International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

From Regulatory State To Regulatory Space: Mapping India's Fragmented Ai Governance Through The Lens Of Comparative Regulatory Theory

Shailja Jha
Department of LLM-IBL, NALSAR University of Law, Hyderabad & Indian Institute of Corporate Affairs, Gurgaon.

Abstract- The rapid proliferation of Artificial Intelligence (AI) technologies has exposed significant limitations in traditional state-centric regulatory frameworks, particularly in complex and diverse jurisdictions such as India. This paper advances the concept of a transition from a "regulatory state" to a "regulatory space," emphasizing the distributed, multi-actor nature of AI governance. Drawing on comparative regulatory theory, the study analyzes how India's AI governance is characterized by institutional fragmentation, overlapping mandates, and sector-specific regulatory interventions rather than a unified legal framework. By examining key regulatory bodies, policy instruments, and emerging guidelines across domains such as data protection, digital markets, and sectoral compliance, the paper maps the contours of India's evolving AI governance ecosystem. It further compares India's approach with global models, including the European Union's risk-based regulatory regime and the United States' market-driven governance structure, to highlight divergences and convergences in regulatory philosophy. The analysis demonstrates that India's fragmented governance structure, while often viewed as a limitation, may also function as a flexible "regulatory space" that enables adaptive, context-sensitive oversight. However, this flexibility comes with challenges related to coordination, accountability, and enforcement consistency. The paper concludes by proposing a hybrid governance model that integrates centralized policy direction with decentralized regulatory innovation, thereby aligning India's AI governance with both domestic priorities and global regulatory trends.

Keywords – Artificial Intelligence Governance, Regulatory State, Regulatory Space, Comparative Regulatory Theory, India AI Policy, Fragmented Governance, Digital Regulation, Data Protection, Multi-Stakeholder Governance, Adaptive Regulation.

I. INTRODUCTION

The construction of a cohesive regulatory structure has lagged behind the rapid expansion of artificial intelligence (AI) in India, which is expected to boost the country's GDP by $450–500 billion by 20251. Emerging AI applications pose serious dangers of data misuse, algorithmic bias, mass surveillance, and privacy erosion, despite the state's previous reliance on private- sector self-regulation in information technology under the Information Technology Act, 2000 (IT Act). This essay makes the case that India's AI governance represents a change from the ideal of a unified regulatory state to a dispersed regulatory environment controlled by a number of public and commercial entities. Enforcing democratic accountability, procedural legitimacy, and enforceable privacy measures requires a formal statutory framework. Without it, the regulatory environment will continue to be open, allowing for chronic under-protection of rights and private capture.

This argument engages three core theoretical themes drawn from comparative regulatory scholarship: explanations of regulation, the regulatory state, and regulatory space. It maps India's current landscape, analyses privacy gaps through the lens of AI risks, and develops a normative case for statutory intervention, reinforced by comparative insights from the EU, UK, and US. The analysis draws directly on the provided readings, particularly Yeung's account of the regulatory state, Hancher and Moran's concept of regulatory space, Levi-Faur's polymorphic regulatory state, and Majone's positive theory of regulatory delegation.

II. THEORETICAL FRAMEWORK

The term regulation, in its most general sense, is used to describe the purposeful design of laws, norms, and organizations that guide behavior for common ends2. There are two major theoretical approaches that dominate the literature. Public interest theories see regulation as the response to problems in the market due to externalities, information asymmetry, or monopoly power with the intention of increasing efficiency and welfare. In contrast, interest group (or "capture") theories, which are rational choice-based approaches, see

regulation as a private gain extracted from organized interests at the expense of the public good. Both these approaches have to be supplemented by institutional and ideational theories to fully understand the phenomenon of regulation in contemporary times.

The "regulatory state" emerged as an analytical construct to describe the post-1970s reconfiguration of governance in advanced capitalist economies6. As Yeung explains, the regulatory state succeeded the welfare state through privatisation, the creation of independent regulatory agencies, and a shift from direct provision ("rowing") to steering via rules and standards7. Majone's influential account of the EU as a regulatory state emphasises delegation to non-majoritarian institutions to credibly commit to market-correcting policies while insulating them from short-term political pressure8. The regulatory state is therefore characterised by three shifts: institutional (hollowing-out of central government), functional (steering rather than rowing), and instrumental (rules and arm's-length oversight rather than hierarchical command)9.

However, comparative research shows a great deal of diversity. According to Levi-Faur, the regulatory state is "thick" and polymorphic rather than monomorphic; it is one of numerous morphs (developmental state, welfare state) that exist inside the capitalist state10. The more radical idea of "regulatory space" is advanced by Hancher and Moran. This analytical construct is characterised by the variety of topics that are subject to public decision-making and are filled by numerous powerful organisations (state agencies, businesses, NGOs) whose boundaries blur public-private differences11. National legal culture, organisational subcultures, problem arenas, and historical context all contribute to the fragmentation, contestation, and shaping of regulatory space12. Instead of using sovereign command, power is exercised through webs of interdependence, inclusion/exclusion, and standard operating procedures13. This framing examines how organisations occupy a shared space rather than the binary public-private dichotomy of the capture argument14.

These concepts are not mutually exclusive. A regulatory state may aspire to coherence through statute and independent agencies; regulatory space describes the empirical reality of fragmentation. India's AI governance, as this essay shows, sits firmly in the latter.

III. INDIAN AI GOVERNANCE LANDSCAPE

The country has followed the principle of private innovation and self-regulation with respect to its IT policy till date. Prior to the enactment of the Digital Personal Data Protection Act, 2023, the IT Act, 2000 (amended) was limited to a mere basic framework addressing cybercrime and e-commerce15. The regulation of AI is far more fragmented. It includes the involvement of agencies such as the MeitY, NITI Aayog, TRAI, RBI, private entities such as NASSCOM, and ethics committees established by industries. There exists no centralized regulator, no prescribed risk categorization, no licensing, and no AI law.

Rather than a regulatory state, this landscape represents a traditional regulatory area16. Instead of utilising hierarchical command, several actors, including government agencies, international tech platforms, local entrepreneurs, and standards organizations, compete for influence through modelling, reciprocal adjustment, and capacity-building17. The growth of self-regulatory groups and voluntary guidelines (like MeitY's 2021 AI Principles) is indicative of the dominance of the private sector18. Such spaces are typified by routine exclusions, as Hancher and Moran predict: big businesses use epistemic communities to set the agenda, whereas civil society voices and privacy advocates are frequently sidelined19.

This is precisely the "fragmentation," as termed by Levi-Faur, that occurs in the case of polymorphic regulatory systems20. There is no institution that possesses both the capacity and

the mandate to oversee the evolution of AI technologies. Instead, there is an emerging process of alliances on specific issue areas, ranging from finances to healthcare AI and surveillance mechanisms, each of which is regulated under its own rules and players21. Path dependence is the key term here; the liberalization period post-1991 ensured the development of IT by the private sector in a conducive setting22.

IV. PRIVACY AND REGULATORY GAPS

The challenges that come along with this fragmented area are apparent from the issues arising from the application of artificial intelligence concerning privacy. Profiling algorithms, automated decisions, and facial recognition create room for discrimination and continuous surveillance23. While the DPDP Act can be commended, it fails to provide protection of artificial intelligence. Mandatory impact assessments, transparency, and ban on risky use of AI are lacking. It operates through consent24. There is little oversight over data fiduciaries, which includes artificial intelligence developers25.

These are structural gaps. Privacy is regarded as a sectoral or contractual matter rather than a constitutional right under a regulatory environment lacking a central statutory anchor (Art. 21, K.S. Puttaswamy26). Comparative theory explains why: democratic input is subordinated to organisational interdependence in regulatory spaces27. Due to financial incentives, private actors underinvest in privacy, which is a well-known public-good issue. Due to unclear regulations, public entities use ad hoc standards or forum shifting28. Yeung notes that in regulatory governments without sufficient

throughput mechanisms, the outcome is precisely the "crisis of democratic legitimacy29."

Empirical evidence from India, deployment of AI-powered surveillance in cities, Aadhaar- linked profiling, and opaque algorithmic lending, demonstrates systemic under-protection30.

Without statutory rules, privacy becomes negotiable rather than non-negotiable, contradicting the constitutional vision of dignity and autonomy.

V. ARGUMENT FOR STATUTORY FRAMEWORK

A formal statutory framework, establishing an independent AI Regulatory Authority with risk- based classification, mandatory audits, and privacy-by-design obligations, would transform India's regulatory space into a more coherent regulatory state31. It would address three critical deficits:

1. **Legitimacy and accountability:** Statutory delegation, subject to parliamentary oversight and judicial review, restores input and throughput legitimacy absent in self-regulation32.
2. **Coherence and predictability:** A single statute would harmonise fragmented rules, reduce forum-shifting, and provide clear ex-ante standards, precisely Majone's rationale for regulatory agencies33.
3. **Privacy protection:** Risk-tiered obligations (e.g., prohibition of unconsented biometric inference, mandatory DPIAs) would operationalise constitutional rights, closing the enforcement gap34.

Critics can point to the efficiency and inventiveness of the private sector. However, the drawbacks of self-regulation, capture, under-enforcement, and externalities, are well known35. The development of India's IT sector happened in spite of, not because of, a regulatory vacuum; public steering is necessary due to AI's societal externalities (bias, spying)36. The EU AI Act shows that reasonable, risk-based regulations may coexist with technical leadership, proving that a legal framework need not hinder innovation37.

VI. COMPARATIVE INSIGHTS

Comparative analysis strengthens the case for statutory intervention by illustrating how different jurisdictions have navigated the regulatory-state/regulatory-space spectrum and the centrality of privacy safeguards.
The most obvious example of a cohesive regulatory state is the European Union's AI Act38 (Regulation (EU) 2024/1689), which went into effect on August 1, 2024, and is currently being implemented gradually (with high-risk responsibilities starting in August 2026). It uses a horizontal, risk-based framework that divides AI systems into four categories: minimal risk (mostly unregulated), high-risk (strict obligations including conformity assessments, transparency, human oversight, and data governance), limited risk (transparency requirements for chatbots and deepfakes), and unacceptable risk (banned outright, e.g., manipulative subliminal techniques or social scoring)39. Fundamentally, privacy is integrated: the Act makes direct reference to the GDPR, prohibits some high-risk data processing techniques that would permit extensive surveillance, and mandates that high-risk systems follow bias reduction and data quality requirements.

National competent authorities are in charge of enforcement. Fundamentally, privacy is integrated: the Act directly references the GDPR, forbids several high-risk data processing methods that would allow for widespread surveillance, and requires high-risk systems to adhere to bias reduction and data quality standards. Fines of up to €35 million, or 7% of global turnover, are enforced by national competent authorities coordinated at the EU level. By enforcing binding, ex ante regulations and democratic accountability procedures, this framework directly opposes the fragmentation of regulatory space, exactly the paradigm Yeung and Majone support for legitimate, rights-protecting governance40.

By contrast, the United Kingdom has pursued a lighter, pro-innovation approach since the 2023 White Paper, relying on existing sectoral regulators coordinated by the Digital Regulation Cooperation Forum (DRCF) rather than a new horizontal statute.41 However, momentum toward statutory underpinning has grown: the Artificial Intelligence (Regulation) Private Members' Bill was re-introduced in March 2025 proposing a central AI Authority, and the Labour government's AI Opportunities Action Plan (January 2025) signals plans for

comprehensive AI legislation in 2026 that would make certain voluntary commitments legally binding while retaining sandboxes and innovation-friendly principles.42 Privacy receives attention through sectoral rules and the UK GDPR, but the framework remains more fragmented than the EU's, closer to a transitional regulatory space that is gradually hardening into a regulatory state. The UK experience demonstrates that even innovation-focused jurisdictions eventually recognise the need for statutory anchors when systemic risks (including privacy erosion) materialise.

India's existing model has a cautionary analogue in the United States. There is currently no comprehensive federal AI law as of April 2026. In order to promote a deregulatory, minimally burdensome approach, the Trump administration revoked Biden's Executive Order 14110 in January 2025 and issued an Executive Order on a "National Policy Framework for AI" in December 202543. This order aims to preempt "onerous" state

laws through litigation and funding requirements.While states have passed a patchwork of targeted laws (e.g., Colorado AI Act on algorithmic discrimination, California and Illinois deepfake and employment rules), federal oversight is still sectoral and executive-driven (FTC enforcement under existing consumer-protection laws, NIST frameworks)44.

The regulatory space is the exact outcome. According to Hancher and Moran, privacy protections are inconsistent, fragmented, contentious, and susceptible to private capture. The result is precisely the regulatory space Hancher and Moran describe: fragmented, contested, and vulnerable to private capture, with inconsistent privacy protections and forum-shifting between federal and state arenas45. This mirrors India's dispersion across MeitY, NITI Aayog, and sectoral bodies, producing enforcement gaps and weak accountability.

For India, the comparative lesson is clear. A hybrid statutory model, drawing the EU's risk- based coherence and privacy integration while incorporating UK-style sandboxes and phased rollout adapted to developmental priorities, would address fragmentation without sacrificing innovation. Such a framework would embed private-sector expertise within publicly accountable rules, operationalise constitutional privacy rights, and position India as a responsible global AI player.

VII. CONCLUSION

Instead of becoming a regulatory state, India's AI governance is a fragmented, contentious, and privately dominated regulatory landscape46. Yeung, Hancher and Moran, and Levi-Faur's theoretical contributions explain why this area leads to accountability problems and privacy deficiencies47. Instead of rejecting the private sector's role, a statutory framework would incorporate it into democratically legitimate regulations, restoring the state's ability to guide while defending constitutional rights. The decision is between cohesive public governance and disjointed private ordering rather than between innovation and regulation. It is not only desirable but also constitutionally and developmentally necessary to enact comprehensive AI legislation.

REFERENCE

1. Black, J. (2002). Critical Reflections on Regulation.
   → Introduces the concept of "regulatory space" and multi-actor governance.
2. Hancher, L., & Moran, M. (1989). Organizing Regulatory Space.
   → Foundational work explaining how regulation is dispersed across institutions.
3. Scott, C. (2001). Analysing Regulatory Space: Fragmented Resources and Institutional Design.
   → Expands on fragmentation and distribution of regulatory authority.
4. NITI Aayog (2018). National Strategy for Artificial Intelligence (#AIforAll).
   → Key policy vision document for AI in India.
5. Ministry of Electronics and Information Technology (various years). Reports on AI, Data Governance, and Digital India.
   → Includes policy papers and AI governance discussions.
6. Digital Personal Data Protection Act.
   → Core legal framework governing data, crucial for AI systems.