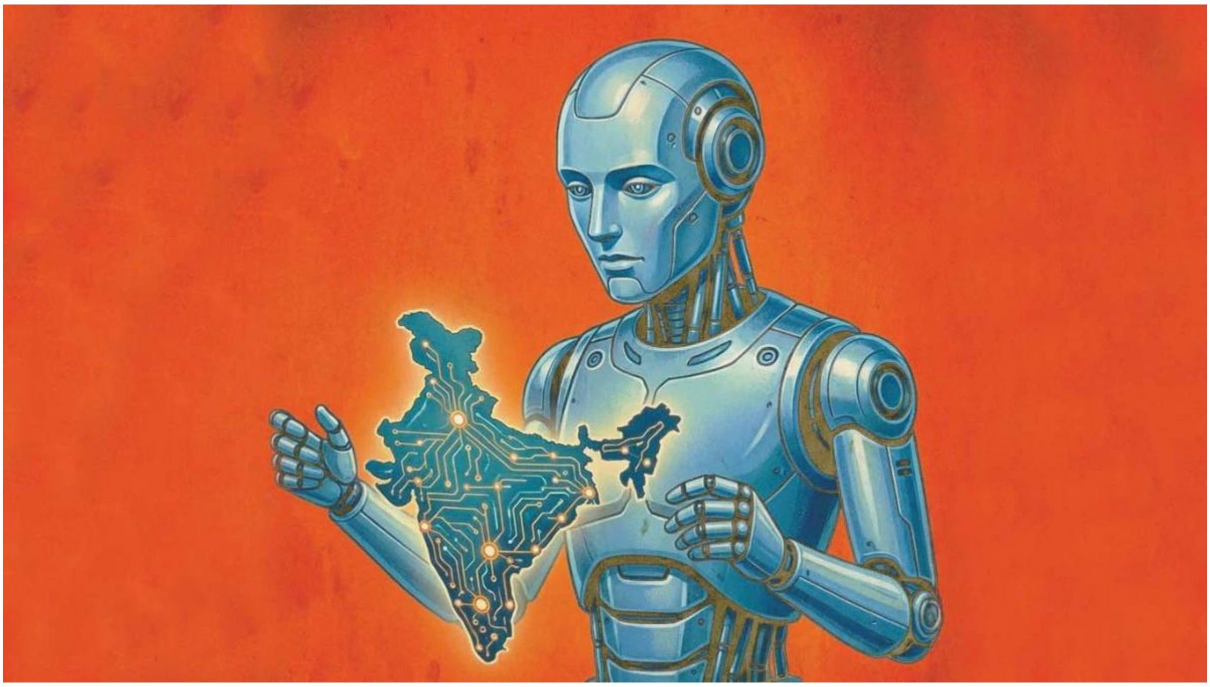
Quote by Devroop Dhar, Co-Founder and CEO, Primus Partners

Published in Business Today
January 4, 2025

How India is trying to balance innovation and safety in its AI governance structure

As AI adoption accelerates across sectors, India's AI governance road map aims to balance innovation with safety, accountability and strategic autonomy

Authored by Nidhi Singal



Read on: https://www.businesstoday.in/magazine/deep-dive/story/how-india-is-trying-to-balance-innovation-and-safety-in-its-ai-governance-structure-509591-2026-01-06

Article Content:

Last year, some social media users came across an advertisement featuring Union Finance Minister Nirmala Sitharaman endorsing an investment plan.

It turned out that the hyper-realistic promo was fake, had been generated using Artificial Intelligence (AI) and Indian citizens who unsuspectingly clicked on an embedded hyperlink, which led to a fraudulent trading platform, had fallen prey to a scam.

Rewind to 2018. The e-commerce giant Amazon abandoned an AI-powered recruiting tool after it was found to be biased against female candidates. The flaw had become embedded in the system from years of data skewed towards men.

Separated by time, geography and context, the episodes had one common link: AI operating without guardrails. They weren't outliers, but early indicators of what happens when AI evolves faster than the rules meant to rein it in.

The Amazon experience served as an early warning of what happens when algorithms inherit historical biases in data sets. Worryingly, by 2025, the deepfake, or AI generated media, threat had moved to the public sphere, as illustrated by the scam targeting Indian citizens.

“AI systems are constantly reflecting biases present in the data they are trained on, and deepfakes have emerged as a serious challenge in India and globally. It is essential that we start building strong ethical frameworks, accountability mechanisms, and governance practices around AI before the risks scale further,” says Nitin Naredi, Partner at professional services major Deloitte India.

The Indian government has now made a significant regulatory leap, drafting guidelines to rein in AI. The guidelines, based on broad principles rather than cast-in-stone regulations, arrive just as AI starts to take deeper root in the Indian economy.

The framework, unveiled in November by the Ministry of Electronics and Information Technology (MeitY), emphasises safe, inclusive and responsible adoption of AI across sectors. Based on the motto “Do No Harm,” the framework brings together ethical principles, a time-bound action plan and practical guidelines for the industry, developers and, of course, regulators.

Measured Approach

Instead of suggesting new laws to govern AI, MeitY has opted for a measured approach that leans on existing laws.

This is because many of the risks that are emerging from the use of AI can be addressed through existing information technology (IT), data protection, intellectual property (IP), competition, media, employment and criminal laws.

Deepfakes used to impersonate individuals, for instance, can be tackled through the IT Act and the Bharatiya Nyaya Sanhita, the criminal code; the Digital Personal Data Protection (DPDP) Act regulates the use of personal data for training AI models without consent. The government indicated that a review of current laws will continue, allowing regulators to identify and plug any legal gaps.

“The country has experienced a significant increase in AI adoption across finance, e-commerce, government platforms and health-tech, along with a steady rise in model development by local start-ups,” says Devroop Dhar, Managing Director and co-founder at management consultancy Primus Partners.

“But India is following a different path from the major regulatory blocs. It is positioning itself between these strategies. The focus is on enabling growth while addressing potential harms that could impact a large and diverse population,” adds Dhar.

The global playbook

Across the world, governments have been drawing lines in the sand on AI governance. The European Union moved first with its AI Act, classifying models by risk tier and imposing strict transparency, safety and data-governance rules.

The US, meanwhile, is leaning on voluntary pledges, industry standards and sector-specific oversight. China has implemented sweeping regulations on deepfakes, recommended algorithms and generative AI platforms, emphasising traceability, data security and platform accountability.

India’s guidelines are timely because they come at a time when the AI economy is approaching an inflection point. A study by the National Association of Software and Service Companies (Nasscom), the IT industry lobby, and the consultancy giant Boston Consulting Group (BCG) pegs the Indian AI market at $17 billion by 2027. India’s policy think tank NITI Aayog’s AI for Viksit Bharat report says AI could inject up to $1.7 trillion into the country’s economy by 2035.

The opportunity is immense, but the foundation is not yet India’s own. Technologies driving the global AI wave, including foundational models, cloud infrastructure and core software stacks, are still primarily built and controlled by overseas companies. With the ecosystem dominated by US and Chinese firms, India remains dependent on external systems.

The dependence creates strategic exposure to geopolitical shifts, export controls and technology access restrictions that can easily reshape India’s long-term digital ambitions.

To address these gaps and secure its future, India has already earmarked Rs 10,371 crore to invest in homegrown AI capabilities under the India AI Mission.

“These guidelines issued by MeitY provide an important directional framework, not just for industry, but for the government itself. MeitY has offered clear recommendations for regulators, state bodies, and public institutions on how they should engage with AI responsibly and work collaboratively towards India’s broader AI mission,” says Naredi of Deloitte.

What Comes Next

For the private sector, these guidelines function as both a signal and a safeguard. They indicate that AI regulation is coming, and they give businesses time to adopt governance practices within a stable policy framework.

Developers and deployers of AI systems are expected to voluntarily adopt governance norms around privacy, security, fairness and non-discrimination, to build accessible grievance redressal systems for AI-related harms and to publish transparency reports assessing risks to society.

The guidelines also encourage the use of privacy-enhancing technologies, “machine unlearning,” algorithmic audits and automated bias-detection tools.

For companies working with AI, whether as providers or as consumers, this shift is already reshaping operations.

At Tech Mahindra, the guidelines are influencing how the company designs, deploys and manages its cloud-based AI platforms, with “traceability, explainability and auditability” now embedded as default features across the cloud computing architecture, especially in high-impact sectors such as banking, financial services and insurance (BFSI), healthcare and public services.

“This involves strengthening lineage tracking for training data, expanding model-level documentation, and integrating mandatory logging and human oversight mechanisms into our deployment pipelines,” says Kunal Purohit, President—Next Gen Services, Tech Mahindra.

There is a broader shift in the industry towards making compliance a part of the product DNA rather than an afterthought.

For Gnani.ai, which builds large Indian-language AI models, the most immediate compliance requirements include enhancing transparency through regular reporting, establishing a clear grievance redressal mechanism for users and strengthening AI safety frameworks.

“Safety testing, especially for high-risk systems, will require more structured documentation and validation, which we are already integrating into our development cycles,” says Ganesh Gopalan, co-founder and Chief Executive Officer, Gnani.ai.

Cost effects

The guidelines do have cost implications. Although they stop short of imposing EU-style penalties or mandatory audits, implementing responsible AI practices will require companies to invest in new processes, tools and talent.

“There’s no denying costs will go up as safety testing, audits, and compute for evaluations aren’t free,” says Subeer Sehgal, Head of AI and Data Governance at Fractal, a data analytics and AI firm.

For the company, this increase will come from safety testing and audits for bias defection and fairness evaluations, resources for evaluation and regulatory sandboxes for high-risk use cases.

Sehgal sees these costs as strategic investments and believes the IndiaAI initiatives such as subsidised graphic processing units (GPUs) and shared datasets will offset some of the burden, making this a moderate increase rather than a barrier.

To be sure, India's flexible approach may introduce challenges in their interpretation, particularly for large enterprises adopting AI at scale.

Arjun Nagulapally, Chief Technology Officer at digital transformation company AIONOS, says the very flexibility offers an opportunity.

"We plan to position ourselves as governance-ready by embedding adaptable, DPDP-compliant governance features in our platform, making it easier for businesses to navigate evolving regulations," he says.

Road to an AI law

The guidelines mark only the first step in what will inevitably be a long and evolving regulatory journey. Many of the toughest questions now remain unresolved.

How will India test and benchmark high-risk AI systems? Who bears the liability when automated decisions cause public harm? What shared standards should govern model evaluation? Can regulators build the technical capacity needed to supervise increasingly complex algorithms?

Until such questions are answered, governance will advance only in parts, says Dhar. The guidelines will need to evolve in step with practical constraints.

The government has avoided rushing into a standalone AI law, but it has not ruled out one. As high-risk applications scale and encompasses more key sectors, statutory clarity will become unavoidable.

Ultimately, India's challenge will not just be to regulate AI but to shape the rules of a technology that will define economic and geopolitical power in the coming decades.