The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DATA GOVERNANCE AND ARTIFICIAL INTELLIGENCE IN INDIA: BALANCING INNOVATION, PRIVACY AND REGULATORY COMPLIANCE

DIVYANSHA SINGH

ABSTRACT

India's increasing adoption of artificial intelligence has exposed significant tensions within a date governance framework that was not designed to regulate algorithmic decision making. This paper examines the relationship between India's policy emphasis on promoting innovation in artificial intelligence, its constitutional and statutory protections for privacy and the regulatory compliance obligations that presently govern AI development. The paper examines the constitutional recognition of privacy as a fundamental right, the statutory framework established by the information technology act, 2000 and the digital personal data protection act, 2023 and the largely non-binding policy instruments particularly NITI Ayog's national strategy for Artificial intelligence that continue to influence AI governance and regulatory compliance in India. Drawing upon doctrinal analysis and a comparative study of the European union's risk based regulatory model it argues that India's reliance on sector specific regulation and voluntary ethical principles leaves significant compliance gaps in addressing algorithmic harms particularly in law enforcement, credit assessment and public welfare administration. Three case studies are examined to evaluate how these regulatory shortcomings operate in practice. The paper concludes that India need not abandon its innovation oriented approach to artificial intelligence but should strengthen the existing legal framework by introducing enforceable compliance obligations for high risk AI systems.

Keywords: Artificial Intelligence, Data Governance, Digital Personal Data Protection Act, Privacy, Regulatory Compliance, Algorithmic Accountability, India.

I. INTRODUCTION

Artificial intelligence has moved from a speculative technology to a working feature of Indian public and commercial life with unusual speed. Credit decisions, welfare eligibility, policing and healthcare diagnostics increasingly rely in some measure on systems that learn from data rather than follow rules written in advance by a human decision maker.[1] This transformation has fundamentally altered the nature of regulatory oversight. A regulator accustomed to reviewing a fixed set of rules now has to reckon with systems whose behaviour can shift as they are trained on new data and whose reasoning is not always fully legible even to the people who built them.

India's policy response has evolved through strategy papers, expert committee reports and sector specific regulatory initiatives while stopping short of enacting a dedicated legislation governing artificial intelligence.[2] This is not necessarily a flaw a number of jurisdictions have chosen to regulate AI through existing legal categories rather than inventing new ones but it does mean that the adequacy depends heavily on how well its surrounding legal infrastructure particularly its data protection regime actually reaches the harms that AI system can cause.

That infrastructure has itself been in motion. The Supreme Court's recognition of privacy as a fundamental right supplied for the first time a constitutional anchor for data protection in India.[3] The Digital Personal Data Protection Act, 2023 followed several years later replacing an earlier more expensive bill that had been withdrawn amid concern about its impact on data driven industry.[4] The result is a data protection statute whose final form reflects the continuing tension between innovation and regulation that also characterizes India's evolving approach to AI governance.

---

[1] Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making* (Aug. 29, 2018), https://ssrn.com/abstract=3240384.
[2] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).
[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[4] Divij Joshi, AI Governance in India – Law, Policy and Political Economy, 10(3) Commc'n Rsch. & Prac. 328 (2024).

This paper asks whether India's current legal architecture constitutional privacy protection The Digital Personal Data Protection Act, 2023 the residential reach of the Information Technology Act, 2000 and a body of non-binding AI policy is capable of holding algorithmic systems accountable for the harms they can cause or whether the emphasis on enabling innovation has left compliance obligations too thin to matter in practice. It proceeds by examining the constitutional and statutory framework the specific governance gaps that arise from AI's technical, characteristics a set of illustrative case studies and a comparative look at the European Union's alternative model before proposing measures for a more balanced and effective regulatory framework.

II. LITERATURE REVIEW

Scholarship on AI governance in India has grown considerably in recent years though it remains divided along several analytical lines. This section surveys the existing literature, identifies where it converges and locates the gap this paper seeks to address.

A significant body works treats the technical characteristics of AI systems as the appropriate starting point for policy analysis. Marda argues that Indian AI policy has historically treated the social and ethical risks of data driven decision making as retrospective concerns, addressed only after deployment rather than built into policy from the outset.[5] Her framework which separates machine learning into the stages of data, model and application demonstrates that bias and discrimination may arises at multiple stages from unrepresentative training data and model design to the context in which an AI system is ultimately deployed.[6] This literature is valuable for showing that consent based, transaction focused data protection law is poorly matched to harms that arise gradually through pattern and inference rather than through a single identifiable act of data collection.

A second strand of scholarship approaches the same subject from a political economy perspective. Joshi argues that India's AI governance instruments do not merely fail to regulate harm, they actively construct and legitimize a particular economic order one in which personal data is framed as a national productive resource and regulatory restraint is

[5] Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making* (Aug. 29, 2018), https://ssrn.com/abstract=3240384.
[6] Id.

framed as an obstacle to growth.[7] On this account the withdrawal of India's original data protection bill and the comparatively permissive from of The Digital Personal Data Protection Act, 2023 that eventually replaced it are better understood as the consequence of a governance approach that consistently prioritises data driven economic growth over individual rights.[8] This literature disagrees with Marda's implicit premise that better designed policy processes could resolve the tension between innovation and accountability, Joshi suggests the tension is structural rather than matter of policy design.

A third strand of scholarship represented by Patra takes a more conventional doctrinal approach cataloguing the statutory and regulatory instruments currently in force the Information Technology Acts's residual provisions, sectoral guidance from the Reserve bank of India and the securities and exchange board of India and NITI Ayog's non-binding strategy documents and arguing that their fragmentation rather than any single missing law is the central problem.[9] This literature converges with Joshi's in identifying self-regulation and voluntary ethical commitments as inadequate but it differs sharply in prescription where Joshi's critique implies that the entire orientation of Indian AI policy would need to change, Patra's recommendation is comparatively modest a risk based statute modelled on the European Union's approach layered onto the existing framework rather than replacing it.[10]

A fourth body of literature situates India's experience within a broader comparative frame. Malik, Gul and Qureshi examine data governance gaps across several developing economies and find a recurring pattern data protection exists on paper but suffer form weak enforcement capacity, limited public awareness and dependence in AI technologies developed and controlled abroad.[11] Their account of India's The Digital Personal Data Protection Act specifically criticizes its centralized control and the absence if an independent oversight authority a criticism that echoes Joshi's concern from a different disciplinary vantage point.[12] This comparative perspective helps determine whether India's

[7] Divij Joshi, AI Governance in India – Law, Policy and Political Economy, 10(3) Commc'n Rsch. & Prac. 328 (2024).
[8] Id.
[9] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).
[10] Id.
[11] Wasmiya Malik, Seema Gul & Gohar Masood Qureshi, Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations, 3(5) J. Soc. Signs Rev. 95 (2025).
[12] Id.

regulatory challenges are unique or reflect broader governance constraints common to developing jurisdictions adopting AI technologies.

Taken together this literature converges on one central point India's existing legal framework, however interpreted was not built with algorithmic decision making in mind and the instruments introduced to address AI specifically have so far been non-binding. Where the literature diverges is on why this is so and what follows from it whether the answer lies in better technical literacy among regulators in confronting the political economy that structure AI policy in consolidating fragmented sectoral rules or in learning from comparable jurisdiction. This paper does not treat these position as mutually exclusive. It draws on the technical framework offered by Marda to understand where harm actually originates in an AI system the structural critique offered by Joshi to explain why voluntary compliance has proven insufficient and the doctrinal and comparative approach offered by Patra to evaluate what a workable regulatory response might look like. This principal gap in the exisiting scholarship is the absence of an integrated assessment connecting these technical, structural and doctrinal perspectives to evaluate whether India's overall compliance framework is capable of governing AI effectively.

III. RESEARCH METHODOLOGY

This study adopts a doctrinal and comparative research methodology to examine the adequacy of India's legal framework governing artificial intelligence and data governance. The doctrinal component analyses constitutional principles, statutory provisions, judicial decisions and regulatory instruments relevant to AI governance including the Information Technology Act, 2000, The Digital Personal Data Protection Act, 2023 and policy documents such as NITI Aayog's national strategy for artificial intelligence, it also considers sector specific guidance issued by regulatory authorities, including the Reserve Bank of India and the Securities and Exchange board of India of to evaluate the existing compliance framework.

The comparative component draws upon the European Union's risk-based approach under the EU AI Act to identify regulatory features that may offer useful guidance for India's evolving AI governance framework. The study relies primarily on legal materials, judicial decisions, government reports and peer reviewed academic literature. The case studies discussed in section VI are based on publicly available reports and existing scholarly

analysis rather than original empirical research consistent with the doctrinal nature of this study. By combining doctrinal analysis with comparative evaluation the paper assesses whether India's existing legal and regulatory framework is capable of addressing the governance and compliance challenges posed by artificial intelligence.

IV. INDIA'S EXISTING DATA GOVERNANCE FRAMEWORK

A. CONSTITUTIONAL FOUNDATION: JUSTICE K.S. PITTASWAMY V. UNION OF INDIA

India's data governance framework did not rest on explicit constitutional foundation until relatively recently. In Justice K.S. Puttaswamy v. Union of India, a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right under article 21 identifying informational privacy control over the collection, use and disclosure of personal data as a distinct facet of that right.[13] The Court called on the Union Government to establish a robust data protection framework, balancing individual privacy with legitimate state interests.[14]

For AI governance this judgment supplies the constitutional vocabulary autonomy, dignity, informational self-determination against which any statutory regime and any AI system built on personal data must ultimately be evaluated. It also means gaps in India's statutory framework are potentially constitutional not merely regulatory since the court envisaged a genuinely protective regime rather than one oriented primarily towards enabling data-driven innovation.

B. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The statutory response to Puttaswamy took several years and multiple drafts. An earlier more expansive personal data protection bill was withdrawn in 2021 amid industry concern that it would impede innovation.[15] The Digital Personal Data Protection Act, 2023 that eventually replaced it is by most scholarly accounts considerably narrower it establishes

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[14] Id.
[15] Divij Joshi, AI Governance in India – Law, Policy and Political Economy, 10(3) Commc'n Rsch. & Prac. 328 (2024).

purpose limitation, data minimization and consent as core principle but substantially reduces individual rights relative to earlier drafts, permits broad government exemptions and allows the Central Government to exempt specified categories of processing altogether.[16]

For AI specifically the Act's deeper limitation in structural. It obligations attach to the collection of data consent at intake, purpose limitation at use not to what happens once that data trains a model. An AI system built on lawfully collected data can still produce discriminatory or inaccurate outputs and the act offers little direct traction over that downstream harm.[17] Nor does it establish an independent data protection authority comparable to Kenya's or Brazil's leaving oversight concentrated within the executive.[18]

C. THE RESIDUAL ROLE OF THE INFORMATIONAL TECHNOLOGY ACT, 2000

Before the DPDP Act and still relevant alongside it is the Information Technology Act, 2000. Section 43A imposes liability on a body corporate that fails to implement reasonable security practices for sensitive personal data, section 66 addresses unauthorized access and related computer offences.[19] Neither was designed with automated decision-making in mind both are triggered by identifiable events such as a breach rather than the continuous often invisible processing that characterizes a machine learning system.

The Acts's intermediary due diligence rules add a further limited layer of obligation. But on the whole, the IT Act functions as a backstop for conventional cyber security failures not as a framework for algorithmic governance it says nothing about model design, feature selection or bias absent a traceable breach. Its continued relevance lies less in what it can do for AI directly and more in the fact that absent a dedicated AI statute, it remains one of the few source of binding obligation available when an AI related failure happens to coincide with a conventional security lapse.

V. CHALLENGES OF AI GOVERNANCE UNDER THE EXISTING FRAMEWORK

[16] Id.
[17] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).
[18] Wasmiya Malik, Seema Gul & Gohar Masood Qureshi, Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations, 3(5) J. Soc. Signs Rev. 95 (2025)
[19] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).

A. ALGORITHMIC DECISION MAKING AND THE LIMITATIONS OF CONSENT BASED REGULATION

The Digital Personal Data Protection Act, 2023 like most data protection statutes is built around consent as its organizing principle: a data principal consents to processing for a specifies propose and that consent largely defines the lawful limits of use. This model works reasonably well for transactional data use processing a loan application, delivering a purchase but far less well for AI because AI's principal harms rarely arise at the point of collection.

Marda's framework locates risk at three stages of the machine learning lifecycle each beyond the reach of consent based regulation.[20] At the data stage, unrepresentative datasets produce discriminatory outcomes for underrepresented groups.[21] At the model stage developers choose which features a system weighs, embedding subjective design decision no data principal could meaningfully consent to in advance.[22] At the application stage a system accurate in aggregate can still produce unfair outcomes in a particular context. One of this involves unauthorized collection so a framework that asks only whether consent was obtained has little to say about any of it.

B. SELF-REGULATION, ETHICAL AI AND THE ACCOUNTABILITY GAP

Where statutory obligations fall short India's AI policy has relied on ethical principles rather than enforceable rules. NITI Aayog's National Strategy and its "Responsible AI for All" roadmap emphasise fairness, transparency and accountability but create no legally enforceable obligation and no remedy for affected individual.[23] MeitY's own discussion papers follow the same pattern voluntary adoption not mandatory compliance.[24]

Joshi argues this preference for ethics over binding regulations reflects a policy orientation in which AI and data are treated primarily as drivers of growth with stricter regulation framed as an obstacle to it.[25] Whether or not that structural critique is accepted in full in the

---

[20] Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making* (Aug. 29, 2018), https://ssrn.com/abstract=3240384.
[21] Id.
[22] Id.
[23] Divij Joshi, AI Governance in India – Law, Policy and Political Economy, 10(3) Commc'n Rsch. & Prac. 328 (2024).
[24] Id.
[25] Id.

practical consequences is clear organisations deploying AI in India face few enforceable obligations to demonstrate fairness or non-discrimination and ethical guidelines function as statements of best practice rather than accountability.

C. FRAGMENTED SECTORAL REGULATION

A further weakness is fragmentation. Absent a comprehensive AI statute sector regulators have stepped in individually the RBI on digital lending and algorithmic credit assessment, SEBI or algorithmic trading and IRDAI on AI driven underwriting and claims.[26] Each is a reasonable response within its own jurisdiction but they do not add up to a coherent regime. A facial recognition system used by police, for instance, falls outside all of them.[27] The result is that the intensity of oversight an AI system receives depends less on the risk it poses than on which regulator if any happens to have jurisdiction over its sector.

VI. CASE STUDIES

This section examines three illustrative applications of AI in India testing the arguments above against practice.

A. AI- ENABLED CREDIT SCORING

Indian fintech platforms increasingly use algorithmic credit assessment like mobile usage patterns, transaction histories, behavioural data to evaluate applicants who lacks conventional banking records.[28] This expands access to credit but the opacity of the decision illustrates a core limitation of India's framework: an applicant whose loan is declined is rarely told why and the DPDP Act creates no general right to explanation since its focus is on lawful collection rather than the transparency of outcomes.[29] The RBI's Digital Lending Guidelines improve disclosure but only within the financial sector leaving no comparable protection elsewhere.[30]

B. FACIAL RECOGNITION AND PREDICTIVE POLICING

---

[26] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).
[27] Id.
[28] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).

[29] Id.
[30] Id.

Facial recognition deployed by police in several states through applications such as FaceTagr, allows officers to photograph individuals in public and query the images against criminal database.[31] As Marda observes AI risk arises not only from technical accuracy but from the context of deployment like decision about whom to photograph reflect existing institutional biases, disproportionately affecting particular communities.[32] Unlike financial sector AI, facial recognition operates without any dedicated statutory framework. It engages the constitutional privacy interest recognition in Puttaswamy but existing law offers little practical guidance on accountability or remedies.

C. ARTIFICIAL INTELLIGENCE IN HEALTHCARE DIAGNOSTICS

AI diagnostic tools are increasingly used in Indian healthcare particularly for early detection of diseases such as tuberculosis and cancer in regions with limited specialist access.[33] The benefits is real but so is the resulting ambiguity where a diagnosis relies substantially on an AI recommendation existing law does not specify who bears responsibility for an error such as the physician, the institution or the model's developer.[34] The DPDP Act governs how patient data is collected but says nothing about liability for the clinical decisions that data goes on to inform.

D. CROSS-CUTTING OBSERVATIONS

Read together these cases resist as single diagnosis which itself instructive. Credit scoring shows a system partly within regulatory reach but still lacking a right to explanation. Facial recognition shows a system almost entirely outside any binding framework. Healthcare shows a system where data collection is regulated but liability is not. None of these gaps would close through stronger consent requirements alone since none turns on whether data was properly collected in the first place. What unites them is a mismatch between where India's compliance obligations concentrate at collection and where AI related harm actually arises which is consistently further downstream.

VII. COMPARATIVE PERSPECTIVES

---

[31] Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making* (Aug. 29, 2018), https://ssrn.com/abstract=3240384.
[32] Id.
[33] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).
[34] Id.

A. THE EUROPEAN UNION'S RISK-BASED MODEL

The EU's AI Act offers the most developed alternative to India's approach. Rather than regulating primarily through consent-based data protection it classifies AI systems by risk from unacceptable risk, prohibited outright, to high-risk systems subject to mandatory obligations, to minimal-risk systems left largely unregulated.[35] High-risk systems a category that would likely capture applications comparable to the credit scoring and facial recognition example in section VI such as face binding requirements, risk assessments, human oversight, documentation and centrally enforced penalties for non-compliance.[36]

This directly addresses this paper's central finding because obligations attach to a system's risk profile rather than to the circumstances of data collection, the EU model reaches exactly the downstream harms biased design, opaque outcomes that a consent-based regime cannot. The trade off is real compliance costs are higher and critics note these obligations may fall disproportionately on smaller firms with less capacity to absorb them.[37]

[35] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).
[36] Id.
[37] Id.

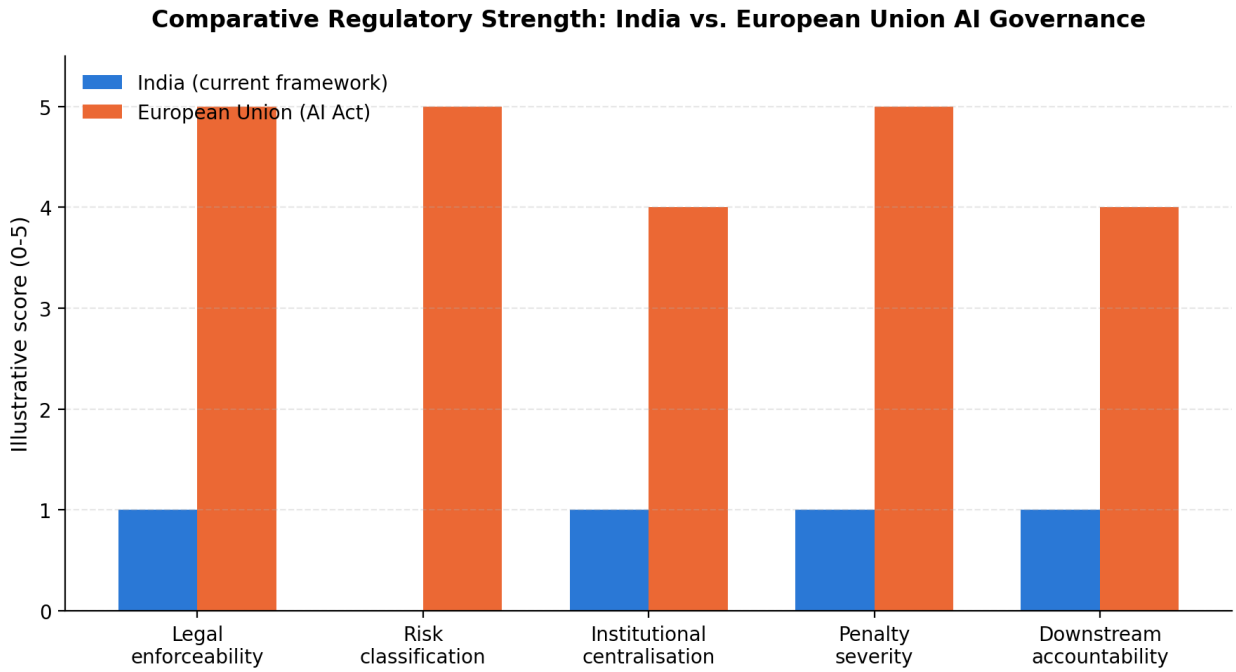

Figure 1: Illustrative comparison of India's current AI governance framework against the European Union's Act based on the qualitative analysis above (0-5 scale, author's own scoring).

B. LESSONS FROM COMPARABLE DEVELOPING ECONOMIES

India is not alone in facing this design choice. Kenya's Data Protection Act,2019 requires impact assessments for high-risk processing but lacks provisions tailored to AI specific risks such as algorithmic bias.[38] Brazil's data protection law goes further granting individuals a right to explanation for decision made solely through automated means a protection India's framework presently lacks.[39] Nigeria's regulation by contrast remains limited in scope and enforcement showing that a data protection statute's mere existence does not guarantee effective oversight.[40]

The pattern across these jurisdictions suggests the central obstacle is rarely an absent ambition to regulate nearly every jurisdiction examined has articulated one. The recurring difficulty is converting that ambition into enforceable, adequately resourced institutional

[38] Wasmiya Malik, Seema Gul & Gohar Masood Qureshi, Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations, 3(5) J. Soc. Signs Rev. 95 (2025).
[39] Id.
[40] Id.

capacity, echoing the gap this paper has identifies between India's ethical commitments and its binding obligations.

C. LESSONS FOR INDIA

India's difference from the European model is not simply the absence of a dedicated AI statute but that it continues to regulate AI through general data protection principles and fragmented sectoral measures without classifying systems by risk or differentiating obligations accordingly. Applications from credit assessment to facial recognition to healthcare diagnostics accordingly receive oversight determined by sector rather than by the degree of risk they pose. This comparison suggests that a risk-based classification discussed further in section VIII, offers the most direct route to closing that gap.

VIII. BALANCING INNOVATION WITH REGULATORY ACCOUNTABILITY

A. WHY INNOVATION AND REGULATION NEED NOT BE OPPOSED

India's policy discourse often frames innovation and regulation as a binary choice with minimum intervention treated as the price of technological advancement.[41] This oversimplifies the issue. What matters is not whether AI is regulated but how a risk-based framework such as the EU's does not impose uniform obligations on every application. It concentrates requirements on high-risk systems while leaving lower-risk development largely unencumbered.

B. EVALUATING INDIA'S CURRENT APPROACH

Measured against this standard India's framework does not fail because it favours innovation it fails because its obligations concentrate at the point of data collection while leaving the subsequent stages of AI design, deployment and operation largely unaddressed. The DPDP Act safeguards how personal data is processed but offers limited oversight of what an AI system does with that afterward. The case studies in section VI make this concrete credit assessment, facial recognition and healthcare AI each show accountability gaps that a collection focused statute cannot reach while the comparative analysis in Section

[41]Divij Joshi, AI Governance in India – Law, Policy and Political Economy, 10(3) Commc'n Rsch. & Prac. 328 (2024).

VII shows that risk-based regimes elsewhere regimes elsewhere are built precisely to reach them.

C. TOWARD A CALIBRATED REGULATORY FRAMEWORK FOR INDIA

This paper's position is that a calibrated set of targeted reforms rather than either extreme best fits India's circumstances. First, a statutory risk classification for AI systems so that obligations correspond to actual potential impact. Second, mandatory impact assessments before deployment of high-risk systems in sectors such as law enforcement, finance and healthcare closing the specific gap the facial recognition case identified. Third, a meaningful right to explanation for individuals affected by high-risk automated decision closing the gap the credit scoring case study identified.

IX. RECOMMENDATIONS

Strengthening India's AI governance does not require restructuring the existing legal regime. Targeted reforms addressing the gaps identified throughout this paper would meaningfully improve accountability while preserving room for continued innovation.

A. A RISK-BASED CLASSIFICATION FOR AI SYSTEMS:

Rather than a single uniform framework, legislation should classify AI systems by risk and impose binding obligations only on high-risk applications those deployed in law enforcement, credit assessment, employment and healthcare.[42] This ensures obligations correspond to actual impact without burdening lower-risk innovation.

B. A COORDINATED FRAMEWORK INSTITUTIONAL FRAMEWORK:

India lacks any dedicated mechanism for coordinating AI governance across sectors. Rather than a wholly regulator a coordinating body plausibly housed within MeitY should issue guidance for high-risk systems and coordinate rather than duplicate the work already done by the RBI, SEBI and IRDAI.[43]

C. REGULATORY SANDBOXES:

high-risk obligations should be paired with a formal sandbox mechanism letting developers test AI Applications under supervision with relaxed compliance timelines

[42] Lokanath Patra, *Regulating Artificial Intelligence in India: Legal Challenges, Ethical Governance, and the Need for a Comprehensive Framework*, 3(5)(III) Royal Int'l Global J. Advance & Applied Rsch. 11 (2026).
[43] Id.

before full deployment addressing the legitimate concern that compliance rest costs fall disproportionately on smaller developers.

D. ENFORCEABLE TRANSPARENCY AND ACCOUNTABILITY:

High-risk systems should be subject to binding documentation and impact assessment requirements before deployment along with a statutory right to explanation for individuals affected by significant automated decisions closing the gaps the facial recognition and credit scoring case studies identified.

E. CROSS-SECTOR COORDINATION:

since AI applications frequently cut across existing regulatory boundaries as the healthcare case study's unresolved liability question shows a formal consultation mechanism between the coordinating authority and sectoral regulators would clarify how liability and compliance obligations are allocated rather than leaving this to develop ad hoc.

X. CONCLUSION

This paper set out to examine India's existing legal architecture constitutional privacy protection, the Digital Personal Data Protection Act, 2023 the residual reach of the Information Technology Act, 2000 and a body of non-binding AI policy is capable of holding algorithmic systems accountable for the harms they can cause. The answer that emerges from this analysis is qualified rather than absolute. India's framework is not without foundation Puttaswamy supplies a genuine constitutional basis for data protection and the Digital Personal Data Protection Act whatever its limitations establishes real obligations around the collection and processing of personal data. What the framework lacks is not a starting point but a mechanism for reaching the specific stage of the AI lifecycle at which the most consequential harms actually occur.

The case studies examined in this paper make that gap concrete rather than theoretical. Credit scoring systems evade meaningful explanation despite falling partly within regulatory reach. Facial recognition systems operate almost entirely outside any binding compliance framework. Healthcare diagnostic tools raise questions of liability that existing law does not purport to answer. In each case the shortfall is not that India has failed to regulate data it is that Indian law regulates data at the point of collection while the harms this paper has documented arise consistently, further downstream in model design and in application.

The comparative analysis of the European Union's risk-based model suggests that this downstream gap is not an inevitable feature of AI governance, but a design choice that other jurisdictions have addressed differently. India need not adopt that model wholesale and this paper has not argued that it should. What the evidence supports is narrower and more achievable a targeted risk classification for high-risk AI applications, paired with enforceable rather than merely aspirational obligations for the systems that classification identifies. This would leave the great majority of AI development in India exactly as unencumbered as it is today, while finally extending binding accountability to the comparatively small set of applications, in policing, credit, and healthcare among them, where the stakes for the individuals affected are highest. India's innovation-oriented posture toward artificial intelligence need not be abandoned to achieve this. It needs, at its edges, to be made accountable.