Legal 500
Country Comparative Guides 2024

India

Artificial Intelligence

Contributor

Fox Mandal &
Associates

Rajesh Vellakkat

Partner | rajesh.vellakkat@foxmandal.in

Gaurav Sahay

Practice Head | gaurav.sahay@foxmandal.in

Akshay Nair

Associate | akshay.nair@foxmandal.in

Sanjana S.

Associate | sanjana.s@foxmandal.in

Kiran Patel

Associate | kiran.patel@foxmandal.in

Ashita Sahay

Legal Associate | ashita.sahay@foxmandal.in

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**

India: Artificial Intelligence

1. What are your countries legal definitions of "artificial intelligence"?

Presently, India does not have dedicated legislation or a governance framework that regulates Artificial Intelligence (AI). This open environment paves the way for innovative approaches, rapid adaptation to technological advancements, and exploration in the AI sector. Additionally, several existing laws and policies already provide a robust foundation for indirectly regulating various aspects of AI. This adaptable framework ensures that as AI evolves, the regulatory landscape can evolve with it, staying relevant and advocating progress.

Nevertheless, the definition of AI and associated systems can be found in various government reports. For instance, the Government of India has established the IndiaAI mission to advance and develop a comprehensive ecosystem catalyzing AI innovation in India. In view of this mission, the Ministry of Electronics and Information Technology (MeitY) constituted four committees on AI, where the 'Report of Committee B on Leveraging AI for Identifying National Missions in Key Sectors' defines 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. For example, pulmonary system in which lungs, chest muscles, blood, etc. all play a role."*

Definition of AI under the Report of the Artificial Intelligence Task Force: *Artificial intelligence "is the science and engineering of making intelligent machines, especially intelligent computer programs", with 'intelligence' being the "computational part of the ability to achieve goals in the world".*

The National Strategy for AI by Niti Aayog provides the following definition of AI: *AI refers to the ability of machines to perform cognitive tasks like thinking, perceiving, learning, problem solving and decision–making.*

2. Has your country developed a national strategy for artificial intelligence?

To encourage Making AI in India and Making AI Work for India, the Government of India, through the IndiaAI mission, has proposed to set up a comprehensive ecosystem in India while promoting the application of AI in various sectors. The mission will be implemented by the 'India AI' Independent Business Division (IBD) under the Digital India Corporation (DIC), which is an Indian not-for-profit company established by the MeitY, Government of India. The components of the mission are:

a. IndiaAI Compute Capacity
b. IndiaAI Innovation Centre
c. IndiaAI Datasets Platform,
d. IndiaAI Application Development Initiative
e. IndiaAI Future Skills
f. IndiaAI Startup Financing
g. Safe & Trusted AI

Moreover, various initiatives by the Government of India and the respective State Governments have been launched to promote the use of AI in India.

US-India AI Initiative. The Indo-U.S. Science and Technology Forum (IUSSTF) launched the US-India AI to promote the growth of AI and aims to explore research and development and collaboration opportunities. It also aims to scout the employment of AI in important sectors essential for national development, such as health, energy, agriculture, etc.

MCA 3.0 portal. Corporates in India find it challenging to make periodic regulatory filings in India. The Ministry of Corporate Affairs (MCA) has proposed a modern portal, version 3.0, that is designed to remove the complexities involved in filing with the help of AI and ML analytics and tools.

Responsible AI for Youth. The National e-Governance Division of the MeitY has established Responsible-AI, which is a national level program for youth in India. The program will aim to impart practical education and skills to school students in schools run by the government.

AI Portal. The AI Portal is a joint venture by MeitY and the National Association of Software and Service Companies (NASSCOM) that will cumulate the latest developments and initiatives in the field of AI in India. The platform will provide experts on AI or any working professional to display, learn, gain, and share knowledge on AI.

Applied AI Research Centre in Telangana. The

Government of the State of Telangana has launched Intel AI in collaboration with IIIT Hyderabad and the Public Health Foundation of India, which carried out research in the area of utilising AI to mitigate and manage changes relating to smart mobility and healthcare in India.

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.

The MeitY had issued two advisories on Artificial Intelligence mainly to tackle the growing use of deepfakes in the online environment. The first advisory, issued on March 1, 2024, placed emphasis on all intermediaries and platforms to ensure that their AI models, large language models (LLMs), generative AI/software(s), algorithm(s), or computer resources did not permit any discrimination or threaten the integrity of the electoral process and prohibited their users from contravening the provisions of the IT Act 2000 and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (“Rules”). The Act and Rules do not permit hosting, displaying, modifying, publishing, transmitting, storing, updating, or sharing unlawful content.

The advisory issued on March 15, 2024, mandated that content generated through AI models must comply with existing content moderation rules under the IT Rules. Intermediaries and AI developers are responsible for ensuring this compliance, particularly to prevent bias, discrimination, and threats to electoral integrity, echoing the OECD Principle on ‘Human-Centered Values and Fairness.’ This advisory emphasized that transparency about AI models’ potential unreliability must be maintained. The advisory mandates that the platforms inform users of the legal consequences of dealing with unlawful information through their Terms of Use and User Agreements. The metadata must be embedded in synthetic content to distinguish it from user-generated content and identify the originator.

The current Indian legal landscape is adaptable and can accommodate the dynamic field of Artificial Intelligence. While there are no AI-specific laws at present, the existing legal framework has the potential to effectively regulate and address various aspects of AI technology.

a. *Cybersecurity*

Information Technology Act, 2000: The act provides the legal framework for electronic governance by giving recognition to electronic records and digital signatures. It addresses cybercrime and electronic commerce, focusing on data protection, cyber offences, and intermediary liabilities.

b. *Healthcare*

Clinical Establishments (Registration and Regulation) Act, 2010: While this act primarily governs the registration and regulation of clinical establishments, it could extend to AI-driven healthcare solutions and devices.

Medical Device Rules, 2017: These rules regulate the manufacturing, import, sale, and distribution of medical devices in India. AI-integrated medical devices, such as diagnostic tools and surgical instruments, fall under this regulatory framework.

The Drugs and Cosmetics Act, 1940: This act regulates the import, manufacture, and distribution of drugs in India. AI applications in drug development and personalized medicine could fall under its ambit.

c. *Law*

The Bharatiya Sakshya Adhiniyam, 2023 (BSA): The new law significantly streamlines the admission of electronic evidence in Indian courts in comparison to the prior legislation, the Indian Evidence Act (IEA) of 1872, and may apply to AI-generated evidence in legal proceedings, particularly in terms of admissibility and reliability. Section 63 of the BSA addresses the development of electronic records and effectively supersedes the IEA’s approach. Previously, electronic documents were considered secondary evidence, necessitating additional procedures for establishing their legitimacy before being recognized as evidence. The BSA addresses this by classifying electronic records as the primary evidence, much like original documents such as paper contracts or handwritten notes. This implies that until disputed, electronic evidence has the same weight as conventional paper documents. It expands on the foundation created by the Information Technology Act (IT Act) of 2000. Section 63 of the IT Act also addresses the admissibility of electronic records. While Section 63 does not specifically address admissibility, it broadens the meaning of “electronic records” as defined under the BSA. The BSA extends the definition to include information generated, sent, received, or stored in various electronic formats like:

i) Semiconductor memory: This covers storage devices like USB drives, flash cards, and memory cards used in smartphones and cameras.

ii) Communication devices: This includes data stored on mobile phones, tablets, and other communication gadgets.

iii) Any other electronic form: This opens the door to admitting data from smart devices, sensors, and emerging technologies.

Consumer Protection Act, 2019: This Act enables a consumer of any product or service to file a complaint in case of any unfair trade practices, restrictive trade practices, defect in goods, deficiency in service, or sale of goods that are hazardous to life and safety. Section 83 of the Consumer Protection Act allows for product liability actions against manufacturers, service providers, or sellers for harm caused by defective products. Users of AI products or services may rely on this section to file a consumer case against the manufacturer or owner of AI.

Indian Contract Act 1872: The Indian Contract Act, 1872, governs contracts in India, covering elements like offer, acceptance, and consideration. AI can streamline the contracting process by automating contract drafting, review, and management. In such an environment, questions about liability and accountability arise if an AI system makes an error or if the contract terms are disputed.

The Indian legal system may need to adapt by introducing specific provisions or amendments to the Indian Contract Act, 1872, to accommodate AI’s role in contract formation and execution. These changes could involve setting standards for AI transparency, ensuring human oversight, and establishing guidelines for the enforceability of AI-drafted contracts.

d. *Finance*

Reserve Bank of India (RBI) Guidelines: The RBI provides guidelines on electronic banking, data protection, and cybersecurity, which could extend to AI-driven financial services.

SEBI (Securities and Exchange Board of India) Regulations: SEBI’s guidelines on algorithmic trading are relevant to AI applications in stock markets.

e. *Education*

National Educational Policy 2020: The policy document underscores the importance of integrating AI into educational curricula, starting from schools to higher education institutions, to equip future generations with necessary AI skills. Additionally, it highlights the need for continuous professional development, ensuring that the existing workforce can effectively apply AI technologies in diverse sectors.

f. *Transport*

Motor Vehicles Act, 1988 (MV Act): This act governs all aspects of road transport vehicles and could potentially cover AI applications in autonomous vehicles and traffic management systems. The government has not come up with any kind of guidelines or rules for self-driving cars. The MV Act establishes ‘No Fault’ liability under Section 140, holding vehicle owners liable for compensation in cases of death or permanent disablement. Section 184 mandates imprisonment for the owner for up to two years for speeding or dangerous driving. However, in accidents involving self-driven cars, the question arises whether ‘No Fault’ liability should apply140 prescribes compensation amounts, but in *Haji Zakaria v. Naoshir Cama*, the Supreme Court ruled that liability cannot be imposed on the owner without negligence. For self-driven cars, negligence would likely lie with the manufacturer, not the owner, shifting the liability accordingly.

g. *E-commerce.*

Consumer Protection Act (E-commerce Rules,) 2020: These rules aim to protect consumer rights and could apply to AI-enabled e-commerce platforms and services.

h. *Intellectual Property*

Patents Act, 1970: This act governs the patenting process in India. As of now, AI cannot be considered an inventor under Indian law, as Sections 2 and 6 of the Patents Act 1970 require inventors to be natural or juridical persons.

Copyright Act, 1957: This act protects original literary, dramatic, musical, and artistic works, among others. As of now, AI is not considered an author under Indian law, as Sections 2(d) and 13(1)(a) of the Indian Copyright Act, 1957, require authors to be natural persons and works to be original, though work created by AI can be considered original.

i. *Bureau of Indian Standards.*

A committee on AI has been constituted by the Bureau of Indian Standards, the national standards body of India, and is proposing draft Indian Standards for AI. It is anticipated that the much-awaited Digital India Act will address the use and misuse of AI specifically.

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?

While defective AI systems or products may lead to significant harm, India currently does not have specific laws addressing them. Nonetheless, existing legal frameworks, including the Consumer Protection Act, Information Technology Act, 2000 (IT Act), contract law, and tort law, provide mechanisms to address these issues effectively.

These laws offer a foundation for holding parties accountable and ensuring the safety and reliability of AI technologies. Defective AI may lead to data breaches, compromising the information it holds, and, in such cases, the IT Act addresses issues related to cybersecurity, data protection, and digital transactions. It provides a legal framework for governance and penalties for cybercrimes, indirectly influencing AI deployment, especially concerning data handling and cybersecurity. Section 87 of the IT Act provides the central government with the power to make rules and regulations to carry out the provisions of this Act.

In addition to the above, if an AI system functions in the capacity of an intermediary, then the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, lay down the duties of an intermediary and provide for the due diligence required to be conducted by the intermediaries, including social media intermediaries.

The advisory referred to earlier also lays down some precautionary measures for intermediaries to protect users against defective AI systems. It states that intermediaries and platforms must ensure that their AI models, LLMs, generative AI, software, or algorithms do not enable users to share unlawful content as specified in Rule 3(1)(b) of the IT Rules or violate the IT Act 2000 and other laws. They must also ensure these technologies do not introduce bias, discrimination, or compromise electoral integrity. It also states that under-tested or unreliable AI models should only be made available in India with accurate labeling of generated outputs. Further, users must be informed via terms of service and user agreements about the consequences of dealing with unlawful information, including access restrictions, account suspension, and legal penalties. Intermediaries must ensure that their products have labels or embedded metadata in any AI-generated or modified content that could be used as misinformation or deepfakes, enabling the identification of responsible users or computer resources.

Non-compliance with the IT Act 2000 and IT Rules may result in prosecution for intermediaries, platforms, and users under the provisions of the IT Act as well as the Indian Penal Code, 1860, or the new Bharatiya Nyaya Sanhita, 2023. The IT Act does impose penalties for damage to computers, computer systems and tampering with source code.

If the result of a defective AI leads to an injury to a person, then the maker of the AI may be held liable under Section 106 of the BNS (Section 304A of the IPC for rash and negligent act), or any other provision of the said laws based on the nature of the injury or harm. The AI may also be liable to the injured on the basis of tort law.

Other than these, a consumer of a defective AI system can file a complaint under Section 35 of the Consumer Protection Act, 2019.

In addition to the aforementioned, depending on the type of harm, several current laws may also apply to AI (summarized above) and its applications in a variety of industries, including cybersecurity, healthcare, law, finance, education, transport, and e-commerce.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems.

In India, AI systems are not recognized as legal persons and cannot be held liable for harm in the same way humans or corporations can. Legal personhood is associated with individual autonomy, which AI lacks due to its reliance on programmed inputs. Consequently, liability is generally assigned to the entities behind the AI, such as developers, users, or owners. Globally, AI is not considered a separate legal entity because it cannot function independently like a human and operates strictly according to its programming. Additionally, AI cannot be punished independently, so the responsibility falls on the human entities controlling it.

As already mentioned, a breach of contract made for the sale or purchase of goods, including A-enabled product or system under the Indian Contract Act, 1872, will result in civil liability. While any offence committed or any act carried out in furtherance of malicious intentions utilising any AI-enabled system or product will attract criminal liability under the Bharatiya Nyaya Sanhita, 2023. Further, the Digital Personal Data Protection Act, 2023 when enforced, will ensure that any non-compliance with the law will result in breach of security and data. At present, the IT Act, 2000, is the primary legislation in India dealing with cybercrime and various means of electronic communication.

Liability for AI can be broadly categorized into criminal and civil liability. Criminal liability requires both *mens rea* and *actus reus*. For AI, *mens rea* is typically attributed to the developer, making them liable for the AI's actions. Developers can also be held accountable if harm caused by AI is a foreseeable consequence of their programming or result of inadequate safeguards. Under tort law, the principle of strict liability applies, especially when the AI operates autonomously, as developers control its design and functionality.

Computer resources utilising AI tools have made the commission of various crimes effortless, and therefore, the following provisions under the IT Act proscribe and penalises the following offences:

a. Punishment for identity theft (Section 66C).
b. Punishment for cheating by personation by using computer resources (Section 66D).
c. Punishment for violation of privacy (Section 66E).
d. Punishment for cyberterrorism (Section 66F).
e. Punishment for publishing and transmitting obscene material in electronic form (Section 67).
f. Punishment for publishing and transmitting material containing sexually explicit acts, etc., in electronic form (Section 67A).
g. Punishment for publishing or transmitting material depicting children in sexually explicit acts, etc., in electronic form (Section 67B).

Users may also bear liability, particularly if they misuse AI or ignore operational guidelines, especially when harm results directly from such misuse. Victims harmed by AI can seek redress under consumer protection laws, filing complaints against manufacturers or service providers for defective AI products. This framework supports holding developers or manufacturers accountable for damages caused by AI products, incorporating principles of strict and vicarious liability.

Civil liability, in the form of damages or compensation, can be imposed alongside criminal penalties. In some cases, under the doctrine of contributory negligence, victims (often users) can be held partially liable if they fail to use AI as prescribed. The allocation of liability depends on the specific circumstances of each case, and currently, India lacks specific legislation to definitively assign liability to a particular person or entity. Generally, developers or programmers are considered primarily liable, with users or victims being liable only in rare instances.

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

Currently, laws that could be applied for harms arising out of AI in India include the Information Technology Act of 2000, the Digital Personal Data Protection Act of 2023 when enforced, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, Consumer Protection Act of 2019, Bharatiya Nyaya Sanhita of 2003, tort principles, etc. However, none of them deal directly with artificial intelligence and the corresponding allocation of liability for harm caused by an AI system.

While no legal system in the world has recognized AI either as a legal entity or a juristic person, the harm caused by AI may be attributed to the entities behind the AI, which are legal or juristic persons that may bear the liability (e.g. Corporate Criminal Liability) such as the owners, developers, users, etc.

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

In India, the burden of proof for a victim seeking compensation for damages caused by artificial intelligence (AI) systems involves several critical factors and legal principles. When it comes to the Consumer Protection Act 2019, Section 2(6)(vii) attributes liability to the product manufacturer in product liability actions. The Act does not mention anything about AI; however, AI product manufacturers can be held liable if their product exhibits manufacturing defects, design flaws, deviations from specifications, lack of adequate instructions, or warranty non-compliance. This places the burden of proof on AI manufacturers to ensure product safety and quality, irrespective of their negligence or fraudulent intent in providing warranties.

Although there is no specific AI liability framework in

India yet, general legal principles and emerging regulations can provide guidance. Here are the key aspects a victim must satisfy to obtain compensation:

a) *Establishing Causation.* The victim must demonstrate a clear causal link between the AI system's actions and the damage suffered. This involves showing that the AI system directly caused the harm, and that the damage would not have occurred without the system's actions.

b) *Demonstrating Harm or Loss.* The victim must provide evidence of the actual harm or loss suffered due to the AI system's actions. This could include physical injury, financial loss, emotional distress, or other quantifiable damages.

c) *Breach of Contract.* In cases where the AI system was used as part of a contractual arrangement, the victim might need to show that there was a breach of contract terms. This includes demonstrating that the AI system failed to perform as promised or that the responsible party did not fulfill their contractual obligations related to the AI system's deployment and operation.

d) *Strict Liability in Certain Contexts.* In some scenarios, especially those involving hazardous or inherently dangerous activities, strict liability principles might apply. Here, the victim does not need to prove negligence but simply that the AI system caused the harm. This is more likely in cases involving significant public safety risks or where statutory regulations impose strict liability.

e) *Expert Testimony and Technical Evidence.* Given the complex nature of AI systems, victims may need to present expert testimony and technical evidence to explain how the AI system operates, where it malfunctioned, and how it caused the damage. This could involve detailed technical analysis, forensic investigation, and expert witness statements.

To obtain an appropriate remedy for damages caused by an AI system, the victim must establish liability by proving the existence of a defect, causation, and actual harm. This involves gathering substantial evidence, potentially including expert testimony, to meet the burden of proof.

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

While there is no specific insurance policy exclusively for AI, various existing insurance products can be tailored to cover the risks associated with AI. Here's an overview:

a. ***Cyber Insurance.***

Applicability. Covers risks associated with data breaches, cyber-attacks, and other digital risks that AI systems may be susceptible to.

Coverage. Data breaches and losses; Network security liability; Cyber extortion; Business interruption due to cyber incidents; Legal and regulatory expenses.

b. ***Professional Liability Insurance (Errors & Omissions Insurance).***

Applicability. Relevant for AI developers, vendors, and service providers to cover claims arising from errors, omissions, or negligence.

Coverage: Claims of negligence or failure to perform; Legal defense costs; Settlements and judgments.

c. ***Product Liability Insurance.***

Applicability. Covers manufacturers and sellers of AI systems against claims of injury or damage caused by their products.

Coverage: Bodily injury or property damage caused by a defective AI product; Legal defense costs; Compensation for damages.

d. ***Technology Errors & Omissions Insurance.***

Applicability. Designed specifically for technology companies, including those developing AI systems.

Coverage: Claims related to technology services provided; Software failures; Breach of contract or performance disputes.

e. ***General Liability Insurance.***

Applicability. Provides broad coverage for businesses, including those deploying AI in their operations.

Coverage: Bodily injury; Property damage; Personal and advertising injury; Legal defense costs.

f. ***Directors and Officers (D&O) Insurance.***

Applicability. Protects company executives from personal losses if they are sued for wrongful acts while managing a company, including decisions related to AI deployment.

Coverage: Legal defense costs; Settlements and judgments; Regulatory investigations.

The following may be seen as challenges in Insuring AI, namely,

Uncertainty and Risk Assessment: The dynamic and complex nature of AI makes it difficult to assess risks accurately.

Lack of Historical Data: Insurers rely on historical data to price policies and predict risks, which is limited for AI technologies.

Rapid Technological Change: AI technologies evolve quickly, potentially outpacing the ability of insurers to keep policies updated.

Complex Liability Issues: Determining liability in AI-related incidents can be complex due to the involvement of multiple stakeholders (developers, users, etc.).

The following are perceived as future trends:

Customized AI Insurance Products: Insurers are likely to develop more tailored products to address specific AI risks as technology becomes more prevalent.

Regulatory Developments: Emerging regulations and standards for AI will influence insurance offerings and risk assessments.

Collaborations with Tech Firms: Insurers may partner with AI companies to better understand the technology and develop appropriate coverage solutions.

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

The Patent Act of 1970 governs the granting of patents in India. Sections 2 and 6 of this Act detail the criteria for recognizing an inventor and the qualifications for an applicant filing for a patent within Indian jurisdiction. According to Section 6, a patent application can be filed by any person who is the true and first inventor of an invention or by an assignee of such a person. Additionally, Section 6(1)(c) specifies that if the inventor has passed away, their heirs or legal representatives are also eligible to apply for a patent. The term ‘person’ in Section 6 encompasses both natural persons (individual humans) and juridical persons (entities such as corporations, firms, and government agencies).

In 2019, more than a dozen countries, including India, received two patent applications listing DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) as the inventor. These applications, filed under the name of Dr. Stephen Thaler, a natural person, claimed that DABUS independently conceived two distinct inventions without human assistance. Consequently, DABUS was listed as the inventor on the patent applications for both inventions.

In India, the Controller General of Patents objected to DABUS in the patent application. The objection, detailed in the Examination Report, cited Sections 2 and 6 of the Patents Act 1970, noting that DABUS cannot be recognized as a person. Consequently, the application failed to pass the formal and technical reviews. This stance is supported by legal precedents, including *V.B. Mohammed Ibrahim v. Alfred Schafranek* (AIR 1960 Mys. 173), where the court ruled that only a natural person who directly contributes their skill and knowledge to an innovation can be legally recognized as an inventor, excluding entities like corporations or financing partners.

In the case of *Som Prakash Rekhi v. Union of India & Anr* (AIR 1981 SC 212), the Hon’ble Supreme Court of India clarified the definition of a “person” in legal terms. The court determined that a juridical person is an entity recognized by law as having legal personality, which includes the right to sue or be sued. An AI, by its nature, lacks the capacity to exercise such legal rights or fulfill the duties of a legal entity independently.

Since AI is not recognized as a legal person, it is unlikely that Indian courts will recognize AI as an applicant for a patent.

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?

Currently, as the regulations and jurisprudence stand in India, AI-generated works do not enjoy the protection of copyright. The requirement of personhood and originality restricts the ability of AI-generated work to get copyright protection.

Section 2(d)(vi) of the Indian Copyright Act, 1957 (Copyright Act) states that the author of a computer-generated work is the person who causes the work to be created. According to this section, the input giver or generator of outputs, even in cases of recent forms of AI software, could be interpreted to include works of Generative AI. However, the Copyright Act determines ownership based on authorship. The jurisprudence behind this attribution is that the concept of intellectual property or copyright is evolving as a law to incentivize creativity so that there are more creative works on the market. For this purpose, the first owner of copyright is always the author (Section 17, Copyright Act, 1957; Rupendra Kashyap v. Jiwan Publishing House, 1996 (38) DRJ 81).

Also, under the current Rules, the application for copyright registration (Form-XIV) requires disclosure of the Applicant's name, nationality and address. However, on a rare occasion, one Mr. Ankit Sahni used a software created by himself that generated paintings based on certain inputs. With the help of this generative AI technology, he created a painting called 'Suryast'. In this, the AI tool was initially considered a co-author. This was subsequently revoked by the Copyright Office on the grounds that the Copyright Act provides that only natural persons or humans can be copyright owners as per Section 2(d) of the Copyright Act.

In addition to the requirement of personality or personhood for applying for copyright, Section 13(1)(a) of the Copyright Act lays down that copyright subsists in "original" work. Although the term originality is ambiguous, the Supreme Court of India in *Eastern Book Company vs. D.B. Modak* ((2008) 1 SCC 1) has laid down the thresholds for originality. It is a combination of the sweat of the brow doctrine and the modicum of creativity theory.

The 161st report of the Parliamentary Standing Committee titled, "Review of the Intellectual Property Rights in India, conducted two years ago to assess the Indian Intellectual Property Rights system, advocated for establishing a new category of rights tailored for Artificial Intelligence and related technologies. It was noted that neither the Indian Patents Act, 1970, nor the Copyright Act, 1957, are well equipped to facilitate inventorship, authorship, and ownership by Artificial Intelligence. It was recommended that a separate category of rights for AI and AI-related inventions and solutions be created for their protection as IPRs. It was also recommended that the existing legislation of the Patents Act, 1970, and the Copyright Act, 1957, be revisited to incorporate the emerging technologies of AI and AI-related inventions into their ambit.

11. What are the main issues to consider when using artificial intelligence systems in the workplace?

When implementing AI systems in the workplace, several key issues must be carefully considered to ensure ethical, legal, and practical implications are addressed effectively. Here are some main issues to consider:

a. *Data Privacy and Security:* AI systems often rely on vast amounts of data, including sensitive employee information. Ensuring compliance with data protection laws and implementing robust security measures to protect employee data from unauthorized access or breaches is essential.

b. *Algorithmic Bias and Fairness:* When AI is used for the process of interviewing, or any situation where the AI has to make a selection, then AI algorithms can unintentionally perpetuate biases present in training data, leading to unfair treatment of certain groups of employees. It is crucial to address algorithmic bias through careful selection of training data, algorithm design, and regular monitoring for biases.

c. *Transparency and Explainability:* Employees should understand how AI systems make decisions that affect them. Ensuring transparency and explainability in AI algorithms can help build trust and mitigate concerns about AI-driven decision-making processes.

d. *Job Displacement and Reskilling:* The deployment of AI systems may lead to job displacement as certain tasks become automated. Employers must consider the impact on employees and invest in reskilling and upskilling initiatives to prepare them for new roles or tasks created by AI adoption.

e. *Worker Surveillance and Privacy:* AI-enabled workplace monitoring tools, such as employee performance tracking or behavior analysis systems, raise concerns about privacy invasion and surveillance. Balancing the benefits of monitoring with respect for employee privacy rights is essential for maintaining trust and morale.

f. *Ethical Use of Data:* Employers must establish clear guidelines for the ethical collection, use, and retention of data by AI systems. This includes obtaining informed consent, limiting data collection to relevant purposes, and avoiding discriminatory practices.

g. *Legal and Regulatory Compliance:* Adhering to applicable laws and regulations governing AI use in the workplace is paramount. This includes compliance with labor laws, anti-discrimination laws, and data protection regulations such as the DPDP Act or relevant local laws.

h. *Accountability and Liability:* Clarifying accountability for AI-driven decisions and establishing mechanisms for addressing errors or biases is essential. Employers should define roles and responsibilities for overseeing AI systems and addressing complaints or disputes arising from their use.

i. *Unintended Consequences and Risk Management:* Assessing potential risks and unintended consequences of AI deployment is essential. Employers should conduct thorough risk assessments, develop mitigation strategies, and regularly monitor AI systems' performance to identify and address issues proactively.

It is expected that the anticipated Digital India Act will address biases arising due to AI algorithms specifically. Employers must ensure any AI tools used for any purpose within the organisation do not raise ethical concerns under the provisions of the Digital India Act once enforced. AI tools and systems can be used by employers merely as a directional tool, but they should not form the basis of conclusive decisions taken by the employers.

12. What privacy issues arise from the use of artificial intelligence?

The use of AI presents significant privacy challenges, including extensive data collection, a lack of transparency, data security risks, algorithmic bias, and compliance with varying regulations. This raises several privacy issues, particularly concerning the collection, processing, and use of personal data. Some key privacy concerns associated with AI are:

a. *Data Collection and Surveillance.*

Extent of Data Collection: AI systems often require vast amounts of data to function effectively, which can lead to extensive collection of personal information.

Surveillance: AI technologies, such as facial recognition and behavior tracking, can enable widespread surveillance, potentially infringing on individuals' privacy.

b. *Data Processing and Usage.*

Unintended Use of Data: Data collected for one purpose may be repurposed for another without individuals' consent, raising ethical and legal issues.

Profiling and Targeting: AI can create detailed profiles of individuals, which can be used for targeted advertising, personalized content, or even discriminatory practices.

c. *Data Security.*

Data Breaches: AI systems are vulnerable to cyberattacks, which can lead to unauthorized access to sensitive personal data.

Insufficient Security Measures: As AI systems become more complex, ensuring robust security measures to protect data can be challenging.

d. *Lack of Transparency.*

Opacity of AI Algorithms: AI systems, especially those using machine learning, often operate as "black boxes," making it difficult to understand how decisions are made and whether personal data is used appropriately.

Informed Consent: Individuals may not be fully aware of or understand how their data is being used by AI systems, making informed consent difficult to obtain.

e. *Bias and Discrimination.*

Algorithmic Bias: AI systems can perpetuate and even exacerbate existing biases if the data they are trained on is biased, leading to discriminatory outcomes.

Fairness: Ensuring that AI systems make fair and unbiased decisions is a significant challenge, especially when they process personal data for critical decisions such as hiring, lending, or law enforcement.

f. *Anonymity and Re-Identification.*

De-Anonymization: AI's ability to analyze large datasets increases the risk of re-identifying individuals from anonymized data, compromising their privacy.

Linkage Attacks: Combining data from different sources can lead to the re-identification of individuals who were meant to remain anonymous.

g. *Compliance with Data Protection Laws.*

Adherence to Regulations: AI systems must comply with existing data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and India's Personal Data Protection Bill (once enacted).

Cross-Border Data Transfers: AI systems that transfer personal data across borders must navigate varying international privacy laws, complicating compliance efforts.

h. *Ethical Considerations.*

Autonomy and Control: The extensive use of AI in personal data processing raises questions about individuals' autonomy and control over their personal information.

Moral Responsibility: Determining who is responsible for ensuring ethical AI use and addressing privacy issues is complex, involving developers, users, and regulators.

13. How is data scraping regulated in your jurisdiction from an IP, privacy and competition

point of view?

Any act of data scraping without the owner's permission constitutes an infringement.

From a privacy perspective, in India, this practice is currently unregulated, with neither the Information Technology Act, 2000, nor the SPDI Rules explicitly addressing or restricting data scraping activities. Most websites in India either prohibit scraping altogether or require prior permission from the website owners. It is crucial for individuals or companies that are collecting data to respect these terms and conditions, as they are legally binding in India. Even without explicit user consent, Indian law generally recognizes electronic contract acceptance methods like click-wrap and browse-wrap agreements as valid.

From a data protection standpoint, the SPDI Rules do not regulate data scraping, nor do they provide specific exemptions. People engaged in data scraping are required to obtain consent when using sensitive personal data. If a collaborative approach is adopted, this liability could potentially be transferred to the website owners. Under the upcoming DPDP Act, data scraping could be interpreted as legal and unregulated if it involves publicly available personal data, thereby exempting such activities from the stringent requirements of the DPDP Act, including privacy notices and data subject rights.

From a competition perspective, any enterprise with a vast amount of data will quickly gain a dominant position in the market. AI/ML is trained on these data sets which further amplifies the market strength of these enterprises. Currently, in India, neither the Competition Act, 2002, nor any other existing law addresses data scrapping activities. The Competition Act, 2002, lists out factors to determine whether an enterprise holds a dominant position in the relevant market.

However, the Government established a Committee on Digital Competition Law, which released a draft Bill in its report. The Committee recommended a comprehensive ex-ante model of competition law to address issues in digital markets. The bill primarily addresses certain features that enable digital enterprises to gain influence in the market. These include: (i) collection of user data, which can allow large incumbent enterprises to enter related markets, (ii) network effects, where the utility of a service increases when the number of users consuming it increases, and (iii) economies of scale, wherein incumbents can offer digital services at lower costs as compared to new entrants.

Subject to the above features, the Committee recommended the designation of Systematically Significant Digital Enterprises (SSDEs) for ex-ante regulation, which may lead to market concentration. The committee further recommended that, apart from the qualitative threshold, the criteria to designate enterprises as SSDEs should be inclusive of enterprise resources and the volume of data aggregated by them.

While data scraping may be regulated under the recommended draft bill in terms of the volume of data aggregated by them to be designated as SSDEs, the fruition of these recommendations is still awaited.

In summary, while the copyright laws do provide some respite, data scraping, in India, is not explicitly regulated. Those involved in data scraping must carefully adhere to website terms and conditions and consider collaborative strategies to ensure legal compliance and minimize liability.

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

A robust 'Terms of Use' of a website, which clearly states the fair use of the content posted on it, is mandatory from the owner's perspective. The Terms of Use of a website create a declaration of a guardrail for 'contractual and legal enforcement' in instances of misuse. If a website's terms of use prohibit downloading content from the website and the visitor or end-user chooses to retrieve data from that website, the user will be in direct breach of the deemed agreement with the entity that owns the website and shall face legal consequences.

A terms of use essentially notifies the liability of the visitor. It also often displays other information about website ownership and copyright to help protect a website's content. These terms of use create protection and legal obligations that inform visitors of the owner's protection by law under the copyright, trademark, patent, trade secret or other intellectual property laws and the content's "permitted use."

Data scraping stealthily mines or collects data from websites. This activity becomes a lot more concerning when the data scraping program gathers confidential information about an entity to gain a competitive, malicious, or illegal advantage that would amount to misappropriation by way of industrial surveillance.

Though there is no specific legislation governing data scrapping, for any such malicious activity by a user, the owner can seek appropriate relief under the Digital

Personal Data Protection Act of 2023 read with the Information Technology Act, 2000, and the various IP laws of the country.

The terms of use ban the purposeful release of malware on the website, bots, and unauthorised clawers from accessing a website. Websites with user interactions usually also attempt to ban spamming or other malicious user activity, often considered abuse.

The terms of use are legally binding and they reduce the website's exposure by creating prohibitive legal and contractual enforcement of the liability of its user(s); nevertheless, the owner must also take definitive technical measures to safeguard the content and information posted on the website, rather than only relying on contractual and legal enforcement once the breach is already done.

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

The regulatory landscape concerning AI in India is evolving, with significant legal developments anticipated in the coming years. However, the establishment of the Data Protection Board of India under the Digital Personal Data Protection Act, 2023, is a crucial step towards addressing concerns related to data protection in the context of AI. There is a strong belief among industry experts that the Data Protection Board might be constituted in the coming months.

a. *Reports and Strategies by NITI Aayog.*

National Strategy for Artificial Intelligence: This document outlines the government's approach to AI, including ethical considerations, data privacy, and the need for a robust regulatory framework.

Recommendations for Responsible AI: The strategy emphasizes responsible AI practices, including fairness, transparency, and accountability, which indirectly address privacy concerns.

b. *MeitY's Role.*

The Ministry of Electronics and Information Technology (MeitY) has been involved in AI and data governance, offering guidelines that impact AI indirectly:

AI Committees and Reports: MeitY has constituted committees on AI that have released reports, such as the 'Report of Committee-B on Leveraging AI for Identifying National Missions in Key Sectors', which include recommendations on ethical AI deployment and privacy considerations.

c. *Key Considerations in These Initiatives.*

Data Privacy and Security: Emphasis on securing personal data and protecting it from unauthorized access or breaches, which is crucial for AI systems handling sensitive information.

Informed Consent: Ensuring that AI systems comply with regulations on informed consent, providing users with clear information about data collection and usage.

d. *Transparency and Accountability:* Encouraging transparency in AI operations and establishing accountability mechanisms for AI-related decisions and data processing activities.

e. *Bias and Fairness:* Addressing the need for AI systems to be free from bias and discrimination, promoting fair and equitable use of AI technologies.

f. *Future Directions.*

While specific guidelines for AI are still being developed, the convergence of data protection regulations and AI ethics suggests that more detailed and focused guidelines are likely to emerge as the AI landscape evolves. The implementation of the Personal Data Protection Bill, along with ongoing work by NITI Aayog and MeitY, indicates a growing recognition of the need to address AI-specific privacy issues.

16. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence?

Currently, the establishment of the Data Protection Board of India, as mandated by the Digital Personal Data Protection Act, 2023, is pending, awaiting constitution by the Central Government. Therefore, there is no designated privacy authority tasked with overseeing matters concerning artificial intelligence (AI) and its implications on privacy within the jurisdiction, though the Indian Computer Emergency Response Team (I-CERT) keeps a close watch on matters concerning breaches and has mandated reporting of the incidents within 6 (six) hours of the alleged breach.

17. Have your national courts already managed cases involving artificial intelligence?

There are cases being adjudicated by Indian courts, that relate to the use of AI. Recently, a famous Indian Bollywood actor, Anil Kapoor, filed a case against certain companies that were using technological tools such as AI and machines learning to create deep fakes of his image and voice, morphing his face onto videos that were obscene. In this case, the Delhi High Court issued an injunction against these parties to stop using AI and other tools to hamper the image of Mr. Anil Kapoor and make a commercial gain out of it (Anil Kapoor v. Simply Life India before the Hon'ble High Court of Delhi CS(COMM) 652/2023).

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

As of today, India does not have a specific regulator or authority dedicated solely to supervising the use and development of AI. However, various government bodies may have jurisdiction over certain aspects of AI regulation and oversight.

a. *Ministry of Electronics and Information Technology (MeitY):* MeitY is the primary government agency responsible for formulating and implementing policies related to electronics, IT, and the internet in India. While it does not specifically focus on AI, it plays a significant role in promoting digital technologies, including AI, through initiatives such as the National AI Portal.

b. *NITI Aayog:* NITI Aayog, the National Institution for Transforming India, serves as a policy think tank of the Government of India. It has launched various initiatives related to AI, such as the National Program on AI and the Responsible AI for Youth program. While NITI Aayog's primary focus is on policy formulation and promoting AI adoption, it does not have regulatory authority.

c. *Data Protection Board of India:* India is in the process of establishing a Data Protection Board under the Digital Personal Data Protection (DPDP) Act, which aims to regulate the processing of personal data in India. While the primary focus of the Board is on data protection, it may have some oversight regarding AI systems' handling of personal data.

d. *Sectoral Regulators:* Certain sectors, such as finance and telecommunications, have their own regulatory bodies that may have jurisdiction over AI applications within their respective domains. For example, the Reserve Bank of India (RBI) regulates AI applications in finance, and the Telecom Regulatory Authority of India (TRAI) may oversee AI use in telecommunications.

19. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited?

In India, the use of AI by businesses is increasing rapidly, with significant adoption across sectors such as IT and technology, finance and banking, e-commerce and retail, healthcare, and manufacturing. Companies in India leverage AI for various applications, including software development, fraud detection, personalized marketing, diagnostic tools, and production automation. Emerging areas like agriculture, education, and transportation are also seeing growing interest in AI solutions for precision farming, personalized learning, and route optimization.

However, challenges such as inadequate digital infrastructure, a shortage of skilled professionals, evolving regulatory frameworks, and data privacy concerns can limit AI adoption. The Indian government supports AI development through initiatives like the National AI Strategy, AI research centers, and public-private partnerships that provide funding and collaboration opportunities. Despite these challenges, the trend leans towards greater AI adoption and innovation in Indian businesses.

20. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how?

Answer: On May 23, 2023, the Supreme Court of India, called participants to bid for a "Design, Development, and Implementation of Artificial Intelligence (AI) Solution, Tools for Transcribing Arguments, and Court Proceedings at the Supreme Court of India." The main purpose of the bidding was to give a transcript of the arguments, to make a true court of record. This is on a trial basis, where AI tools are used to transcribe the arguments, and it is proofread later. Although the implementation of this has been slow, this is a step in the right direction. The Supreme Court of India also developed a software called "Supreme Court Vidhik Anuvaad Software" (SUVAS), which is a machine assisted translation tool trained by Artificial Intelligence. It is specifically designed to translate judicial documents, orders, and judgements into 10 other vernacular languages (https://pib.gov.in/PressReleasePage.aspx?PRID=1947490).

However, the courts are hesitant to rely on chatbots for the purpose of evidence. For example, in the case of

Christian Louboutin v. Shutiq, the Delhi High Court (2023 SCC OnLine Del 5295) observed that chatbots or AI tools cannot be the basis for adjudication of factual issues in a court of law. The information generated by these chatbots is dependent on a host of factors, including the nature and structure of the query put in by the user, the training data, *etc*. It was further observed that there are possibilities of incorrect responses, fictional case laws, imaginative data, etc.

21. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

AI presents significant challenges for lawyers in terms of regulatory uncertainty, technical complexity, liability issues, data protection, and algorithmic fairness. However, it also offers substantial opportunities for innovation in legal practice, new specializations, improved access to justice, enhanced due diligence, and expanded advisory services. Some of the key challenges may be summarized as follows:

a. *Limited Understanding of Legal Nuances:* AI systems often struggle with complex legal terminology and intricate interpretations. This can lead to inaccuracies and misinterpretations, making human oversight crucial to ensuring accurate legal advice and decision-making.

b. *Ethical Implications and Potential Bias:* AI systems may perpetuate biases present in training data, raising ethical concerns about fairness and transparency. Lawyers must ensure AI decisions are unbiased and navigate the ethical challenges AI presents, as AI lacks the capacity for moral judgments.

c. *Data Privacy and Security Risks:* AI requires access to vast amounts of sensitive data, raising concerns about client confidentiality, data retention, regulatory compliance, and potential data breaches. The legal ramifications of relying solely on AI to handle such sensitive information add to these risks.

d. *Lack of Human Empathy and Sensitivity:* Lawyers provide not just legal counsel but also emotional support and guidance to clients. AI lacks the ability to replicate genuine human emotions and empathy, which are crucial for building strong client-attorney relationships.

e. *Risk of Liability in Complex Legal Procedures:* Legal proceedings involve tasks beyond research and analysis, such as negotiation, mediation, and trial advocacy. AI systems may not handle these complex tasks effectively, and if an AI system provides inaccurate advice or fails to identify essential legal implications, law firms could face serious repercussions.

22. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months?

In the Indian jurisdiction, significant legal developments in artificial intelligence (AI) over the next 12 months are expected to revolve around the establishment of regulatory frameworks and guidelines addressing AI governance, ethics, and liability. With the pending formation of the Data Protection Board of India and the evolving landscape of data protection laws, including the Digital Personal Data Protection Act, 2023, there is anticipation for specific provisions addressing AI-related data processing, privacy, and accountability. Additionally, legal precedents may emerge from court cases involving AI technologies, shaping liability standards and legal responsibilities for AI developers, operators, and users. Moreover, advancements in AI technology and its integration into various sectors may prompt lawmakers to adapt existing regulations or introduce new legislation to address emerging challenges and ensure ethical and responsible AI deployment.

In addition to the foregoing discussions, in the next 12 months, several significant legal developments related to AI are expected to emerge in India.

a. *Regulatory Framework for AI:* A committee on AI has been constituted by the Bureau of Indian Standards, the national standards body of India, and is proposing draft Indian Standards for AI. It is anticipated that the much-awaited Digital India Act will address the use and misuse of AI specifically.
b. *Data Protection and Privacy Laws:* The Digital Personal Data Protection Act, 2023, mandates stringent compliance and penalises data breaches resulting from any non-compliance by the Data Fiduciary, and the same is expected to be implemented in the next 12 months.
c. *Ethical Guidelines for AI Use:* Stakeholders in India, including legal professionals, policymakers, and industry bodies, are expected to develop and promote ethical guidelines for the responsible use of AI. These guidelines may address issues such as algorithmic transparency, fairness, accountability, and the ethical implications of AI-driven decision-making in legal contexts.
d. *Case Law and Precedents:* As AI technologies continue to be integrated into various aspects of legal

practice, there may be notable developments in case law and judicial precedents related to AI. Legal disputes and regulatory challenges arising from AI applications in areas such as intellectual property, liability, privacy, and consumer protection may shape the legal landscape and provide guidance for future cases.

e. *Industry-Specific Regulations:* Certain sectors, such as healthcare and finance, may see sector-specific regulations or guidelines addressing the use of AI technologies.

Contributors

Rajesh Vellakkat **Partner**	rajesh.vellakkat@foxmandal.in	
Gaurav Sahay **Practice Head**	gaurav.sahay@foxmandal.in	
Akshay Nair **Associate**	akshay.nair@foxmandal.in	
Sanjana S. **Associate**	sanjana.s@foxmandal.in	
Kiran Patel **Associate**	kiran.patel@foxmandal.in	
Ashita Sahay **Legal Associate**	ashita.sahay@foxmandal.in	