Regulation of Artificial Intelligence in India: Implications for Business Innovation and Risk Management

Authors

[1]Ms. Aarushi Gupta, [2]Ms. Suman, [3]Dr. Gaurav Srivastava, [4]Ms. Simran Bharti

[1]Assistant Professor, Innovative Institute of Education and Technology, Greater Noida (U.P.)

[2]Assistant Professor, Innovative Institute of Education and Technology, Greater Noida (U.P.)

[3]Associate Professor/ HOD, Innovative Institute of Law, Greater Noida (U.P.)

[4]Assistant Professor, Innovative Institute of Law, Greater Noida (U.P.)

Abstract

Artificial intelligence has moved from a laboratory technology to an operational layer of Indian business. Enterprises use AI in finance, health, logistics, e-commerce, customer service, compliance and public-facing platforms, yet India still lacks a single consolidated statute dedicated exclusively to AI. Instead, the present regulatory environment is distributed across constitutional principles, the Information Technology Act and subordinate rules, the Digital Personal Data Protection Act, 2023, sectoral supervision and soft-law guidance on responsible AI. This paper examines how that fragmented but evolving framework affects business innovation and risk management in India. It argues that India has chosen a calibrated approach that prefers sector-specific governance and principle-based oversight over an omnibus AI law, at least for now.

The paper studies the legal and policy architecture relevant to AI deployment, including NITI Aayog's responsible AI principles, MeitY's 2024 advisory on generative AI and synthetic content, the Digital Personal Data Protection Act, 2023 and emerging compliance expectations for high-impact AI systems. It further evaluates how this framework influences innovation incentives, governance costs, accountability structures and enterprise risk allocation. The analysis concludes that India's present model offers flexibility and room for experimentation, but it also creates legal uncertainty for firms because compliance duties must be assembled from multiple sources rather than derived from a single comprehensive code.

The paper proposes a business-oriented regulatory strategy for India built on risk-tiering, sectoral coordination, documentation duties, algorithmic impact assessments, human oversight in consequential decisions and stronger clarity on synthetic media, intellectual property and cross-border governance. Such a framework would preserve India's innovation ambitions while reducing uncertainty for enterprises and improving public trust in AI systems.

Keywords: Artificial Intelligence, Regulatory framework, Business management, Digital personal data, NITI Aayog.

1.1 Introduction

Artificial intelligence now affects the basic mechanics of commercial decision-making. Businesses use AI to automate credit scoring, customer targeting, fraud detection, recruitment, pricing, contract analytics, warehouse optimization and predictive maintenance. In India, this growth aligns with the policy vision of "AI for All," first developed in the National Strategy on Artificial Intelligence and later elaborated through NITI Aayog's responsible AI papers.[21][24] Those documents recognize AI's capacity to increase productivity and solve social problems, but they also stress the need to balance innovation with safety, equality, accountability, privacy and transparency.[24]

For Indian businesses, AI is both an opportunity and a source of structured legal risk. The opportunity lies in lower transaction costs, scalability, personalization and faster decision-making. The risk lies in biased models, opaque decision systems, privacy breaches, insecure training pipelines, misleading synthetic content, discriminatory outcomes and uncertain liability chains when automated systems cause harm.[24][12][17] Regulatory governance therefore matters not only as a public-law issue but also as a strategic business concern tied to compliance, litigation exposure, consumer trust and corporate governance.

India's AI regulation is unusual because it is not contained in one "Artificial Intelligence Act." Instead, businesses must navigate a layered environment. Constitutional values influence interpretation of fairness and equality; the Digital Personal Data Protection Act, 2023 regulates digital personal data processing; the Information Technology legal framework shapes intermediary duties and platform accountability; NITI Aayog guidance articulates responsible AI principles; and sectoral regulators increasingly frame AI expectations in finance and other regulated industries.[17][12][24] This regulatory pluralism creates flexibility, but it also raises questions about coherence, certainty and the cost of compliance.

This paper addresses those questions by evaluating the present Indian framework and its consequences for commercial innovation and enterprise risk management. It also seeks to identify what kind of regulatory model would best support responsible business adoption of AI in India.

1.2 Scope and Limitations of Study

Scope

This study focuses on regulation of artificial intelligence in India from the standpoint of businesses that develop, deploy, procure, or rely upon AI systems. It examines statutory law, delegated legislation, policy documents, advisories and public official positions relevant to AI governance. The core legal sources assessed

are the Digital Personal Data Protection Act, 2023, NITI Aayog's responsible AI framework and MeitY's advisory concerning generative AI, algorithmic fallibility, bias, unlawful content and synthetic media labeling.

The paper also considers sectoral implications for entities in finance, e-commerce, platform services, health technology and consumer-facing digital business models. It evaluates AI regulation primarily through the lenses of business innovation and risk management rather than through criminal law, military AI, or purely philosophical debates on machine autonomy.

Limitations

First, India's AI framework is evolving rapidly and some institutional or sectoral developments may continue to change after the date of this paper. The analysis therefore reflects the legal and policy position visible through the sources used here. Second, because India does not yet have a single codified AI law, the study necessarily synthesizes dispersed legal materials and policy signals, which may leave unresolved interpretive gaps. Third, the paper focuses on publicly available sources and does not include proprietary compliance practices or confidential corporate governance documents. Fourth, judicial precedent specifically addressing advanced generative AI in India remains limited, so some conclusions are doctrinally inferential rather than case-driven. Fifth, the study does not attempt a full comparative review of the EU, U.S., U.K., or China, except where such comparison assists evaluation of India's regulatory direction.

1.3 Research Methodology

This paper adopts a doctrinal and analytical legal research methodology. The doctrinal component examines primary and secondary legal materials, including the Digital Personal Data Protection Act, 2023, official policy papers, official advisories and statements of governmental position on intellectual property issues connected to AI-generated works. The analytical component evaluates how these materials interact with business decision-making, governance architecture and enterprise risk controls.

The study uses qualitative content analysis to identify recurring regulatory themes: privacy, fairness, safety, transparency, accountability and responsible innovation. It then applies a business-law perspective to map these themes onto operational issues such as model deployment, vendor management, internal controls, consumer protection, data governance and board oversight. A limited policy-comparative lens is used conceptually to distinguish India's distributed model from omnibus AI legislation, though the paper remains principally grounded in Indian sources.

The methodology is normative as well as descriptive. It not only describes the present regulatory landscape but also evaluates its adequacy and proposes reforms. In doing so, it aims to connect legal doctrine with managerial consequences for business entities that use AI systems in high-impact settings.

2.0 Conceptual Foundations of AI Regulation

Artificial intelligence regulation is not only about controlling technology. It is also about structuring power, responsibility and trust in environments where automated systems affect legal rights, economic opportunity and social inclusion. NITI Aayog's 2021 document identifies several "systems considerations" and "societal considerations" such as explainability, bias, exclusion, accountability, privacy, security, impact on jobs and malicious profiling.[24] These issues translate directly into business law concerns because companies increasingly use AI to make or influence consequential decisions about customers, workers and counterparties.

A useful conceptual distinction exists between innovation governance and harm governance. Innovation governance seeks to encourage adoption, experimentation and investment. Harm governance seeks to prevent or mitigate discrimination, unsafe deployment, security failures and unlawful processing of personal data. The challenge for regulators is that overbroad ex ante restrictions may chill innovation, while weak oversight may externalize the cost of harm onto consumers and society. NITI Aayog explicitly frames the task as finding a balance between enabling adoption and governing risk.[24]

In business settings, this balance often takes the form of risk-based regulation. Not every AI tool should face identical duties. A spell-checker, a recommendation engine for entertainment and an AI-assisted credit underwriting model clearly differ in social consequence. Indian policy thinking already moves in that direction by discussing calibration according to the risk associated with different applications and by identifying contexts where opacity, exclusion, or bias are especially serious.[24] That risk-sensitive orientation provides an important foundation for a future Indian regulatory model.

2.1 Evolution of India's AI Governance Approach

India's formal policy approach to AI emerged from NITI Aayog's 2018 strategy and its later responsible AI papers. The framework uses the phrase "AI for All," reflecting a developmental orientation that treats AI as a tool for public welfare, inclusion and growth rather than merely as a subject of restriction.[21][24] The 2021 principles paper emphasizes that AI governance in India must be grounded in constitutional values and must address both system-level and societal risks.[24]

The responsible AI paper identifies seven broad principles: safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability and reinforcement of positive human values.[24] These principles are not enacted as binding legislation, but they function as a normative template. For businesses, such soft-law principles can influence procurement conditions, internal ethics frameworks, future regulation and standards of due care. Soft law often becomes the precursor to harder obligations once sectoral regulators or courts begin to rely on it.

A more enforcement-oriented signal appeared in MeitY's March 2024 advisory. It advised intermediaries and platforms to ensure that AI models or generative systems available through their computer resources do not enable unlawful content, bias, discrimination, or threats to electoral integrity; it also addressed under-testing or unreliable AI and recommended labeling or metadata for synthetic or deepfake-like content.[12] Although the advisory did not itself create a comprehensive AI code, it indicated that the Indian government is willing to use existing information technology powers to shape AI governance in practical ways, especially where public harm or misinformation risk is evident.[12]

At the same time, the Digital Personal Data Protection Act, 2023 established a binding horizontal data protection regime for digital personal data, which is highly relevant to AI because many business AI systems depend on collection, training, inference, or profiling involving personal data.[17] The result is an evolving but recognizable governance architecture: principle-based responsible AI guidance, existing IT-law enforcement levers and binding data governance obligations under the DPDP Act.

3.0 Existing Legal Framework Governing AI in India

3.1 Constitutional and Public Law Values

Although India does not yet have an AI-specific constitutional amendment or dedicated rights charter for automated decision-making, public law values remain central to any regulatory analysis. NITI Aayog expressly grounds responsible AI in constitutional morality and links AI governance to equality, non-discrimination, accountability and protection of individual rights.[24] This matters because many future disputes about AI deployment in India will likely be interpreted through constitutional values, particularly where state use, delegated public functions, or essential services are involved.

For businesses, constitutional values matter indirectly as well. Private firms increasingly perform quasi-public digital functions such as payments, communication, employment matching and access facilitation. Where large platforms or regulated entities deploy opaque or exclusionary AI systems, courts and regulators may draw upon fairness and non-arbitrariness norms even if the immediate dispute is framed under statute, contract, consumer law, or sectoral regulation.

3.2 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is currently the most important binding statute affecting AI governance in India.[17] The Act applies to processing of digital personal data within India and also to processing outside India when connected with offering goods or services to persons within India.[17] This extraterritorial feature is highly relevant to multinational AI businesses serving Indian users from outside the country.

The Act permits processing of personal data only for lawful purposes based on consent or certain legitimate uses.[17] It requires notice, valid consent, rights of withdrawal, grievance redressal, correction and erasure and reasonable security safeguards and it obliges data fiduciaries to notify breaches to the Board and affected data principals in the prescribed manner.[17] These obligations directly affect AI developers and deployers because model training, user analytics, recommendation systems, behavioral inference and automated decision tools often depend upon personal data collection and downstream processing.

Several provisions have particular importance for AI governance. Section 8 requires data fiduciaries to ensure completeness, accuracy and consistency where personal data is likely to be used to make decisions affecting data principals or to be disclosed to another fiduciary.[17] This provision is significant because inaccurate or poor-quality data is a major driver of unfair or unreliable AI outcomes. Section 10 authorizes designation of Significant Data Fiduciaries based on volume and sensitivity of data, risk to rights, impact on sovereignty, risk to electoral democracy, security and public order and imposes additional duties such as data protection officers, audits and data protection impact assessments.[17] Those criteria closely track the logic of high-risk AI regulation even though the statute is formally about personal data rather than AI.

The Act also contains children's data protections, restrictions on behavioral monitoring and targeted advertising directed at children, provisions on cross-border transfers and exemptions for startups or specific fiduciaries in certain contexts.[17] From a business perspective, the Act creates both an opportunity and a compliance burden. It promotes trust and data discipline, but it also raises governance costs for enterprises whose AI value proposition depends on extensive personal data processing.

3.3 Information Technology Framework and the MeitY Advisory

The Information Technology legal ecosystem remains an important source of authority for AI-related platform governance, especially in the context of intermediaries and user-generated content. MeitY's 1 March 2024 advisory directed intermediaries and platforms to ensure that AI or generative tools made available through their computer resources do not permit unlawful content or bias and discrimination, do not threaten electoral integrity and, where synthetic content may be used as misinformation or deepfake, are labeled or embedded with permanent metadata or identifiers.[12] The advisory also emphasized consequences of non-compliance with the IT Act and IT Rules.[12]

For businesses, the advisory has three broad implications. First, generative AI is no longer treated purely as a neutral innovation space; it is subject to expectations of active governance, especially on misinformation and harmful outputs. Second, labeling and disclosure expectations for synthetic content may become part of ordinary platform compliance and product design. Third, firms offering under-tested or experimental AI systems face elevated scrutiny if outputs may materially mislead or harm users.[12]

Even where some elements of the advisory were debated in public discourse, its larger significance is clear: the Indian state is prepared to regulate AI deployment through existing digital governance tools while a fuller AI-specific regime remains under development. Businesses cannot therefore assume that absence of a dedicated AI Act means absence of enforceable obligations.

3.4 NITI Aayog's Responsible AI Framework

NITI Aayog's responsible AI papers are not binding legislation, but they are central interpretive materials in the Indian AI governance ecosystem.[24][21] The papers identify major concerns around explainability, bias, exclusion, privacy, security and accountability and they recommend calibrated implementation according to risk.[24] For businesses, these documents function as normative compliance benchmarks. They signal what future regulation, judicial expectations and sectoral standards are likely to prioritize.

The practical value of the framework lies in its business relevance. Safety and reliability translate into testing and validation; equality and inclusivity translate into bias assessments and representational data practices; privacy and security translate into data minimization and cybersecurity controls; transparency translates into documentation and user-facing disclosures; accountability translates into audit trails, governance ownership and grievance processes.[24] In that sense, the NITI framework already supplies the skeleton of an enterprise AI governance program.

3.5 Intellectual Property and AI-Generated Works

AI regulation also intersects with innovation incentives through intellectual property law. In February 2024, the Government stated in Parliament that India's existing copyright and patent regimes are considered well-equipped to protect AI-generated works and related innovations and that there is no current proposal to create a separate IP right specifically for AI-generated content.[22] The same statement emphasized that commercial users of generative AI must obtain permission where copyrighted works are used in ways not covered by fair dealing exceptions under section 52 of the Copyright Act.[22]

For business innovation, this position offers continuity rather than wholesale reform. Companies can continue to structure product development and commercialization around the existing IP framework. At the same time, legal uncertainty remains on authorship, ownership, training-data use and the boundary between human-created and AI-assisted works. For risk management, enterprises using generative AI for content production, marketing, software generation, or design must maintain licensing discipline and provenance controls because infringement risks remain enforceable under existing law.[22]

4.0 Implications for Business Innovation

4.1 Regulatory Flexibility as an Innovation Enabler

One of the strongest arguments in favor of India's present approach is flexibility. Because India has not yet imposed a rigid omnibus AI statute, businesses enjoy room to experiment with AI use cases across sectors, particularly where risks are low or where data governance can be managed under existing law.[17][24] This is attractive for startups and innovation-led firms that would struggle under highly prescriptive ex ante approvals for every model iteration.

The DPDP Act itself contains some flexibility. It permits processing for consent-based lawful purposes and certain legitimate uses and it allows the government to notify exemptions or differential obligations for certain fiduciaries, including startups, in specified situations.[17] That structure can support experimentation, especially when combined with sectoral supervision rather than blanket restrictions.

Soft-law guidance also assists innovation where it provides directional clarity without imposing immediate over-compliance. NITI Aayog's framework encourages responsible design while still emphasizing adoption and public trust.[24] For firms seeking investment, partnership, or government procurement opportunities, alignment with those principles can become a market advantage rather than a pure compliance cost.

4.2 Innovation Through Trust and Market Legitimacy

Innovation is not only about freedom from regulation. It also depends on consumer trust, investor confidence and predictable rules of market participation. NITI Aayog explicitly links responsible AI to public trust and wider adoption.[24] From a commercial perspective, this is important because AI products fail not only when they are technically weak, but also when users see them as unsafe, opaque, biased, or unlawful.

A privacy and accountability framework can therefore function as innovation infrastructure. Enterprises that can document lawful data use, explain high-impact outputs, handle grievances and respond to incidents are more likely to scale AI products in regulated and consumer-sensitive sectors such as health, finance, insurance and education.[17][24] Trust becomes a competitive differentiator. The absence of trust, by contrast, can make even technically advanced systems commercially unusable.

4.3 Innovation Costs of Regulatory Fragmentation

The main downside of India's current framework is fragmentation. Businesses must infer applicable duties from multiple legal sources: data protection law, platform regulation, sectoral directions, procurement

conditions, consumer law and soft-law guidance.[17][12][24] Large enterprises may manage such complexity through legal and compliance teams, but startups often face disproportionate uncertainty.

Fragmentation increases transaction costs in at least four ways. First, companies must perform legal mapping for each use case rather than rely on a unified risk taxonomy. Second, cross-functional governance becomes harder because product, legal and engineering teams lack a single reference framework. Third, vendor and procurement contracts become more complex when responsibilities for bias, security, explainability and data rights are not statutorily standardized. Fourth, investors may discount scale potential where legal predictability is weak. Thus, while India's flexibility encourages experimentation, its fragmented structure may slow commercialization of high-impact AI applications.

4.4 Sector-Specific Innovation Impacts

Different sectors experience the regulatory environment differently. In consumer platforms and social media, MeitY's advisory makes synthetic content labeling, unlawful-content control and output governance central design considerations.[12] In finance and insurance, decision-impacting AI systems implicate data accuracy, accountability, auditability and possibly future high-risk expectations under sectoral regulation.[17][24] In health technology, privacy, reliability, safety and human oversight become especially important because errors may affect life, bodily integrity, or access to treatment.[24]

This sectoral variation suggests that a single innovation narrative is misleading. AI regulation may be comparatively light for low-risk productivity tools but significantly more demanding for high-impact or data-intensive applications. Businesses that understand this gradient can innovate more effectively by aligning product architecture to likely risk exposure from the outset.

5.0 Implications for Risk Management

5.1 Privacy and Data Governance Risk

Data risk is the most immediate legal risk for most enterprise AI systems in India. The DPDP Act requires valid consent structures where consent is the basis of processing, clear notices, rights of withdrawal, grievance mechanisms, security safeguards and breach notification.[17] AI systems often challenge these requirements because model development can involve secondary uses, training-data aggregation, inferential analytics and continuous improvement loops that are difficult to explain in simple notice language.

The Act's requirement that data used for decisions affecting individuals be complete, accurate and consistent raises a particularly important operational issue.[17] Businesses cannot treat data quality as a purely technical matter. It becomes a compliance obligation connected to legal defensibility of AI-assisted decisions. Poorly

governed datasets can therefore produce simultaneous business risks: degraded model performance, discriminatory outcomes, customer complaints and regulatory exposure.

5.2 Bias, Equality and Discrimination Risk

NITI Aayog identifies bias and unequal outcomes as core concerns of responsible AI.[24] For businesses, algorithmic bias creates layered risks: discrimination claims, consumer unfairness allegations, employee grievances, procurement exclusion, reputational damage and possible invalidation of automated decision processes. These risks are especially pronounced where AI is used in hiring, lending, pricing, insurance, educational admissions, ranking, or benefit eligibility.

Indian law does not yet offer a single AI anti-discrimination code for private business, but that does not reduce the seriousness of the risk. Courts, regulators and complainants can approach the issue through constitutional values, labor principles, consumer law, contract, sectoral oversight, or privacy-linked fairness arguments. Enterprises therefore need bias governance even before a dedicated statute compels it.

5.3 Explainability and Accountability Risk

Opaque AI systems create legal and managerial problems when affected persons ask why a decision was made, why a service was denied, or why a risk score changed. NITI Aayog repeatedly emphasizes explainability, auditability and accountability as critical to safe deployment and public trust.[24] For businesses, explainability is not merely an ethics concern. It is essential for dispute resolution, compliance review, incident response, model debugging and vendor oversight.

Accountability risk also becomes acute in outsourced or multi-vendor ecosystems. A business may rely on foundation models, third-party APIs, cloud providers, data brokers and downstream deployers. Yet the legal responsibility often remains with the enterprise that determines purposes and means of processing or that puts the AI-driven product into the market.[17] This means contractual risk transfer alone is insufficient. Firms need technical and governance controls that support actual oversight, not only indemnity clauses.

5.4 Synthetic Media and Misinformation Risk

Generative AI creates distinctive risk for platforms, media businesses, advertising firms and any enterprise with user-generated or public-facing content. MeitY's 2024 advisory highlights the risks of misinformation, deepfakes, electoral distortion, bias and unlawful content and it encourages labeling or metadata embedding for synthetic content.[12] For business risk management, this means firms must assess not only content moderation after publication but also model design, watermarking, provenance tools, user prompts, abuse monitoring and escalation protocols.

The reputational consequences here can be severe. A platform that fails to identify manipulated or synthetic content may face not only state scrutiny but also rapid public distrust, advertiser withdrawal and contract loss. As synthetic media grows more persuasive, content authenticity will become a core governance function rather than an optional product feature.

5.5 Cybersecurity and Model Integrity Risk

The DPDP Act requires reasonable security safeguards to prevent personal data breach.[17] NITI Aayog likewise identifies privacy and security as fundamental principles of responsible AI.[24] In AI systems, security risk extends beyond conventional database breaches. It includes model inversion, data poisoning, prompt injection, unauthorized fine-tuning, training-set leakage, insecure APIs and manipulation of model outputs.

For business risk management, this implies that AI security must be integrated with enterprise cybersecurity, vendor assurance and software lifecycle governance. A breach involving a model or training corpus can trigger legal duties, customer harm and large reputational costs even where the system's core algorithm remains intact.

5.6 Governance and Board-Level Risk

Where organizations qualify or may later qualify for heightened scrutiny, governance maturity becomes central. The DPDP Act contemplates stronger duties for Significant Data Fiduciaries, including data protection officers, audits and periodic data protection impact assessments.[17] These are governance devices, not merely technical steps. They indicate that boards and senior management will increasingly be expected to supervise data-intensive AI systems at an institutional level.

For businesses, AI risk therefore belongs in enterprise risk management frameworks alongside cyber, financial and regulatory risk. Internal audit, legal, information security, procurement, compliance and product teams must collaborate. Without that structure, AI failures are likely to be treated as governance failures rather than isolated technical accidents.

6.0 Adequacy of India's Present Model

India's present model has real strengths. It is pragmatic, adaptive and relatively innovation-friendly. By using existing legal tools and policy principles rather than prematurely freezing a rigid technology-specific statute, India retains room to support experimentation and sectoral tailoring.[17][24] The model also reflects institutional realism: many AI problems overlap with pre-existing fields such as data protection, intermediary liability, intellectual property, competition and consumer protection.

However, the model also suffers from under-specification. Businesses lack a clear statutory classification of high-risk AI uses, a standardized duty to conduct algorithmic impact assessments outside data-protection

contexts, explicit enterprise obligations on explainability for consequential decisions and clear liability allocation for autonomous or semi-autonomous systems. The result is regulatory ambiguity: firms know the direction of travel but not always the exact compliance threshold.[12][24]

In effect, India currently has a governance framework but not yet a complete regulatory architecture for AI. That distinction matters. A governance framework can express principles and general duties. A regulatory architecture must also provide calibrated categories, procedures, institutional coordination, enforcement pathways and predictable compliance safe harbors. India is moving toward that architecture, but the transition is incomplete.

7.0 Suggestions and Recommendations

1. Adopt a Risk-Based AI Framework

India should adopt a formal risk-tiered framework for AI systems. Low-risk uses should face light-touch obligations, while high-risk systems that affect rights, safety, finance, employment, healthcare, elections, or access to essential services should face stronger duties such as documentation, testing, human oversight and auditability.[24][17] This would preserve flexibility for innovation while giving businesses clearer compliance categories.

2. Enact Targeted AI Rules Rather than an Overbroad Blanket Statute

A single sweeping AI law may become obsolete quickly if drafted too rigidly. India should instead consider a framework statute or coordinated rules that define core principles, institutional roles and high-risk obligations while allowing sectoral regulators to issue context-specific standards. This approach would be consistent with India's current distributed model but would reduce fragmentation through clearer coordination and terminology.[24][12]

3. Mandate Algorithmic Impact Assessments for High-Impact Systems

The logic of the DPDP Act already supports impact assessment for significant fiduciaries.[17] India should extend this governance tool to high-impact AI systems even where the risk is not limited to personal data. Such assessments should examine data quality, fairness, explainability, human oversight, security, foreseeable misuse and redress pathways. For businesses, this would convert abstract ethics into auditable operational discipline.

4. Clarify Duties on Explainability and Human Review

Where AI materially affects legal rights, economic opportunity, or access to important services, enterprises should be required to provide meaningful explanation and access to human review. NITI Aayog's concerns

about explainability and exclusion support this direction.[24] Clear statutory or regulatory articulation would help both firms and affected individuals by reducing uncertainty about what counts as adequate disclosure and redress.

5. Create Clear Synthetic Content and Provenance Standards

MeitY's advisory already highlights labeling and metadata for synthetic information.[12] India should build on that by issuing standard technical and legal requirements for provenance, watermarking where feasible, platform disclosures and rapid complaint handling. Uniform standards would reduce business uncertainty and prevent inconsistent implementation across platforms.

6. Strengthen Sectoral Regulatory Coordination

AI risk often cuts across multiple regulators. Finance, health, telecom, education, consumer protection, competition and data governance all intersect with AI in different ways. India should create an institutional coordination mechanism, perhaps through a nodal inter-regulatory council or technical secretariat, to harmonize definitions, reporting expectations and high-risk classifications. This would reduce duplicative compliance and improve predictability for businesses operating across sectors.

7. Develop Safe Harbors for Good-Faith Compliance

To encourage innovation, India should provide limited safe harbors or mitigation credit where businesses can show documented good-faith compliance: testing, impact assessments, prompt incident response, synthetic content labeling, vendor diligence and meaningful user redress. This would avoid a purely punitive model and reward responsible deployment.

8. Clarify Intellectual Property Rules for AI Training and Output Use

While the Government has stated that existing IP law is presently adequate, uncertainty remains for training-data use, authorship thresholds and commercial deployment of AI-generated outputs.[22] India should issue interpretive guidance or undertake targeted reform to clarify these points. Greater IP certainty would materially improve business planning in media, software, advertising, publishing and design industries.

9. Encourage Standardized Enterprise AI Governance

Regulators and industry bodies should promote model governance standards covering lifecycle documentation, approval workflows, vendor management, red-teaming, monitoring, rollback protocols and board reporting. Such standardization would especially benefit medium-sized firms that cannot build bespoke frameworks from scratch.

10. Build Capacity in Adjudication and Enforcement

Effective regulation requires institutional capacity, not only normative aspiration. The Data Protection Board and relevant regulators will need technical understanding of AI systems, data flows and algorithmic evidence.[17] Capacity-building in investigation, audit methods and technical expertise is therefore necessary if AI governance is to become credible and business-relevant.

8.0 Conclusion

The regulation of artificial intelligence in India is best understood as an evolving mosaic rather than a settled code. The present framework combines binding data protection law, information technology enforcement tools, responsible AI soft law and sector-sensitive governance signals.[17][12][24] This model has enabled policy flexibility and avoided the premature rigidity of a single all-encompassing AI statute. It therefore offers real advantages for innovation, particularly in a developing digital economy that wants to encourage entrepreneurship, investment and socially useful AI adoption.

At the same time, the costs of fragmentation are now increasingly visible. Businesses face uncertainty over explainability duties, liability allocation, high-risk categorization, synthetic media governance and enterprise standards for responsible deployment. The result is not deregulation, but partial regulation with uneven clarity. That environment may be manageable for large firms, but it can burden startups, complicate compliance design and weaken public trust when harms occur.

A more coherent next phase of Indian AI regulation should therefore preserve the strengths of the current model while addressing its gaps. The most suitable path is a calibrated, risk-based framework that integrates data governance, fairness, security, accountability and sectoral coordination without choking experimentation. For Indian businesses, such reform would not merely reduce legal exposure. It would also create the trust architecture necessary for durable innovation. In that sense, responsible AI regulation is not the enemy of enterprise. It is a condition for legitimate and scalable AI-driven growth in India.[24][17]

References

1. Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code, https://www.indiacode.nic.in/handle/123456789/22037?view_type=browse.
2. The Digital Personal Data Protection Act, 2023, Ministry of Electronics & Information Technology, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.
3. Ministry of Electronics & Information Technology, Government of India, Advisory on AI/LLM/Generative AI and Synthetic Content (Mar. 1, 2024), https://regmedia.co.uk/2024/03/04/meity_ai_advisory_1_march.pdf.
4. NITI Aayog, Government of India, Principles for Responsible AI: Towards Responsible AI for All (Feb. 2021), https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.

5. NITI Aayog, Government of India, Operationalising Principles for Responsible AI (Aug. 2021), https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf.
6. NITI Aayog, Government of India, Responsible AI for All, https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf.
7. NITI Aayog, Government of India, Responsible AI, https://www.niti.gov.in/sites/default/files/2024-07/Responsible%20AI%20AIForAll.pdf.
8. Press Info. Bureau, Gov't of India, Existing IPR Regime Well-Equipped to Protect AI Generated Works and Related Innovations (Feb. 8, 2024), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2004715.
9. Press Info. Bureau, Gov't of India, India AI Governance Guidelines - Press Release (Nov. 4, 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.
10. MeitY, Draft AI Governance Comments Notice (Oct. 21, 2025), https://www.meity.gov.in/static/uploads/2025/10/38be31bac9d39bbe22f24fc42442d5d1.pdf.
11. NeGD, AI for All: India's Blueprint for a Smarter Future (Sept. 15, 2025), https://negd.gov.in/blog/ai-for-all-indias-blueprint-for-a-smarter-future/.
12. NeGD, MeitY Unveils India AI Governance Guidelines Under IndiaAI Mission to Ensure Safe, Inclusive, and Responsible AI Adoption (Nov. 5, 2025), https://negd.gov.in/press_release/meity-unveils-india-ai-governance-guidelines-under-indiaai-mission-to-ensure-safe-inclusive-an.
13. RBI's FREE-AI Committee Report in the Financial Sector, KPMG, https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2025/09/rbis-free-ai-committee-report-in-the-financial-sector.pdf.
14. Analysing RBI's AI Framework, Nat'l Inst. of Pub. Fin. & Pol'y, https://www.nipfp.org.in/publication-index-page/blog-index-page/analysing-rbis-ai-framework/.
15. AI in ICAI, Inst. of Chartered Accountants of India, https://ai.icai.org/articles_details.php?id=281.
16. Existing IPR Regime Well-Equipped to Protect AI Generated Works and Related Innovations, Press Info. Bureau, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2004715.
17. Digital Personal Data Protection Bill, 2023, PRS India, https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital%20Personal%20Data%20Protection%20Bill,%202023.pdf.
18. The Digital Personal Data Protection Bill, 2023, PRS India, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.
19. Decoding India's AI Governance Strategy and Its Implications for the U.S.-India Bilateral Relationship, 5 Indian Pub. Pol'y Rev. 4 (2024), https://ippr.in/index.php/ippr/article/view/301.
20. Global AI Governance Law and Policy: India, IAPP, https://iapp.org/resources/article/global-ai-governance-india.
21. Strengthening AI Governance Through Techno-Legal Framework, PSA, https://psa.gov.in/CMS/web/sites/default/files/publication/AI-WP_TechnoLegal.pdf.
22. India AI Governance Guidelines 2025: Key Principles, Pillars, and the Future of AI, Bettering Results, https://betteringresults.in/india-ai-governance-guidelines-2025-key-principles-pillars-and-the-future-of-ai/.
23. Sound Public Policy to Boost Government's AI Governance Guidelines, Inst. of Soc. & Pub. Pol'y, https://www.ispp.org.in/sound-public-policy-to-boost-governments-ai-governance-guidelines/.
24. AI Governance in India, Nat'l Bureau of Asian Res., https://www.nbr.org/publication/ai-governance-in-india/.
25. Regulating AI in India, Scribd, https://www.scribd.com/document/782938670/Regulating-AI-in-India.
26. AI Regulations in India 2025: Complete Compliance Guide, American Chase, https://americanchase.com/generative-ai-regulations-india/.

27. Navigating AI Governance in India: Insights from MeitY's 2025 Report, Securiti, https://securiti.ai/ai-governance-in-india-meity-2025-report/.
28. The Bluebook Online, T2.18 India, https://www.legalbluebook.com/bluebook/v21/tables/t2-foreign-jurisdictions/t2-18-india.
29. Bluebook Citation for Indian Supreme Court Cases, Supreme Today, https://supremetoday.ai/search/bluebook-citation-supreme-court-cases.
30. Bluebook 101: Citing Generative AI, Gallagher Law Library, https://lib.law.uw.edu/bluebook101/genai.