



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

BEYOND ALGORITHMS: REIMAGINING THE LEGAL ARCHITECTURE OF ARTIFICIAL INTELLIGENCE IN INDIA

~ *Mahek Thacker*

1. ABSTRACT

India has seen rapid growth in artificial intelligence (AI) in both public and private sectors, but the legal system has not kept up. Currently, India uses a mix of laws and policies to handle AI-related risks. For instance, the Information Technology Act 2000 and the Indian Penal Code address cybercrimes, deepfakes, and AI-driven fraud, while the Digital Personal Data Protection Act 2023 (DPDP Act) outlines broad data protection requirements.

This paper examines the legal situation surrounding AI in India. We analyze legislation, court rulings, and policy reports to explore how current laws apply to AI and their shortcomings. Academic literature frequently points out regulatory gaps and underscores the need for specific AI-related regulations. We also look into recent initiatives, including NITI Aayog's AI strategy, Supreme Court white papers on AI, and DPIIT's working paper on AI and copyright, to evaluate India's policy response.

Our findings indicate an urgent need for dedicated AI legislation in India. A clear framework should establish transparency and accountability, define liability and authorship, and balance innovation with protecting fundamental rights. This article consolidates legal sources and expert advice to assist policymakers in shaping India's AI governance according to national priorities and international standards.

2. INTRODUCTION

India has rapidly adopted AI in areas like healthcare, finance, agriculture, law enforcement, and the judiciary. Projects like the e-Courts Project and AI-enhanced financial services highlight AI's potential for efficiency. However, experts caution that the legal and regulatory

framework has not evolved to keep pace. Unlike other jurisdictions considering an EU-style AI Act, India has not created a separate AI law. Instead, regulators rely on existing laws and fragmented guidelines. For example, NITI Aayog's 2018 strategy pushed for AI ("AI for All") but did not establish new legal responsibilities. The courts have begun to react: in late 2025, the Supreme Court published a white paper on AI in the judiciary, stressing that judges must verify all AI outputs. The Court has ruled that referencing AI-generated fake case law counts as judicial misconduct.

This fragmented approach raises essential questions: Who is responsible when AI causes harm? How can we protect privacy when AI systems process vast amounts of data? Can works created by AI be copyrighted or patented under current Indian law? Overall, India's dependence on outdated laws creates uncertainties regarding liability, data rights, algorithm fairness, and evidence reliability. This paper outlines these issues by integrating current research and official documents to suggest a way forward.

3. LITERATURE REVIEW

3.1 REGULATORY FRAGMENTATION

Scholars consistently highlight that India lacks a comprehensive AI law. Governance is scattered through the IT Act 2000, which addresses cyber offenses and data breaches, sector-specific rules, and policy documents. For instance, Satarkar (2026) and Suraj (2025) note that current statutes "only partially cover" AI issues, leading to regulatory uncertainty and calls for unified legislation. Government plans, such as NITI Aayog's AI principles and MeitY's draft AI guidelines, often remain largely aspirational. There is a clear agreement in academia: India needs a specific AI framework to ensure clarity and protect rights.

3.2 LIABILITY AND PERSONHOOD

A key topic is determining who is responsible for AI-related harms. As Sayyed (2024) notes, AI's autonomy complicates accountability. Since AI cannot be a legal person, responsibility must fall on human actors, such as developers, operators, or deployers. Legal experts discuss modifying tort or contract laws for AI cases. Some suggest holding developers or companies liable for harm caused by their AI, similar to product liability. Others advocate for human-in-the-loop measures, requiring that deployers maintain enough control for courts to attribute negligence. Some fringe ideas suggest limited "algorithmic personhood," but Indian scholars mostly reject this idea due to practical and constitutional challenges. Overall, while there is no

clear agreement on specifics, the literature emphasizes the need for clear laws concerning AI liability so that victims can seek compensation.

3.3 DATA PROTECTION & PRIVACY

Many papers focus on data law as a key aspect of AI governance. The new DPDP Act (2023) is seen as an important step, but scholars highlight its shortcomings for AI use. Jha et al. (2026) analyze the Act and find that its consent-driven design is "functionally unworkable" for large AI training datasets. Additionally, the Act lacks a clear "right to explanation" for automated decisions, raising concerns about profiling and unclear credit or job application algorithms. Commentators argue that fundamental rights, particularly privacy (as established in *K.S. Puttaswamy v. Union*, 2017), provide some constitutional protection. However, without AI-specific regulations, entities may exploit DPDP Act exemptions for security purposes to implement surveillance without checks. Sahil & Jeet (2025) warn that broad government exceptions could lead to AI-enabled policing with little oversight. Overall, while India's data law is evolving, many contend it requires improvements to address AI-related issues such as unbiased profiling, extensive data analytics, and cybersecurity for AI systems.

3.4 INTELLECTUAL PROPERTY

The literature highlights significant tensions in intellectual property (IP) concerning AI. Indian copyright law mandates that a human be the author, and the Patents Act excludes computer programs and algorithms from patent eligibility. Scholars (Ranjan 2024; Jha et al. 2026) describe the conflict: training generative AI on copyrighted works could violate copyright laws, yet there is uncertainty over the ownership of the outputs. The narrow "fair dealing" exceptions in Section 52 likely do not permit extensive data mining for AI. Jha et al. argue that AI training does not meet the fair use standard in India. Regarding the outputs, AI-created music, art, or inventions currently lack a designated author or inventor. This gap could dissuade AI investment or unfairly benefit AI companies. Many commentators, therefore, call for legal reform, including options to grant copyright to the AI developer or user or to create a new *sui generis* right for AI-generated content. India's DPIIT is actively engaging in dialogue on these matters. Patent issues are similar: if AI contributes to an invention, courts will need to determine how inventors are named. Until this is clarified, the literature suggests that current regulations fall short of supporting AI innovation.

3.5 JUDICIAL OVERSIGHT AND ETHICS

Several analyses examine the judiciary's approach to AI. The Supreme Court's 2025 white paper and related discussions emphasize both opportunities and risks. Media reports highlight that the Court has noted dangers such as "hallucinations," which refer to AI fabricating citations, algorithmic bias, and data privacy violations in courts. Crucially, the judiciary insists that AI should only assist and must be fully audited by humans. Legal experts anticipate that Indian courts will apply principles regarding fundamental rights to AI-related issues. This may include striking down discriminatory AI practices that violate equality or enforcing due process guarantees when the state uses automated decision systems. Without clear legislation, early case law will likely set the standards, as has happened in other areas.

In summary, the literature converges on a common view: India's adoption of AI is outpacing its legal framework. Studies consistently call for a risk-based, rights-protective AI law that clarifies liability, requires transparency, and updates IP and privacy statutes. The shared emphasis is on engaging multiple stakeholders in policymaking while aligning with international best practices like the EU AI Act and OECD/UNESCO AI principles, all while respecting India's unique legal landscape.

4. METHODOLOGY

This research employs doctrinal legal analysis. We systematically review relevant laws and regulations, including the IT Act 2000, IPC/Bharatiya Nyaya Sanhita, Evidence/Bharatiya Sakshya Adhinyam, DPDP Act, and Consumer Protection Act. We also examine official policy documents like NITI Aayog strategies, MeitY AI guidelines, DPIIT working papers, and RBI AI reports, as well as significant court rulings and white papers related to AI use. The analysis incorporates insights from law review articles, working papers, and expert blogs to identify areas of agreement and disagreement. When relevant, we compare India's approach to international standards such as the EU's proposed AI Act and OECD/UNESCO guidelines.

Using this methodology, we investigate how existing laws are applied to AI and reveal gaps where AI's unique characteristics, such as autonomy, scale, and opacity, clash with legal assumptions. This approach provides a detailed and policy-focused overview of AI law in India as of 2026.

5. EXISTING LEGAL AND POLICY FRAMEWORK

5.1 CORE STATUTES

- **INFORMATION TECHNOLOGY ACT, 2000:** The IT Act is India's main cyberlaw. It punishes offenses like hacking, data theft, and the spread of obscene digital content. AI-related crimes, such as deepfake pornography and fraud driven by AI, can also fall under this law or relevant IPC sections like cheating and defamation. Notably, Section 43A of the IT Act requires organizations to maintain reasonable security for sensitive personal data, while Section 72A makes it a crime to breach data confidentiality. Although these sections were not created with AI in mind, they have been used to tackle data breaches and privacy violations involving automated systems. The Act also offers immunity to intermediaries under certain conditions, which could apply to AI platforms. Thus, the IT Act acts as a temporary solution for many AI issues, but it does not include specific rules for AI, such as norms for algorithmic fairness.
- **INDIAN PENAL CODE (AND BHARATIYA NYAYA SANHITA, 2023):** The IPC, India's criminal law, has always addressed acts like fraud, defamation, and mischief. These rules apply when AI systems are used to commit crimes. For example, using an AI bot to impersonate someone could lead to prosecution under IPC Section 499–500 for defamation or 467–468 for forgery, depending on the situation. In 2023, India replaced much of the IPC with the Bharatiya Nyaya Sanhita (BNS). The BNS includes rules for cyber and tech-related crimes, with the aim of addressing crimes involving new technologies. For instance, the BNS has sections for unauthorized access to computers and cyber fraud. While it does not specifically mention AI, its broad wording covers harmful AI uses, such as data theft via AI. As a result, criminal law is gradually being updated, but it still lacks provisions on AI autonomy or AI as a person (or not). The key issue remains: determining intent when an AI learns on its own.
- **DIGITAL PERSONAL DATA PROTECTION ACT, 2023:** Enacted in August 2023, the DPDP Act is India's first all-encompassing data protection law. It resets the data privacy landscape with rights and obligations partly based on the GDPR. Key provisions relevant to AI include:
 - **DATA PRINCIPALS' RIGHTS:** Individuals (data principals) have the right to access, correct, and erase their personal data, as well as be informed of data breaches. They can also object to certain processing activities. This allows individuals to seek redress if an AI system misuses their data.

- **DATA FIDUCIARY OBLIGATIONS:** Entities controlling data (data fiduciaries) must ensure consent, specify the purpose, and secure data. For AI training, this means organizations must handle personal data carefully and ensure a proper legal basis for its use. Notably, Section 43A (consent requirement) and Section 43E (cross-border transfer restrictions) can affect large AI datasets that include sensitive or foreign data.
- **SIGNIFICANT DATA FIDUCIARIES (SDFS):** Large companies designated by the government must comply with enhanced standards. The DPDP Rules (2025) require SDFs to conduct algorithmic audits and Data Protection Impact Assessments focusing on bias detection. This represents the clearest AI-specific requirement in any Indian law: major AI firms must regularly test their systems for fairness and address identified biases.
- **EXEMPTIONS:** Section 10 permits the government to exempt itself or its agencies from data protection rules under public order and security. Experts caution these exemptions are broad and might be used to justify AI surveillance, such as mass face recognition or predictive policing, without sufficient oversight. Some have called for narrowing these exemptions or subjecting them to judicial review.

In short, the DPDP Act creates a strong framework for personal data privacy. For AI, its enforcement—particularly regarding consent and purpose limits—will affect how training data is collected and applied. The auditing requirement for SDFs is a vital move towards accountability. However, experts like Jha et al. point out that some AI uses, such as mining large public datasets, may not strictly fit within the Act, indicating a need for further interpretation or changes.

- **CONSUMER PROTECTION ACT, 2019:** The CPA offers protection for buyers of goods and services. AI-powered products, including robotics, software, and medical devices, fall under this Act when sold to consumers. The CPA has product liability rules: a faulty AI product could make the manufacturer or service provider responsible for harm under the “deficiency in service” or “defective product” standards. Moreover, the Consumer Protection (E-commerce) Rules, 2020 ban “unfair trade practices” like dark patterns. AI-driven recommendation engines or interfaces that use deceptive design

could potentially face legal challenges under these rules. However, Indian courts have yet to rule on AI-specific CPA claims, leaving its practical impact untested.

- **SECTORAL REGULATORS:** Regulators have started to issue AI guidelines in their areas. The Reserve Bank of India (RBI) released a “Responsible AI” framework (2024) for banking, requiring explainability and model risk management. The Insurance and Securities regulators (IRDAI, SEBI) have issued advisories on algorithmic trading and underwriting. The Competition Commission published a report recommending AI audits for anti-competitive bias. The CDSCO (Drugs Controller) introduced draft rules for AI in medical devices. These sectoral guidelines are not legally binding but may influence enforcement by making compliance part of licensing or supervisory expectations.

5.2 GOVERNMENTAL POLICIES AND GUIDELINES

Instead of a formal statute, India has developed soft-law strategies for AI:

- **NITI AAYOG – NATIONAL AI STRATEGY (2018):** Named “AI for All”, it identified priority sectors (health, agriculture, education, mobility, smart cities) for AI development. It focused on encouraging access to data (through open datasets) and skill development but did not suggest regulatory measures. It did highlight the necessity of a solid IP regime and data governance for AI. This strategy set a developmental agenda but did not establish any legal obligations.
- **NITI AAYOG – RESPONSIBLE AI (2021):** This policy paper outlined seven principles for AI (safety, reliability, equality, inclusivity, privacy, security, transparency, accountability, and support for human values). Although not legally binding, these principles have been referenced by government ministries and courts as reflective of India’s AI values. They echo constitutional ideals (non-discrimination, justice, etc.) and act as a standard for both public and private AI initiatives.
- **INDIA AI GOVERNANCE GUIDELINES (NOV 2025):** In November 2025, the Ministry of Electronics & IT (MeitY) released draft India AI Governance Guidelines. These recommend an “innovation-first, risk-aware” regulatory approach. Notably, the guidelines suggest mandatory labeling of AI-generated content: platforms must label media created synthetically if it covers at least 10% of the content. They also propose unique identifiers for AI systems and standardized documentation. While not yet law,

these draft guidelines indicate a move toward more structured governance. If enacted, the labeling rule would make India one of the first countries to require the disclosure of AI-generated content.

- **JUDICIAL GUIDELINES (2025):** The Supreme Court's White Paper on Artificial Intelligence and the Judiciary (Dec. 2025) is an important policy document. It details how Indian courts use AI (through tools like SUPACE and translation aids) and lists associated risks, such as false citations, embedded bias, and privacy breaches involving court data. The White Paper advocates for human oversight for all AI used in courts, security audits, and the use of closed-system AI (avoiding public web tools). It essentially lays out ethical guidelines for judicial use of AI, emphasizing that technology cannot replace human judgment.
- **DPIIT WORKING PAPER ON AI-COPYRIGHT (DEC 2025):** The Department for Promotion of Industry and Internal Trade has established a committee on AI and copyright. Part I of its working paper (Dec 2025) explores options for licensing AI training data. Its summary notes that the committee rejected a zero-cost licensing model, which would undermine creative incentives. Instead, it proposed a hybrid licensing structure: AI developers would receive a blanket license for properly accessed content for training, with royalties owed only when the AI tool is commercialized. A central fund would collect and distribute these royalties. The draft is open for public comment, thus it is not final law, but it signifies India's serious efforts to balance AI development with copyright concerns.
- **DRAFT REGULATORY AMENDMENTS:** MeitY has shared draft amendments to the IT Rules 2021. Key proposed changes include: mandatory labeling of AI-generated audiovisual content, user verification for content declarations, and penalties for failure to label AI outputs. If enacted, these proposals would create legal obligations for platforms concerning generative AI. Additionally, the Technology Minister has suggested broader amendments to IT and other laws to address AI, although specifics are still pending.

In summary, India's AI policy framework is sectoral and evolving. It focuses on guidelines and amendments to existing laws rather than establishing a single AI statute. This strategy aligns with India's development goals but leaves some questions unanswered. The following sections will explore the key challenges this framework encounters.

6. CHALLENGES IN LIABILITY AND PERSONHOOD

One of the trickiest issues is figuring out who is responsible for harms caused by AI. Current Indian law assumes a human or company is responsible. If an AI system acts on its own, the question arises: Should the developer, the user, or even the owner be held accountable? For now, Indian courts would likely rely on tort principles. The Consumer Protection Act, 2019 (Chapters VI–VII) allows claims against defective products or services; an AI app or robot might be seen as a "good" under this law. Affected individuals could seek compensation if they can prove negligence or a defect. However, there is no clear rule for when an AI's error is excused, such as with the "black box" defense.

Criminal liability is equally complicated. If someone uses an AI tool to commit fraud, the human users face charges under IPC sections covering cheating or cyber-fraud. The AI itself cannot be charged. This raises concerns about immunity if a criminal designer creates a hidden AI agent. Sayyed (2024) points out that Indian courts may struggle with mens rea (criminal intent) in AI cases, especially since the Bharatiya Nyaya Sanhita has updated penalties but still assumes human intent.

Many scholars suggest that we can avoid the need for AI personhood by focusing on strict liability laws for certain products. For example, the government could consider autonomous vehicles or medical AI devices as inherently risky, requiring mandatory insurance or registration for developers' liability. This approach would be similar to discussions in the EU AI Act. Others suggest statutory "duty of care" requirements: for instance, mandating human oversight in high-stakes AI systems and punishing companies that deploy completely unmonitored AI.

A clear example of judicial reasoning appeared in 2026: the Supreme Court ruled that a lawyer or judge who relied on AI-generated fake case citations engaged in "misconduct." This case (though not a liability lawsuit) shows that existing professional accountability rules will still apply to AI contexts. It indicates that until the law is updated, courts will use current concepts (negligence, misconduct) to regulate AI misuse. Legal scholars emphasize the need for proactive reform: clarify that responsibility lies with the human operator or organization in all AI applications, and define defenses (such as "reasonableness" of AI reliance).

In short, assigning liability is still unclear. The literature generally agrees that legal reforms are needed: establish strict liability for high-risk AI, require mandatory human oversight, and

possibly create a special AI regulatory body to determine fault. Without such clarity, victims of AI errors may find it hard to get compensation, which could erode public trust.

7. DATA PROTECTION, PRIVACY, AND SURVEILLANCE

AI's demand for data makes privacy and cybersecurity critical issues. The DPDP Act and its related rules are now the primary data laws. The Act's consent-based approach and purpose limitation restrict how personal data is collected and used for AI training. In theory, any personal data (including the training inputs for AI models) must be processed with consent and for specific purposes. People have the right to know how their data is used in automated decisions. The DPDP Rules mandate regular data audits and breach notifications for those in charge.

However, experts have raised several concerns:

- **SCALE OF CONSENT:** Getting individual consent for millions of data points (which AI models often require) is impractical. Jha et al. (2026) argue that the DPDP Act's framework does not easily fit modern AI workflows. This could force many AI projects to either avoid personal data (which limits effectiveness) or take advantage of exemptions. Some suggest a legislative exemption for "aggregated analytics" with strong safeguards, similar to research exceptions in other laws.
- **AUTOMATED DECISION SAFEGUARDS:** Unlike the EU GDPR's Article 22, the DPDP Act does not explicitly grant a "right to explanation" for automated decisions. While it allows individuals to withdraw consent, it does not require businesses to clarify AI outcomes. Legal scholars note this gap, suggesting that courts may have to interpret Article 21 (right to privacy) to demand a degree of AI transparency. Currently, if an AI denies someone a bank loan, the applicant has little legal recourse to discover how that decision was made.
- **STATE SURVEILLANCE EXEMPTIONS:** The Act broadly exempts the government for law enforcement and security purposes. Academics (e.g., Sahil & Jeet 2025) caution that this could enable AI-driven surveillance (like predictive policing or facial recognition) without proper checks. They recommend judicial review of such exemptions, similar to the requirement for some form of rule of law in state actions, as seen in the Puttaswamy II privacy judgment. Indian Intelligence Services (e.g., CCTNS, law enforcement databases) are already using AI tools; strong safeguards (like

specifying which algorithms and data can be used) are essential to prevent abuse of rights.

- **CYBERSECURITY:** AI systems can also create new security risks. The IT Act's general cyber offenses (Section 66 et seq.) will apply if an AI is used for hacking or if an AI system is breached. For instance, tampering with a machine learning dataset could potentially be prosecuted under existing sabotage or cybercrime laws. However, India currently lacks AI-specific cyber regulations (in contrast to the EU's proposal for AI security standards). Some technologists suggest developing Indian standards for AI system security (which the BIS is exploring), but these are not yet formalized.

In summary, India's data protection law provides a strong foundation (consent, responsibilities, rights of data subjects), but it is not specifically designed for AI. Legal scholars agree that clarifying how the DPDP Act functions with big data and setting clear limits on automated profiling will be essential. The current "privacy by design" language in Section 10 could be interpreted as requiring AI impact assessments, but more precise regulations (or guidelines from the Data Protection Board) would ensure compliance. Simultaneously, India needs to carefully monitor how broad surveillance powers are applied, considering the AI tools now available to law enforcement.

8. INTELLECTUAL PROPERTY AND AI-GENERATED CONTENT

Under India's current IP laws, AI-generated works and inventions are not well-defined. The Copyright Act of 1957 protects computer-generated works, but "authorship" refers to a human creator. Thus, a painting or poem created entirely by AI has no human author and, therefore, no copyright. Additionally, training AI on copyrighted content can lead to possible infringement issues. There is no clear text-and-data-mining exception in Indian law. The DPIIT working paper from December 2025 explicitly addresses this issue, stating that using copyrighted material to train AI without permission carries legal risks. The proposed hybrid license model, which includes a blanket training license and royalties on commercialization, aims to address this gap.

For patents, Section 3(k) of the Patents Act excludes algorithms and inventions made by non-humans. If an AI invents a drug, the patent system requires listing a human inventor. Many experts believe that in practice, a human operator or a team will be credited, effectively claiming ownership. However, uncertainty remains about whether completely autonomous AI innovations can receive protection. As innovations like AlphaFold and generative design

become more common, India will likely face demands to change patent laws or create special provisions for inventions contributed by AI.

The general consensus among experts is that India needs to clarify IP rules to foster AI innovation and protect creators. Shubhi Priyadarshi (2026) argues that AI training does not meet India's fair dealing standards, suggesting a need for reform or clear legal protections. Without clarity, two negative outcomes could arise: (a) AI developers may avoid Indian works to reduce legal risks, hindering AI progress, or (b) there could be widespread unlicensed use of creative works, discouraging human creators. The DPIIT's open consultation and the EU's experiences suggest that India may consider a compulsory licensing or levy system that ensures creators are compensated while allowing AI training. Until a clear law or rule is implemented, Indian publishers and tech companies will have to navigate a complex situation, possibly resorting to litigation to test the limits of fair use, as is occurring in many countries.

9. ROLE OF JUDICIARY AND CASE LAW

Even without specific AI laws, Indian courts are already influencing AI governance through interpretation and oversight. No significant AI-specific case has been decided yet, but existing legal norms provide useful insights:

- **EVIDENCE AND PROCESS:** The Indian Evidence Act, which will soon be replaced by the Bharatiya Sakshya Adhinyam, 2023, does not mention AI. Courts currently evaluate digital evidence by applying reliability tests, like Section 65B for electronic records. If an AI-generated report is presented as evidence, lawyers may challenge its authenticity. The Supreme Court White Paper recommends transparency and accountability in any AI evidence use. This means if a party wants to use AI analysis, such as a predictive analytics score, the court may require cross-examination of the system or a human expert. Over time, we may see precedents regarding the admissibility of AI-assisted testimony or expert reports.
- **JUDICIAL DEPLOYMENT:** Judges also use AI tools. The Supreme Court portal, SUPACE, employs AI for research, and many courts utilize AI for translation and transcription. The judiciary's approach, reflected in the White Paper and public remarks, leans toward cautious experimentation with strict controls. Notably, the Court's warning in 2026—that judges and lawyers should not depend on AI to cite fake cases—indicates that the courts will self-regulate AI within the judicial process through ethical guidelines. Bar associations have started issuing advisories indicating that lawyers

cannot blindly trust AI for legal research. This self-awareness helps manage AI risks in the legal field.

- **CONSTITUTIONAL SAFEGUARDS:** Several experts predict that Indian courts will apply fundamental rights to regulate AI. For example, if a government agency uses an algorithm to deny benefits, an affected citizen could contest this as a violation of Articles 14 (equality) and 21 (due process). Even without a specific “right to explanation,” courts have previously overturned unclear government actions (like the Aadhaar rulings). Article 19 (free speech) might be relevant if AI is deployed for mass surveillance or censorship. The judiciary’s recognition of privacy as a constitutional right in 2017 offers a legal basis to challenge invasive AI applications.

In summary, while legislatures are in discussion, courts and tribunals will shape AI law through analogy and principles. Civil judges, cybercrime tribunals, and regulatory bodies may interpret existing laws, like the IT Act and DPDP Act, in innovative ways. Practitioners should watch for early rulings on AI-related cases, especially in areas like finance (such as loan denial disputes) and employment. Currently, the Indian judiciary’s proactive commentary through white papers and judgments plays a critical role in ensuring that AI deployment aligns with legal standards.

10. CASE FOR AI-SPECIFIC LEGISLATION

Across various fields, scholars and policy experts contend that fragmented measures are not sufficient. The alternative is a unified AI regulatory framework (an “AI Act” or a comprehensive amendment to technology laws). The aims of such legislation, as gathered from the literature, would include:

- **RISK-BASED CLASSIFICATION:** Not all AI systems carry the same level of impact. Many suggest a multi-tiered approach similar to the EU’s: prohibit or closely regulate “unacceptable” AI (such as social scoring and generative weapons); impose strict checks on “high-risk” AI (like biometrics, justice, health, and employment algorithms); and permit “low-risk” AI (like spam filters) with minimal regulation. A risk-based law would help focus resources and not hinder valuable innovation.
- **TRANSPARENCY AND ACCOUNTABILITY:** Require disclosure of key features of AI systems. This could mean mandating documentation of data and logic for high-stakes algorithms or establishing a public registry of AI systems used in sensitive

sectors. Some propose a legal “right to explanation,” requiring entities to clarify AI decisions. Others suggest setting standards for fairness and privacy, such as implementing differential privacy methods. Essentially, the law should enforce what self-regulation often fails to achieve: transparency about how AI functions.

- **DEFINED LIABILITY:** Clarify who bears legal responsibility for AI actions. This might involve establishing statutory presumptions, for instance, presuming that the creator or deployer is liable for harm unless they can demonstrate compliance with best practices. Some propose mandatory insurance or compensation funds for specific AI applications, similar to discussions around robotic technologies. The law could also define how to distribute damages when multiple parties (developer, implementer, user) share responsibility.
- **DATA GOVERNANCE FOR AI:** Establish rules for data used in AI. These rules could include safe harbors for anonymized or public-interest AI research, guidelines for data sharing between companies/government under strict oversight, and limits on surveillance applications. The DPIIT’s working paper suggests a possible path: a licensing framework for copyrighted data. India could also adopt a data trust or commons model for certain data types (like health and agriculture) to encourage innovation while adhering to agreed privacy standards.
- **SECTORAL OVERLAY:** Although a general law could establish baseline rules, sector-specific regulations might be required for certain AI applications (like medical AI certification and autonomous vehicle regulations). Combining a general AI Act with empowered regulators, as some scholars propose, could ensure both adaptability and effectiveness.
- **ETHICAL AND HUMAN RIGHTS SAFEGUARDS:** Any AI legislation should clearly incorporate values such as non-discrimination, human dignity, and privacy. For example, it could prohibit the use of race or religion by automated systems when making decisions about public services. Incorporating India’s constitutional guarantees—similar to the principles advanced by NITI Aayog—would help align AI deployment with fundamental law.

Crucially, many Indian analyses highlight the need for flexibility. As AI technologies change rapidly, the law should enable regulators to update rules, possibly through delegated legislation or by establishing a specialized AI regulator, without requiring new Acts each time. Some

suggest a regulatory sandbox approach for testing new AI before full rollout, allowing for observation of effects in a controlled scenario.

Comparative experiences provide valuable lessons. Often-cited examples include the EU's proposed AI Act (2021) and the OECD's AI Principles (2019). Several Indian authors explicitly recommend adopting a risk-based classification like the EU while taking into account India's specific context. The prevailing view is that India can adopt lessons from global standards but must customize any law to address local needs, such as focusing on digital inclusion and rural effects.

A single AI law would also streamline various guidelines into a cohesive framework, making compliance easier for businesses. It would offer clearer legal standards for citizens and strengthen enforcement through penalties or even criminal consequences for misuse. Given India's influential role in the Global South, some experts note that a solid AI law could also improve India's reputation in international AI governance discussions, such as at the G20 or the Global Partnership on AI.

11. CONCLUSION AND RECOMMENDATIONS

India's current approach, an "innovation-first, but patchwork" model, has the virtue of flexibility but suffers from uncertainty and risk. The analysis above indicates that relying on legacy laws alone will leave many issues unresolved: victims of AI errors may have no remedy, personal data may be used unethically, and creators' rights may be undermined by automated processes. At the same time, over-regulation could stifle the very technology that India aims to champion for development.

Based on the evidence and scholarship surveyed, we recommend the following path forward:

1. **ENACT COMPREHENSIVE AI LEGISLATION:** Parliament should draft a law specifically addressing AI. This law would define key terms (e.g. "AI system," "high-risk AI"), establish categories of prohibited or regulated AI uses, and embed the principles of transparency and accountability. The law should also stipulate liability frameworks and mandatory oversight measures (like audits).
2. **CLARIFY DATA AND PRIVACY REGIMES:** Amend or clarify the DPDP Act and associated rules for AI. For instance, create a legal exception or statutory license for AI training under strict conditions, and narrow government exemptions to prevent

unchecked surveillance. Explicitly grant data principals rights regarding algorithmic decisions (e.g. to receive an explanation).

3. **REFORM IP LAWS FOR AI:** Consider legislative changes to handle AI creations. Options include amending the Copyright Act to allow AI-generated works to have a designated owner, or creating a special statutory scheme for AI outputs. The DPIIT's proposed license model could be adopted into law, ensuring fair compensation for artists and authors when their works fuel AI systems.
4. **STRENGTHEN OVERSIGHT AND STANDARDS:** Institute independent oversight for AI – either by empowering an existing regulator (like a strengthened Bureau of Standards for AI systems) or by establishing an AI-specific agency. Mandate adherence to technical and ethical standards (e.g. through industry certifications). Incorporate enforceable requirements for testing AI algorithms for bias and safety (the DPDP Act's auditing requirement could be expanded).
5. **JUDICIAL CAPACITY BUILDING:** Encourage the judiciary to continue articulating AI norms. This includes training judges on AI issues and incorporating AI ethics into legal education. Courts should also ensure litigants can challenge AI-driven government actions, building case law that enforces accountability.
6. **STAKEHOLDER ENGAGEMENT:** Maintain a transparent policy-making process. The ongoing consultations by DPIIT and MeitY should include civil society, technologists, and academia. India may also consider a parliamentary committee on emerging technologies to keep AI law under review.

In final analysis, India must balance the promise and perils of AI. The recommendations above aim to secure innovation – by providing legal certainty and protecting rights – rather than merely constrain technology. By codifying fairness, safety, and accountability into law, India can encourage responsible AI development that serves its society and economy. As one study concluded, without an “integrated statutory framework for permissible [AI] practices,” legal uncertainty will undermine both AI innovation and public trust. Our survey of sources underscores that the time for such a framework in India is now.

12. REFERENCES

12.1 STATUTES & OFFICIAL DOCUMENTS

- Digital Personal Data Protection Act, No. 22 of 2023 (India).
- Information Technology Act, No. 21 of 2000 (India).
- Bharatiya Nyaya Sanhita, 2023 (India).
- Bharatiya Sakhya Adhiniyam (Evidence Act), 2023 (India).
- NITI Aayog, *National Strategy for Artificial Intelligence: #AIForAll* (2018).
- NITI Aayog, *Responsible AI for All: NITI Aayog's AI Ethics Principles* (2021).
- Supreme Court of India, *White Paper on Artificial Intelligence and the Judiciary* (Nov. 2025).
- Press Information Bureau (GoI), "*DPIIT Publishes First Part of Working Paper on AI–Copyright Interface*" (Dec. 9, 2025).

12.2 ACADEMIC ARTICLES & REPORTS

- Aman Kumar Jha, Mohit Jain & Tanishk Bhawsar, *Intellectual Property and Personal Data in AI Datasets Under India's DPDP Act 2023*, 4(2) *Trends in Intellectual Property Research* 1 (Apr. 2026).
- Hifajatali Sayyed, *Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges*, 10(1) *Cogent Social Sciences* 2343195 (2024).
- Abdul Hakeem, *India's Legal Shift: Addressing AI Challenges with New Criminal and Data Protection Laws*, *Int'l J. for Multidisciplinary Research* 1 (Vol. 7, Issue 6, Nov. 2025).
- C.S. Suraj, *Regulating Artificial Intelligence in India: Constitutional Challenges and the Need for a Comprehensive AI Law*, *Int'l J. Adv. Res. in Sci., Comm. & Tech.* (Dec. 2025).
- Gaurav Gupta & Nancy Roy, *Text and Data Mining vs India's DPDP Act, 2023: A Critical Study of the Legal Landscape*, *Bridge Counsel Blog* (2025).
- A. Hakeem, *India's Legal Shift: Addressing AI Challenges with New Criminal and Data Protection Laws* *International Journal For Multidisciplinary Research*, Nov. 2025.
- A. Jha, M. Jain, and T. Bhawsar, *Intellectual Property and Personal Data in AI Datasets Under India's DPDP Act 2023*.
- S. Ranjan, *Artificial Intelligence, Data Protection: A study of Copyrights Scenario in India*.

- *Tamanna and S. Thakur, Legal Personality of Artificial Intelligence : Rights, Liabilities And Jurisprudential Perspectives International Journal For Multidisciplinary Research, vol. 7, no. 5, Oct. 2025.*
- *G. S. SATARKAR, Regulating Artificial Intelligence in India: Legal Frameworks, Governance Challenges, and the Path toward a Dedicated AI Law, Mar. 2026.*
- *Adv. C. S. Suraj, Regulating Artificial Intelligence in India: Constitutional Challenges, and the Need for A Comprehensive AI Law, International Journal of Advanced Research in Science, Communication and Technology, Dec. 2025.*
- *Balancing Intelligence and Privacy: A Legal and Technological Examination of AI-Driven Data Use, Aug. 2025.*
- *Sahil and Dr. S. Jeet, Predictive Policing, AI Surveillance, and Privacy in India: A Legal Analysis under the DPDP Act 2023, Nov. 2025.*
- *P. K. Mishra & Shruti Tripathi, Artificial Intelligence in Environmental Governance: Legal and Ethical Challenges for India, 7 International Journal For Multidisciplinary Research (2025).*
- *Amit Singh, Legal Implications of Artificial Intelligence: Navigating the Future, 379 (2024).*

12.3 POLICY & INDUSTRY GUIDES

- CMS Legal India, *AI Laws and Regulations: Expert Guide – India (2025).*
- Reserve Bank of India, *Report of the Committee on Responsible AI in Financial Services (FREE-AI) (2024).*
- Internet and Mobile Association of India (IAMAI), *AI in India – Policy, Strategy and Ethics Framework (2022).*

12.4 NEWS & ONLINE SOURCES

- Prabhanu Kumar Das, “*Explained: How Indian Courts Are Using AI And Why The SC Wants Humans In The Loop*”, MediaNama (Dec. 4, 2025).
- Aakriti Bansal, “*SC Declares AI-Generated Fake Citations ‘Misconduct’*”, MediaNama (Mar. 3, 2026).
- Shubhi Priyadarshi, “*Fair Dealing Cannot Be Presumed: Why AI Training Fails the Purpose Test under Indian Copyright Law,*” Bar & Bench (2026).

12.5 INTERNATIONAL SOURCES

- European Parliament, *Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act)* (Apr. 2021).
- Organization for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence* (2019).
- UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (Nov. 2021).