

INDIA

Shailendra Bhandare & Sourav Dan
Khaitan & Co

This chapter forms part of:

ARTIFICIAL INTELLIGENCE

Law Over Borders Comparative Guide 2026

www.globallegalpost.com/lawoverborders

227

INTRODUCTION

The Government of India has not adopted a single and universal formal definition of artificial intelligence (AI). Different governmental departments have approached the conceptualisation 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 (Reserve Bank of India (RBI)) and India’s telecommunications regulator (Telecom Regulatory Authority of India (TRAI)), have set out their own definitions of AI, in 2025, the Government of India’s Ministry of Electronics and Information Technology (MeitY) adopted a pragmatic and adaptive stance, explicitly choosing not to provide a catch-all definition of AI. MeitY has observed 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: “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.

Unlike the EU, which has introduced comprehensive legislation through the EU AI Act, India has no statute governing AI. However, MeitY has been proactive in issuing regular advisories for the use of AI across various sectors.

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 five years. The IndiaAI Mission is structured around seven strategic pillars:

- **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. The IndiaAI Compute Portal, launched in March 2025, provides subsidised access to GPUs, thereby democratising computing access and providing a foundation for attracting top AI talent.
- **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.

- **IndiaAI datasets platform (AIKosh).** The AIKosh centralises anonymised, non-personal datasets, toolkits, and AI models across sectors to facilitate the development of AI solutions and promote use cases of AI. The beta version, launched in March 2025, features over 1,300 datasets, 210 AI models and 13 development toolkits. It provides a use case library and development environment to explore and share datasets.
- **IndiaAI application development initiatives.** 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.
- **IndiaAI FutureSkills.** The IndiaAI FutureSkills initiative aims to provide support to over 500 PhD fellows, 5,000 postgraduates and 8,000 undergraduates. Further, 27 AI/data labs are being established in several Indian cities.
- **AIStartup financing.** This initiative provides targeted funding and compute subsidies to early-stage AI startups.
- **Safe and trusted AI.** The NITI Aayog published policy papers on a “Responsible AI” approach, establishing ethical principles and exploring risk-based regulation. Further, the 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.

Further, on 5 November 2025, MeitY, issued the AI Governance Guidelines (AI Guidelines) setting out India’s framework for safe and trusted AI. The stated objective of the AI Guidelines is to balance pro-innovation adoption of AI with measures to mitigate risks to individuals, communities and national security. The AI Guidelines are sector agnostic and outline the core principles, key recommendations, an action plan and practical guidance for industry actors and regulators to support compliance, transparency and accountability.

1. CONSTITUTIONAL LAW AND FUNDAMENTAL HUMAN RIGHTS

The Constitution of India does not explicitly address AI, but its core principles are directly engaged in several ways. The intersection of AI and constitutional principles in India is becoming increasingly important as AI systems begin to affect rights, governance and accountability especially the “golden triangle” of Articles 14 (equality), 19(1)(a) (freedom of speech), and 21 (right to life and personal liberty, including privacy).

1.1 Domestic constitutional provisions

As mentioned above, the intersection of India’s constitution with AI is largely on the golden triangle of fundamental human rights.

Article 14, Right to equality. AI systems (especially those underlying models trained for hiring, lending, insurance and policing) can have inherent bias and

therefore amplify it when used in decision making processes. Under Article 14, use of AI by the state must be non-arbitrary and ensure equal protection of laws. Algorithmic opacity raises concerns about whether automated decisions can meet the “reasonableness” and “non-arbitrariness” standards developed by Indian courts and enshrined in the constitution. In its 2024 advisory (which was directed to intermediaries and AI platforms under the Information Technology Rules, 2021) MeitY has also directed that platforms must ensure that their AI models do not permit bias or discrimination.

Article 21, Right to life and personal liberty. The Supreme Court of India’s ruling in *Justice KS Puttaswamy (Retd) and Anr v. Union of India* (AIR 2017 SUPREME COURT 416) recognised privacy as a fundamental right. AI systems, which often rely on extensive data collection, raise significant concerns about the handling and protection of personal data. Further, AI systems that rely on large-scale personal data (for example, facial recognition and predictive analytics) must comply with privacy, dignity and autonomy requirements. This also links to emerging concerns around surveillance and social profiling. The absence of specific AI regulations intensifies these concerns, increasing the risk of privacy violations.

Article 19(1)(a), Freedom of speech and expression. AI-driven content moderation, recommendation algorithms, and generative AI affect what speech is visible or suppressed. AI systems (ranking, filtering, takedowns) directly influence visibility and reach of speech. Under the Constitution of India, any restriction must meet Article 19(2) standards (legality, necessity, proportionality). Current AI models may violate this right by way of over-removal (false positives), where legitimate speech (such as satire) gets suppressed, and under-removal (false negatives), where harmful content persists, raising regulatory inefficiency. Since fundamental rights are only actionable against the state, if the state uses or mandates such systems, restrictions must satisfy the “reasonable restrictions” test under Article 19(2).

Further, excessive reliance on AI by the state raises questions about the delegation of decision-making power. Constitutional principles require that essential functions remain accountable to human authorities, with clear lines of responsibility. Indian courts have begun engaging with technology-related rights, and the Supreme Court is using AI and machine learning based tools for case management, curing filing defects and meta data extraction. The AI-based tool, Supreme Court Portal Assistance in Court Efficiency (SUPACE), is being developed to include a module to understand the factual matrix of cases using an intelligent search of the precedents. This is currently at an experimental stage of development. At the time of writing, Indian courts are not using AI technologies as part of the decision-making process.

1.2 Human rights decisions and conventions

India doesn’t yet have a standalone “AI and human rights” statute, so the framework emerges from a blend of constitutional jurisprudence, international commitments, and soft-law policy instruments. At present, India has not directly seen any AI issues in relation to human rights decisions or its interactions with international human rights conventions.

2. INTELLECTUAL PROPERTY

Artificial intelligence is reshaping the landscape of innovation at a rapid pace, but its convergence with intellectual property rights gives rise to intricate legal, ethical, and judicial issues. Ranging from disputes over the ownership and attribution of AI-generated works to questions about rights over training data, AI is reshaping some of IP's major foundational assumptions. Conventional copyright and patent regimes – built around concepts like originality, authorship and inventorship – are increasingly being strained as AI systems independently produce text, music and art. At the same time, these systems depend heavily on human-created datasets, giving rise to complex questions around fair use, attribution, compensation and the moral rights of creators.

2.1 Patents

AI is starting to stress-test Indian patent law at multiple levels – patentability, inventorship, disclosure and enforcement. India does not yet have AI-specific patent legislation. The patent system as it exists today was designed to recognise and protect human-driven innovation, giving concrete form to human creativity. However, with AI systems, the resulting outputs may be generated by machines rather than individuals. Since the core objective of patent law is to encourage human innovation for societal benefit, it becomes necessary to adapt the framework to address these emerging challenges.

The primary issue in patent applications pertains to ownership and inventorship: should the AI application be named as an inventor or co-inventor? If AI systems cannot hold ownership, should specific criteria determine how human ownership or inventorship is attributed or should this decision be left to private arrangements? Indian law requires a “person” (human) to be listed as the inventor. AI systems like DABUS (Device for the Autonomous Bootstrapping of Unified Sentience), developed by Dr. Stephen Thaler, are not considered legal entities that can hold patent rights as an inventor.

Section 3(k) of the Indian Patents Act, states that algorithms, mathematical methods, and computer programs *per se* are not patentable. Therefore, AI must be linked to a tangible, industrial, or technical application, not just a standalone algorithm in order to sail over the section 3(k) restriction.

2.2 Copyright

The (Indian) Copyright Act, 1957 (“Copyright Act”) is based on the principle of human authorship and creativity, and AI cannot be recognised as an author under the Copyright Act. Additionally, the application for copyright registration requires disclosure of the author's name, nationality and address. Purely AI-generated content lacks protection, though work with significant human creative control may be copyrighted. Section 2(d)(iv) of the statute provides that, in the case of a “computer-generated work”, the “author” is the person who causes the work to be created. Accordingly, the definition of authorship under the Indian Copyright Act places emphasis on the involvement of a human person.

Historically, courts have generally maintained that the author of a copyrighted work must be a natural person. On this basis, it may be argued that AI systems cannot themselves be recognised as “authors” or granted copyright protection.

However, these earlier judicial decisions did not arise in the context of AI-generated works and therefore did not directly consider the possibility of AI systems being treated as authors or co-authors.

As a result, uncertainty exists on certain aspects like:

- 1) whether fully AI-generated outputs qualify for copyright protection;
- 2) the threshold of human creativity required;
- 3) whether prompts alone constitute sufficient authorship; and
- 4) whether ownership vests in the user, developer, or platform provider.

With respect to (1), there has been some guidance through administrative and judicial bodies. Back in 2020, Mr Ankit Sahni (the applicant) had 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, as it was a non-human author. His second application, naming both himself and the AI (RAGHAV) as co-authors, was initially granted registration in November 2020. Later, however, the ICO issued a contentious withdrawal notice for the registration. Mr. Sahni responded to the ICO notice arguing that the ICO did not have the authority to review its own decision. At present, no action appears to have been taken on the copyright registration.

Another aspect which is being widely debated globally is the use of copyrighted material for training large language models without obtaining authorisation or consent. AI models are trained on massive datasets containing books, articles, music, films, artistic works, software code and online content.

Under Indian law, potential questions include:

- whether dataset ingestion and copying amount to reproduction;
- whether temporary or intermediate copies are infringing;
- whether AI training could fall within fair dealing exceptions under section 52;
- whether text and data mining is implicitly permitted; and
- whether consent or licensing is required for commercial AI training.

India presently does not have a specific text-and-data-mining exception comparable to some other jurisdictions. Further, India follows a closed-list “fair dealing” doctrine as set out in section 52 of the Copyright Act (unlike the broad fair use exceptions provided in the US). Exceptions exist for private/personal use, research, criticism, review or reporting current events. Whether large-scale commercial AI training qualifies is hotly debated and is pending adjudication in *ANI Media Pvt Ltd v. OpenAI* (filed in 2024), where a news agency alleged that unauthorised use of its content for training ChatGPT amounted to infringement. The arguments have been heard in this case, and the court has reserved its decision.

In its 2025 working paper, *One Nation, One License, One Payment*, the Government of India proposed a “hybrid model”. Its key features include:

- a mandatory blanket licence permitting AI developers to use all lawfully accessed copyrighted works for AI training;
- a statutory right to remuneration in favour of copyright owners;
- a centralised royalty collection and distribution mechanism;
- a single-window licensing framework; and
- government-supervised determination and administration of royalties.

Importantly, under the proposed framework, copyright owners would not have the ability to opt out of AI training uses once works are lawfully accessible.

2.3 Trade secrets and confidentiality

AI innovations, such as models, algorithms, training data sets and proprietary processes, are often more effectively protected as trade secrets rather than through patents or copyright. Patent protection requires extensive public disclosure and can face subject-matter eligibility concerns, while copyright protection is generally confined to the expression of a work and does not extend to underlying ideas, functionality or methods. By maintaining confidentiality, businesses can preserve their competitive advantage for an indefinite period. Similarly, proprietary datasets and specialised or curated training methodologies may derive substantial commercial value and competitiveness from remaining confidential and can qualify for trade secret protection where appropriate safeguards and confidentiality measures are implemented.

India does not have legislation regulating trade secrets. Protection of trade secrets and confidentiality is achieved by contract law (under the Indian Contract Act, 1872) through confidentiality agreements, non-disclosure agreements, employment contracts and restrictive covenants. It is also protected via common law principles, such as breach of confidence and claims under tort and copyright law). Criminal remedies are also available for breach of trust under the Indian Penal Code, 1860 (now Bharatiya Nyaya Sanhita) and hacking/unauthorised access under the Information Technology Act, 2000.

There is a proposed Trade Secrets (Protection and Enforcement) Bill, 2024 which aims to create a *sui generis* framework with clear definitions, misappropriation remedies (civil and potentially criminal), and protections for AI-related assets like algorithms, training methodologies, model weights and proprietary datasets. It remains in draft form but could provide stronger, uniform enforcement.

2.4 Notable IP cases

Patents

The AI system DABUS, developed by Dr. Stephen Thaler, raised questions of AI as an inventor in the context of patent applications. Dr. Thaler filed an Indian patent application naming DABUS as the “true and first inventor”. However, the Indian Patent Office rejected the application (202017019068), holding that the existing Indian patent law framework permits only natural persons to be recognised as inventors

Copyright

Connected to the DABUS AI system, Dr. Stephen Thaler submitted a plea on copyright protection of an AI-generated artwork. Dr. Thaler created DABUS, which is capable of creating artwork without human input. He filed an application to register a copy of an artwork produced by 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 is whether an artwork produced by AI, where there is no human element, can be copyrighted in accordance with 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 from the date 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.

The question of whether copyrighted material can be used to train AI is a key issue in the case of *ANI Media Pvt Ltd v. OpenAI OPCO LLC*, where an Indian news agency, ANI Media Pvt Ltd, alleged that OpenAI unlawfully used and stored its copyrighted content to train its LLMs, such as ChatGPT. ANI sought an interim injunction against OpenAI, claiming that its use of ANI's content constitutes copyright infringement. Additionally, ANI asserted that it had previously sent a notice to OpenAI objecting to the unauthorised storage and use of its content, and OpenAI responded by acknowledging its use of ANI's data. Open AI has opposed the suit and raised two key arguments. First, OpenAI challenged the jurisdiction of the court, arguing that the suit lacked maintainability since its chatbot servers are not located in India. Second, OpenAI claimed that ANI had not provided evidence of content being reproduced within India to substantiate its infringement allegations. Additionally, recognising the relevance of the issue for news agencies, certain entities filed intervention applications, among others the Federation of Indian Publishers (FIP) and Digital News Publishers Association (DNPA). The court has heard the pleadings and has reserved its verdict.

3. DATA

3.1 Domestic data law treatment

While neither India's Digital Personal Data Protection (DPDP) Act, 2023 (DPDP Act) nor the DPDP Rules 2025 explicitly mention "artificial intelligence" in its text, its principles create significant functional boundaries for how AI models are trained, deployed and managed in India from a data protection perspective. The DPDP Rules 2025 have further clarified these interactions to an extent especially in relation to consent and algorithms, introducing specific mandates for algorithmic fairness and transparency. Since AI systems frequently rely on large-scale collection, processing, profiling and analysis of personal data, the DPDP Act has direct implications for the development, deployment and governance of AI technologies in India.

The DPDP Act regulates AI through the lens of "data fiduciaries" (entities that determine the purpose of data processing). Any AI company collecting personal data from Indian users must adhere to these pillars:

- **Specified purpose and consent.** AI models cannot simply "scrape" personal data for training. Data collection must be for a specific, lawful purpose, backed by "free, specific, informed, and unambiguous" consent.
- **Notice requirements.** Before processing, users must receive a notice (in English or any of the 22 languages in the 8th Schedule of the Constitution of India) explaining exactly what data is being used for the AI model.
- **Data minimisation.** AI developers are technically required to collect only the data necessary for the model's specific function, challenging the "more is better" philosophy of LLM training.

Some of the key privacy issues that may emerge out of development, including training and use of AI include:

- **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.
- **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.
- **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.
- **Data minimisation.** AI systems often need large and diverse datasets for research and analysis which may conflict with the principle of only collecting data strictly necessary for a specified purpose.
- **Transparency.** AI systems may produce unexplainable and unanticipated outcomes and it may be hard to provide meaningful privacy notices.
- **Retention limitation.** AI systems may need to retain data for extended periods for AI training, traceability, audit and oversight purposes.
- **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.

3.2 General data protection regulation

Published in August 2023, the DPDP Act is India's first comprehensive data protection law. It applies to digital personal data collected within India, or data processed outside India for offering goods/services to individuals within India.

Key actors

- **Data principal.** The individual to whom the data relates.
- **Data fiduciary.** Entity determining the purpose/means of processing (similar to a controller).
- **Data processor.** Processes data on behalf of a fiduciary.

Core requirements

- **Consent.** Must be free, informed, specific and revocable.
- **Children's data.** Requires verifiable parental consent.
- **Obligations.** Data fiduciaries must implement security safeguards, report breaches and comply with data minimisation.

Implementation

Along with the notification of the 2025 Rules, the government has notified a phased timeline for implementing the DPDP Act as follows:

- Immediately effective:
 - definitions under the DPDP Act;
 - provisions establishing the Data Protection Board of India (Board);

- the rule-making and transitional powers of the Government of India; and
- the ability to make amendments to the DPDP Act.
- After one year (i.e. 13 November 2026): The conditions for registration and operation of consent managers as well as the Board's corresponding jurisdiction over being intimated of any breach of such conditions.
- After 18 months (i.e. 13 May 2027): The core operational provisions of the DPDP Act, relating to:
 - consent and corresponding aspects;
 - obligations applicable to data fiduciaries;
 - obligations applicable to significant data fiduciaries; and
 - the remaining powers of the Board.

3.3 Open data and data sharing

The Information Technology Act, 2000 (IT Act) provides penalties and compensation for unauthorised downloading, copying or extraction of any data, computer database or information from a computer or 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.

However, 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. Given this, AI developers may be able to scrape public profiles and datasets for training without needing explicit consent, provided the data was made public by the user themselves. 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 once the entire DPDP Act is enforced and operational. 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.

With respect to cross-border data transfers, the DPDP Act permits cross-border transfers except to countries specifically restricted by the Government of India.

3.4 Biometric data: voice data and facial recognition data

Biometric and facial recognition data would fall under “sensitive personal data or information” (SPDI) and such data must be processed according to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules). For collecting such SPDI, written consent must be obtained and the purpose of collection must be informed. The DPDP Act once fully operational will repeal the SPDI Rules, but until then the SPDI Rules remain applicable. Non-compliance may result in compensation under the IT Act. Under the IT Act, a body corporate that is negligent in implementing reasonable security practices for protection of SPDI, and thereby causes wrongful loss or gain, may be liable to pay compensation. The quantum is uncapped and determined case-by-case by the relevant forum.

4. BIAS AND DISCRIMINATION

4.1 Domestic anti-discrimination and equality legislation treatment

Indian AI regulations heavily rely on existing constitutional and statutory laws to manage discrimination, with Article 14 (equality), Article 15 (prohibition of discrimination), and Article 16 (equality in public employment) of the Constitution forming the core framework against algorithmic bias. While the DPDP Act governs personal data, explicit AI-specific anti-discrimination mandates are nascent, often requiring judicial interpretation or non-binding ethical guidelines to enforce fairness.

5. CYBERSECURITY AND RESILIENCE

5.1 Domestic technology infrastructure requirements

The Indian Computer Emergency Response Team (CERT-In) established under the IT Act functions as a national agency for responding to cybersecurity incidents. CERT-In operates the National Cyber Coordination Centre (NCCC), which serves as a control room to facilitate coordination between different agencies to mitigate cybersecurity threats.

In order to address cybercrimes comprehensively, the Indian government has also set up the I4C. A core component of I4C is the National Cyber Crime Reporting Portal (NCRP), which allows the public to report cybercrime, so that prompt criminal action can be initiated under the provisions of the IT Act, and the Bharatiya Nyaya Sanhita, 2023 (BNS) (Indian penal law). In January 2024, NCRP introduced a “Report suspect” feature for quick reporting of suspicious websites.

6. TRADE, ANTITRUST AND COMPETITION

6.1 AI-related anti-competitive behaviour

The principal legal basis for regulating dark patterns in India is the Consumer Protection Act, 2019.

Dark patterns may amount to:

- unfair trade practices;
- misleading advertisements; and
- violation of consumer rights.

Dark patterns

India became one of the first jurisdictions to expressly regulate dark patterns through the Guidelines for Prevention and Regulation of Dark Patterns, 2023 (“2023 Guidelines”). India’s Central Consumer Protection Authority (CCPA) notified Guidelines for Prevention and Regulation of Dark Patterns, 2023 (“Dark Pattern Guidelines”), under section 18 of the Consumer Protection Act, 2019 (CPA), on 30 November 2023. The Guidelines define “dark patterns” as “practices or deceptive design patterns using user interface (UI) or user experience (UX) interactions on any platform that is designed to mislead or trick users into doing something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice, amounting to misleading advertisement or unfair trade practice or violation of consumer rights”.

Scope

The 2023 Guidelines apply to:

- e-commerce platforms;
- online intermediaries;
- advertisers;
- sellers; and
- service providers operating in India.

Definition

The 2023 Guidelines define dark patterns as deceptive UI/UX practices designed to mislead, trick or manipulate users into actions they did not originally intend.

Although, the 2023 Guidelines initially focused on e-commerce, regulatory scrutiny is expanding into:

- fintech;
- banking;
- OTT platforms;
- mobility apps; and
- subscription businesses.

For example, the Reserve Bank of India has proposed draft rules in February of 2026 addressing mis-selling and dark-pattern-based consent mechanisms in financial services.

Algorithmic collusion

The Competition Commission of India (CCI) has given an indication that they are getting prepared to take action against anti-competitive practices that might emerge in the artificial intelligence front, including algorithmic collusion. In 2025, CCI had conducted a market study on AI's impact on competition and identified potential anti-competitive conduct. Potential areas of violation include concentration in AI value chain, algorithmic collusion, targeted price discrimination, self-preferencing and opaqueness in the AI applications and tools.

6.2 Domestic (antitrust) regulation

India currently does not have AI-specific competition regulations issued by the Competition Commission of India (CCI) that are legally binding. Instead, the CCI has taken a policy and market-study approach and has made it clear that existing provisions of the Competition Act, 2002 are capable of addressing AI-related anti-competitive conduct. In April 2024, the CCI formally launched a market study on AI and competition to understand:

- AI market structures;
- competition concerns arising from AI deployment;
- data concentration;
- compute and infrastructure bottlenecks;
- AI partnerships and ecosystem arrangements; and
- regulatory approaches globally.

The final report was released in October 2025. The CCI expressly stated that competition law remains an important tool for addressing AI-related anti-competitive conduct.

7. AGENTIC AI

7.1 Legal status and recognition of AI agents

Indian law does not currently recognise AI agents as legal persons or entities, treating them instead as tools, software or property. AI lacks the legal personality required to enter contracts independently, sue or be sued. Liability for AI actions lies with developers, users or owner.

7.2 Sector-specific agentic AI regulations

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. India does not yet have a standalone statute specifically regulating “Agentic AI” and has not enacted a law equivalent to the EU AI Act specifically for AI agents or autonomous systems. MeitY released the India AI Governance Guidelines in November 2025 under the India AI Mission. These guidelines are currently the closest thing to a national AI governance framework. The guidelines adopt a principle-based, innovation-oriented approach rather than a strict regulatory model and aim to:

- promote safe, trusted and inclusive AI;
- encourage innovation and economic growth;
- manage risks associated with AI systems;
- balance technological advancement with societal protection; and
- support India’s “Viksit Bharat 2047” vision.

Unlike the EU AI Act, India’s framework is not primarily prohibition-driven. Instead, it relies heavily on:

- existing laws;
- sectoral regulation;
- voluntary compliance;
- co-regulation; and
- risk-based governance.

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 five 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:
 - 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
 - undertake due diligence to ensure that users do not upload/transmit unlawful content.

Thereafter in 2026, amendments to the IT Rules required digital platforms to label AI-generated content (including text, audio and video) and ensure technical traceability. It also mandated faster takedowns, wherein platforms must remove “deepfakes” and illegal synthetic content within three hours of receiving a complaint.

- **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 IT Act and IT Rules.

Key laws regulating the use of AI

- **IT Act and IT Rules.** The IT Act provides safe harbour for “intermediaries” provided that such “intermediaries”:
 - do not initiate or select the receiver of transmission or select or modify the information contained in the transmission;
 - observe due diligence while discharging their duties under the IT Act and guidelines of the Government of India; and
 - 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.
- **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 Section 4, above.
- **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.
- **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.
- On 5 November 2025, MeitY issued the **AI Governance Guidelines** (Guidelines) setting out India’s framework for safe and trusted AI. The stated objective of the Guidelines is to balance pro-innovation adoption of AI with measures to mitigate risks to individuals, communities and national security. The Guidelines are sector-agnostic and outline the core principles, key recommendations, an action plan and practical guidance for industry actors and regulators to support compliance, transparency and accountability.

Voluntary standards

The Telecommunication Engineering Centre, under the Department of Telecommunications, has introduced a voluntary standard for the fairness assessment and rating of AI systems to promote unbiased and responsible AI practices, particularly in the 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.

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 draft 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.
- The Reserve Bank of India (RBI) has taken the most advanced sectoral approach toward AI governance. In 2025, the RBI released the Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) report for regulated financial entities. The framework addresses governance, accountability, audits, explainability, cybersecurity and risk management for AI systems used in banking and financial services.
- SEBI amended the SEBI Intermediaries Regulations in 2025 to formally introduce provisions relating to the use of AI and machine learning by regulated entities in the securities market. Further, with respect to algorithmic trading, new 2026 regulations mandate that AI-driven trading agents that "learn" and adjust strategies in real-time must be pre-approved by SEBI. They require "Decision Logic Documentation" – a record of why the agent took a specific trade, ensuring it is auditable during market volatility.
- India has also begun developing AI governance frameworks for the healthcare sector. The Ministry of Health and Family Welfare reportedly launched initiatives such as the Strategy for Artificial Intelligence in Healthcare for India (SAHI), aimed at safe and ethical deployment of AI in healthcare ecosystems.

8. PRODUCT LIABILITY AND AI

8.1 Application of existing product liability frameworks to AI

As there is no specific legislation governing AI in India, potential liability for development and deployment of defective AI systems will likely be assessed based on 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.

Consumer Protection Act, 2019

An AI-enabled product or service could be construed as a “product” under the Indian Consumer Protection Act, 2019 (CPA). Under the CPA, regardless of whether the product in question is a physical device or 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. 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:

- provide information that ends up causing harm;
- provide adequate instructions/warnings; or
- conform to express warranties/contract terms governing such service.

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.

Law of torts

The developer of a defective AI system could incur tortious liability if the developer has acted negligently and breached a duty of care to ensure that the AI system does not have any inherent manufacturing or design defects.

IT Act

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

BNS (Indian Penal Code)

As covered in response to Section 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. Also, if an AI is used to generate and spread misinformation that incites public fear or violence, the same would be actionable under the BNS.

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 (i.e. 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 implement reasonable security safeguards to prevent personal data breach or to adhere to the legal grounds of processing personal data as set out thereunder.

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 protected personality rights from misuse of deepfake technology and issued takedown orders for deepfake content circulated online.

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 held the deployer of an algorithmic decision-making system to be liable for decisions made autonomously through such a system.

8.2 Strict liability and AI systems

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* (a guilty act/offence) and the presence of *mens rea* (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 the deployer of an algorithmic decision-making system to be liable for decisions made autonomously through such a system.

8.3 Product recall and safety measures

Please see our response to Sections 8.1 and 8.2, above

8.4 Notable AI liability cases and trends

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 Sections 8.1 to 8.3, above.

In *Google LLC v. DRS Logistics (P) Ltd.* (2023) 4 HCC (Del) 515, it has been held that Google is 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 increasingly curtailed the unauthorised use of AI-generated likenesses and voices in deepfakes, acknowledging the importance of safeguarding personality rights against misuse through emerging technologies. In such matters, courts have granted injunctions directing intermediaries, AI platforms and users to remove the impugned content and restraining them from further creation or dissemination of such material. 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. Conversely, on 19 July 2025, the Kerala High Court issued the Policy Regarding Use of Artificial Intelligence Tools in District Judiciary which restricted the use of AI in judicial decision-making and cautioned against reliance on AI for legal reasoning.

9. DOMESTIC LEGISLATIVE DEVELOPMENTS

9.1 Proposed and/or enacted AI legislation

At the time of writing, India does not have a standalone, comprehensive AI law.

Key 2026 regulatory developments focus on mandatory labelling of synthetic content and strict, rapid takedown timelines for deepfakes, primarily enforced through amendments to the IT Rules, 2021 and include:

- **AI content rules (February 2026).** Amendments to the IT Rules require digital platforms to label AI-generated content (including text, audio and video) and ensure technical traceability.
- **Faster takedowns.** Platforms must remove “deepfakes” and illegal synthetic content within three hours of receiving a complaint.
- **User obligations.** Users are required to declare if content is AI-generated upon uploading to social media platforms.
- **AI Governance Guidelines (2025/2026).** MeitY proposed a seven-principle framework, emphasising trust, safety, and a people-first approach over stringent licensing.
- **Digital India Act.** The proposed Digital India Act is being designed to replace the IT Act, aimed at introducing risk-based classification for AI systems.
- **Voluntary self-regulation.** While mandatory rules exist for content, there is heavy reliance on voluntary, ethical and self-regulatory frameworks for AI development.
- **Upcoming copyright reforms.** The Department for Promotion of Industry and Internal Trade (DPIIT) is exploring regulations for AI training data, including licensing and royalty regimes for copyrighted content (through the DPIIT working paper) and a committee has been set up in this regard to assess the current copyright regime.

9.2 Proposed and/or implemented Government strategy

It is likely that India will see significant legal developments in the field of AI over the next 12 months. The full implementation of the DPDP Act would bring in strict consent, purpose limitation, and data minimisation requirements, all of which may directly impact developers and deployers alike. The proposed Digital India Act 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 sectoral regulations, entities like 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 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 training of AI content, 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.

10. FREQUENTLY ASKED QUESTIONS

Can AI-generated content be protected under Indian intellectual property law?

Under current Indian law, copyright and patent protection is fundamentally premised on human authorship and inventorship. While AI-assisted works may qualify for protection where there is sufficient human creativity, purely autonomous AI-generated outputs remain in a grey area.

Who is liable if an AI system causes harm or makes a wrong decision?

India does not currently recognise AI systems as separate legal persons. Depending on the facts and level of control, liability therefore generally continues to attach to:

- developers;
- deployers;
- operators; and
- enterprises using the AI system.

Can companies use publicly available internet data to train AI models?

Not automatically. The legality depends on:

- copyright ownership;
- platform terms of use;
- consent requirements;
- data protection obligations;
- fair dealing exceptions; and
- nature of the data being scraped or processed and the location of the activity.

What are the biggest legal risks companies face when deploying AI?

The primary legal risks generally include:

- data privacy violations;
- copyright infringement;
- inaccurate or hallucinated outputs;
- bias and discrimination;
- cybersecurity vulnerabilities;
- regulatory non-compliance;
- lack of explainability; and
- reputational harm.

Are there any AI-specific laws or regulations in India?

India does not yet have standalone AI legislation comparable to the EU AI Act.

However, AI systems are already governed through a combination of:

- the DPDP Act;
- the IT Act, 2000;
- consumer protection laws;
- competition law;
- sectoral regulations; and
- emerging AI governance frameworks (such as the 2026 Deepfake Guidelines).

AUTHOR BIOGRAPHIES



Shailendra Bhandare

Shailendra Bhandare is a Partner in the Intellectual Property (IP) Practice Group at the Mumbai and Pune offices of Khaitan & Co. With nearly two decades of experience working in boutique IP firms and IP teams of full-service firms, Shailendra's expertise in IP extends to the entire lifecycle of IP (prosecutions, enforcements, contentious matters, management, and transactional work). He advises several multinational and domestic conglomerates including Fortune 500 companies. Similarly, he also takes special interest in *pro bono* matters. He is actively involved in policy/advocacy initiatives and educational initiatives in India for organisations such as the International Trademark Association (INTA) and Global Intellectual Property Alliance (GLIPA). He has also authored articles on the developments in Indian IP law for several publications such as World Trademark Review and the Oxford Journal of Intellectual Property Law & Practice. Shailendra is the recipient of the Outstanding Practitioner (India) Award (Asialaw Regional Awards 2019) and the INTA Membership Champion Award (2022) and has been recognised in various rankings, including WTR 1000, Chambers and Partners, and WWL.

Continued on the following page.

Continued from the previous page.



Sourav Dan

Sourav Dan is Counsel in the Intellectual Property (IP) Practice Group of Khaitan & Co and is based out of the Bangalore office. With more than a decade of experience in IP laws across various industry sectors, Sourav's expertise extends to the entire gamut of IP laws, with a focus on IP transactions, advisory, open-source software advisory and compliance, negotiating commercial IP agreements, technology laws, domestic and international IP prosecution, and contentious matters. He has advised domestic and international companies in navigating IP laws, including technology-focused startups. He is also actively involved in the International Trademark Association's (INTA) and ITechLaw's policy/advocacy initiatives in India. Sourav is part of INTA's well-known trade mark committee and ITechLaw's dispute resolution and IP and AI committees. He has been recognised in various rankings such as WTR 1000, WIPR Leaders, Managing IP's Rising Stars and IP Stars and The Legal 500.

FIRM PROFILE

Khaitan & Co

Khaitan & Co is one of India's oldest full-service law firms having been founded in 1911. The firm currently has presence in Mumbai, Kolkata, New Delhi (National Capital Region), Bengaluru, Chennai, Ahmedabad, Pune, and Singapore. The firm is among India's most prominent and elite full-service law firms with domain expertise in all practice areas, including corporate/commercial advisory, competition/antitrust, intellectual property, dispute resolution, banking & finance, tax, funds, white-collar crime, energy & infrastructure, capital markets, real estate, technology, media & entertainment, and labour & employment. The firm is backed by over 100 years of legal heritage, delighted clients from across the globe, and topical, commercial and specialised services. The firm's Intellectual Property (IP) Practice Group, which is around 100 members strong, provides full service across the lifecycle of patents, designs, trade marks, copyrights, plant varieties, domain names, geographical indications, biodiversity, trade secrets and confidential information. We assist clients across industries in diverse areas such as local/international filings, prosecution, advisory, transactions and enforcement. Our team comprises legal and technical professionals, collaboratively leveraging on clients' commercial, strategic and technical interests to offer bespoke, pragmatic as well as cost-effective solutions. The IP team is equipped to handle all aspects of IP practice in India and overseas.