

# Legal 500

## Country Comparative Guides 2025

### India

### Artificial Intelligence

### Contributor

**Khaitan & Co LLP**



#### **Supratim Chakraborty**

Partner | [supratim.chakraborty@khaitanco.com](mailto:supratim.chakraborty@khaitanco.com)

#### **Shailendra Bhandare**

Partner | [shailendra.bhandare@khaitanco.com](mailto:shailendra.bhandare@khaitanco.com)

#### **Tanu Banerjee**

Partner | [tanu.banerjee@khaitanco.com](mailto:tanu.banerjee@khaitanco.com)

#### **Anushka Sharda**

Partner | [anushka.sharda@khaitanco.com](mailto:anushka.sharda@khaitanco.com)

#### **Ishan Johri**

Partner | [ishan.johri@khaitanco.com](mailto:ishan.johri@khaitanco.com)

#### **Sumantra Bose**

Counsel | [sumantra.bose@khaitanco.com](mailto:sumantra.bose@khaitanco.com)

#### **Sourav Dan**

Counsel | [sourav.dan@khaitanco.com](mailto:sourav.dan@khaitanco.com)

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in India.

For a full list of jurisdictional Q&As visit [legal500.com/guides](https://legal500.com/guides)

# India: Artificial Intelligence

## 1. What are your country's legal definitions of "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..."*

While various sectoral regulators, such as India's financial regulator ie, the Reserve Bank of India ("RBI") and India's telecommunications regulator ie, the Telecom Regulatory Authority of India ("TRAI"), have also set out their own definitions of AI, 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.

## 2. Has your country developed a national strategy for artificial intelligence? If so, has there been any progress 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 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.

(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, 4 startups have been selected which focus on open-source foundational AI models for public service, healthcare, education and multi-lingual capabilities.

(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 1300 datasets, 210 AI models, and 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 IndiaAI portal 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 are being 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:** This mission is explicitly designed to promote research by funding startups and research teams and constitutes 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 was announced in January 2025, to address AI risks and safety challenges. The IndiaAI Safety Institute will work with all relevant stakeholders, including academia, startups, industry and government ministries/departments, towards ensuring safety, security and trust in AI. It will also help in promoting indigenous research and development, based on Indian datasets and contextualized to India's social, economic, cultural, and linguistic diversity.

**3. Has your country implemented rules or guidelines (including voluntary standards and ethical principles) on artificial intelligence? If so, please provide a brief overview of said rules or guidelines. If no rules on artificial intelligence are in force in your jurisdiction, please (i) provide a**

**short overview of the existing laws that potentially could be applied to artificial intelligence and the use of artificial intelligence, (ii) briefly outline the main difficulties in interpreting such existing laws to suit the peculiarities of artificial intelligence, and (iii) summarize any draft laws, or legislative initiatives, on artificial intelligence.**

India has not yet enacted a comprehensive legislation for the regulation of AI, however, the Government of India has issued advisories to guide AI development and use. These are primarily recommendatory in nature and aim to promote responsible AI while addressing risks such as bias, privacy concerns, deep fakes and misinformation.

**(i) Advisories by MeitY on use of AI by intermediaries/platforms in India**

- **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 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 ("IT 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 and platforms. 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 IT Rules and has been elaborated in response to Question 15 below.

**(ii) Key laws regulating the use of AI**

- **IT Act and IT 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 IT 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.

- *Bharatiya Nyaya Sanhita 2023 ("BNS")*: The Government of India has asserted that provisions of the BNS are "technology-neutral", and they 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, etc. A few instances of the AI related criminal liability under the BNS are summarised in response to Question 4 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 a product contains a 'defect' (as defined under the CPA) that causes 'harm', the aggrieved consumer may seek a remedy under the CPA, as discussed in response to Question 4 below.
- *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 10 below.
- *SEBI's directions on AI Use*: India's securities market regulator, the Securities and Exchange Board of India ("SEBI") amended various securities related laws/regulations to impose sole responsibility upon any entity regulated by SEBI for its use of AI and ML tools. These include 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 on SEBI's 2019 disclosure regime, which required quarterly reporting by brokers and depository participants using AI/ML applications/systems.

### (iii) 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.

### (iv) 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. Developers and healthcare providers must ensure transparency, explainability, and robust risk mitigation mechanisms in clinical decisions involving AI.

### (v) Draft laws and legislative initiatives on AI in India

In addition to the initiatives undertaken with respect to the NITI Ayog's National Strategy for AI, 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, recent news reports suggest that the timeline for the introduction of the bill remains uncertain.

Further, MeitY is reportedly working on a voluntary code of conduct and ethics for AI. These guidelines are expected to cover training, deployment, and commercial distribution of AI and prevent its misuse.

## **4. Which rules apply to defective artificial intelligence systems, i.e. artificial intelligence**

### systems that do not provide the safety that the public at large is entitled to expect?

As discussed above, 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

As discussed in response to Question 3 above, 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.

#### (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

As covered in response to Question 3 above, 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) Digital Personal Data Protection Act 2023 ("DPDP Act")

The DPDP Act is India's first comprehensive legislation on privacy and data protection, and once notified, 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 but is not yet in force. 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 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.

### 5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems. Have there been any court decisions or legislative developments clarifying liability frameworks applied to artificial intelligence?

While there is no legislative framework specifically governing AI in India, persons affected by the actions of an AI system have recourse to general remedies under civil and criminal laws, briefly covered in response to Question 4 above. Notably, Indian courts have been proactive in providing injunctive and preventive relief in



disputes concerning the use of AI tools to generate deepfakes. For instance, courts have previously protected personality rights from misuse of deepfake technology, and issued takedown orders for deepfake content circulated online.

## 6. Who is responsible for any harm caused by an AI system? And how is the liability allocated between the developer, the deployer, the user and the victim?

Since AI systems are not conferred with legal personality, liability for actions undertaken through AI systems may generally be attributed to persons in control of the AI system, such as its end-users, developers, deployers, or owners, depending on the facts of each case.

Concerning civil liability, the developer, deployer or user (*depending on the facts*) of an AI system can be held liable for negligent or unlawful acts committed by them. Risk attribution matrices may also be set out in contracts. Where it can be shown that a defect in the AI system has caused the injury or harm, strict liability may fall on the developer of the AI system under the CPA or law of torts. However, this liability burden may shift if contributory negligence is established on the part of the deployer/user.

Concerning criminal liability, criminal law requires both the commission of *actus reus* (ie, *guilty act/offence*) and the presence of *mens rea* (i.e., *guilty mind/intention*). AI systems cannot be said to possess the necessary intention to commit a crime, and hence, persons in control of an AI system or for whose benefit it operates, would potentially be liable for criminal acts conducted by such an AI system.

While attribution remains a fact-specific enquiry, the Delhi High Court in *Google LLC v. DRS Logistics (P) Ltd.*, (2023) 4 HCC (Del) 515, has previously held that the deployer of an algorithmic decision-making system to be liable for decisions made autonomously through such a system.

## 7. What burden of proof will have to be satisfied for the victim of the damage to obtain compensation?

The precise standard of proof for damages is contingent upon the form of action preferred by the injured party. That said, the following may be relevant factors to determine the standard of proof in cases involving AI systems:

- i. Existence/breach of duty: An affected person must first establish that: (a) a legal duty existed on the part of the deployer/developer/end user of a given AI system, and (b) the actions committed by the AI system, acting under the control of the person on whom the duty existed, has breached the said obligation.
- ii. Causation: Causation would need to be established in two separate phases. First, a causal link between the person supposedly in control of an AI system, and actions taken by it, and second, the harm caused to an affected person must result from the AI system's actions.
- iii. Proximity of harm: The harm caused must be proximate to the actions undertaken by the AI system, since damages in Indian law are generally compensatory. Under contract law, for instance, compensation for the loss caused due to a contractual breach can be awarded only if: (a) such damage was ordinarily foreseeable by the parties, or (b) the parties had special knowledge that such harm would arise from the breach.
- iv. Special liability regimes in certain cases: Special liability regimes may apply in certain cases. For instance, damages under the CPA may extend to granting punitive damages for mala fide conduct or gross negligence.

## 8. Is the use of artificial intelligence insured and/or insurable in your jurisdiction?

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.

## 9. Can artificial intelligence be named an inventor in a patent application filed in your jurisdiction?

The Patents Act 1970 ("**Patents Act**") does not define the term "inventor". However, it is implied in the Patents Act that an inventor must be a natural person and the courts have affirmed this understanding.

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 Controller General of Patents, Designs and Trade Marks published New Guidelines for Examination of Computer Related Inventions, 2025, where AI generated or created inventions are excluded from patentability.

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

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. 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.

Notably, 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.

## 11. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations 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, 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, *inter alia*, the Industrial Disputes Act 1947 ("IDA"), and state specific Shops and Establishments Acts. These statutes, *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.

The Government of India has also enacted the Industrial Relations Code 2020 ("IRC") (ie, one of the four major labour codes proposed by the Government of India to consolidate and amend the laws relating to trade unions, conditions of employment in industrial establishments/undertakings, investigation and settlement of industrial disputes). While awaiting enforcement, the provisions relating to termination and retrenchment of workers under the IRC are similar to the IDA.

### (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 other compliance requirements, obtain 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.

## 12. What privacy issues arise from the development (including training) and use of artificial intelligence?

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 activities, particularly where sensitive data is involved.
- 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.

## 13. How is data scraping regulated in your jurisdiction from an IP, privacy and competition point of view? Are there any recent precedents

### addressing the legality of data scraping for AI training?

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.

#### (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.



#### 14. 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.

#### 15. Have the privacy authorities of your jurisdiction issued guidelines on artificial intelligence?

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 issue advisories and guidance under the IT Act. The Data Protection Board of India ("DPB"), the enforcement body under the DPDP Act, is yet to be constituted.

In March 2024, MeitY issued the AI use advisory addressing the use of AI technologies by intermediaries and platforms. This AI use advisory, *inter alia*, requires adherence to the following compliance measure by intermediaries and platforms:

- i. Ensuring that use of AI on or through its computer resource does not permit its users to host, display, etc. any unlawful content under the IT Rules or violate the IT Act and other applicable laws;
- ii. Use of AI should not permit any bias or discrimination or threaten the integrity of the electoral process; and
- iii. Under-tested/unreliable AI foundational models or further developments on such models should be made available to users in India only after appropriately

disclosing and labelling the possible inherent fallibility or unreliability.

Sectoral regulators, such as TRAI and SEBI, are actively formulating recommendation papers and proposing guidelines to regulate the use of AI in their respective sectors. For instance, as discussed in response to Question 1 above, in July 2023, TRAI in its recommendation paper released in 2023 highlighted the need to: (i) adopt a sector neutral regulatory framework; and (ii) establish an independent authority for responsible AI development. Further, SEBI in its consultation paper released in 2025, outlined certain best practices for AI/ML implementation, such as: (i) skilled human oversight; (ii) requisite disclosures to clients; and (iii) processes and controls to remove biases, etc. Moreover, to encourage the responsible and ethical adoption of AI in the financial sector, the FREE-AI Committee was constituted by the RBI, and the RBI released its report in August 2025. In the paper, the RBI recommended several measures to foster innovation such as (i) the establishment of shared infrastructure to democratise access to data and compute and the creation of an AI innovation sandbox; (ii) the development of indigenous financial sector-specific AI models; and (iii) the formulation of an AI policy to provide necessary regulatory guidance. Further, to mitigate AI risks, the RBI recommended measures such as (i) the formulation of a board-approved AI policy by regulated entities; (ii) the expansion of product approval processes, consumer protection frameworks and audits to include AI related aspects; and (iii) the augmentation of cybersecurity practices and incident reporting frameworks.

#### 16. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

While India does not have a dedicated privacy authority, pending enforcement of the DPDP Act, the data protection regime under the SPDI Rules remains applicable. A violation of Section 43A of the IT Act (under which the SPDI Rules have been framed), where the claim value of below INR 5 crores (approximately USD 5.7 million) may be brought before an Adjudicating Officer ("AO") under the IT Act. An appeal against the AO's order lies before the Telecom Disputes Settlement and Appellate Tribunal (an independent body established to adjudicate disputes and appeals in the telecommunications and cyber space). However, if the compensation claimed exceeds INR 5 crores, jurisdiction rests with a civil court.

This multi-tiered framework will remain in force until the formal constitution and operationalisation of the DPB under the DPDP Act. The DPB is expected to serve as the central authority for enforcement of the new data protection regime, including matters arising out of the use of AI in processing personal data.

### 17. Have your national courts already managed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

Yes, Indian courts have begun engaging with legal issues arising from the use of AI, particularly in the areas of copyright, personality rights, and deepfake regulation. One prominent example is a pending copyright suit filed by ANI Media against OpenAI before the Delhi High Court. The court's decision in this case is expected to clarify the legal permissibility of data scraping for training large language models under Indian copyright law.

Further, the Delhi High Court in *Google LLC v. DRS Logistics (P) Ltd.*, (2023) 4 HCC (Del) 515, held Google responsible for decisions made by it for allocating advertisements on its webpages, even though these decisions were made by AI powered algorithmic decision-making systems.

Courts have also restricted the unauthorized use of AI-generated likeness and voice in deepfakes, recognizing the need to protect personality rights from misuse by emerging technologies. Courts in such cases have issued injunctions against intermediaries, AI platforms, and users to takedown and refrain from creating such content further.

In other instances, courts have taken a technology-first approach to adjudication. In *Rashtravadi Aadarsh Mahasangh v. Election Commission of India*, W.P. (C) 435 of 2025, the Delhi High Court directed the Election Commission to explore the use of AI to eliminate duplicate entries in voter rolls. At the same time, on 19 July 2025, the Kerala High Court issued a policy titled "Policy Regarding Use of Artificial Intelligence Tools in District Judiciary" ("**Kerala Policy**"), limiting the use of AI in judicial decision-making and cautioning against its deployment for legal reasoning (more elaborately set out in response to Question 20 below).

### 18. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence?

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.

### 19. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited? Which sectors have seen the most rapid adoption of AI technologies?

Indian businesses have begun embracing the use of AI extensively, and certain sectors have already incorporated large-scale deployment of AI in their everyday functions. In a 2024 survey on AI adoption conducted by NASSCOM, out of 500 firms spanning key industries, about 87 percent reported running AI experiments, and 40 percent have moved projects into regular production. In another report by the Boston Consulting Group, it was reported that India leads global AI adoption, with 30 percent of Indian companies having maximised AI's value potential, surpassing the global average of 26 percent.

Various industries are similarly leveraging AI to improve efficiency and expand access. For instance, in finance, AI is being leveraged for determining loan eligibility and recovery, developing alternative credit scoring models, fraud detection, automated claims processing, enhancing customer service, credit default predictions, KYC authentication, and designing financial products. In healthcare, AI is being applied to enhance diagnostic accuracy, promote telemedicine, and extend healthcare services to rural populations. Manufacturing companies, meanwhile, are adopting AI for supply chain management, predictive maintenance, and productivity improvements. In retail, AI is used for inventory management, demand forecasting, price optimization, and personalization of consumer offerings. The media and entertainment sector relies on AI for content personalization, monetization, targeted advertising, and audience engagement.

### 20. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns surrounding them?

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. India's apex court, the Supreme Court of India is piloting AI tools, including transcription tools and as well as prototypes for fixing defects and extracting data and metadata, to be integrated with its e-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". Further, the Kerala 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. It further explicitly warns against the indiscriminate use of AI due to inherent risks like privacy violations, data security breaches, and the potential erosion of trust in judicial decision-making and further requires members of the judiciary and employees assisting them must participate in the training programs on the ethical, legal, technical and practical aspects of AI.

## 21. 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 (*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 action of 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 can identify key clauses, flag

non-standard terms and highlight 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 clients of relevant changes, such as issuance of new circulars, advisories and regulations and enable prompt assessment of impact.

## **22. 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 TRAI, SEBI, and RBI are likely to intensify efforts to regulate AI through release of 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](mailto:supratim.chakraborty@khaitanco.com)



**Shailendra Bhandare**  
**Partner**

[shailendra.bhandare@khaitanco.com](mailto:shailendra.bhandare@khaitanco.com)



**Tanu Banerjee**  
**Partner**

[tanu.banerjee@khaitanco.com](mailto:tanu.banerjee@khaitanco.com)



**Anushka Sharda**  
**Partner**

[anushka.sharda@khaitanco.com](mailto:anushka.sharda@khaitanco.com)



**Ishan Johri**  
**Partner**

[ishan.johri@khaitanco.com](mailto:ishan.johri@khaitanco.com)



**Sumantra Bose**  
**Counsel**

[sumantra.bose@khaitanco.com](mailto:sumantra.bose@khaitanco.com)



**Sourav Dan**  
**Counsel**

[sourav.dan@khaitanco.com](mailto:sourav.dan@khaitanco.com)

