Tuli & Co
Solicitors and Advocates

Date: 2 June 2026

AI Regulation in India: Emerging Compliance Themes

Introduction

India is well-positioned to capitalise on the growth and transformative potential of artificial intelligence ("**AI**"). With over six million people employed across the technology and AI ecosystem, over USD 1.1 billion in proposed Government investment, and a projected economic contribution of USD 1.7 trillion by 2035[1], India is poised to become a key driver in the global AI economy. At the same time, regulatory oversight is increasingly viewed as necessary to address concerns relating to transparency, accountability, bias, data privacy, cybersecurity, and consumer protection. The challenge for policymakers, therefore, lies in achieving a balance between fostering innovation and promoting responsible AI deployment.

In this context, this article explores recent developments in India's AI governance landscape, including emerging policy initiatives, Government guidance, and the application of existing legal frameworks to AI systems. It also considers how these developments may translate into practical compliance expectations for organisations developing or using AI-enabled systems.

AI Regulation in India

Unlike certain jurisdictions (such as the European Union), India does not have a single, comprehensive legislative framework governing AI. Instead, India has thus far adopted a relatively light-touch approach to AI regulation. Accordingly, the present position is best understood not as a regulatory vacuum, but as an emerging layered framework under which AI-related risks may be addressed through a combination of existing laws, non-binding guidance, targeted amendments, and sector-specific requirements. Set out below are some recent key AI-related policy developments in India:

AI Governance Guidelines

In November 2025, the Ministry of Electronics and Information Technology ("**MeitY**") released the AI Governance Guidelines ("**Guidelines**"), which adopt a principles-based rather than prescriptive approach to AI governance. The Guidelines are anchored in seven guiding principles: trust, human-centric design, innovation, fairness/equity, accountability, understandability, and safety, resilience, and sustainability.

Whilst the Guidelines are non-binding, they are likely to influence the shape of forthcoming AI-related regulation. Importantly, the Guidelines do not recommend the immediate introduction of

1 For further information on AI in India, see the Press Release titled "*Transforming India with AI*" of 30 December 2025, posted by the Press Information Bureau.

Article

standalone AI legislation. Instead, they indicate that existing laws, including those relating to information technology, data protection, consumer protection, and criminal liability, can be used to govern AI applications [2]. That said, the Guidelines recognise the need for enforcement, as well as for a comprehensive review of existing frameworks to address AI-related regulatory gaps through targeted legal amendments and regulations [3].

In February 2026, India hosted the AI Impact Summit, organised under the India AI Mission by MeitY. The Summit concluded with the adoption of the New Delhi Declaration on AI Impact, which was endorsed by 92 countries and international organisations[4]. Thematically, the AI Impact Summit drew on the seven principles set out in the Guidelines, while also including more practical discussions around India-specific risk assessment models, governance infrastructure, AI incident reporting mechanisms, and sector-specific frameworks. Accordingly, while the Guidelines establish the overarching principles for AI governance in India, we are also beginning to see a gradual transition toward operationalisation.

White Papers

The Office of the Principal Scientific Adviser to the Government of India issued a series of non-binding "*White Papers*". These do not represent formal policy positions, but provide useful explanatory briefs on specific nuances within the AI ecosystem. So far, three White Papers have been issued, which focus on the following:

- "*Democratising*" access to AI infrastructure by making compute resources, datasets, and AI models accessible and affordable (ie, through a Digital Public Infrastructure ("**DPI**") approach, whereby shared digital platforms and common technical standards are used[5]).

- A "*techno-legal*" approach to AI development, which advocates a compliance-by-design framework whereby safeguards and controls are embedded into AI systems from the outset. This prevents harmful outcomes through system design rather than relying on regulatory intervention or enforcement after deployment[6].

---

2 The Guidelines note that "*Existing laws (for e.g. on information technology, data protection, consumer protection and statutory civil and criminal codes, etc.), can be used to govern AI applications. Therefore, at this stage, a separate law to regulate AI is not needed given the current assessment of risks. However, timely and consistent enforcement of applicable laws is required to build trust and mitigate harm*."

3 Although the Guidelines note that existing laws may sufficiently address AI risk at this stage, they also say that: "*At the same time, there is an urgent need to conduct a comprehensive review of relevant laws to identify regulatory gaps in relation to AI systems. For example, the Pre-Conception and Pre-Natal Diagnostic Techniques (PC-PNDT) Act should be reviewed from the perspective of AI models being used to analyse radiology images, which could be misused to determine the sex of a foetus and enable unlawful sex selection. In priority sectors such as finance, where such analysis is already underway, regulatory gaps should be quickly identified and plugged in with targeted legal amendments and regulations.*"

4 For further information, see the Press Release titled "*AI Impact Summit 2026 Concludes with Adoption of New Delhi Declaration*" of 21 February 2026, posted by the Press Information Bureau, and the Press Release titled "*India AI Impact Summit 2026: Landmark Global Declaration and Major AI Investment Commitments*" of 2 March 2026, also posted by the Press Information Bureau.

5 See the Office of the Principal Scientific Adviser to the Government of India's White Paper of December 2025 titled "*Democratising Access to AI Infrastructure*".

6 See the Office of the Principal Scientific Adviser to the Government of India's White Paper of January 2026 titled "*Strengthening AI Governance Through Techno-Legal Framework*".

- Advancing "*indigenous foundation models*" by supporting the development of domestic AI models trained on Indian languages and datasets, thus reducing reliance on foreign models and promoting systems aligned with India's linguistic diversity and cultural context[7].

Taken together, the White Papers underscore India's objective of promoting AI development and expanding access to AI infrastructure and resources. They reflect a pro-innovation approach that encourages AI adoption while embedding safeguards into system design. In practice, organisations developing AI systems remain subject to baseline data protection and cybersecurity obligations, as well as any additional AI-related requirements imposed by sector-specific regulators.

Existing Frameworks

As noted above, the Guidelines suggest that many AI-related risks can be addressed through existing laws, provided these are enforced and reviewed in a timely manner. In this regard, we note below certain key frameworks that are relevant to the governance of AI systems in India:

- **Intermediary Rules**: The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026 ("**Intermediary Rules**") came into force on 20 February 2026. The Intermediary Rules are among the first binding Indian norms to address a specific AI-related risk (ie, the creation, labelling, traceability, and dissemination of "*Synthetically Generated Information*[8]", defined as any audio, visual, or audio-visual information created artificially or algorithmically).

  The Intermediary Rules require "*intermediaries*[9]" offering a computer resource enabling such "*Synthetically Generated Information*" to: (i) deploy technical measures to monitor and

7 See the Office of the Principal Scientific Adviser to the Government of India's White Paper of March 2026 titled "*Advancing Indigenous Foundation Models*".

8 The Intermediary Rules define the term "*Synthetically Generated Information*" as "*audio, visual or audio-visual information which is artificially or algorithmically created, generated, modified or altered using a computer resource, in a manner that such information appears to be real, authentic or true and depicts or portrays any individual or event in a manner that is, or is likely to be perceived as indistinguishable from a natural person or real-world event*".

9 §2(w) of the Information Technology Act 2000 states that an "*intermediary*", with respect to any particular electronic records, means "*any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online marketplaces and cyber cafes*".

prevent unlawful AI-generated information[10], (ii) label such AI-generated information[11], (iii) embed permanent metadata or technical markers to enable traceability[12], and (iv) act expeditiously against unlawful AI-generated information[13]. Given that these technical measures are now mandated under law, the Intermediary Rules continue to advance the Government's "*techno-legal*" approach.

- **DPDP Act**: The Digital Personal Data Protection Act 2023 ("**DPDP Act**") and accompanying rules establish a comprehensive framework governing the processing of personal data in India. The framework is to be operationalised in stages, with provisions relating to the constitution of the Data Protection Board of India ("**DPB**") coming into force first, followed by consent management and core compliance requirements. Full compliance is required by May 2027.

The DPDP Act introduces various requirements on personal data processing, including obtaining valid consent[14], limiting processing to specified purposes[15], and implementing reasonable security safeguards[16]. These obligations directly impact the deployment of AI systems relying on

---

10 R3(3)(a)(i) of the Intermediary Rules is in the following terms:

"(3) Due diligence in relation to synthetically generated information: (a) Where an intermediary offers a computer resource which may enable, permit, or facilitate the creation, generation, modification, alteration, publication, transmission, sharing, or dissemination of information as synthetically generated information, it shall ensure that,

(i) it deploys reasonable and appropriate technical measures, including automated tools or other suitable mechanisms, to not allow any user to create, generate, modify, alter, publish, transmit, share, or disseminate, as the case may be, any such synthetically generated information that violates any law for the time being in force, including the Act, Bharatiya Nyaya Sanhita, 2023 (45 of 2023), Protection of Children from Sexual Offences Act, 2012 (32 of 2012), Explosive Substances Act, 1908 (6 of 1908), and includes any such synthetically generated information that,- (…)"

11 R3(3)(a)(ii) of the Intermediary Rules is in the following terms:

"(ii) every such information not covered under sub-clause (i) of clause (a) is prominently labelled in a manner that ensures prominent visibility in the visual display that is easily noticeable and adequately perceivable, or, in the case of audio content, through a prominently prefixed audio disclosure, that can be used to immediately identify that such information is synthetically generated information which has been created, generated, modified or altered using a computer resource and such information shall be embedded with a permanent metadata or other appropriate technical provenance mechanisms, to the extent technically feasible, including a unique identifier, to identify the computer resource of the intermediary used to create, generate, modify or alter such information;"

12 Ibid 11.

13 R3(3)(cb) of the Intermediary Rules is in the following terms:

"(cb) where an intermediary becomes aware, either on its own accord or upon receipt of actual knowledge or on the basis of any grievance, complaint or information received under these rules, of any violation of sub-rule (3), in relation to the creation, generation, modification, alteration, hosting, displaying, uploading, publishing, transmitting, storing, updating, sharing or otherwise dissemination of information as synthetically generated information covered under sub-clause (ii) of clause (a), it shall take expeditious and appropriate action, including those specified in sub-clause (ii) of clause (ca);."

14 §4 of the DPDP Act states that a person may process personal data for a lawful purposes "*for which the Data Principal has given her consent*" or "*for certain legitimate uses*". §6 of the DPDP Act further requires the Data Principal's consent to be "*free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose*."

15 Ibid 14.

16 R6(1) of the Digital Personal Data Protection Rules 2025 is in the following terms:

personal data. In particular, organisations deploying AI systems will need to consider whether personal data is used for model training, profiling, decision-support, automated analysis, or other downstream purposes, and whether such processing remains consistent with the purpose for which the personal data was collected. Additionally, the DPB is empowered to penalise non-compliance, thereby creating accountability mechanisms for organisations involved in AI-related processing activities[17].

- **Sector-Specific Regulation**: By way of illustration, in the insurance sector, Insurers are increasingly adopting AI for underwriting, claims processing, fraud detection, distribution monitoring, and enhancing customer experience. The Insurance Regulatory and Development Authority of India ("**IRDAI**") has also encouraged AI usage, including for video-based customer identification processes[18]. Separately, the regulatory framework now recognises "*Cyber or New Age Fraud*" as a category of insurance fraud carried out through digital or new age technologies[19]. This is relevant to AI governance because AI-enabled tools may be used to detect sophisticated fraud and, conversely, to perpetrate fraud through deepfakes, synthetic documents, manipulated images, or similar methods.

The IRDAI's Cyber Security Guidelines 2026 ("**Cyber Guidelines**") also have implications for the use of AI by regulated entities. The Cyber Guidelines require Insurers to classify data based on sensitivity and criticality, implement corresponding security measures (including encryption for

---

"6. Reasonable security safeguards. — (1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum, —

(a) appropriate data security measures, such as securing of personal data through encryption, obfuscation, masking or the use of virtual tokens mapped to that personal data;

(b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor, wherever applicable;

(c) visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;

(d) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, such as by way of data-backups;

(e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;

(f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor, wherever applicable, for taking reasonable security safeguards; and

(g) appropriate technical and organisational measures to ensure effective observance of security safeguards."

17 The Guidelines similarly note that "*The DPDP Act introduces obligations of consent, purpose limitation, and data minimisation that have direct bearing on AI model training and deployment. It prohibits processing of personal data without consent, requires safeguards against misuse of sensitive data, and empowers the Data Protection Board to investigate harms caused by misuse of AI-driven profiling. These provisions create accountability pathways for AI developers and deployers handling personal data at scale*."

18 ¶(m) under Annexure II of the IRDAI Master Guidelines on Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) of 1 August 2022 states that "*Insurers are encouraged to take assistance of the latest available technology (including Artificial Intelligence (AI) and face matching technologies etc.) to strengthen and ensure the integrity of the process as well as the confidentiality of the information furnished by the customer/beneficiary. However, the responsibility of identification shall rest with the insurer*."

19 ¶6 of the IRDAI (Insurance Fraud Monitoring Framework) Guidelines 2025.

confidential and restricted information), and maintain oversight of outsourced providers. These requirements directly affect the governance of AI systems within the insurance sector, particularly where such systems involve personal data, confidential information, cloud-based tools, third-party vendors, or automated support. In addition, the IRDAI recently called upon Insurers to assess their exposure to emerging AI-driven cyber threats and strengthen defences against advanced AI-enabled attacks. In this regard, while the insurance framework does not yet contain a dedicated AI governance code, further guidance in this area may be expected.

- **AI Bill**: Although not yet enacted, the Artificial Intelligence (Ethics and Accountability) Bill 2025 ("**AI Bill**") was introduced in December 2025. The AI Bill proposes the establishment of an Ethics Committee for AI, which would be responsible for developing ethical guidelines for AI systems, monitoring compliance with such standards, and reviewing instances of misuse, bias, and other violations[20]. This proposal reflects an intended focus on compliant AI development/usage and accountability.

Concluding Remarks

India is emerging as a global hub for AI development and adoption, supported by Governmental initiatives and a policy approach emphasising innovation and principles-based governance rather than prescriptive regulation. Given the pace of technological advancement and expanding use of AI across industries, the landscape is likely to continue evolving, and the absence of standalone AI legislation should not be understood as the absence of legal or regulatory risk.

For organisations using AI systems in India, practical compliance is likely to focus on documenting use cases, assessing risk, maintaining human oversight, reviewing vendor arrangements, protecting personal data, strengthening cybersecurity controls, and ensuring that AI systems can be explained, tested, monitored, and audited where necessary. Accordingly, even in the absence of a standalone AI law, organisations may benefit from internal AI governance frameworks capable of demonstrating transparency, accountability, fairness, safety, and regulatory oversight.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

For further information on this topic please contact Tuli & Co

[20] The AI Bill was introduced as Bill No. 59 of 2025 by MP Smt Bharti Pardhi. §4 of the AI Bill is in the following terms:

"4. The Committee shall,—

(a) develop and recommend ethical guidelines for AI technologies;

(b) monitor compliance with ethical standards in AI systems;

(c) review cases of misuse, bias or violations of the provisions of this Act;

(d) promote awareness and capacity-building among stakeholders;

(e) undertake such other functions as the Central Government may, from time to time, prescribe."

T: +91 120 693 4000, E: lawyers@tuli.co.in, or W: www.tuli.co.in

Author(s)

Anuj Bahukhandi

Partner

Armaan Tuli

Associate

Article