MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

सत्यमेव जयते

Digital India
Power To Empower

AI
IMPACT
SUMMIT
भारत 2026 INDIA

सर्वजन हिताय | सर्वजन सुखाय
WELFARE FOR ALL | HAPPINESS OF ALL

INDIAai

India AI
Governance Guidelines

Enabling Safe and Trusted AI Innovation

2.3 Policy & Regulation

The overarching goal of India's AI governance framework is to encourage innovation, adoption and technological progress, while ensuring that actors in the AI value chain are mitigating risks to individuals and society. In that respect, the Committee has reviewed the current legal framework and suggested areas where regulatory intervention is necessary.

Applicability of existing laws

In recommending a suitable regulatory approach, the Committee has paid close attention to the existing system of laws and regulations in India, comprising constitutional provisions, statutory laws, rules, regulations, and guidelines. This includes laws and regulations across domains such as information technology, data protection, intellectual property, competition law, media law, employment law, consumer law, criminal law, amongst others.

The Committee's current assessment is that many of the risks emerging from AI can be addressed through existing laws. For example, the use of deepfakes to impersonate individuals can be regulated by provisions under the Information Technology Act and the Bharatiya Nyaya Sanhita; and the use of personal data without user consent to train AI models is governed by the Digital Personal Data Protection Act. The Annexure to this report contains examples of how existing laws can be applied to deal with other AI harms.

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,[xvii] regulatory gaps should be quickly identified and plugged in with targeted legal amendments and regulations.

Ongoing deliberations

There are a few domains in which deliberations are already underway to study regulatory issues relating to AI governance and potential gaps. Some of these engagements are by way of inter-ministerial consultations, rulemaking under newly adopted laws, and expert committees. In this section, the Committee outlines a few such areas.

(a) Classification and Liability

The Information Technology Act, 2000 (IT Act) is the primary legislation that deals with the classification of digital platforms, their obligations under law, and related liability.

The IT Act, given that it was drafted more than two decades ago, requires an update in relation to how digital entities are classified, specifically in the context of AI systems. For example, there is a need to define clearly the roles of various actors in the AI value chain (developer, deployer, users, etc.) and how they will be governed under current definitions ('intermediary', 'publisher', 'computer system', etc.). At present, the term intermediary is broadly defined to mean any entity that "on behalf of another person receives, stores or transmits [an electronic record] or provides any service with respect to such record". Under current laws, it includes telecom service providers, search engines and even cyber cafes.[xviii] However, there is a need to provide clarity, especially with regard to how this definition would apply to modern AI systems, some of which generate data based on user prompts or even autonomously, and which refine their outputs through continuous learning.

Another important question is how liability should be apportioned across the AI value chain. Under Section 79 of the IT Act, legal immunity is available to intermediaries for unlawful third-party content, provided they do not initiate the transmission of data, select the recipient of the data or modify it. It appears that such legal immunity would not be applicable to many types of AI systems that generate or modify content. Further, the liability of AI developers and deployers who fail to observe due diligence obligations under the IT Act also needs further deliberations.

Therefore, the Committee is of the view that the IT Act should be suitably amended to ensure that India's legal framework is clear on how AI systems are classified, what their obligations are, and how liability may be imposed.

(b) Data Protection

The Digital Personal Data Protection Act (DPDP Act) which governs the collection and processing of all digital personal data in India, was adopted by Parliament in August 2023 and will be in force once draft rules to implement various aspects of the law are notified. Even as the rulemaking process for the DPDP Act is underway, new questions have emerged about the impact of data protection regulations on AI development and risk mitigation.

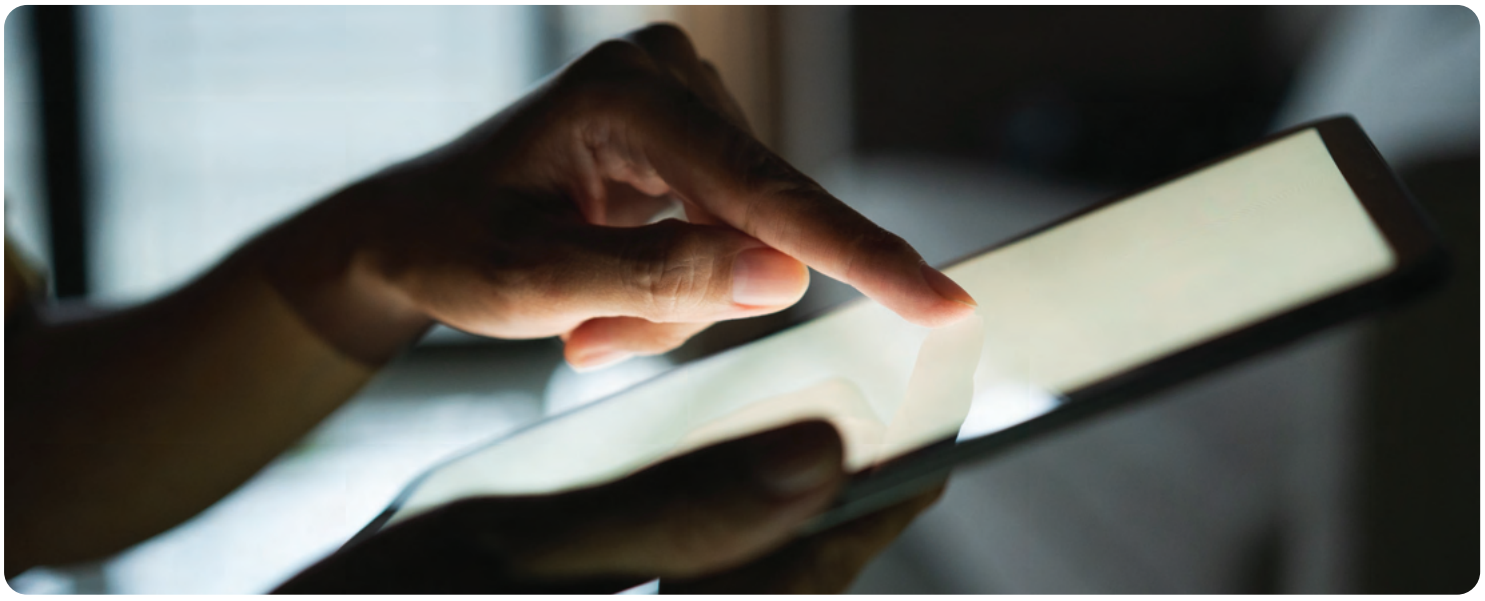
Key issues include for example, the scope and applicability of exemptions available for the training of AI models on publicly available personal data;[xix] whether the principles of collection and purpose limitation are compatible with how modern AI systems operate;[xx] the role of 'consent managers' in AI workflows and the value of dynamic and contextual notices in a world of multi-modal AI and ambient computing;[xxi] the scope of the research & 'legitimate use' exception for AI development;[xxii] and various other issues.

The Committee believes that resolving these issues are central to a robust AI governance framework. Further, some of the issues raised above may require legislative amendments to take effect, and the Committee recommends a detailed review by relevant bodies such as the AI Governance Group, which this committee has suggested establishing.

(c) Content Authentication

Generative AI technologies, including image, video, and music generation tools offer significant opportunities for creativity, human expression, access to knowledge and innovation. At the same time, the risks of misuse are significant. The creation and distribution of deepfakes and other unlawful material, such as child sexual abuse material (CSAM) and non-consensual images ('revenge porn'), have the potential to cause serious harm, especially to vulnerable groups.[xxiii] India's AI governance framework should therefore preserve the benefits of these technologies while addressing their misuse.

In this context, the Committee has examined the issue of content authentication and provenance, i.e. the determination of whether or not any piece of information was generated or modified by an AI system.



A popular method for content authentication is the use of watermarks. Such labels and other unique identifiers can be used to authenticate whether or not any piece of information was generated or modified by an AI systems.[xxiv]

This principle of using unique identifiers for content authentication and provenance is embedded in existing industry standards such as the Coalition for Content Provenance & Authenticity (C2PA).[xxv]

A related issue is content traceability, i.e. tracing the origin of a particular piece of content generated or modified by AI. Various forensic tools and attribution methods currently exist for this purpose (for e.g. watermarking to trace the origin of AI-generated content, dataset provenance tools to identify training data sources in copyright infringement cases, attribution methods to determine if harmful content originated from a specific AI model).[xxvi] Such attribution tools have potential utility for both content authentication and provenance. At the same time, their inherent limitations must also be examined (for e.g. the ability of malicious actors to bypass these safeguards and risks to citizen privacy).[xxvii]

The issue of harmful deepfakes is a growing menace to society and immediate action is required. Therefore, it is recommended to set up a committee of experts with representatives from government, industry, academia and standard-setting bodies to develop global standards around content authentication and provenance. These standards, governance frameworks and technical measures may be presented in standard-setting bodies and subjected to rigorous testing to ensure that these measures are effective.

In parallel, it is recommended that the proposed AI Governance Group (AIGG), with support from the Technology & Policy Expert Committee (TPEC), described later in this report, should review the regulatory framework in India applicable to content authentication and make recommendations to relevant agencies, such as MeitY, including the use of appropriate techno-legal solutions and additional legal measures if necessary in order to tackle the problem of AI-generated deepfakes in India.

(d) Copyright

Copyright is a contested issue in AI governance, particularly in relation to generative AI systems. Public consultations on this topic have yielded strong and divergent views from technology companies, news publishers, content creators and civil society on the issue of how legal frameworks can protect creative labour without stifling innovation.[xxviii]

Following the publication of the draft report on 'AI Governance Guidelines Development' published in January, 2025, the Department for Promotion of Industry and Internal Trade (DPIIT) established a committee in April, 2025 to deliberate on this issue.[xxix] The DPIIT committee's mandate includes examining the legality of using copyrighted work in AI training and its implications, evaluating the copyrightability of works produced by generative AI systems, and reviewing international practice to propose a balanced copyright framework suited to India's needs.

As part of its deliberations, this Committee has specifically examined the implications of using copyrighted materials in the training and development of AI models.

According to Section 52 of the Indian Copyright Act, limited 'fair dealing' exceptions apply for private or personal use, including research. These exceptions are restricted to non-commercial use and do not extend to organisational or institutional research. As a result, they may not cover many types of modern AI training.

Based on current practice, AI models are often trained on large collections of publicly available data to improve accuracy and relevance of the model, and to promote inclusivity. Various lawsuits have been filed claiming that such practices constitute infringement based on the limited exception provided under Indian copyright law.[xxx]

Globally, some groups are in support of a 'Text and Data Mining' (TDM) exception to enable AI development. Some jurisdictions, such as the EU, Japan, Singapore and the UK have adopted this approach in varying capacities.[xxxi] This Committee is of the view that the committee set up by DPIIT for this purpose may consider a balanced approach, which enables Text and Data Mining, with the objective of fostering innovation and enabling provisions to protect the rights of copyright holders.

The Committee awaits the DPIIT committee's detailed recommendations on these issues.

Global diplomacy on AI governance

Given the strategic importance of technology in protecting national security and sovereignty, AI governance is a critical element of foreign diplomacy. This is clearly demonstrated in the centrality of international AI governance in various national AI strategies (see for example, the US 'AI Action Plan'[xxxii] and China's 'Global AI Governance Action Plan').[xxxiii]

The Committee is of the view that India's balanced approach to AI governance could benefit countries in the Global South, i.e. a majority of the world's population.

AI governance should therefore be integrated into India's strategic engagements and foreign policy. India should continue its participation in multilateral AI governance forums, such as the G20, UN, OECD, and deliver tangible outcomes as host of the 'AI Impact Summit' in February 2026.

Foresight on AI governance

The pace of progress in AI makes it challenging for regulation to keep up. For example, highly autonomous 'AI agents' are demonstrating new capabilities, such as self-directed action and multi-agent collaboration, which may require us to rethink our current approaches to governance.

Potential risks also include autonomous AI-to-AI communication and coordination. Advanced AI systems may create covert protocols or collaborate with each other in ways that amplify security concerns, run disinformation campaigns, and cause disruptive loss of control. Governance frameworks must therefore have clear monitoring standards, audit trails, and ensure that human-in-the-loop mechanisms are in place at critical decision points. This is explained in more detail in the next section under mitigating loss of control.

The Committee recommends that governance frameworks should be future looking, flexible and agile, such that they enable periodic reviews and reassessments.

As the ecosystem in India matures, the Committee recommends undertaking foresight research, policy planning, and simulation exercises to anticipate future issues and demands so that policy and regulation can be adapted accordingly.

Recommendations

- Develop governance frameworks that are balanced, agile, flexible, and principle-based, and enable monitoring and recalibration based on feedback.
- Review the current legal framework to evaluate risks and regulatory gaps.
- Consider targeted legislative amendments to encourage innovation (for eg. in copyright and data protection) and to clarify issues around classification and liability.
- Develop common standards and benchmarks to achieve regulatory objectives (e.g., on content authentication, data integrity, cybersecurity, fairness, etc.).
- Establish a committee of international experts from government, industry, academia and standard-setting bodies to develop global standards around content authentication, with a focus on certifying information as genuine.
- The proposed AI Governance Group (AIGG), with support from the Technology & Policy Expert Committee (TPEC) should examine issues of content authentication in detail and issue appropriate guidelines.
- Create regulatory sandboxes to enable the development of cutting-edge technologies in constrained environments affording reasonable legal immunities, provided these tests produce evidence with published details of what was tested, guardrails applied, risks observed, etc.
- Support strategic engagements and foreign diplomacy in national, regional and multilateral forums to further India's interests on AI governance issues.
- Conduct horizon-scanning and scenario planning analysis to anticipate future developments in AI that may require policy or regulatory responses.