



Article

October 2026



AI Liability and Regulation for India's GCCs

Introduction

India's Global Capability Centres ("GCCs") have evolved significantly from their traditional back-office functions. They are increasingly developing and deploying generative and agentic AI, not to mention adopting the use of AI in several functions. The use of AI may raise questions under data protection, intellectual property, employment, consumer protection, cybersecurity and sector-specific laws, while the nature of the system itself may raise separate questions about autonomy, human oversight, decision-making and accountability. A GCC therefore needs to assess both the legal framework applicable to a particular AI system and the how it operates.

An AI tool that assists an employee in a GCC to prepare a recommendation is different from a system that independently makes decisions and acts. Consequently, the risks associated with each also differ. Before deployment, a GCC therefore needs to understand why each AI system will be used and how the AI will operate, including the level of autonomy involved, the information and data on which the AI will rely for the output, the role of human oversight and the potential consequences of an inaccurate, biased or otherwise inappropriate output, particularly where the consequences affect individuals, whether because the output is to be depended on or the system/operation involves personal data or in financial decisions.

1. Indian Regulatory Framework

At present, India does not have standalone, comprehensive legislation that governs either the development or the use of AI. Instead, AI-related risks are addressed through existing legislation, sectoral regulation and policy frameworks. The India AI Governance Guidelines released by the Ministry of Electronics and Information Technology ("MeitY") in November 2025 suggest the continued application of existing laws to different AI-related risks. Consequently, the legal requirements applicable to an AI system depend on the particulars of the system itself. To illustrate: an AI system used for recruitment may raise questions concerning bias and discrimination at the time of selection, depending on the information used to train the AI. Similarly, an AI model trained using employee or customer information may give rise to obligations under the Digital Personal Data Protection Act, 2023, and the use of copyrighted material in training or developing an AI model may be subject to scrutiny under the Copyright Act, 1957. The MeitY guidelines also emphasise a proportionate, risk-based approach to AI governance. Thus, GCCs should determine the risks involved in an AI system, depending on the role/business of the GCC and the purposes for which the AI is being used, before its deployment into their processes, so that such risks can be managed accordingly.

The same assessment is relevant to liability: if an AI system produces an inaccurate or offensive output, responsibility may depend on the role played by the GCC, the technology provider, the parent company and the human decisionmaker, as well as the degree of control and oversight exercised over the system. A system may also produce an inaccurate or biased outcome despite appropriate training and testing. It is therefore important to consider not only whether an AI system can make a particular decision, but also whether there are appropriate safeguards to review the output that the system produces, identify errors and intervene where required. The Delhi Court's order in an interim application in ANI Media Pvt. Ltd. v. OpenAI OPCO LLC, illustrates the fact-specific nature of this assessment: ANI alleged that OpenAI had copied and stored its copyrighted works for training its AI models without authorisation. While the Delhi High Court held that OpenAI's use of ANI's works was *prima facie* covered by the fair-dealing exception under Section 52(1)(a) of the Copyright Act, 1957, that finding was fact-specific, and cannot provide a general assurance that training or operating an AI system on third-party content is lawful. A GCC should therefore establish the source of the data and the legal basis for using it before deployment to ensure its legal permissibility.

2. Cross-border legislative considerations

For GCCs which support parent companies having a multinational presence, the assessment cannot be limited to Indian law. An AI system may be developed in India, but the output is to be used by the parent company or a customer in another jurisdiction. An example of a law having extraterritorial application is the EU AI Act (2024/1689) ("**Act**"), which, in specified circumstances, extends to providers or deployers located outside the European Union when the output produced by their AI systems is used within the European Union. The fact that a GCC is in India therefore does not, by itself, determine whether laws such as the Act are relevant. A GCC developing an AI system in India for an EU-based group company may need to consider whether the system falls within the scope of the Act and, if so, what obligations are applicable to them.

The jurisdiction in which an AI system or its output is used should therefore form part of the assessment alongside the purpose, functionality and possible risks of the AI system. For GCCs, this creates an additional layer of analysis because their AI development and deployment activities are often undertaken for global businesses and may consequently have regulatory implications beyond the jurisdiction in which the GCC itself is located.

3. Sector Specific Considerations

Many GCCs support banking, financial services and insurance groups, which are heavily regulated in most jurisdictions and therefore sectoral regulations also must be considered. In India, the Reserve Bank of India's FREE-AI report released in 2025, is a set of recommendations and outlines what regulated entities should expect – *inter alia*, board-approved AI policies and risk-based AI audits while the Securities and Exchange Board of India has made regulated entities solely responsible for the data security, outputs and legal compliance of AI tools they use, whether built in-house or procured from third parties. Other jurisdictions will likely have or come up with similar regulations or guidelines. Since the service recipients from GCCs in these sectors would remain responsible and answerable to their regulators, GCCs should expect its parent/associate companies to require the GCCs to contractually be bound by these requirements, have audit and incident-reporting commitments and map each AI system with its regulatory implications.

The Way Forward

These developments point towards the need for GCCs to move from a standard AI policy to one that involves an AI assessment mechanism that can help evaluate the risks associated with each AI system and determine the safeguards required before deployment. Before deployment, the GCC should assess the purpose and function of the system, the degree of autonomy involved, the information used to develop and operate it, the potential for inaccurate or discriminatory outcomes, the applicable Indian and sectoral laws, any relevant foreign regulatory requirements, the allocation of responsibility and the safeguards required. The assessment should also be revisited when there is a material change in any of these factors or any change in the functioning of the GCC itself. For GCCs, therefore, the objective should not simply be to demonstrate that an AI policy has been adopted, but to demonstrate that each AI system was assessed against these factors before it was deployed.

Disclaimer

This article has been written for the general interest of our clients and professional colleagues and is subject to change. This article is not to be construed as any form of solicitation. It is not intended to be exhaustive or a substitute for legal advice. We cannot assume legal liability for any errors or omissions. Specific advice must be sought before taking any action pursuant to this article. For further clarification and details or advice on the above, you may write to Siddhi Ghatlia (sghatlia@almtlegal.com) or Malini Mukherjee (mmukherjee@almtlegal.com).