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

GOVERNING ARTIFICIAL INTELLIGENCE IN INDIA: LEGAL CHALLENGES, REGULATORY GAPS AND THE PATH TO ACCOUNTABLE INNOVATION

~Navya Srivastava

ABSTRACT

Artificial Intelligence (AI) has transitioned from a specialized computational technology into an integral facet of economic activity, public administration, communication, employment, healthcare and education and digital platforms. The fast implementation of Artificial Intelligence, through generative and algorithmic systems has given rise to legal concerns involving privacy, consumer protection, accountability. In India, these concerns occur in a regulatory, blending constitutional safeguards, the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, intellectual property legislation, sectoral regulation and nascent government initiatives. The regulatory milieu has been dynamic evolving with the Digital Personal Data Protection Rules, 2025 and amendment to the Information Technology Rules concerning synthetically generated information. This paper evaluates whether India's existing and how recent legal framework manages the challenges presented by AI. Through adopting a doctrinal and analytical approach, it reviews the provisions of statutes, constitutional principles, judicial verdicts, regulatory developments, government policy documents and relevant comparative perspectives. The paper argues that the major impediment of India lies not in a comprehensive, AI-dedicated statute, but the disjointed nature of existing legal mechanisms and difficulty of allocating accountability between developers, deployers, platforms and users. The paper explores the issues of privacy data protection, intellectual property, AI generated content and the use of deepfakes, algorithmic discrimination. To conclude the paper explores a coordinated, risk-oriented and rights focused on governance of framework underpinned by the principles of transparency, human oversight, accountability and institutional coordination.

1. INTRODUCTION

Artificial Intelligence has become one of the most transformative technological developments of the twenty-first century, shifting how information is generated, decisions are made and services are provided. Modern AI systems have an ability to detect patterns in large datasets, generate content, make predictions and aid or shape decisions based upon varying levels of human involvement. Generative AI has enhanced these capabilities by allowing the generation of text, images, audio, video and other forms of content. As AI becomes further integrated into everyday digital surroundings, the effects ripple beyond into the world of law.

The legal relevance of AI emerges from its ability to simultaneously fall within various categories of the law. An AI system may deal with personal information, produce potentially copyrightable content, copy from protected content, mediate employment or consumer decisions, form synthetic media and cause damage for which accountability is challenging to pinpoint. Hence AI cannot simply be considered using the lens of a single legal statute. Its legal effects necessitate an analysis involving constitutional rights, information technology law, data protection, intellectual property, accountability, consumer protection and sectoral regulation. India's approach has been developed in this interlacement of existing legal, regulatory mechanisms, judicial doctrines and policy initiatives rather than the creation of a single comprehensive artificial intelligence statute. The Information Technology Act, 2000 and Information Technology Rules, 2021 continue[1] to serve as a key technology and intermediary regulation regime while the Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 establish a growing legal framework for digital personal data. MeitY's[2] current materials also include the 2026 amendments to the IT Rules regarding synthetically generated information. These show that India's AI-relevant legal framework is evolving within the context existing regulatory regimes, rather than entirely not being subject to regulation. A key problem however is applying legal doctrines developed concerning identifiable human actors and conventional modes of action to technologically complex systems. A damaging result might involve a developer who designs a model, an organisation that implements it, an intermediary that facilitates its output and an end user who employs them. Allocating causation, predictability and accountability may therefore become more challenging when the mechanics of the system are complex or obscure. The fundamental legal

[1] Information Technology Act, No. 21 of 2000, §§ 69A, 79 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[2] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette of India, G.S.R. 120(E) (Feb. 10, 2026).

problem therefore involves whether AI needs to be regulated or how accountability distribution needs to be addressed when AI acts as an intermediary between human actions and legal results.

Privacy is a prime example of this problem as AI development and deployment often involves significant amounts of information, raising issues involving legal processing, authorisation, security and accountability. The Supreme Court's acceptance of privacy as a constitutionally guaranteed right in Justice K.S. Puttaswamy (Retd.) v. Union of India[3] provides an important constitutional foundation for considering these concerns. However AI brings further questions arising over on the scale of data processing, the creation of models and to extent to which individuals can meaningfully understand or control how their information is used. AI poses further challenges to established principles in intellectual property law. Generative systems can be capable of generating outputs similar to existing works while model creation might involve the processing of datasets containing protected content. This raises questions to infringement, originality, authorship and ownership. Similarly, AI-generated and synthetically produced content can raise issues involving privacy, reputation, freedom of expression and intermediary liability where issues such as where deepfakes imitate individuals or create misleading representations. India's evolving intermediary framework therefore becomes particularly important in determining how to allocate accountability for synthetic content.

These challenges arise alongside with greater questions of discrimination and accountability. When systems reproduce biases present in their data training or generate discriminatory results, the issue raises not only not technical accuracy but also equality and fairness. Article 14[4] of the Constitution thereby provides an important basis for investigating discriminatory or arbitrary employment of automated decision making, while Article 21 comes into play where the AI-facilitated processing or decision-making impacts privacy, dignity or personal autonomy. Meanwhile regulation of AI must consider the technological innovation. Overly broad or unclear regulation might discourage innovation and increase compliance burdens while a lack of protection might allow for technological developments to externalise cost on individuals. The appropriate legal response must balance innovation with meaningful protections against high impact harms. India's emerging governance initiatives including the India AI Mission and institution development within MeitY show their increased focus on responsible and human centred AI.

[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[4] INDIA CONST. arts. 14, 21.

With this backdrop, the current study explores how effective India's existing legal framework is in addressing the risks and rights-based concerns associated with AI. Rather than the finding the presence of a comprehensive AI statute as proof of a regulatory vacuum, this paper examines the interplay between the various legal regimes for different AI-related consequences. It develops the idea that the major challenge faced India does not just rest upon the absence of AI-specific legislation, but the fragmentation of legal accountability across existing statutes, regulatory mechanisms and institutions. The presence of existing legislation provides important instruments for tackling certain harms but its application to AI creates uncertainty surrounding accountability, transparency, explainability, authorship, data governance and remedies. The paper adopts a doctrinal and analytical approach. It reviews primary legal materials including constitutional provisions, legislation, subordinate legislation and judicial decisions, in addition to government policy documents and relevant literature. Comparative materials are utilised at discretion where it assists in assessing potential approaches for India. The analysis proceeds across the constitutional aspects of AI, data protection and privacy, intellectual property, AI-generated content and intermediary liability questions of accountability and selected application examples in employment, consumer protection and the justice system. It then reviews India's emerging governance framework, identifies regulatory gaps and proposes a coordinated, risk-sensible and rights-oriented approach centred upon transparency, human oversight, accountability and institutional coordination.

2. CONCEPTUAL AND LEGAL FOUNDATIONS OF ARTIFICIAL INTELLIGENCE

Artificial Intelligence is an umbrella[5] term describing computational systems capable of functions commonly associated with human intelligence, such as learning, pattern detection, predicting, classification, language processing and content generation. Its legal relevance stems not just from technical innovation but its capacity in influencing decisions, creating information and interacting with individuals and institutions at scale. Unlike conventional software generally functions generally involves predetermined instructions, machine learning systems detect statistical patterns in data and may create outputs that are hard to explain via a simple input output model. Generative AI takes this further in creating text, images, audio, video and other content. This complexity can mean challenging in identifying why a certain output was created, whether bias was used in its creation or which actor should accountable for an unlawful

[5] Ministry of Electronics & Information Technology, Government of India, India AI Mission, India AI

consequence. AI presents a challenge of accountability. Under normal law rights and duties of action are ascribed to identifiable persons, entities or organisations. an AI system does not acquire legal personality simply for performing autonomous or semi-autonomous operations. Accountability must therefore remain tied to the human or institutional actors involved in the development, deployment, controlling or use of the system. The data-based nature of AI connects multiple areas of law. Personal data might implicate data protection laws, protected creative works raise copyright concerns, discriminatory outcomes engage constitutional equality and synthetic content can implicate privacy, defamation and intermediary liability. A single AI application might produce multiple results governed by various legal regimes, at the same time. India's approach reflects this multi-dimensional nature. Instead of the exclusive use of an AI-specific legislation, this merges aspects of information technology law, data protection, intellectual property, constitutional safeguards, sectoral regulation and policy initiatives. The India AI Mission, including its "Safe & Trusted AI" pillar shows the mix of technology advancement and responsible use objectives. The creation of an AI Governance[6] and Economic Group by MeitY in April 2026 shows ongoing institutional evolution. The main issue therefore is not whether or not AI should be treated as a legal category independent on its own, but which existing principles are effective when applied to AI. This creates the basis for reviewing India's constitutional framework, data protection, intellectual property and accountability apparatus.

3. LITERATURE REVIEW AND RESEARCH METHODOLOGY

A. LITERATURE REVIEW

The legal area surrounding artificial intelligence in India emerges with the technology itself. Existing literature generally explores AI through questions of privacy, data governance, intellectual property, constitutional rights, intermediary accountability and regulatory oversight. An emerging issue is that existing legal rules generally were designed before contemporary generative and data-intensive AI systems became prevalent. Consequently, scholars disagree on the extent to which existing doctrines can be adapted or whether India requires a dedicated AI-specific legislative framework. A large strand of scholarship focuses on issues of privacy and data protection. The relevant scholarship[7] highlights the ways in which

[6] Ministry of Electronics & Information Technology, Government of India, Constitution of AI Governance and Economic Group (AIGEG), Office Memorandum (Apr. 13, 2026).
[7] Balamurugan S. & Nikitha Sree, Regulating Artificial Intelligence in India: Constitutional Challenges to Privacy, Equality, and Due Process, 6(7) Indian Journal of Legal Review 164, 164–70 (2026).

AI systems rely on large datasets and produce risks not only from the collection of personal information but also through profiling, inference and the automated decision-making. The constitutional recognition of privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India has become an important basis for analysing AI-related data practices. The emergence of the DPDP Act, 2023 has shifted the discourse towards an understanding of the dynamic between constitutional privacy and statutory data governance particularly with regard to consent, accountability, data accuracy and individual rights. Another body of scholars explores intellectual property and generative AI[8]. Issues around ownership, authorship, originality, training data and infringement become increasingly important in the in the extent to which AI systems can produce text, images, music and other works of creative output. While existing Indian copyright principles provide a starting point, the extent to which concepts developed around human creativity can accommodate machine-created or machine-assisted works is contested. The body of legal scholarship increasingly addresses algorithmic accountability and discrimination. The concern is that ostensibly neutral systems can reproduce embedded biases in training data or institutional practices. This raises questions around the issues of equality, transparency, explainability and remedies, particularly where AI is used in high-impact contexts. Related literature around the intermediary liability and synthetic media explores the difficulties arising through the creation of deepfakes, mis information and impersonating and explores if existing rules of information technology can provide proportionate safeguards without unduly restricting lawful expressions. The literature however presents a broader research void. Much of the analysis focuses on individual legal problems in a stand-alone manner i.e. privacy, copyright, or intermediary liability while comparatively little focus is paid to the interaction between these regimes when the same AI system gives rise to effects in several legal spheres. This paper fills this gap by exploring the nature of AI as a cross-cutting legal issue and explores whether India's existing framework is capable of providing coherent accountability throughout the lifecycle of AI.

B. RESEARCH METHODOLOGY

This study adopts a doctrinal and analytical methodology of legal research. The doctrinal approach reviews the law as it currently exists through primary legal sources such as the Constitution of India, legislative bills by the Parliament, subordinate legislation, judicial rulings and official regulatory materials. Particular focus given is given to the Information

[8] Intersection of Generative Artificial Intelligence and Copyright: An Indian Perspective, 17(1) Journal of Science and Technology Policy Management 118, 118–33 (2026)

Technology Act, 2000, the Information Technology Rules, 2021, the Digital Person Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025 and relevant intellectual property legislation. The analytical approach analyses the adequacy of these legal rules in their application to the unique characteristics of AI. The study therefore moves beyond the analysis of statutory provisions to review questions of accountability, legal attribution, proportionality, transparency, human oversight and the practical impossibilities of applying traditional doctrines of human accountability to complex AI systems. Judicial decisions are examined at discretion where it establishes principles relevant to AI-related constitutional or technology issues including privacy, freedom of expression and State accountability. Comparative materials, especially with developments the European Union, are only used where is assists in assessing potential for regulatory approaches for India. The research is focused on India and does not seek to undertake a comprehensive comparative survey. The study primarily depends upon authoritative legal and government materials and uses scholarly literature to highlight existing debates and interpretive perspectives. Given the rapid development of AI regulation, recent legislative, regulatory and institutional developments are considered alongside established legal principles. The methodology accordingly aims to ascertaining the current scope of Indian law and the areas requiring clarification, coordination or targeted reforming.

4. CONSTITUTIONAL DIMENSIONS OF ARTIFICIAL INTELLIGENCE IN INDIA

The Constitution offers the normative context against which the usage and regulation of artificial intelligence need to be assessed. While predating contemporary AI, its guarantees of equality, liberty, privacy, dignity and freedom of expression remain relevant where automated systems impact rights and interests. The key problem is how the existence constitutional rights work in a situation where decisions, classifications and information flows are mediated by algorithms.

A. EQUALITY AND ALGORITHMIC DISCRIMINATION

Article 14[9] ensures equality before law and equal protection of the laws and prohibit of arbitrary State actions. Their relevance with AI is raised where automated systems classify individuals, allocate opportunities or aid decision-making. An algorithm may seem impartial while repeating biases contained training data or design. This is particularly pertinent where AI plays a role in recruitment, credit assessing, allocating of public benefits or law enforcement.

[9] INDIA CONST. art. 14.

Where such systems are implemented by public authorities, the use of technology cannot shift governmental action beyond constitutional scrutiny. The legal principles of equality and non-arbitrariness must be continued irrespective of whether a decision is produced by an official or aided by an algorithm. AI thus needs attention not just on the motive behind a system but also to its design, training data and effects. High-impact governmental decisions should therefore provide meaningful human oversight and avenues for review of potential discriminatory outcomes.

B. PRIVACY, DIGNITY AND INFORMATIONAL AUTONOMY

Justice K.S. Puttaswamy (Retd.) v. Union of India[10] recognised privacy as a constitutionally protected liberty covering informational privacy and interests in dignity and autonomy. This right has direct relevance to the context of AI applications involving facial recognition, profiling, recommendation systems, predictive analytics and other forms of extensive data processing. The constitutional protection of privacy extends beyond issues of disclosure. AI may create novel information or behavioural trends based upon existing material, presenting questions as to whether individuals can understand or effectively control subsequent uses of their information. Restrictions concerning privacy are therefore required to satisfy constitutional requirements rather than just being dictated by technological capabilities. This constitutional protection intersects with statutory legislation on data protection separately, but Puttaswamy confirms the underlying proposition that technological advances cannot completely eliminate claims involving privacy, dignity and autonomy.

C. FREEDOM OF SPEECH AND EXPRESSION

AI also presents a complex intersection between the regulation of technologies and the constitutional protection of freedom of speech and expression under Article 19(1)(a)[11]. While generative AI may assist in various forms of political, artistic, journalistic and educational expression, it may also generate deceptive material and impersonation. Regulation must therefore distinguish between appropriate expression and legally cognisable harm. In Shreya Singha v. Union of India, the Supreme Court invalidated Section 66A of the Information Technology Act, 2000 and highlighted the constitutional protection of expression on the Internet under Article 19(1)(a), limited to its grounds specified under Article 19(2).[12] These

[10] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 260–63.
[11] INDIA CONST. art. 19, cl. 1(a).
[12] Shreya Singhal v. Union of India, (2015) 5 SCC 1, 80–82.

considerations remain relevant for AI content: the technological status of generative content is not directly determinative of whether expression falls outside of constitutional protections or not. The regulation of deepfakes, or similar generated material, must therefore focus on legally cognisable harms and remains constitutionally proportionate.

D. TRANSPARENCY, FAIRNESS AND HUMAN OVERSIGHT

The complexity of AI systems may make it hard to understand or contest decisions by affected. Indian constitutional law[13] does not grant an overall right to an explanation for all algorithmic outputs, but fairness and principles of non-arbitrariness and natural justice may be relevant where automated decision-making significantly impacts legal rights or interests. The potential impacts of the decision increase, the more justification there must be for meaningful human monitoring and oversight. An AI-generated output may have an authoritative appearance alongside factual or legal inaccuracies; technological sophistication is therefore not sufficient to replace the accountability of the public authority or decision-maker that relies upon it.

E. CONSTITUTIONAL BALANCE BETWEEN INNOVATION AND RIGHTS

The regulation of AI must balance both the development of technology and the protection of individual rights. Innovation can contribute to both economic progress and improve public services, but efficiency is not sufficient justification to infringe on fundamental rights. Conversely, regulation should not take that technological development is automatically harmful. The constitutional balance is therefore appropriate for a principle of rights-compatible innovation: greater safeguards should be coupled with those AI applications with a greater potential impact upon the areas of equality, privacy, dignity, autonomy and freedom of expression. This constitutional balance forms the building block in how statutory and regulatory structures may function in particular contexts of AI.

5. DATA PROTECTION AND PRIVACY IN THE AGE OF AI

Artificial intelligence is fundamentally reliant upon data. Where data processes involving personal data occur during the training, deployment or interaction with users of an AI system, issues arise concerning the privacy, autonomy and control of personal information. The Digital Personal Data Protection Act, 2023 ("DPDP Act"), paired with the Digital Personal Data

[13] Maneka Gandhi v. Union of India, (1978) 1 SCC 248, 272–73.

Protection Rules,2025 provide the cornerstone modern statutory protections against these concerns.[14]

A. APPLICATION OF THE DPDP FRAMEWORK TO AI

The DPDP Act defines "personal data" as being about an individual who can be identified individually or through relation to such data and broadly defines "processing" to cover automated operations including collection, storage, retrieval, use, combination, sharing and erasure.[15] This broad definition is important where the activities involved in an AI system's lifecycle can be deemed to be processing. While an AI-based customer service system may process information that identifies users and their interactions, information may be processed within an analytics system to make predictions or classifications. The Act's primary burden of compliance falls on the Data Fiduciary, even for processing processes for by a Data Processor. [16]Section8.1 requires that compliance with the Act and Rules occur, appropriate technical and organisation measures, security measures and security breaches, as well as accuracy and consistency in situations where personal data is likely to be used to reach a decision affecting the Data Principal. This is particularly applicable where erroneous data may result in erroneous AI-assisted decisions. Section 5 and 6 further set out requirements[17] concerning notice and consent, though AI's poses challenges for reconciling between legal compliance and meaningful transparency. An individual may receive notice that technically identifies the processing's purpose without comprehending the way data may be subsequently used within a complex AI system. The legal question is thus concerned with whether the existing requirements are sufficient to provide meaningful awareness of substantial AI-related practices concerning processing.

B. CONSENT, PURPOSE AND AI TRAINING

Consent, is particularly problematic within the context of AI. The DPDP Act provides for mechanisms through which Data Principals can grant, manage, review and withdraw consent, recognising however that there are specified legitimate purposes. AI can process information for model development, improvement, personalisation or inference, throwing up issues concerning whether consent given for a primary service will adequately cover any non-

[14] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Digital Personal Data Protection Rules, 2025, Ministry of Electronics & Information Technology, Government of India (2025).
[15] Digital Personal Data Protection Act, No. 22 of 2023, § 2(t), (i), INDIA CODE (2023).
[16] Digital Personal Data Protection Act, No. 22 of 2023, § 8, INDIA CODE (2023).
[17] Digital Personal Data Protection Act, No. 22 of 2023, §§ 5–6, INDIA CODE (2023).

apparent subsequent use of the given information. This challenge is particularly prevalent in the case of generative AI and the large-scale development of models. The availability of the information does not directly determine the legality of using the data. Where publicly available information constitutes personal data, the involved processing must be considered in the applicable statutory framework. Accordingly, accessibility of data should not be equated to its legal processing.

C. ACCURACY, ERASURE AND THE AI LIFECYCLE

The framework for DPDP also poses problems associated with implementation concerns of correction and erasure. Section 12 empowers Data Principals with the rights of correction of corrections, completion, updating and erasure of personal data, restricted to statutory conditions and exceptions[18]. Section 8, further provides for the erasure of data where the specified purpose is not being fulfilled, though there are applicable legal requirements for retention. The technology of AI presents challenges for these rights where deleting information from a database is not necessarily equivalent in effect to removing the impact on a trained model; determining whether particular data points has had an effect on model parameters or outputs can be technically challenging. This does not mean that the right to erasure necessitates a specific technical method of "unlearning", however, it does highlight the challenge in applying familiar data-governance concepts to machine learning systems. Accuracy raises a similar consideration. Where personal data is used to make decisions affecting the individuals concerned, the requirements of the Act concerning completeness, accuracy and consistency become ever more significant. Effective accountability will thus depend on organisations to able to trace relevant data practices and to able to react when inaccurate information underpins adverse outcomes.

D. THE EVOLVING REGULATORY FRAMEWORK

The DPDP Act was granted assent by the President in August 2023 and its implementation has been implemented on a phased timeline[19]. The notification of commencement in November 2025 foresees staggered commences of specified provisions from 13 November 2025, as well as several major provisions from eighteen months later. The Digital Personal Data Protection

[18] Digital Personal Data Protection Act, No. 22 of 2023, § 12, INDIA CODE (2023).
[19] Digital Personal Data Protection Act, No. 22 of 2023, Ministry of Electronics & Information Technology, Government of India (assented to Aug. 11, 2023); Ministry of Electronics & Information Technology, Digital Personal Data Protection Rules 2025-Enforcement Timeline (Nov. 14, 2025)

Rules, 2025 were notified on 14 November 2025 and further staggered commencement[20]. The DPDP regime should be viewed as an evolving framework rather than fully absent or perfectly matured. Its effectiveness at mitigating risks to privacy associated with AI will depend on implementation, institutional capacity and interpretation of its requirements as technologies develop. Notwithstanding, the framework offers a significant basis because it attaches responsibilities onto identifiable organisations, rather than perceiving of AI systems as autonomous legal entities. Their requirements regarding lawful processing, notice, consent, accuracy, security, erasure and accountability are able to address important aspects of privacy risks associated with AI. The continued challenge remains whether these general provisions are sufficiently able to respond to issues emerging with large-scale model training, automated decision making, inference and the challenges of tracking the personal information through complex AI systems. Data protection is thus not independent of the of AI, but constitutes one of its key elements. As AI systems become more increasingly data intensive, it is the that proper governance will require organisations to demonstrate lawful, transparent and accountable data practices throughout the AI's life cycle.

6. ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY RIGHTS

Artificial intelligence poses significant challenges to traditional intellectual property law. The principal legal issues involve the use of copyrighted material for AI training, protection of AI-generated works, attribution of authorship and the treatment of AI-assisted inventions under patent law.

A. COPYRIGHT AND AI-GENERATED WORKS

The Copyright Act, 1957 is primarily concerned with human creativity[21] and with recognised categories of works which have copyright subsistent. Section 13 identifies literary, dramatic, musical and artistic work, cinematograph films and sound recordings as categories to copyright subsist, as well as defining section 2(d) the definition of "author" by reference to human or juridical actors linked with various categories of works[22]. This gives rise to uncertainty where an output is generated substantially through an AI system. It would be difficult to recognise an AI system as an independent author under existing Indian legal framework because legal rights

[20] Digital Personal Data Protection Rules, 2025, Ministry of Electronics & Information Technology, Government of India (Nov. 14, 2025).
[21] Copyright Act, No. 14 of 1957, §§ 13, 14, INDIA CODE (1957).
[22] Copyright Act, No. 14 of 1957, § 13, INDIA CODE (1957), Copyright Act, No. 14 of 1957, § 2(d), INDIA CODE (1957).

and obligations are usually attributable to human or juridical persons, rather than software. A more sustainable approach in the legal context is examining the nature and extent of the human creative contribution. Where a person maintains meaningful creative control over the selection, arrangement or modification of AI-generated material, existing principles of copyright can be continued to be applicable. Where there is insufficient human creative contribution when producing outputs, however, the case of independent copyright protection is significantly reduced. This leads to uncertainty regarding ownership. Where copyright subsists for an AI-assisted output work, if the rights belong the owner of user, the developer, commissioning entity, or other actor depends upon the circumstances and applicable contractual and statutory principles. The absence of a specific AI-specific authorship rule hence creates uncertainty in terms of the attribution of ownership for creators and the business application of generative AI.

B. AI TRAINING AND COPYRIGHT INFRINGEMENT

A further challenge involves the use of copyrighted works as training material. AI developers may process vast datasets containing literary, artistic, audio-visual or other types protected works. The legal question is not necessarily resolved by the fact that the final AI output differs from the training material; potential infringement may arise from the initial copying or processing of protected works for the development of models. Indian copyright law offers statutory exceptions, including fair dealing under section 52. It is not clear as to which forms of AI training fall within an exception, so as to what precise copy of copyrighted material is used. It is thus inappropriate to assume that either all AI training is automatically infringing or that all training activity is protected to be infringing. The challenge highlights the difficulty of incorporating conventional copyright categorisations to AI. Traditional copyright law addresses identifiable acts of reproduction and communication, while AI development may include large-scale computational processing of various works for purposes not envisioned when developing the statutory framework. India must therefore be between a balance between incentivising creators and fostering legitimate technological developments.

C. PATENTS AND AI-ASSISTED INVENTIONS

AI poses another set of questions as concerns inventorship and human contributions under patent law. The Patents Act, 1970 is shaped around legal persons and the concept of an inventor, causing difficulties where an AI system is suggested to have created an independent invention

independently[23]. The stronger of the status quo is the up to maintain the legal status of patent rights and inventorship with human accountability and not bestow independent legal personalities upon AI systems. While AI may serve as tools in the invention process, it is up to the legal system to determine the human actor and responsible for the invention and patenting process. This maintains the existing structure of the patent system but acknowledges the increasing role of machine assistance. India IP regime hence offers principles capable of answering several potential AI issues, however uncertainty remains regarding issues with training information, attribution and ownership. Specific clarification may be preferable to an entirely isolated IP regime concerning AI.

7. AI-GENERATED CONTENT, DEEPFAKES AND INTERMEDIARY LIABILITY

AI systems can generate realistic text, images, audio and video, giving rise to legal issues including impersonation, fraud, reputational damage and misinformation. Deepfakes pose the most important as they can cause potentially made material to be hard to distinguish from genuine content. India's main regime concerning content on the Internet remains the Information Technology Act, 2000 and the Information Technology Rules, 2021. Section 79 grants intermediary protection subject to specific conditions, while the Rules provide for due diligence obligations[24]. The 2026 changes to the IT Rules regarding synthetically-generated information show India's attempt to mitigate synthetic media through the statutory regime of technology, rather than a separate AI-specific statute. The major legal issue lies in assigning responsibility between the creator of harmful synthetic content and the intermediary where through which it is disseminated. Unlimited platform liability for content could possibly cause overabundant removal of lawful content, while solely relying upon individual users may be deficient where potentially harmful material proliferates quickly. Responsibility should be balanced according to creation, distribution, knowledge and control. This regime also needs to remain consistent with Article 19(1)(a).[25] The creation of AI-generated content is not unlawful merely because it is AI-generated; regulation should instead respond to legally cognisable harms within the constitutional provisions that allow for such in Article 19(2).[26] The goal should be to mitigate misleading or harmful synthetic content without creating an overbroad scheme that can stifle legitimate expression.

---

[23] Patents Act, No. 39 of 1970, §§ 2(1)(p), 6, 7, INDIA CODE (1970).
[24] Information Technology Act, No. 21 of 2000, § 79, INDIA CODE (2000); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–4.
[25] INDIA CONST. art. 19, cl. 1(a).
[26] INDIA CONST. art. 19, cls. 1(a), 2; Shreya Singhal v. Union of India, (2015) 5 SCC 1, 80–82.

8. LIABILITY, ACCOUNTABILITY AND ATTRIBUTION IN AI SYSTEMS

AI raises complex legal issues regarding responsibility if an AI-assisted system causes damage. Traditional legal concepts generally identify a person or an entity in terms of whose actions can be traced to the infliction of harm, while AI may be a number of parties, including developers, deployers, users and platforms during different stages of the lifecycle of the system. An unexpected or erroneous AI output is cannot immediately lead to treating the technology as an independent legal carrier of legal burdens. Depending on the circumstances, responsibility may arise through established concepts of negligent, contractual responsibility, consumer protection or other applicable legal concepts.[27] The main problems lie around the issues of causality, foreseeability and the extent of each party's control. India should to keep human and institutional accountability but calibrate responsibility according to the role of an actor the designing, deployment, supervision of using an AI system. High-impact applications should be accompanied by adequate documentation, monitoring and human review. However, the lack of a uniform AI liability regime creates issues of uncertainty regarding responsibility during the AI life cycle. Specific clarification could help enhance predictability but ensure the courts' ability to base cases on well-established principles according to factual circumstances.

9. ARTIFICIAL INTELLIGENCE IN EMPLOYMENT, CONSUMER PROTECTION AND THE JUSTICE SYSTEM

Artificial intelligence increasingly plays a role in employment processes, consumer engagement and legal procedures, throwing into legal issues concerning fairness of accuracy, accountability and human supervision. These implementations show that the legal impact of AI depends not only upon the technology but the significance of the decision in which the technology is used.

A. EMPLOYMENT AND ALGORITHMIC DECISION MAKING

AI-assisted recruitment and work systems can increase efficiency but risk perpetuate discriminatory factors contained in past information. Indian law lacks a comprehensive AI-specific regime governance algorithm employment decision.[28] Constitutional equality remains relevant for employment by the State, as well as applicable labour, contractual and anti-discrimination principles may determine private employment based on circumstances.

---

[27] Indian Contract Act, No. 9 of 1872, INDIA CODE (1872); Consumer Protection Act, No. 35 of 2019, INDIA CODE (2019).
[28] INDIA CONST. art. 14.

B. CONSUMER PROTECTION

AI-driven chatbots, recommendation systems, personal advertising and automated decision making can have significant impact on consumer choices. The Consumer Protection Act, 2019 provides us a framework of principles surrounding consumer rights, unfair trade practices and misleading advertisements.[29] Automation does not eliminate accountability where an AI-produced representation leads to actionable consumer harm. Accountability must therefore be tethered to the business operating the system, especially where consumers cannot realistically confirm the accuracy of an automated representation.

C. ARTIFICIAL INTELLIGENCE AND THE JUSTICE SYSTEM

AI can facilitate legal research, document analysis and case management, but inaccurate feedback and artificial authorities raise concerns about accuracy and formal integrity. AI should thus serve as an auxiliary tool, but not replace judicial reasoning. Responsibility for legal conclusions must therefore be transferred to the human decision maker, who must verify the material generated by the AI independently. The extent of the legal fallout of an AI-assisted conclusion the stronger the obligations of human oversight, reviewability and accountability.

10. INDIA'S EMERGING AI GOVERNANCE FRAMEWORK: A CRITICAL ASSESSMENT

India's AI governance is emerging through legislative instruments, sectoral regulation, government initiatives and institutional mechanisms. Its fragmented nature enables current legal principles to persist in the face of technological change, although presenting possibilities of ambiguity where a single application of AI simultaneously interacts with multiple legal regimes. A sector-based approach ensures flexibility, but a comprehensive statute could ensure standard definitions and accountability mechanisms. A hybrid structure should therefore be adopted: maintaining sectoral regulation, but establishing common baseline safeguards for a better impact Artificial Intelligence, including transparency, accountability, oversight and risk assessment. The European Union's AI [30]Act provides a potential framework for comparison through its risk-based framework. India does not need to pursue this exact model, given the varying nature of its constitutional composition, institutions and economic conditions. Stricter obligations may be necessary where AI can have the potential impact fundamental rights or

[29] Consumer Protection Act, No. 35 of 2019, §§ 2(9), 2(47), 21, INDIA CODE (2019).
[30] Regulation (EU) 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).

important economic and social considerations. India therefore needs more coherence, but does not necessarily require an omnibus AI statute yet. The more viable aim is to reconcile current legal protections by common principles of accountability, while allowing for sectoral regulation to effectively address sector-specific risks.

11. REGULATORY GAPS IN INDIA'S AI FRAMEWORK

India does not exist in full regulatory vacuum, but notable gaps exist. Its legal framework is fragmented, it’s across parties across developers, deployers, platforms and users remain undefined and its general requirements of transparency and explainability are insufficiently developed. Questions about AI-generated works and training data remain unresolved and while algorithmic discrimination is complex to address, as it may be a byproduct of indirect bias in data or system design. Another problem is evidentiary. Even where a legal remedy is available, an impacted individual will face difficulties establishing how an AI system produced a certain result, or which actor was responsible for it. This establishes the importance of transparency and documentation, not merely as a regulatory preference, but necessary conditions of meaningful legal accountability. The speed of technological development also creates a structural challenge for law-making that must move at a slower pace, despite the speed of technological innovation. These gaps provide a rationale for a coherent governance architecture that reconciles existing protections with focused obligations where standard legal principles are insufficient.

12. RECOMMENDATIONS

India should embrace a principle of accountable risk sensitive innovation. This entails that the low-risk Artificial Intelligence should avoid imbalances in compliance requirements, while high impact systems impacting fundamental rights, employment, vital services, financial access or other important interests should benefit from stronger safeguards. High-impact AI should be associated with meaningful human oversight, documentation, the ability, transparency in terms of purpose, important data practices, limitations and responsibility. Responsibility should be distributed between developers, deployers and users, based on their respective roles and control, knowledge and contribution to the relevant harm, rather than on technical ownership of the system. India must also strengthen its protections against algorithmic discrimination, with accessible review and redress mechanisms. Coordination between multiple authorities dealing with data protection, consumer protection, intellectual property, online content and sectoral regulation should be improved. Regulation must remain

technology-agnostic and flexible, subject to periodic review to reflect advancements to technological development.

13. CONCLUSION

AI challenges existing legal assumptions regarding privacy, equality, intellectual property, freedom of expression, role of intermediaries and their liability. India's existing framework provides important mechanisms to deal with these harms, but gaps exist in terms of its coherence, uncertainty over accountability, insufficient algorithmic transparency and discrimination, training data and AI-generated works. The major challenge, therefore, is not whether an independent AI statute for India, but whether its extant legal architecture allows for clear accountability were technology cuts across conventional legal boundaries. India should thus seek to promote accountable, risk-sensitive innovation: stronger protections for high-impact systems, proportionate regulation for lower-impact systems and effective human responsibility across the AI lifespan. The goal is not to completely remove artificial intelligence through regulation, but to ensure that technological innovation is still compatible with constitutional rights, legal certainty and public trust. The legitimacy of India's AI framework will always depend upon assuring that greater technological capability does not lead to reduced legal accountability.