

Legal 500

Country Comparative Guides 2026

India

Artificial Intelligence

Contributor

Khaitan & Co



Supratim Chakraborty

Partner | supratim.chakraborty@khaitanco.com

Sumantra Bose

Partner | sumantra.bose@khaitanco.com

Tanu Banerjee

Partner | tanu.banerjee@khaitanco.com

Ishan Johri

Partner | ishan.johri@khaitanco.com

Shailendra Bhandare

Partner | shailendra.bhandare@khaitanco.com

Anushka Sharda

Partner | anushka.sharda@khaitanco.com

Madhav Khosla

Partner | madhav.khosla@khaitanco.com

Sourav Dan

India: Artificial Intelligence

1. What is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

The Government of India has not adopted a single and universal formal definition of artificial intelligence ("AI"). Different governmental departments have approached the conceptualization of AI through policy documents and reports which reflect both, a general and sector-specific view of AI. The National Institution for Transforming India ("NITI Aayog"), as the premier policy think tank of the Government of India, provided an early and comprehensive definition of AI in its policy paper titled "National Strategy for Artificial Intelligence" in June 2018 ("2018 Paper"). NITI Aayog explicitly defined AI as: "the ability of machines to perform cognitive tasks like thinking, perceiving, learning, problem solving and decision making" and noted that AI is "a constellation of technologies that enable machines to act with higher levels of intelligence and emulate human capabilities of sense, comprehend, and act..."

The Government of India's Ministry of Electronics and Information Technology ("MeitY"), in 2025, adopted a pragmatic and adaptive stance, explicitly choosing not to provide a catch-all definition of AI. MeitY noted that:

"Most definitions attempt to be future ready but are unlikely to capture how the technology may evolve. Other definitions tend to go too broad thereby creating uncertainty as traditional software could also be interpreted to be in scope. Definitions are probably useful when they are used to pinpoint certain kinds of technologies for which specific regulatory provisions are to be mandated. However, both the definitions and the manner of identifying systems for regulatory purposes is evolving and requires deeper evaluation."

This is a significant departure from MeitY's earlier position, which defined AI as: "An AI application or AI system is one which combines many AI/machine learning algorithms with the right data and knowledge from diverse sources to accomplish useful work for end users...." This marks an evolution in MeitY's understanding of AI and reflects a business-friendly approach to AI regulation.

Various other regulators have also set out their own

definitions of AI. The Reserve Bank of India ("RBI") in its 2025 report titled FREE-AI Committee Report Framework for Responsible and Ethical Enablement of Artificial Intelligence ("FREE-AI Committee Report") defines AI as: "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment." The Securities Exchange Board of India ("SEBI") in the SEBI (Intermediaries) (Amendment) Regulations 2025 adopted a sector specific definition of AI noting that: "any application or software program or executable system or a combination thereof, offered by the person regulated by the Board to investors/stakeholders or used internally by it to facilitate investing and trading or to disseminate investment strategies and advice or to carry out its activities including compliance requirements and the same are portrayed as part of the products offered to the public or under usage for compliance or management or other business purposes."

Further, while not expressly defining 'AI', the amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 ("2021 Rules") in February 2026 coined the term 'synthetically generated information' ("SGI"), to mean "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."

The Centre for Research and Planning of the Supreme Court of India, ie, the apex court's in-house think tank has offered a definition in its white paper on Artificial Intelligence and Judiciary ("White Paper"). The White Paper describes AI as: "machine-based systems capable of performing functions that ordinarily require human cognitive abilities, such as reasoning, pattern recognition, language comprehension, and structured decision-making." The White Paper also describes generative AI as: "a class of artificial intelligence models designed to create new content such as text, images, audio, or code based on patterns learned from vast datasets. Unlike

traditional AI systems that primarily classify, predict, or retrieve information, generative models can produce original outputs in response to user-provided 'prompts'."

Further, in June 2026, the Supreme Court released a preliminary draft of the Regulations for Use of AI in Courts ("SC Draft AI Regulations"), which define AI as "a machine-based system that infers, learns, and generates decisions, predictions, and recommendations from data, with a varying degree of autonomy, such as, algorithms, computational processes, and software, deployed for court processes, excluding general-purpose software or digital tools, unless such software or tools are specifically embedded with, augmented by, or functionally dependent upon, artificial intelligence".

The absence of a single, unified definition reflects the evolving nature of AI regulation in India. Until a statutory definition is established, what constitutes AI will continue to depend on the regulatory or judicial context in which the question arises.

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made in its implementation? Are there plans for updates or revisions?

India's national strategy for AI is driven by a vision of inclusive growth and societal transformation and was articulated in the 2018 Paper. This vision has since evolved into the comprehensive IndiaAI Mission, approved in March 2024 with a substantial budget outlay of INR 10,371.92 crore (approximately USD 1.2 billion) over 5 years. The IndiaAI Mission is structured around 7 strategic pillars:

(i) IndiaAI Compute Capacity: This pillar focuses on building a scalable AI computing ecosystem to support India's AI startups and research community, while also boosting the semiconductor industry.

Implementation: The IndiaAI Compute Portal, launched in March 2025, provides subsidised access to GPUs, thereby democratizing computing access and providing a foundation for attracting top AI talent. From an initial target of 10,000 GPUs, India has now achieved 38,000 GPUs, providing affordable access to world-class AI resources.

(ii) IndiaAI Innovation Centre: This pillar is dedicated to driving indigenous AI advancements by supporting Indian researchers, startups, and entrepreneurs in building state-of-the-art foundational AI models.

Implementation: Pursuant to a call for proposals launched in January 2025, 10 startups which focused on open-source foundational AI models for public service, healthcare, education and multi-lingual capabilities were selected.

(iii) IndiaAI Datasets Platform ("AIKosh"): The AIKosh centralizes anonymized, non-personal datasets, tool-kits, and AI models across sectors to facilitate the development of AI solutions and promote use cases of AI.

Implementation: The beta version, launched in March 2025, features over 12,000 datasets, 300 AI models, and over 13 development toolkits. It provides a use case library and development environment to explore and share datasets.

(iv) IndiaAI Application Development Initiatives: This pillar supports AI solutions in critical sectors which address real-world problem statements from government ministries and other institutions.

Implementation: More than 30 applications have been approved, and will be provided financial support by the Government of India. The initiative features various case studies showcasing AI applications, such as revolutionising legal document review, predicting chronic kidney disease, and diagnosing malaria.

(v) IndiaAI FutureSkills: This initiative funds AI talent development through large-scale national scholarship programs and the establishment of AI/data Labs in Tier-2 and Tier-3 cities.

Implementation: The IndiaAI FutureSkills initiative aims to provide support to over 500 PhD fellows, 5,000 post-graduates and 8,000 undergraduates. Further, 27 AI / data Labs have been established in Tier-2 and Tier-3 cities.

(vi) IndiaAI Startup Financing: This initiative provides targeted funding and compute subsidies to early-stage AI startups.

Implementation: The initiative is explicitly designed to promote research by funding startups and research teams, not large IT or AI firms, and has selected companies which have received direct financial and infrastructure support.

(vii) Safe & Trusted AI: This pillar emphasizes ensuring responsible AI through the implementation of "Responsible AI" projects, development of indigenous tools and frameworks, and comprehensive guidelines.

Implementation: The NITI Aayog published policy papers

on "Responsible AI" approach, establishing ethical principles and exploring risk-based regulation.

Further, IndiaAI Safety Institute ("AISI") was announced in January 2025, to address AI risks and safety challenges. India also adopted a principle-based AI governance framework anchored in seven Sutras to enable safe, trusted, and inclusive AI innovation across sectors.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

India has not yet enacted a comprehensive legislation for the regulation of AI, however, the Government of India has amended certain legislations to include AI-usage within its ambit and issued advisories to guide AI development and use. These advisories are primarily recommendatory in nature and aim to promote responsible AI use while addressing risks such as bias, privacy concerns, deepfakes and misinformation.

(i) Advisories by MeitY on use of AI

- 2023 Advisory

In 2023, MeitY issued an advisory to "significant social media intermediaries" (social media intermediaries with over 5 million registered users) to exercise due diligence and make reasonable efforts to identify and take down misinformation and deepfakes within 36 hours of reporting.

- Deepfake Advisory

In 2024, the MeitY issued an advisory requiring intermediaries to: (a) communicate to users that the 2021 Rules prohibit the transmission / sharing of deepfakes on their platforms; and (b) undertake due diligence to ensure that users do not upload / transmit unlawful content.

- AI Use Advisory

In 2024, MeitY issued another advisory concerning the use of AI by intermediaries. This AI advisory requires intermediaries and platforms to adhere to specific compliance measures, regarding the use of AI, in line with their due diligence obligations under the Information Technology Act 2000 ("IT Act") and 2021 Rules.

(ii) Advisory by the Indian Computer Emergency Response Team ("CERT-In")

On 26 April 2026, CERT-In issued an advisory with a 'high' severity rating on 'Defending Against Frontier AI Driven Cyber Risks' ("CERT-In AI Advisory"). Although framed as guidance, the CERT-In AI Advisory reflects a clear regulatory shift which treats AI-incident preparedness as a baseline compliance expectation. It applies across the ecosystem, including organisations, micro, small and medium enterprises ("MSMEs") and individual users, on the basis that AI-driven cyber risks are systemic and capable of cascading compromise of interconnected systems and services.

(iii) SEBI's Advisory on Emerging Advanced AI Tools for Vulnerability Detection

On 5 May 2026, the SEBI issued an advisory on the emerging cybersecurity risks posed by advanced, AI-driven vulnerability detection tools (such as Claude Mythos), which can identify and potentially exploit existing vulnerabilities at speed and scale, and may raise concerns over data confidentiality, application integrity, and the reliability of outputs. Given the interconnectedness of market participants, it sets out a coordinated approach to vulnerability management for SEBI's regulated entities ("SEBI REs").

The advisory constitutes a task force, 'cyber-suraksha.ai', comprising representatives from Market Infrastructure Institutions, Qualified Registrars and Transfer Agents, all Qualified Regulated Entities, and other stakeholders. Its mandate includes examining cybersecurity risks posed by AI-based models and devising uniform mitigation strategies, facilitating threat intelligence sharing, reporting cyber incidents and vulnerabilities relevant to securities markets, and reviewing the cybersecurity posture of third-party service providers, etc.

(iv) Key laws regulating the use of AI

- IT Act and 2021 Rules: The IT Act provides safe harbour for "intermediaries" provided that such "intermediaries": (a) do not initiate or select the receiver of transmission or select or modify the information contained in the transmission; (b) observe due diligence while discharging their duties under the IT Act and guidelines of the Government of India; and (c) do not conspire, abet, aid or induce the commission of an unlawful act and upon receipt of actual knowledge of unlawful content on its platform, expeditiously remove / disable access to such content. The 2021

Rules elaborate on the required due diligence standards for intermediaries. Entities providing or hosting AI services may be liable for unlawful content on their platforms in case of violation of the IT Act. Further, the 2021 Rules require intermediaries to: (a) remove SGI content within 3 hours of receiving notice from a court order or a written communication; (b) ensure that all lawful synthetically generated information is labelled; (c) embed metadata or unique technical markers in AI-generated content to enable traceability back to its original source; (d) deploy automated detection systems to disallow unlawful synthetically generated information; and (e) resolve grievances within 7 days.

- **Bharatiya Nyaya Sanhita 2023 ("BNS"):** The Government of India has asserted that provisions of the BNS are "technology-neutral", as the provisions are applicable irrespective of whether the underlying content is AI-generated or not. Accordingly, AI-based harms are also actionable under the BNS and would therefore be directly relevant to AI-generated fraudulent schemes, impersonations, and defamatory content. A few instances of the AI related criminal liability under the BNS are summarised in response to Question 7 below.
- **Consumer Protection Act 2019 ("CPA"):** An AI-enabled product or service could be construed as a 'product' under the CPA, regardless of whether the product in question is a physical device or a software. If an AI-enabled product contains a 'defect' (as defined under the CPA) that causes 'harm', the aggrieved consumer may file a product liability action under the CPA, as discussed in response to Question 7 below.
- **The Copyright Act 1957 ("Copyright Act"):** The Copyright Act does not explicitly address AI-generated works, and as such, the authorship and/or originality of such works is currently not addressed. An analysis of the position under the Copyright Act has been set out in response to Question 11 below.
- **SEBI's directions on AI Use:** SEBI has amended various securities related laws/regulations to impose sole responsibility upon any entity regulated by SEBI for its use of AI and machine learning tools ("AI/ML"), making the entity liable for the privacy and security of stakeholder data, the outputs generated by the AI systems, and compliance with all applicable

laws. These amendments build upon a foundational disclosure regime established by the SEBI in 2019, which mandated quarterly reporting by stockbrokers and depository participants using AI/ML applications/systems.

(v) Challenges in application of existing laws to the use of AI

Applying current laws to AI presents challenges due to AI's unique features, such as opacity, autonomy, and rapid evolution, which do not align congruently with traditional legal concepts.

- **Lack of Specificity and Gaps in Coverage:** Existing laws focus on data and human actions, not AI-specific issues like algorithmic bias, explainability, or autonomous decision-making, leading to interpretive ambiguities. For instance, determining accountability for biased AI outputs is difficult without clear rules on model training or auditing.
- **Challenges in Attribution and Enforcement:** AI's "black box" nature complicates proving causation or intent (and assign liability accordingly) as AI decisions may not stem from human negligence. Enforcement is further hindered by the absence of mechanisms for AI risk assessment or cross-sectoral oversight.

(vi) Voluntary standards

- The Telecommunication Engineering Centre, under the Department of Telecommunications, Government of India has introduced a voluntary standard for the fairness assessment and rating of AI systems to promote unbiased and responsible AI practices, particularly in telecom and information and communication technologies domain. This code outlines procedures for evaluating AI/ML systems to mitigate unintended biases.
- The Indian Council of Medical Research, the apex body in India for the promotion of biomedical research, released guidelines on ethical AI-use in 2023 ("ICMR Guidelines"). Developers and healthcare providers must ensure transparency, explainability, and robust risk mitigation mechanisms in clinical decisions involving AI.
- MeitY published the India AI Governance Guidelines, ("IAGG") in 2025 guiding industry

actors to: (a) comply with all applicable Indian laws including the IT Act, Digital Personal Data Protection Act 2023 ("DPDP Act") and CPA, governing AI development and deployment, and demonstrate such compliance when called upon by regulators; (b) adopt voluntary measures on privacy, security, fairness, inclusivity, non-discrimination, and transparency; (c) establish grievance redressal mechanisms to enable reporting of AI-related harms; (d) publish transparency reports evaluating risks of harm to individuals and society in the Indian context; and (e) explore techno-legal solutions including privacy-enhancing technologies, machine unlearning, algorithmic auditing, and automated bias detection.

(vii) Draft laws and legislative initiatives on AI in India

While currently in draft form, the SC Draft AI Regulations, once notified by the Chief Justice of India for the Supreme Court of India and by the Chief Justice of each respective High Court, will apply to the use, deployment, or integration of AI in any judicial, adjudicatory, or administrative function of the Supreme Court, High Courts, and all other courts, including tribunals and statutory commissions performing adjudicatory functions, in India. The SC Draft AI Regulations adopt a broad, technology-neutral definition of "Artificial Intelligence", while excluding general-purpose software or digital tools unless specifically embedded with, augmented by, or functionally dependent upon artificial intelligence. The SC Draft AI Regulations are grounded in fourteen general principles governing AI adoption, including human primacy and judicial independence, rule of law, fairness and non-discrimination, transparency, accountability, data protection, proportionality, and cyber security.

The SC Draft AI Regulations distinguish permissible from prohibited uses. With prior written approval, AI systems may be used for case management, transcription, translation, legal research, document summarisation, administrative functions, conversational assistants, accessibility services, document verification, anonymisation of judgments, and analytical tools.

Absolute prohibitions apply: no judicial outcome may be reached through algorithmic decision-making alone; no adjudication or sentencing may occur without mandatory human-in-the-loop; and no AI system may be used for risk scoring or to profile parties, witnesses, or representatives. Safeguards include mandatory impact assessments, controlled testing, an AI Register, periodic audits, an AI Incident Database, an Annual Transparency

Report, and DPDP Act and IT Act compliance.

In addition to the initiatives undertaken, it is critical to note that the Digital India Act ("DIA") has been slated to replace the IT Act and is expected to regulate high risk AI applications. However, news reports have suggested that timelines for the introduction of the bill are still evolving.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

Indian laws do not mandate requirements for AI explainability or audits, but require transparency and/or disclosure of use of AI for generation of content under the following laws:

(i) IT Act and 2021 Rules

Under the IT Act and the 2021 Rules, an intermediary that enables or facilitates the creation, modification, or sharing of SGI is subject to specific due diligence obligations. Such intermediaries are required to: (a) inform users that the generation, modification or sharing of unlawful SGI may attract penalty or punishment under applicable laws; (b) deploy reasonable and appropriate technical measures, including automated tools, to prevent users from generating or disseminating unlawful SGI; (c) periodically inform users of the consequences of non-compliance of the 2021 Rules; (d) report mandatorily reportable offences; and (e) prominently label non-prohibited SGI, embedded with permanent metadata and a unique identifier, without enabling removal of such labels. A significant social media intermediary, ie, a social media intermediary having at least 5 million registered users in India are required to: (a) require users to declare whether information is SGI; (b) verify such user declaration using technical measures; and (c) label confirmed SGI for public disclosure. If an intermediary fails to observe the 2021 Rules, then such intermediary may lose the safe harbour provided under the IT Act and will be liable under applicable laws in force.

(ii) CPA

While the CPA does not specifically regulate AI systems, AI-enabled products and services which are consumer-facing fall within the scope of the CPA.

The CPA define a 'misleading advertisement' to include advertisements which deliberately conceals important information, falsely describes a product or service, or conveys a representation that would constitute an 'unfair

trade practice'. Under the CPA, 'unfair trade practice' means any unfair method or deceptive practice, including false representations as to the standard, quality, or characteristics of goods or services.

Accordingly, where a business deploys an AI chatbot or virtual assistant, failure to disclose that a consumer is interacting with an AI system rather than a human representative could, depending on the facts, be characterised as concealment of material information or a deceptive practice, particularly where the AI influences purchasing decisions, provides advice, or collects sensitive information.

Further, the Central Consumer Protection Authority's Guidelines for Prevention and Regulation of Dark Patterns 2023 prohibit deceptive interface practices, including "disguised advertisements" that mask advertising as other content.

(iii) Sector-Specific Guidance on Explainability and Audits SEBI has introduced sector-specific regulatory-facing reporting requirements relating to the use of AI / ML systems by certain regulated entities. Since 2019, specified market participants have been required to periodically report information concerning their deployment of AI/ML applications and systems to SEBI. In addition, the SEBI has undertaken consultations regarding the responsible use of AI/ML technologies within the securities market. In particular, SEBI's 2025 consultation paper on responsible AI/ML usage ("SEBI AI/ML Paper") proposes governance, accountability and risk-management measures for regulated entities deploying AI systems. However, such proposals remain subject to the consultation process and should not presently be regarded as binding regulatory obligations.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

(i) 2021 Rules

As per the 2021 Rules, if an intermediary becomes aware, on its own accord or actual knowledge or a complaint, of any violation in relation to the creation or sharing of unlawful SGI in violation of the 2021 Rules, the intermediary is required to take expeditious and appropriate action including: (a) immediate disabling of access to / removal of unlawful SGI; (b) suspension / termination of the relevant user account; (c) identification of the user to a complainant; and/or (d) if an offence under Indian laws, reporting such violation to law enforcement authorities. Pursuant to the amendments in

2026 to the 2021 Rules, the timelines for removal of unlawful SGI are stricter (ie, 3 hours) in case the intermediary receives a court order or law enforcement authorities requiring removal of such unlawful SGI.

In addition, the 2021 Rules also require intermediaries to appoint a grievance officer who is required to acknowledge complaints within 24 hours, in case of request for removal of access to unlawful SGI, remove such access within the stipulated timelines, and mandatorily resolve complaints within 7 days. Therefore, while the 2021 Rules do not expressly require human oversight over the use of AI and allow for the deployment of automated detection tools, regulatory expectations of intermediary due diligence and response timelines implicitly require human oversight.

(ii) Financial Sector Developments

The RBI's FREE-AI Committee Report identifies "People First" as a core governance principle and emphasises human oversight, accountability and human empowerment in the deployment of AI systems. As per the FREE-AI Committee Report, entities that deploy AI should be responsible and remain fully accountable for the decisions and outcomes that arise from the use of these systems, regardless of their level of automation or autonomous functioning. Accountability should be clearly assigned, as it cannot be delegated to the model and underlying algorithm. The FREE-AI Committee Report served as an important source for the human-centric principles subsequently adopted in the IAGG.

SEBI's AI/ML Paper establishes a core governance framework for AI across capital markets. The guidelines explicitly place absolute legal and operational responsibility for AI-generated outcomes on regulated entities rather than the AI systems themselves, preventing market participants from avoiding liability by attributing lapses to automated tools. To mitigate risks across high-stakes operations like algorithmic trading and portfolio management, SEBI mandates robust testing frameworks, such as shadow testing with live traffic, alongside human-in-the-loop oversight to ensure all outcomes remain explainable, fair, and fully compliant with existing regulatory obligations.

Although these frameworks do not generally prescribe mandatory human-in-the-loop review for every AI-assisted activity, the allocation of legal and regulatory responsibility to regulated entities creates a strong expectation that appropriate human oversight mechanisms will be maintained over material AI-driven processes.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

India does not currently have a dedicated legislation specifically addressing algorithmic bias, discrimination, or fairness in AI systems. However, several Indian policy frameworks and sector-specific guidance documents provide relevant principles and requirements in this area. These frameworks span multiple sectors, including financial services, capital markets, judiciary, and healthcare, reflecting a growing recognition of the need to address fairness concerns in AI deployment.

(i) IAGG: The IAGG, published by MeitY, provides foundational guidance on fairness in AI. The IAGG stipulates that any person involved in developing or deploying AI systems in India should adopt voluntary measures with respect to fairness, inclusivity, and non-discrimination. While these measures are voluntary, they establish important normative standards for the industry.

(ii) FREE-AI Committee Report: One of the seven guiding principles provided in RBI's FREE-AI Committee Report provides that AI systems should be designed and tested to ensure that outcomes are unbiased and do not discriminate against individuals or groups. Further, the FREE-AI Committee Report mentions that while AI should uphold fairness, it should not accentuate exclusion and inequity and that AI should be leveraged to address financial inclusion and access to financial services for all.

(iii) SEBI AI/ML Paper: SEBI's AI/ML Paper similarly addresses fairness concerns in capital markets. The Paper provides that AI/ML models should be fair and should not discriminate or favour one group of clients or customers over another. Market participants are required to implement appropriate processes and controls to identify and remove biases from data sets.

(iv) CERT-In Blueprint: From a cybersecurity perspective, the CERT-In has issued a Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure on 25 May 2026 ("CERT-In Blueprint"). This CERT-In Blueprint supports organisations in strengthening resilience against AI-enabled cyber threats and lays down key areas for secure AI governance, operational resilience, risk management, and protection of AI-enabled organisational environments. Notably, the CERT-In Blueprint identifies 'AI Security Assessment and Assurance' as a critical focus area, which includes assessing behavioural integrity, bias, fairness, robustness, explainability, and

unsafe outputs.

(v) SC Draft AI Regulations: From a judicial standpoint, the SC Draft AI Regulations require that AI systems used in court processes be designed, trained and deployed in a manner that promotes fairness and avoids discrimination. Additionally, such AI systems must be trained on data that is accurate, representative, lawfully obtained and, to the extent feasible, free from discriminatory bias.

(vi) ICMR Guidelines: From healthcare perspective, the ICMR Guidelines recognise data bias as "the greatest threat to data driven technology like AI for health." Accordingly, the guidelines mandate that prior to deployment of AI technologies, the possibilities of biases should be considered, identified and thoroughly scrutinized. Training data should be free from sampling bias, and users of AI technology should be educated about the various forms of bias that may emerge during clinical use. The ICMR Guidelines further emphasizes that AI should never serve as a tool for exclusion, and special attention must be given to under-represented and vulnerable groups, including children, ethnic minorities, and persons with disabilities. AI developers are expected to promote the active inclusion of women and minority groups.

In summary, while India lacks a unified legislative framework specifically targeting algorithmic bias and discrimination in AI systems, a patchwork of sector-specific guidelines and policy documents has emerged to address these concerns. The consistent themes across these frameworks include the need for unbiased training data, proactive identification and mitigation of biases, fairness in AI-driven decision-making, and the protection of vulnerable and under-represented groups.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

There is no specific legislation governing AI in India. Potential liability for development and deployment of defective AI systems will likely be assessed basis the pre-existing liability frameworks under Indian law, which are grounded in product liability, torts, intermediary liability, statutory safety norms, data protection, and criminal law.

(i) CPA

The manufacture and supply of under-trained or defective AI systems or supply of AI systems without adequate instructions of correct usage could lead to claims of deficiency of service. Further, if an AI developer/deployer acts as a service provider for a particular product, it may be subject to a product liability action, in case of, among others, a failure to: (a) provide information that ends up causing harm, (b) provide adequate instructions/warnings, or (c) conform to express warranties/contract terms governing such service

(ii) Indian Contract Act 1872 ("ICA")

If an AI system breaches contractually agreed performance standards or the express representations and warranties made by the developer/supplier in relation to the AI system, liability under the terms of the contract and ICA may follow.

(iii) Law of torts

The developer of a defective AI system could incur tortious liability if the developer has acted negligently and committed breach of a duty of care to ensure that the AI system does not have any inherent manufacturing or design defects. Importantly, in a recent ruling, the Calcutta High Court has held in *IndiaMart Inter Mesh Limited v OpenAI Inc.*, that good faith business decisions made by AI platforms and/or the parameters and preferences of AI models cannot give rise to a cause of action against the developer, even if these decisions cause economic harm – unless the party affected can demonstrate that vested rights (such as intellectual property or contractual rights) are being violated.

(iv) IT Act

In the event an AI tool is used for an unlawful purpose or its usage results in a cyber offense, liability under the IT Act could be triggered, including for identity theft and personation, violation of privacy, unauthorized access to computer resources, installation of a computer contaminant and failure to protect data.

(v) BNS

The BNS provides for the prosecution of harms caused by a defective AI system through its "technology-neutral" provisions. For instance, if developers/deployers of a defective AI system deliberately manufacture and supply the same knowing that harm may be caused, the developer/deployer may be liable for cheating/mischief. In cases of gross negligence leading to a defective AI system being manufactured and supplied, any consequent physical injury/death, and/or any prohibited act being committed as a result of the AI system's

malfunction could trigger appropriate offences under the BNS (such as the offence of causing hurt, grievous hurt, death by negligence, etc.) depending on the facts of the case. Illustratively, if AI is used to generate and spread misinformation that incites public fear or violence, the same would be actionable under the BNS.

(vi) DPDP Act

The DPDP Act is India's first comprehensive legislation on privacy and data protection and is currently being implemented in a phased manner. Once fully enforced (with effect from 13 May 2027), it will repeal the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("SPDI Rules"), which is the current law governing collection and processing of SPDI.

The DPDP Act was enacted in August 2023. The DPDP Act defines data processing to include any wholly or partly automated set of operations. Accordingly, use and development of AI systems requiring processing of personal data, must be in compliance with the provisions of the DPDP Act. Any entity acting as a data fiduciary (ie, any person or entity who determines the purpose and means of personal data processing) may be held liable for offences under the DPDP Act including for failure to take reasonable security safeguards to prevent personal data breach or adhering to the legal grounds of processing personal data as set out thereunder.

8. What cybersecurity obligations apply to AI systems?

There are no specific AI cybersecurity laws in India. However, the CERT-In AI Advisory is recommendatory in nature and, inter alia, requires organizations to review and maintain incident response and cyber crisis management plans; conducting regular phishing and social engineering awareness training for all employees; adopt AI enabled defensive security tools; automate continuous software updates across IT and production systems; enforce strong password rules and account lookout policies; maintain an up-to-date contact list including of sectoral regulators, CERT-In, legal counsels, security service providers; and ensure compliance with the directions issued by the CERT-In, etc.

Moreover, the key areas covered under the CERT-In Blueprint includes: governance and accountability mechanisms; exposure reduction strategies; technical defensive controls; AI-aware security operations; vulnerability and exposure management; supply-chain security; incident response and cyber resilience;

continuous security validation; and workforce preparedness and operational readiness. While compliance with the CERT-In Blueprint is not mandatory, organisations are encouraged to implement the recommendations contained therein in a risk-informed manner, taking into account operational criticality, technology dependencies, and prevailing threat conditions. Further, the CERT-In Blueprint provides that given the rapidly evolving nature of AI-assisted cyber threats, it is advisable for organizations to continuously reassess their exposure, validate security controls, strengthen resilience capabilities, and enhance operational preparedness through ongoing audits, monitoring, testing, and coordinated cybersecurity governance.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

There is no express guidance by either Indian courts or the legislature on whether use of AI is insurable in India. The ICA provides that an agreement whose object is contrary to public policy is void. However, there is limited judicial guidance concerning whether there are public policy restrictions under ICA on what subject matter can be insured. Having said that, as part of emerging developments in the technology space, cyber insurance policies covering losses associated with cyber breach incidents are becoming increasingly common in India.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

No, as on date an AI cannot be identified as an inventor or a co-inventor in a patent application. While the Patents Act 1970 ("Patents Act") does not define the term "inventor", previously, the AI system 'DABUS' (Device for the Autonomous Bootstrapping of Unified Sentience), developed by Dr. Stephen Thaler, raised questions of AI as an inventor. Dr. Thaler filed an Indian patent application naming the AI, DABUS, as the inventor. The Indian Patent Office has in its first examination report objected to AI being named as an inventor, since it is not a person. Recently, the Indian Patent Office rejected application 202017019068, where Dr. Thaler had named the AI system DABUS as inventor. On the question of naming DABUS as the "true and first inventor", the Indian Patent Office held that the existing patent law framework

permits only natural persons to be recognised as inventors.

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

The Copyright Act is based on the principle of human authorship and creativity, and AI cannot be recognized as author under the Copyright Act. Additionally, the application for copyright registration requires disclosure of the author's name, nationality and address.

In *Tech Plus Media Private Ltd. v. Jyoti Janda*, (2014) 60 PTC 121, it was affirmed that a juristic person is incapable of being the author of any literary work in which copyright may exist, though it may own copyright. Further, in 2020, Mr Ankit Sahni submitted two copyright applications for AI-generated artworks. The Indian Copyright Office ("ICO") rejected his first application, which listed 'RAGHAV' (Robust Artificially Intelligent Graphics and Art Visualizer) as the sole author. His second application – naming both himself and the AI as co-authors, was initially granted registration in November 2020. Later, however, the ICO issued a contentious withdrawal notice for the registration. Mr. Sahni had responded to the notice arguing that the ICO did not have the authority to review its own decision. As on date, no action appears to have been taken on the copyright registration.

Recently, the Delhi High Court has mandated the ICO to make a decision within eight weeks on a plea submitted by Dr. Stephen Thaler on copyright protection on AI-generated artwork. Stephen Thaler, who created an AI system capable of creating artwork (named as DABUS) without human input. He registered a copy of a work of art produced by this DABUS under Indian copyright law. The ICO, however, objected on the basis that Indian copyright law only recognises 'human authors'. This prompted the case to be taken to the Delhi High Court. The key question in this case is whether an art, produced by AI and where the human element is not involved, can be copyrighted in accordance with the Indian legislation. While the Court never resolved the question, it left the ICO to review the query of Dr. Thaler and issue a justifiable verdict within eight weeks of the order. The Court acknowledged that it is a complicated and dynamic question, particularly in the wake of the fast development of AI technologies.

Further, back in May 2025, the Government of India constituted an eight member expert panel to evaluate whether the Copyright Act adequately addresses the challenges presented by generative AI. The committee is yet to publish its findings.

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

At present, India does not have any law that expressly regulates the use of AI in the workplace. As such, when deploying AI systems in the workplace, key considerations would revolve around compliance with existing employment laws that may indirectly apply to such decisions; such as the below:

(i) Compliance with key anti-discrimination provisions under employment laws

If AI-driven/AI-assisted decisions result in adverse changes in conditions of employment or termination, or exhibit bias in recruitment, employers must ensure that they remain compliant with anti-discrimination provisions, such as the Transgender Persons (Protection of Rights) Act 2019, the Rights of Persons with Disabilities Act 2016, Code on Wages 2019, Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989 and other key employment laws.

(ii) Compliance with key provisions regulating termination under employment laws

In the context of workforce reductions potentially facilitated by AI systems, employers must adhere to procedural safeguards under the Industrial Relations Code 2020. This statute, inter alia, impose restrictions on retrenchment and termination of employees, and typically require the service of due notices on employees, and payment of retrenchment compensation in certain cases.

(iii) Compliance with data protection laws regarding AI-enabled employee monitoring

In the event that an employer collects sensitive personal data or information (such as biometric information, medical records, etc) ("SPDI"), such data must be processed according to the SPDI Rules. Prior to collecting an employee's SPDI, employers must among others secure an employee's written consent and provide employees with an accessible privacy policy which

specifies the information collected, the specific purposes for usage, and its disclosure practices.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

As the DPDP Act will be fully in force from 13 May 2027, some of the key privacy issues that may emerge out of development, including training and use of AI include:

i. Legal basis for processing: Limited availability of legal bases for processing personal data may not support the full range of AI development and deployment

ii. Consent: AI systems often rely on passively collected data, which may make it difficult to meet the consent requirements of free, specific, informed, unconditional, unambiguous consent with a clear affirmative action from individuals.

iii. Purpose limitation: AI use may conflict with the purpose limitation requirement, as data is often repurposed for secondary or evolving use cases beyond its original purposes.

iv. Data minimization: AI systems often need large and diverse datasets for research and analysis which may conflict with the principle of collecting data strictly necessary for a specified purpose.

v. Transparency: AI systems may produce unexplainable and unanticipated outcomes and it may be hard to provide meaningful privacy notices.

vi. Retention limitation: AI systems may need to retain data for extended periods for AI training, traceability, audit and oversight purposes.

vii. Data principal rights: AI may make it difficult to facilitate the exercise of data subject rights, including access, correction, deletion, and the right to obtain meaningful information about the logic involved in processing.

Further, in the context of AI, both AI developers and AI deployers are likely to be classified as data fiduciaries under the upcoming DPDP Act depending upon the role that they play in determining the purpose and means of processing personal data. This will create complexities on strategies for compliance with the DPDP Act based on

the use case of the AI solution. Moreover, data fiduciaries are also responsible for the actions of data processors, who process personal data on their behalf. The development of AI systems may lead to potential friction with core data protection principles and the legal obligations set out under the DPDP Act.

India currently does not have a dedicated privacy regulator or authority. MeitY is responsible for formulating and implementing national policies and programs aimed at the electronics and IT industry, and issues advisories and guidance under the IT Act. The Data Protection Board of India, the enforcement body under the DPDP Act, is yet to be constituted.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

Data scraping is increasingly raising complex legal considerations across IP, privacy, and competition laws in India as summarized below:

(i) Privacy: The IT Act provides for penalty and compensation for unauthorized downloading, copying or extracting any data, computer database or information from a computer, computer system/network. Given the broad definition of data and information under the IT Act, data scraping in contravention of the above may result in claims. The DPDP Act excludes from its scope, personal data that is "made publicly available" either by the data principals themselves, or by any person under a legal obligation. The DPDP Act also provides an exemption for processing personal data for research purposes, provided such processing is not used to make decisions specific to data principals and complies with prescribed safeguards. However, the practical application of these exemptions remains to be seen. A challenge also exists from a contractual perspective as, typically, the terms of use/terms and conditions of websites and applications have restrictions prohibiting data scraping or such data's commercial use.

(ii) Intellectual Property: Generally speaking, if data scraping violates the copyright of the owner, the same could result in copyright infringement (unless the purpose of the activity falls under the defences enumerated under the Copyright Act). The Delhi High Court is expected to rule on the legal permissibility of data scraping for the purposes of training large language models in a copyright infringement suit instituted by ANI Media Private Limited

against OpenAI. The arguments have been heard and the Court has reserved its decision.

(iii) Competition: Data scraping is not directly regulated under the Competition Act 2002. The draft of the erstwhile proposed Digital Competition Bill ("DCB") prohibited certain enterprises to: (a) intermix or cross use personal data; and (b) permit use of such data by any third party, without the consent of the concerned end user/business user. However, reportedly, the Government of India has decided to withdraw the DCB.

15. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

The terms of use for a website are enforceable so far as they meet the conditions necessary for the formation of a contract. Courts have previously affirmed the validity of contracts made through electronic means, which are specifically provided for under the IT Act. Having said that, we anticipate that it is likely to be more challenging to prove the existence of contract in cases involving browsewrap agreements, or where the terms of use have not been specifically accepted by a user.

Whether terms of use can prohibit data mining is a complex question and many factors may influence it, including: (i) the nature of the data which is hosted on the website (such as personal data, intellectual property, etc.), (ii) the purpose for which the data is intended to be scraped (such as private use or training AI or for publication), (iii) the form in which the terms of use are published for acceptance (such as click wrap or browse wrap agreements or a pop up notice), and (iv) whether the website uses technical measures such as CAPTCHAs or bot detection.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

India does not have a dedicated statutory regulator yet, that is exclusively responsible for supervising the development and use of AI. However, supervision regarding the development and use of AI is emerging due to the ongoing efforts of MeitY, various sectoral regulators and other policy and legal interventions by the Government, as highlighted in response to Question 3 above.

In this regard, as set out briefly above in Question 4, the

Government of India has recently amended the 2021 Rules to add certain due diligence obligations for online intermediaries concerning the use/publication/hosting/uploading of SGI, which can include AI-generated content, on their platforms.

Since India does not have a dedicated statutory regulator for AI, various different regulators have authority to enforcement AI-related laws / policies / regulations within their own domains. However, the breadth of such powers is contingent on the facts of each case, and the regulatory body / government entity involved.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

Indian businesses have begun embracing the use of AI, and certain sectors have already incorporated large-scale deployment of AI in their everyday functions. A 2026 report by Deloitte ("Deloitte Report"), reported that 34% of companies are starting to use AI to deeply transform businesses, 30 percent are redesigning key processes around AI and the remaining 37% are only using AI at a surface level with little or no change to underlying business processes. In another report on AI by KPMG ("KPMG Report"), it was reported that India ranks third globally in AI competitiveness.

The sectors which primarily stand out for rapid and substantive adoption of AI are industrial and automotive, consumer goods and retail, banking, financial services and insurance, and healthcare; which cumulatively contribute around 60% of AI's total value in India. As per the KPMG Report, ~38% of the financial services industry, ~67% of the healthcare industry, ~33% of the manufacturing sector and ~67% of the consumer and retail sector have deployed AI at scale, relying on AI for automation, personalisation, inclusion, productivity enhancements and increased efficiency.

As per the Deloitte Report, firms have begun applying physical AI in logistics to automate package sorting and routing, granting warehouse robots more autonomy to decide where and how to store items to maximize floorspace. The aviation industry is using AI agents to help customers complete common transactions, such as rebooking a flight or rerouting bags, freeing up time for human agents to address more complex matters.

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are

AI-driven legal tools widely adopted, and what are the main regulatory concerns?

Yes, AI is being used in the legal sector both by lawyers and in-house counsels for various use cases. Several top law firms in India have announced partnerships with global AI platforms and some are also developing in-house AI solutions to enhance client delivery services. In this regard, some of the most popular use cases of AI include:

- (i) Contract drafting and review: Drafting of contracts, proofreading and ensuring consistency across complex legal contracts.
- (ii) Due diligence: Automating the identification and extraction of key information from large volumes of documents as part of due diligence for corporate transactions and large-scale compliance exercises.
- (iii) Legal Research: Assisting in primary and secondary research (for example, by preparing AI-generated summaries and relevant precedent mapping for case laws).
- (iv) Document Automation: Streamlining the generation of standardized legal documents, improving efficiency, consistency, and turnaround time, while enabling lawyers to focus on complex tasks.
- (v) eDiscovery and Litigation Services: Conducting analysis of documents and evidence using advanced tools which support complex litigation, regulatory inquiries, and investigations, thereby enabling efficient case management.
- (vi) AI chatbots: Deployment of virtual AI assistants which enables users to securely use queries and prompts to generate responses which aid in drafting emails and summarizing documents or precedents.

Further, the Indian judiciary has implemented several AI-driven initiatives aimed at enhancing efficiency, transparency, and accessibility. These include AI-based transcription tools being piloted in Constitutional Benches of the Supreme Court, and with testing prototype AI tools for curing defects, data, and meta data extraction to be integrated with its electronic filing module. That said, the Delhi High Court in *Christian Louboutin SAS v The Shoe Boutique Shutiq*, (2023) SCC OnLine Del 5295 observed that "AI cannot substitute either the human intelligence or the humane element in the adjudicatory process".

One of the regulatory concerns that has emerged in the

Indian judiciary, is the rise of hallucinated cases generated by AI, being cited in petitions. The Supreme Court in *Gummadi Usha Rani v. Sure Mallikarjuna Rao*, SLP(C) No. 7575/2026, observed that "At the outset, we must declare that a decision based on such non-existent and fake alleged judgments is not an error in the decision making. It would be a misconduct and legal consequence shall follow". The Bombay High Court in *Deepak Shivkumar Bahry vs Heart & Soul Entertainment Ltd.* (Writ Petition 8390 of 2009), ordered the respondent to pay costs amounting to INR 50,000, for submitting a 'non-existing' judgment generated through AI which the court and its clerks could not find and thus deprecated such practice of 'dumping' non-existing and irrelevant materials on the court.

To combat issues with use of AI by lawyers, such as submission of non-existent judgements and over reliance on AI, courts in India have issued the following guidelines:

- The SC Draft AI Regulations aims to establish a framework for responsible AI adoption in the judiciary and reinstates the importance of human primacy in performing judicial functions. The SC Draft AI Regulations mandate disclosure of AI-generated content in courts and recommend the setting up of AI committees in the Supreme Court and every High Court.
- Kerala High Court's "Policy Regarding Use of Artificial Intelligence Tools in District Judiciary" prohibits sole reliance on AI tools for decision-making or legal reasoning. This policy mandates that AI be used solely as an assistive tool under strict human supervision, ensuring adherence to core judicial values such as transparency, fairness, confidentiality, and accountability.
- The Gujarat High Court's "Policy On The Use Of Artificial Intelligence" prohibits use of AI for any form of decision-making, judicial reasoning, order drafting, bail sentencing considerations, or any substantive adjudicatory process. It restricts use of AI for generating fabricated cases, and also prohibits entering names, addresses, or identifying information of parties, details of pending proceedings or unreported orders, privileged communications or confidential legal strategies, and sensitive personal data into AI.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for

lawyers in your jurisdiction?

Some of the key challenges may be summarized as follows:

- (i) Determination of liability: While existing laws address liability for harm caused by AI, specific mechanisms may be required for ascertaining responsibility for AI decisions (e.g., developer, deployer or user).
- (ii) Accuracy of output: While AI helps streamline legal work, human review of AI output is paramount as AI may also not understand legal nuances and apply incorrect legal standards.
- (iii) Unclear permissibility of use of AI in legal profession: There is a need for a code of best practices for AI use by legal professionals, inter alia, to ensure client confidentiality and data security, mandatory disclosure and informed consent for AI-assisted work.
- (iv) Confidentiality: Since legal professionals handle highly sensitive client data, confidentiality remains a key concern. This can be addressed by adopting encrypted, on-premises AI solutions with strict data-erasure protocols and implement mandatory periodic audits of data handling practices.
- (v) Bias and discrimination: AI systems trained on uneven or outdated datasets can perpetuate societal biases, leading to discriminatory legal advice. As such, legal AI tools in India should be validated against representative Indian data pools and undergo ongoing performance monitoring and bias checks.

Some of the key opportunities are:

- (i) Enhanced efficiency and practice transformation: AI can streamline legal work and practice management by automating routine tasks, and enabling rapid clause selection, risk-flagging and translation services.
- (ii) Competitive market positioning: Early AI adopters gain advantages through faster service delivery and improved accuracy. The growing legal AI market creates opportunities for both established firms and smaller practices.
- (iii) Democratized access to justice: AI-powered legal platforms provide instant guidance to underserved populations, particularly in rural areas lacking adequate legal representation.
- (iv) AI-driven due diligence in corporate transactions: In mergers, acquisitions and fundraising deals, AI tools can rapidly sift through vast volumes of contracts, financial

records and regulatory filings. Natural language processing identifies key clauses, flags non-standard terms and highlights potential compliance issues, dramatically accelerating due diligence.

(v) Continuous compliance monitoring and regulatory intelligence: AI-powered compliance engines can monitor legal and regulatory updates in real time to keep pace with the dynamic regulatory developments. Automated alerts can inform lawyers and corporate clients of relevant changes, such as issuance of new circulars, advisories and regulations to enable prompt assessment of impact.

20. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

It is likely that India will see significant legal developments in the field of AI over the next 12 months. The implementation of the DPDP Act would bring in strict

consent, purpose limitation, and data minimization requirements, all of which may directly impact developers and deployers alike. The proposed DIA may include provisions prohibiting the development and deployment of harmful emerging technologies and protecting users from biased or discriminatory outcomes resulting from technology driven decision making.

In terms of ongoing efforts, sectoral regulators such as Telecom Regulatory Authority of India, SEBI, and RBI are likely to intensify efforts to regulate AI through release of more recommendation papers, which may mature into more concrete frameworks for consideration. Further, the adoption of AI is also expanding across various use cases. For instance, the Central Board of Direct Taxes is exploring the use of data analytics and AI to enhance tax compliance and detect tax evasion. Courts are also likely to increasingly adjudicate on AI-related cases, particularly those involving violations of personality rights, deepfakes used for defamation and impersonation, consumer protection claims arising from reliance on AI-generated outputs, infringement of IP rights in AI-generated works, and disputes with AI providers due to malfunctioning AI tools.

Contributors

Supratim Chakraborty
Partner

supratim.chakraborty@khaitanco.com



Sumantra Bose
Partner

sumantra.bose@khaitanco.com



Tanu Banerjee
Partner

tanu.banerjee@khaitanco.com



Ishan Johri
Partner

ishan.johri@khaitanco.com



Shailendra Bhandare
Partner

shailendra.bhandare@khaitanco.com



Anushka Sharda
Partner

anushka.sharda@khaitanco.com



Madhav Khosla
Partner

madhav.khosla@khaitanco.com



Sourav Dan
Counsel

sourav.dan@khaitanco.com

