–55 (FOUND. & TRENDS IN THEORETICAL COMPUT. SCI., Vols. 9–10, Nos. 3–4, 2014).

³³ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 102–11 (Harvard Univ. Press 2015).

³⁴ EUR. BANKING AUTH., *Report on Machine Learning for Internal Ratings-Based Models* 65–74 (2021).

³⁵ Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1098–1112 (2018).

lending markets. Above all, integration shifts the regulatory paradigm from reactive enforcement to proactive governance, enabling regulators to treat privacy failures as potential sources of systemic risk and to intervene early, before distortions escalate into market instability. This accords with broader trends in financial regulation towards building resilience through macroprudential oversight.³⁶

VII. POLICY AND TECHNICAL RECOMMENDATIONS

The preceding sections have established that AI-based credit scoring within India's digital lending ecosystem generates systemic risks that neither consent-centric data protection nor consumer-focused financial regulation can adequately address on its own. A coordinated combination of policy and technical intervention is required to manage these risks while treating privacy as an essential component of credit-risk governance. This section sets out targeted recommendations to implement that recalibration while preserving the benefits of innovation and financial inclusion.

A. Integrated oversight of data protection and financial regulation

A primary policy priority is to coordinate the enforcement of data protection with the supervision of financial institutions. The current separation between data-protection authorities and financial regulators risks creating blind spots in the oversight of AI-based lending systems. By developing joint monitoring and audit structures, such as coordinated supervisory task forces or shared audit procedures, regulators can observe data-collection and data-use practices at both the micro level of individual consumers and the macro level of financial markets. Coordination of this kind does not require a merger of regulatory bodies, but it does require functional cooperation between them. Data-protection authorities bring expertise in lawful processing, data minimisation and accountability; financial regulators bring expertise in prudential risk and market stability. Treating AI systems as socio-technical infrastructure allows regulators to supervise them against the combined demands of compliance and stability, rather than as isolated compliance questions.

B. Mandatory algorithmic impact assessments for digital lending

Algorithmic impact assessments, directed at how data is used, how models operate and how they affect consumers, should be required both before and after the deployment of AI-driven credit-scoring systems. Unlike ordinary compliance checks, such assessments focus on a lender's data use, feature selection, the potential for models to propagate bias and the risk that

³⁶ Hilary J. Allen, *Driverless Finance*, 10 HARV. BUS. L. REV. 157, 187–203 (2020).

they generate feedback loops. Embedding them within regulatory frameworks shifts regulation from a reactive to a proactive posture, allowing regulators to identify problems before they become systemic and to require corrective action before vulnerabilities materialise. These assessments should be proportionate and risk-based, concentrating on high-risk lending applications rather than imposing uniform burdens on all financial technologies.

C. Institutionalising algorithmic audits and governance structures

Algorithmic audits should become an integral part of enterprise risk management for all digital lending entities. Unlike traditional information-technology audits, which examine static or historical system performance, algorithmic audits assess the real-time, dynamic behaviour of systems, including bias, drift and interaction effects. Such audits help to reveal emerging risks before they crystallise through a market disruption.³⁷ At the firm level, lenders should establish AI risk councils drawing on legal, technical and risk-management expertise to oversee model development, deployment and ongoing monitoring. The principal function of such councils should be to ensure that privacy is integrated into the organisation's strategic planning rather than treated as a discrete compliance obligation.

D. Normative alignment with financial inclusion and market stability

The need to manage the risks of AI-based lending must be balanced against its capacity to extend credit to the financially excluded. AI-based lending offers considerable opportunities to improve access to credit for underserved populations, but these will be realised only where adequate governance prevents exclusionary or exploitative practices. Treating privacy as part of credit-risk management links inclusion with stability by encouraging data practices that enhance both model reliability and borrower trust. Normatively, treating privacy as an enabler of sustainable digital finance, rather than an obstacle to it, provides a framework for constitutionally aligned digital lending markets and for resilience within them.

VIII. CONCLUSION

This paper has shown that India's digital lending system uses AI to transform borrowers' personal data into predictions of their capacity to repay. It has demonstrated that, once such data is consolidated into a single judgment about repayment, each loss of control over personal data creates a new vulnerability capable of destabilising the credit market, excluding otherwise eligible borrowers and undermining regulatory coherence. The prevailing regulatory settlement,

³⁷ Inioluwa Deborah Raji et al., *Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing* 6–12 (Proc. 2020 Conf. on Fairness, Accountability & Transparency, 2020).

built on the consumer's right to control personal data and to be protected from predatory lending, cannot govern these dynamics.

The paper has identified three mechanisms through which the loss of privacy in digital lending generates systemic vulnerability. First, algorithmic inference dissolves the informational boundaries that protect personal data. Second, automated decision-making displaces the borrower's capacity to give meaningful informed consent. Third, where an algorithm produces a biased or unreliable assessment of creditworthiness, it can propagate discriminatory lending across a large segment of the market. As data flows through standardised infrastructure and decision architecture, these mechanisms create systemic risks that are difficult to detect and mitigate with traditional supervisory tools. Treated as a peripheral ethical concern, the failure to protect borrower privacy obscures the central role that privacy plays in the reliability and resilience of AI-driven credit markets. To address AI-induced systemic risk, the paper has proposed a conceptual framework that recasts privacy as a means of governing credit risk, and has outlined regulatory strategies, including privacy-by-design, transparency requirements for AI-driven models, algorithmic auditing and monitoring, and integrated oversight.

This framework is especially pertinent to India, which is rapidly digitising its economy, relying increasingly on alternative data to assess creditworthiness, and operating within a decentralised and fragmented regulatory environment. The approach accords with India's constitutional commitment to dignity and equality and offers a means of promoting sustainable innovation in digital finance. Ultimately, the paper underscores the importance of regulatory approaches capable of addressing the risks posed by AI systems in financial markets, and the limits of existing regimes that attend primarily to technological capability rather than to the structural risks associated with automation, inference and scale.
