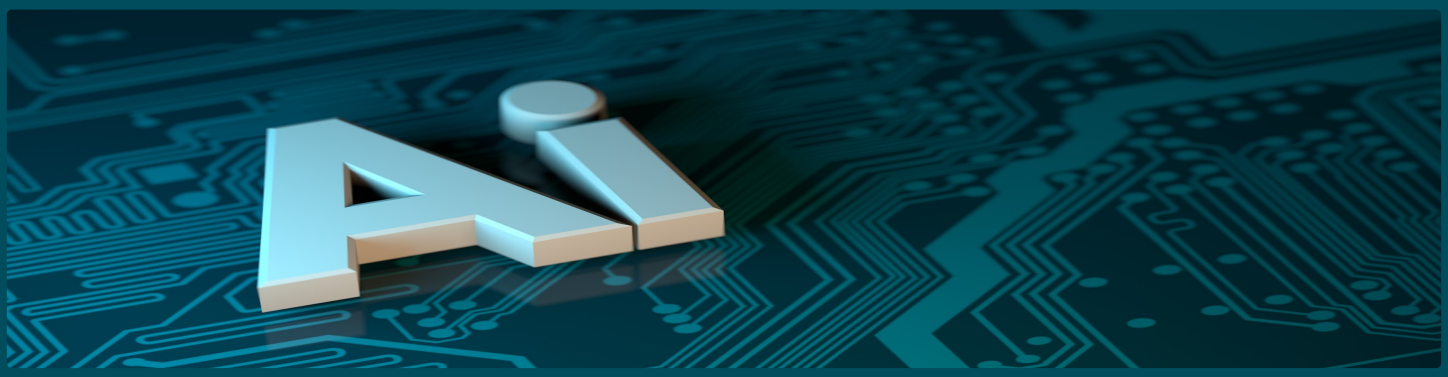
INDIALAW



DATA PRIVACY

Regulating The Machine Mind: AI, Privacy, And Intellectual Property Under India's 2025 AI Governance Guidelines

AUTHOR Appurv Bhatia

PUBLISHED 20 November 2025

Abstract

Artificial intelligence (AI) now permeates every aspect of human activity from algorithmic governance and healthcare diagnostics to generative creativity. Yet, AI's reliance on vast quantities of personal and creative data challenges traditional legal categories. The release of India's AI Governance Guidelines (November 2025) by the Ministry of Electronics & Information Technology (MeitY) has brought India squarely into global conversations about AI ethics, accountability, and innovation.

This article explores the intersection of law, AI, data privacy, and intellectual property (IP) through the lens of India's emerging regulatory architecture.

Introduction: From Innovation to Accountability

AI's rapid evolution has outpaced legal imagination. Traditional frameworks anchored in human authorship, identifiable data subjects, and clear chains of liability strain under the pressure of machine learning systems that learn, adapt, and create.

India, one of the world's fastest-growing AI markets, now faces the twin challenge of promoting innovation while safeguarding constitutional rights to privacy and expression. The India AI Governance Guidelines (2025) represent the country's first comprehensive framework for responsible AI. While not a law, the Guidelines form a voluntary, techno-legal governance architecture emphasizing accountability, transparency, and innovation-friendly regulation. Their guiding philosophy "innovation over restraint" acknowledges that regulation should enable technological progress while embedding ethical and legal safeguards.

The Seven Sutras: A New Ethos for Indian AI

At the heart of the Guidelines are seven foundational principles, or sutras, that frame India's approach to responsible AI. These are:

1. Trust as the Foundation
2. People First
3. Innovation over Restraint
4. Fairness and Equity
5. Accountability
6. Understandable by Design
7. Safety, Resilience and Sustainability.

Together, they create a holistic vision of AI governance built on transparency, human dignity, inclusivity, explainability, and sustainability, while ensuring that regulation does not stifle innovation. This framework mirrors global standards such as the OECD AI Principles and UNESCO's AI Ethics Recommendations but grounds them in India's constitutional and socio-economic realities.

Data Privacy: Aligning AI with the Digital Personal Data Protection Act (2023)

AI's dependence on large datasets makes privacy compliance not optional but existential. The Guidelines explicitly tether AI governance to the Digital Personal Data Protection Act (DPDP) 2023, requiring AI actors to embed privacy into their design and deployment. Lawful processing, consent, and purpose limitation are central to compliance.

Training AI on personal data requires explicit consent and a clear purpose; "publicly available" data cannot be assumed to be freely usable. Transparency obligations require AI systems to disclose when users are interacting with AI or AI-generated content. The rights of data principals access, correction, and erasure must be honored, even if the data has been used in model training. Developers relying on cross-border data or offshore compute are advised to ensure compliance with localization norms under the DPDP Act.

For Indian startups and enterprises, this means implementing strong data governance systems, tracking dataset provenance, and ensuring that personal data is processed lawfully. For multinationals, it necessitates reassessing cross-border AI training pipelines to prevent violations of Indian privacy norms.

Intellectual Property and Generative AI: Redrawing Creative Boundaries

The Guidelines acknowledge that AI's creative capacities blur the lines of authorship and ownership. Under current Indian copyright law, which predicates protection on human authorship, AI-generated works occupy a grey zone. The Guidelines signal that this ambiguity may soon be addressed through a review of the Copyright Act, 1957, potentially introducing new "related rights" to recognize AI-assisted creations.

A more immediate challenge lies in the use of copyrighted works as training data for AI models. The Guidelines recommend revisiting Section 52 of the Copyright Act, which sets out fair dealing exceptions, to clarify whether text and data mining (TDM) for AI training qualifies as lawful use. They also suggest developing a licensing or collective management framework to allow rights-holders to authorize or monetize such use. Furthermore, developers are encouraged to maintain documentation demonstrating the legal provenance of their datasets. This would strengthen transparency and reduce future litigation risks.

For AI developers, the implications are clear: dataset documentation and rights management are no longer optional. For creators and publishers, the Guidelines mark a step toward greater recognition of their interests in the AI training ecosystem.

Liability and Accountability in AI Deployment

India's Information Technology Act, 2000 (IT Act) remains the foundation of digital regulation but offers limited clarity for AI systems. Section 66D penalizes impersonation through computer resources, extending to AI-generated deepfakes, while Section 79 and the 2021 Intermediary Guidelines impose due diligence duties on platforms to monitor and remove unlawful AI content.

However, legal immunity under Section 79 may not apply to autonomous AI models that create or alter data independently. The AI Governance Guidelines, 2025 therefore propose clear definitions of AI actors- developers, deployers, and users and call for shared liability, transparency, and accountability. This forward – looking approach aims to balance innovation with responsible AI regulation through amendments to the IT Act.

Trusting What We See: Authenticity in AI-Generated Content

Generative AI technologies covering image, video, and music generation, offer significant benefits for creativity, innovation, and access to knowledge. However, they also pose serious risks, including the creation of deepfakes, child sexual abuse material (CSAM), and non-consensual content.

To balance innovation with safety, the Guidelines emphasize content authentication and provenance through digital watermarks and unique identifiers, in line with global standards like the Coalition for Content Provenance and Authenticity (C2PA). These tools, along with forensic and attribution methods, support traceability and accountability by verifying whether content was generated or altered by AI.

Recognizing their limits and privacy risks, the Guidelines propose that the AI Governance Group (AIGG) and Technology & Policy Expert Committee (TPEC) review India's regulatory framework and recommend techno-legal solutions to curb harmful deepfakes. A multi-stakeholder committee is also envisioned to develop global standards for authentication and provenance ensuring India's approach remains both responsible and innovation-friendly.

The Guidelines advocate for strong privacy safeguards, responsible IP management, and transparency mechanisms to protect creators and users alike. By combining these measures with technical tools for verification and traceability, India aims to preserve innovation while minimizing misuse, maintaining the guiding principle of innovation over restraint.

Bridging Data Privacy and IP: The Convergence Challenge

AI sits at the intersection of personal data protection and intellectual property rights, often pulling these legal regimes in opposing directions. Privacy law limits data usage and protects individuals from misuse of personal information, while IP law grants exclusive rights over creative works to encourage innovation. AI systems, however, depend on both. This creates friction when models are trained on personal data or copyrighted materials. The Guidelines implicitly recognize this tension and call for harmonization, urging policymakers to design a unified framework that balances the rights of individuals, creators, and innovators.

Trade secret concerns also arise when developers are asked to disclose training data to ensure transparency, potentially exposing proprietary information. The next phase of India's AI governance framework is therefore expected to clarify the interface between privacy, IP, and confidentiality laws.

Business and Startup Implications

For India's AI ecosystem, the Guidelines translate into concrete operational imperatives. AI companies must now prioritize lawful data collection and maintain audit trails to prove compliance with the DPDP Act. They must avoid unlicensed use of copyrighted materials during model training, labeling AI-generated content clearly in public-facing applications to enhance transparency. High-risk AI systems must undergo internal or third-party impact assessments before deployment. The Guidelines also encourage organizations to designate AI ethics or compliance officers responsible for governance oversight and to participate in regulatory sandboxes that allow controlled experimentation under official supervision. These measures aim to encourage innovation responsibly, ensuring that Indian startups remain globally competitive without compromising on ethics or legality.

Interaction with Existing and Emerging Laws

The AI Governance Guidelines do not operate in isolation but build upon India's broader legal infrastructure. The Digital Personal Data Protection Act, 2023 anchors privacy and consent obligations for all AI data processing. The Copyright Act, 1957 remains central to managing training data and protecting creative outputs, with revisions anticipated to address AI-generated content and text/data mining exceptions. The Information Technology Act, 2000, which governs online intermediaries and cyber liability, is likely to be amended to define the roles of AI developers and deployers. Meanwhile, the Consumer Protection Act, 2019 may apply to misleading or biased AI outputs that affect consumers. Together, these laws form the scaffolding upon which India's AI regulatory architecture will evolve, culminating in the anticipated AI Bill which is expected to codify many of the Guidelines' principles into binding legislation.

India in the Global Context

Compared globally, India's 2025 AI Governance Guidelines occupy a middle path between the stringent regulatory approach of the European Union and the decentralized, innovation-driven model of the United States. While the EU AI Act imposes legally binding obligations and detailed risk classifications, and the U.S. relies on agency-led directives under its 2023 AI Executive Order, India's Guidelines remain voluntary for now but are poised to transition into enforceable standards. They align closely with the DPDP Act for privacy, anticipate reforms to the Copyright Act for IP, and emphasize "innovation over restraint" as a guiding philosophy. In doing so, India seeks to combine the ethical oversight of the European model with the entrepreneurial dynamism of the American approach a pragmatic balance suited to its digital economy.

Conclusion: The Way Forward

The India AI Governance Guidelines (2025) mark a turning point in India's digital regulation towards accountable AI. While non-binding, they establish a moral and procedural compass for what responsible AI should look like. They also recognize that AI cannot be confined within siloed frameworks: its legal implications span privacy, intellectual property, liability, and human rights. For legislators, the next step is to translate these guiding principles into enforceable norms through Bills and amendments to the Copyright and IT Acts. For businesses, the responsibility is immediate document data practices, secure IP clearances, label AI outputs, and operationalize ethical AI principles across product lifecycles.

As India positions itself as both a creator and regulator of artificial intelligence, the message of the Guidelines is unmistakable: trust, fairness, and transparency must define the next generation of innovation.

For more details, write to us at: contact@indialaw.in

Related Practice Areas

Technology Law