

RACHANA RAUTRAY

Anagram Partners

rachana.r@anagrampartners.in

If you have any questions regarding the matters discussed in this publication, please contact the attorney(s) listed above or call your regular contact at Anagram.

Introduction

Following the release of the Digital Personal Data Protection Rules 2025, the Ministry of Electronics and Information Technology (“MeitY”) also released its report on AI Governance Guidelines, outlining a regulatory roadmap for the AI industry. In this article, we explore the implications of the recommendations made by the sub-committee set up by MeitY on November 09, 2023 (“Sub-Committee”), as a roadmap to regulate AI.

On January 06, 2025, the Sub-Committee released its findings from a gap analysis undertaken on existing legal frameworks to propose recommendations to develop a comprehensive approach to ensure “**trustworthiness**” and “**accountability**” of AI systems in India. Its recommendations as set out below, have drawn largely on *inter alia* Organization for Economic Co-operation and Development’s AI principles released in 2019 ([see here](#)):

- ▶ A ‘**whole of government approach**’ must be adopted to implement and coordinate on AI governance. This committee/group should bring together key institutions, such as regulators and government departments having visibility on AI systems to set out a roadmap and coordinate on AI governance.
- ▶ A technical advisory body should be established by MeitY to *inter alia* assess risks to consumers, for issues such as online safety, anti-trust, data governance, etc., engage with the industry to operationalize responsible use of AI, identify gaps which may not be adequately addressed through delegated legislation.
- ▶ An AI incident database as a repository of problems experienced with AI from real world cases to guide responses of mitigation or avoidance of repeated negative outcomes to be developed.
- ▶ Engagement with industry to drive voluntary baseline commitments that complement legal frameworks across the AI ecosystem.
- ▶ Assessing the suitability to introduce technological measures, such as technology artefacts into models of AI interaction, and track negative outcomes “**real time**”.
- ▶ Constitution of a sub-group under MeitY to suggest measures under the proposed Digital India Act to harmonize the legal framework, regulatory and technical capacity and adjudication of grievance redressal.

Insights into the Government's Approach to AI & its Implications

Harm Based Approach

It is evident from the Sub-Committee's recommendations that the Government's perception of AI, is that this technology poses unique or greater risks compared to existing technologies. The emphasis on creating an '*AI incident*' database and deploying regulations to address real-time negative outcomes suggests that future legislation will focus on limiting AI's scope of deployment based on its harm.

However, a key flaw in this approach lies in the assumption that all AI systems are developed, deployed, and used under similar global circumstances. As demonstrated by the European Union's regulatory model, a harm-based approach may stifle industry innovation in the long run.

Aspects of AI Requiring Regulation Remains Unidentified

In addressing AI's perceived harm, the Sub-Committee relies heavily on broad global principles like '*transparency*', '*accountability*', '*privacy*', '*do no harm*' and '*inclusiveness*'. This approach misses a critical opportunity to clearly define which aspects of AI should be regulated and how these principles should be applied within that context. For example, prior to amendments to India's Information Technology Act, 2000 ("*IT Act*"), the Expert Committee constituted by MeitY in 2005 identified specific aspects of digital transactions that required regulation—such as digital contracts for e-commerce and mitigating data breach risks due to increasing technology adoption.

By defining the scope of regulation first, the committee could better tailor the amendments. A similar approach could help shape a more India-specific AI regulatory framework.

AI Stakeholders that could be Potentially Regulated

In line with the Digital Personal Data Protection Act 2023, the Sub-Committee has made initial efforts to identify key stakeholders in the AI ecosystem, such as the data principal, data provider, AI developers, AI deployers, and end users. While this is a positive initial step, the Sub-Committee falls short in clarifying the distinctions between these roles, such as the difference between '*data principal*', '*data provider*', and '*end user*' and how these roles might shift or overlap in practice.

Techno-Legal Approach to Regulations

Although the Sub-Committee acknowledges the rapid growth of AI tools, its recommendation to integrate regulatory compliance directly into these tools through '*techno-legal*' measures is overly broad. The challenge with this approach is that the purpose and use of each AI tool can vary significantly on a case-by-case basis. As a result, the effectiveness of a uniform regulatory requirement may vary depending on the context.

For instance, while B2B AI tools may be used by enterprise customers to process personal data, requiring the tools to incorporate a consent artefact at the outset could be premature, especially if the enterprise customer does not ultimately use the tool for processing personal data.

Expanding the Scope of Incident Reporting

A key shortcoming of the Sub-Committee's findings is its recommendation to separately regulate '*AI incidents*' on the assumption that these incidents extend beyond traditional cyber incidents. According to the report, an AI incident could include "**adverse or harmful outcomes resulting from AI use that could disadvantage individuals, businesses, and societies**", encompassing issues such as malfunctions, unauthorized outcomes, discriminatory results, unforeseeable consequences, emergent behavior, system failures, privacy violations, and safety concerns.

For context, the Digital Personal Data Protection Act, 2023 defines a personal data breach as "**unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data**", while the CERT-In rules define a cyber incident as any real or suspected event that *inter alia* compromises the confidentiality, integrity, or availability of data, causes unauthorized access to data or systems, disrupts services or networks, threatens public safety or violates security policies.

While it is debatable whether certain AI tools present a greater societal risk, the Sub-Committee fails to set out its reasons on why the current scope of data breach laws is inadequate to address breaches arising from AI-related issues.

'AI – Labelling' likely Inevitable

Even before the Sub-Committee's recommendations, the Government had consistently advocated for using watermarks, platform labeling, and other fact-checking tools to identify AI-generated content and mitigate the impact of deepfakes. This was reinforced by CERT-In's advisory on November 27, 2024 (CIAD-2024-0060), which called for watermarked media and detection protocols for deepfakes. Similarly, on January 16, 2025, the Election Commission advised political parties to label AI-generated or altered materials with terms like "**AI-Generated**", "**Digitally Enhanced**" or "**Synthetic Content**".

While labeling may be an initial step to combat deepfakes, it overlooks the potential business impact. AI-labeled content may be viewed skeptically by end users, as the intent of AI is often to enhance material without revealing its computer-generated nature.

Industry Takeaway

In summary, while the Sub-Committee's recommendations represent a thoughtful attempt to regulate AI technology, specifically by encouraging baseline commitments from the industry, several gaps remain in terms of the Government's outlook towards AI regulation. The harm-based approach, while well-intentioned, risks stifling


innovation by imposing broad, one-size-fits-all regulations. It will be crucial for the respective committees / technical body proposed to be set up by MeitY to engage with the industry, on identifying the roles of various stakeholders and the instances or sectors where '*techno-legal*' compliance model could be feasible.

This publication is for educational and informational purposes only and is not intended and should not be construed as legal advice.

anagrampartners

Mumbai | Delhi

Follow us for more

 / anagrampartners.in

0201–2025