

THE LEGAL CONUNDRUM OF AI USAGE IN INDIA: AN ANALYSIS

Anitha K N

Associate Professor
Government Law College, Hassan

ABSTRACT

India stands at a critical inflection point in its relationship with Artificial Intelligence. As the world's most populous democracy and a rapidly emerging digital economy, India is simultaneously a massive consumer, an ambitious developer, and a prospective global standard-setter for AI technologies. Yet the country's legal architecture — spanning constitutional guarantees, sector-specific statutes, tort principles, and nascent regulatory instruments — was designed for an analogue era and is profoundly ill-equipped to address the multifarious challenges that AI systems pose. This article undertakes a comprehensive doctrinal and policy analysis of the legal conundrum surrounding AI usage in India. It examines five overlapping legal domains: data protection and privacy, intellectual property, civil and product liability, sector-specific regulation, and constitutional rights. Across each domain, the article identifies critical lacunae, contradictions, and interpretive ambiguities in the existing legal framework. Drawing on comparative jurisprudence from the European Union, United States, and United Kingdom, and engaging with the Government of India's evolving policy posture — including the National Strategy for Artificial Intelligence, the Digital Personal Data Protection Act 2023, and the draft frameworks emerging from MEITY and NITI Aayog — the article argues that India requires a dedicated, risk-tiered AI governance statute, supported by institutional capacity building, judicial training, and international alignment, to realise the transformative potential of AI while safeguarding fundamental rights.

Keywords: Artificial Intelligence law India, DPDP Act 2023, AI liability, algorithmic accountability, intellectual property AI, constitutional rights AI, AI regulation India, digital governance

1. INTRODUCTION

India's digital economy is experiencing unprecedented growth. With over 900 million internet users, a booming fintech ecosystem, a globally competitive IT sector, and ambitious government digitalisation programmes — from Aadhaar to Digital India to the Unified Payments Interface — the conditions for large-scale AI adoption are firmly in place. Indian enterprises across healthcare, agriculture, finance, education, and manufacturing are integrating AI tools at accelerating pace, and the Government of India has expressly positioned AI as central to its vision of becoming a USD 5 trillion economy.

Yet the enthusiasm for AI adoption has outpaced the development of legal and regulatory safeguards. As AI systems increasingly mediate consequential decisions — credit approvals, disease diagnosis, criminal risk assessment, employment screening, content moderation — the absence of clear legal rules governing their development, deployment, and accountability creates systemic risks: to individual rights, to market integrity, and to democratic governance itself. India confronts what may be termed a 'legal conundrum': the challenge of governing a fast-evolving, technically complex, and socially pervasive technology within a legal framework designed for a fundamentally different technological era.

This conundrum has several distinctive dimensions in the Indian context. First, India's legal system reflects a colonial inheritance substantially modified through post-independence constitutional and statutory development, but not yet adapted to address AI-specific challenges. Second, India's regulatory capacity is uneven across sectors: some domains, such as financial services and telecommunications, have relatively sophisticated regulatory institutions, while others, such as healthcare AI and autonomous systems, remain largely ungoverned. Third, India's democratic context — characterised by a strong fundamental rights framework under Part III of the Constitution, an independent judiciary with a robust tradition of public interest litigation, and deep social inequalities that AI systems risk entrenching — makes the stakes of governance choices especially high.

Central Argument: India does not merely face a gap between existing law and emerging technology — it faces a structural legal conundrum that requires not piecemeal amendment but a coherent, rights-centred, risk-proportionate AI governance architecture built expressly for the challenges of the twenty-first century.

This article proceeds as follows. Section 2 surveys India's current AI policy landscape. Section 3 analyses the data protection and privacy dimensions of AI law. Section 4 examines intellectual property challenges raised by AI. Section 5 addresses liability frameworks. Section 6 reviews sector-specific regulatory challenges, set out in a comparative table. Section 7 considers AI's implications for constitutional rights. Section 8 undertakes a comparative analysis. Section 9 offers conclusions and recommendations.

2. INDIA'S EVOLVING AI POLICY LANDSCAPE

2.1 From National Strategy to Regulatory Intent

India's engagement with AI governance began in earnest with the publication of the National Strategy for Artificial Intelligence (NSAI) by NITI Aayog in 2018. The NSAI framed AI primarily through an economic development lens — emphasising AI's potential to add USD 957 billion to India's GDP by 2035 — while acknowledging, in more general terms, the need to address ethical and social concerns. It identified five priority sectors for AI deployment: healthcare, agriculture, education, smart cities and infrastructure, and smart mobility.

Subsequent policy documents reflected a gradual deepening of governance thinking. The Responsible AI for All report (2021) by NITI Aayog introduced the concept of a principles-based approach to AI ethics, identifying safety, reliability, fairness, privacy, transparency, accountability, and prevention of harm as core principles. However, these documents remained advisory in character, with no statutory backing. The critical regulatory gap persisted: India had an AI aspiration but not an AI law.

2.2 The MEITY Posture and the Advisory on LLMs

The Ministry of Electronics and Information Technology (MEITY) has been the primary locus of AI regulatory activity within the central government. In March 2024, MEITY issued an advisory requiring that AI platforms accessible to Indian users obtain government approval before deployment, and that outputs of AI systems carry watermarks or other disclosure labels. The advisory generated significant controversy — characterised by critics as constituting prior restraint on AI services — and was subsequently withdrawn and reissued in modified form without the prior approval requirement.

The episode was instructive. It illustrated both the government's genuine concern about AI risks — particularly around electoral misinformation and deepfakes — and the institutional inexperience in translating that concern into legally precise and proportionate regulatory

instruments. It also highlighted the tension between the government's simultaneous objectives of promoting India as an AI innovation hub and addressing AI-related harms.

2.3 The Digital Personal Data Protection Act, 2023

The most significant recent legislative development affecting AI is the Digital Personal Data Protection Act, 2023 (DPDP Act), which received Presidential assent in August 2023 and whose substantive provisions await notification. The DPDP Act establishes a framework for the processing of digital personal data, introduces the role of the Data Protection Board as an adjudicatory authority, and imposes obligations on 'data fiduciaries' — entities that determine the purpose and means of data processing. Its relevance to AI is substantial, since AI systems are fundamentally data-processing systems that often process personal data at massive scale.

However, as discussed in Section 3 below, the DPDP Act leaves critical AI-specific issues unaddressed, and its adequacy as an AI governance instrument is seriously in question.

3. DATA PROTECTION, PRIVACY, AND AI

3.1 The Constitutional Foundation: Puttaswamy and Its Implications

The constitutional basis for AI-related privacy claims in India was dramatically strengthened by the Supreme Court's landmark nine-judge bench ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The Court unanimously held that the right to privacy is a fundamental right under Articles 14, 19, and 21 of the Constitution. The judgment is significant for AI governance in several respects: it recognised informational privacy — the right to control personal data — as a component of the right to privacy; it established that privacy may only be limited by law that is just, fair, and reasonable; and it acknowledged the emerging significance of data protection in the digital context.

Puttaswamy provides a constitutional foundation for challenging AI-related privacy violations, including mass surveillance through facial recognition, profiling through data aggregation, and inferences drawn by AI systems about sensitive attributes. However, the translation of this constitutional principle into operative legal rules requires statutory elaboration that the DPDP Act only partially provides.

3.2 Critical Lacunae in the DPDP Act vis-a-vis AI

The DPDP Act represents a significant advance over the pre-existing legal vacuum, but its adequacy as an AI governance instrument is circumscribed by several important omissions. First, the Act contains no provision on automated decision-making or profiling analogous to Article 22 of the EU General Data Protection Regulation, which grants individuals the right not to be subject to solely automated decisions with significant effects, and the right to obtain human review. In an environment of rapidly expanding algorithmic decision-making in credit, employment, and public services, this omission is particularly consequential.

Second, the Act's consent framework — which relies on notice-and-consent as its primary legitimating mechanism — is poorly suited to the realities of AI training. Modern AI systems are trained on enormous datasets that may include personal data scraped from public sources, collected for unrelated purposes, or generated as a byproduct of digital activity. Obtaining meaningful, granular consent for such training is practically impossible, yet the Act provides no adequate alternative basis for processing personal data for AI training.

Third, the Act establishes no right of explanation — no mechanism by which an individual affected by an AI-driven decision can access an intelligible account of how that decision was reached. Without a right of explanation, the formal remedies the Act provides are of limited

practical value: an individual cannot effectively contest a decision whose basis they cannot understand.

Key Gap: The DPDP Act, 2023 is silent on automated decision-making, profiling rights, and the right to explanation — three pillars of AI accountability that are foundational in comparable international frameworks.

4. ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY LAW

4.1 Authorship of AI-Generated Works

The Copyright Act, 1957, as amended, defines 'author' in section 2(d) to mean, in the case of a computer-generated work, 'the person who causes the work to be created'. This provision, introduced in the 1994 amendment to address computer-assisted works, was drafted long before the emergence of AI systems capable of generating independently original creative expression. The critical question is whether a person who provides a prompt to a generative AI system — without creative contribution to the substantive output — 'causes' the work to be created in a legally meaningful sense.

Indian courts have not yet addressed this question, but the analogical interpretation of section 2(d) is contested. A narrow reading would deny copyright protection to outputs where the AI's creative contribution predominates, leaving such works in the public domain. A broad reading would vest copyright in the user of the AI system, regardless of the depth of creative contribution. Neither outcome is entirely satisfactory: the former creates uncertainty around the commercial value of AI-generated content, while the latter may grant windfall rights to entities that have contributed nothing of creative substance.

4.2 Training Data and Copyright Infringement

The process by which large AI models are trained — ingesting billions of text, image, audio, and video files to identify statistical patterns — raises profound copyright questions. Much of this training data is protected by copyright. The training process involves reproduction of the data in model weights, and the outputs of trained models may in some cases reproduce elements of training data in recognisable form. Whether this constitutes infringement under Indian law depends on several unresolved questions: whether the act of training constitutes 'reproduction' within the meaning of section 14 of the Copyright Act; whether any exception — including the fair dealing provision of section 52 — applies; and whether Indian courts will follow the emerging trend in some jurisdictions of recognising a 'text and data mining' exception.

The Copyright Act's section 52(1)(a), which permits fair dealing for the purposes of research or private study, may offer limited protection, but its application to commercial AI training at massive scale is uncertain. The absence of a dedicated text and data mining exception — which has been adopted in the European Union, Japan, and Singapore — constitutes a significant competitive disadvantage for the Indian AI industry and creates legal uncertainty for both developers and copyright holders.

4.3 Patentability of AI-Assisted Inventions

The Patents Act, 1970, requires that an invention be made by a 'person' to be patentable. Section 3(k) of the Act explicitly excludes mathematical methods, business methods, and computer programs per se from patentability, a provision historically interpreted to exclude a wide range of software-related inventions. The application of these provisions to AI-assisted inventions — where an AI system plays a substantive role in identifying inventive solutions — is deeply uncertain.

The Indian Patent Office's Guidelines for Examination of Computer-Related Inventions (2017, revised 2019) provide some guidance on software patentability but do not address AI-generated inventions. The question of whether an AI system can be named as an inventor — resolved in the negative by courts in the United States, United Kingdom, Australia, and the European Patent Office in the DABUS cases — has not been definitively addressed in India, though the requirement of a human inventor appears implicit in the Act's statutory scheme.

5. CIVIL LIABILITY AND AI: AN UNCHARTED TERRITORY

5.1 The Attribution Problem

Civil liability for AI-caused harm raises what scholars have termed the 'attribution problem': when an AI system causes injury, who bears legal responsibility? The chain of causation in AI-mediated harm typically involves multiple actors — the developer of the underlying model, the entity that fine-tuned or adapted the model for deployment, the operator who incorporated the model into a product or service, and the end user whose instructions shaped the AI's output. Traditional tort law, developed around dyadic relationships and proximate cause analysis, is poorly equipped to disaggregate liability across this chain.

Under Indian tort law — largely judge-made and drawing on common law principles, with some statutory codification in specific contexts — liability for AI harm could in principle be established under negligence (failure to exercise reasonable care in development or deployment), strict liability (if the AI system constitutes an 'inherently dangerous activity' under the rule in *M.C. Mehta v. Union of India*), or vicarious liability (if the AI acts as an agent of the operator). However, none of these doctrines maps cleanly onto AI-specific scenarios, and courts have not yet had occasion to develop AI-specific liability principles.

5.2 Consumer Protection and Product Liability

The Consumer Protection Act, 2019 introduced product liability provisions in Chapter VI that impose liability on manufacturers, sellers, and service providers for defective products and deficient services. The applicability of these provisions to AI systems is uncertain for several reasons. First, it is unclear whether AI software constitutes a 'product' under the Act's definition, or whether AI-enabled services constitute 'services' subject to deficiency claims. Second, the Act's product liability framework focuses on manufacturing defects and design defects in physical products, making its application to emergent AI behaviours — where harms arise from the system's learned responses to novel inputs rather than from a flaw in the design as originally implemented — conceptually strained.

The Central Consumer Protection Authority (CCPA) has not yet issued guidance specifically addressing AI-related consumer harms, and the sector-specific regulators that oversee the domains where AI is most heavily deployed — the RBI, SEBI, IRDAI, and the emerging digital health ecosystem — have addressed AI only in piecemeal fashion.

5.3 The Case for a Dedicated AI Liability Regime

The inadequacy of existing liability frameworks suggests the need for a dedicated AI liability statute that specifies: the standard of care applicable to AI developers and deployers; the allocation of liability across the AI supply chain; the evidentiary rules governing proof of AI-caused harm (including presumptions that shift the burden to defendants in possession of the relevant technical information); and the remedies available to AI-harmed individuals, including compensation, injunction, and mandatory disclosure. The EU AI Liability Directive — which introduces a rebuttable presumption of causation in AI cases where the plaintiff

demonstrates breach of duty and plausible causation — offers a useful model, though its specific provisions would require adaptation to India's legal context.

6. SECTOR-SPECIFIC REGULATORY CHALLENGES

The following table sets out the principal legal gaps in key sectors where AI deployment is most intensive in India:

Legal Domain	Current Statute	Gap / AI-Related Challenge
Data Protection	DPDP Act, 2023	No explicit regulation of automated decision-making; consent framework inadequate for AI training datasets; no right to explanation of algorithmic decisions.
Intellectual Property	Copyright Act, 1957; Patents Act, 1970	AI-generated works lack authorship under existing law; training data ingestion may infringe copyright; patentability of AI-assisted inventions unsettled.
Liability & Tort	IPC, 1860; Consumer Protection Act, 2019	No statutory framework for product liability of algorithmic systems; negligence attribution in autonomous decision chains unclear.
Financial Services	SEBI, RBI, IRDAI Regulations	Algorithmic trading rules exist but generative AI in investment advice, credit scoring, and insurance underwriting lacks comprehensive oversight.
Healthcare	Drugs & Cosmetics Act; MCI Regulations	AI-assisted diagnostics and surgical robotics unaddressed; liability of AI clinical decision support systems undefined.
Criminal Justice	CrPC, 1973 (now BNSS, 2023)	Use of facial recognition and predictive policing without statutory mandate; admissibility of AI-derived evidence contested.
Competition Law	Competition Act, 2002	Algorithmic collusion and data monopoly by AI platforms not explicitly addressed; CCI capacity gaps in technical market analysis.

Across these sectors, a common pattern emerges: India has sophisticated regulatory institutions with substantial technical expertise, but their mandates, instruments, and human capital were developed for pre-AI technologies and require systematic adaptation. The Reserve Bank of India's guidance on model risk management, SEBI's algorithmic trading regulations, and IRDAI's emerging digital insurance frameworks each represent incremental adaptations, but the sum of these parts does not constitute a coherent AI governance architecture.

7. AI AND CONSTITUTIONAL RIGHTS

7.1 Right to Equality and Non-Discrimination

Article 14 of the Constitution guarantees equality before law and equal protection of laws. Article 15 prohibits discrimination on grounds of religion, race, caste, sex, or place of birth. AI systems that perpetuate or amplify existing social biases — as has been documented in facial recognition systems less accurate on darker-skinned faces, credit-scoring models that proxy caste or religion through correlated variables, and hiring algorithms that disadvantage women or religious minorities — raise serious constitutional concerns under these provisions.

The constitutional framework for algorithmic discrimination has not yet been tested before Indian courts, but the doctrinal basis for such challenges is strong. The Supreme Court's expansive reading of Article 14 — which requires not merely formal equality but substantive reasonableness of classification — provides a potential basis for challenging AI systems whose outputs systematically disadvantage constitutionally protected groups. The question is one of standing, evidence, and institutional competence: how can an affected individual demonstrate that an AI system discriminated against them on prohibited grounds, when the system's reasoning is opaque and its developers possess all the relevant technical information?

7.2 Freedom of Speech and AI-Mediated Information

Article 19(1)(a) of the Constitution guarantees freedom of speech and expression. AI systems that generate, amplify, or suppress speech — including generative AI content, algorithmic content moderation, and AI-driven recommendation systems — raise complex Article 19 questions. The government's 2024 advisory on LLM watermarking and disclosure, and the Intermediary Guidelines and Digital Media Ethics Code (IT Rules, 2021) as amended, impose obligations on digital platforms that have significant implications for AI-generated and AI-curated content.

The constitutional validity of content moderation mandates imposed on AI systems — which require AI to identify and remove certain categories of content — has not been definitively adjudicated, though the Supreme Court's decision in *Shreya Singhal v. Union of India* (2015), which struck down section 66A of the IT Act on grounds of overbreadth and vagueness, provides a framework for evaluating the constitutionality of AI-related speech regulations.

7.3 Surveillance, Facial Recognition, and Article 21

The most pressing constitutional challenge raised by AI in India concerns the state's deployment of facial recognition technology (FRT) for law enforcement and public management purposes. India has deployed or piloted FRT across multiple contexts — the Automated Multi-modal Biometric Identification System (AFIS), police deployments at public gatherings, the Smart Cities Mission, and Aadhaar-linked identity verification — without any statutory basis specifically authorising such surveillance, and without adequate mechanisms for oversight, redress, or data minimisation.

In *Puttaswamy*, the Supreme Court identified proportionality as a constitutional requirement for any limitation of fundamental rights, including privacy. The deployment of mass FRT surveillance — which affects the privacy and expressive freedom of all persons in public spaces, not merely those suspected of wrongdoing — almost certainly fails a proportionality test absent specific statutory authorisation, a clear legitimate aim, necessity and subsidiarity requirements, and robust oversight mechanisms. The absence of litigation directly

challenging FRT deployments reflects practical barriers to access to justice rather than constitutional legitimacy.

Constitutional Alert: India's widespread deployment of facial recognition technology for surveillance and law enforcement lacks a dedicated statutory basis and appears inconsistent with the proportionality requirements established in Puttaswamy — creating a profound constitutional lacuna.

8. COMPARATIVE PERSPECTIVES: LESSONS FOR INDIA

8.1 The European Union: Comprehensive Risk-Based Regulation

The EU AI Act (2024) offers the most comprehensive binding AI governance framework currently in operation. Its risk-tiered architecture — categorising AI applications as unacceptable risk (prohibited), high risk (stringent pre-market requirements), limited risk (transparency obligations), and minimal risk (voluntary codes) — provides a model for calibrating regulatory intensity to actual harms. The Act's requirements for high-risk AI systems are particularly instructive for India: mandatory conformity assessments, technical documentation, human oversight mechanisms, transparency to users, robustness and accuracy requirements, and registration in a public EU database.

The EU framework also establishes the European AI Office as a supervisory body with specific authority over general-purpose AI models, and introduces significant penalties — up to 7% of global annual turnover — for the most serious violations. India can draw on the EU model for its tiered risk approach and institutional design, while adapting its specific provisions to India's legal culture, democratic context, and development objectives.

8.2 The United Kingdom: Principles-Based Sector-Led Governance

The United Kingdom's post-Brexit AI governance framework, articulated in the 2023 AI White Paper and subsequent implementation documents, takes a deliberately light-touch, principles-based approach, delegating implementation to existing sector regulators under five cross-cutting principles: safety, security and robustness; transparency and explainability; fairness; accountability and governance; and contestability and redress. The UK approach reflects a conscious policy choice to avoid ex ante comprehensive regulation in favour of adaptive, sector-specific governance.

India might draw on the UK model's flexibility and its emphasis on building regulatory capacity within existing institutions. However, the UK approach's reliance on voluntary adoption by industry and existing regulators' technical capacity — both of which are more limited in India than in the UK — suggests that a purely sector-led approach would be insufficient in the Indian context.

8.3 Singapore: Practical Governance Tools

Singapore's AI governance approach — centred on the Model AI Governance Framework, the AI Verify testing toolkit, and the Tripartite Guidelines on Fair Employment Practices — is notable for its emphasis on practical implementation tools rather than abstract principles or comprehensive legislation. The AI Verify framework provides organisations with a structured methodology for testing AI systems against a defined set of ethical principles, generating verifiable reports that can be shared with regulators and the public.

For India, Singapore's approach offers a useful model for building AI governance capacity incrementally, providing enterprises with practical compliance tools before comprehensive

legislation is enacted, and establishing the empirical evidence base needed to inform future regulation.

9. CONCLUSIONS

The foregoing analysis establishes that India confronts a genuine legal conundrum in AI governance: a technology of transformative power and pervasive social reach that its existing legal framework is structurally inadequate to govern. The inadequacy is not merely a matter of gaps to be filled by incremental amendment; it reflects a deeper mismatch between the assumptions underlying India's legal architecture — individual agency, proximate causation, authorial creativity, stable product characteristics — and the realities of AI systems that are probabilistic, emergent, opaque, and continuously evolving.

The following recommendations are advanced to address this conundrum:

- **Enact a dedicated AI Governance Act** that establishes a risk-tiered regulatory framework, defines categories of prohibited and high-risk AI applications, imposes mandatory transparency, accountability, and human oversight requirements on deployers of high-risk systems, and creates enforcement mechanisms with meaningful penalties.
- **Establish an AI Regulatory Authority of India (AIRAI)** with technical expertise, adequate resourcing, cross-sectoral jurisdiction, and a mandate that includes standard-setting, conformity assessment oversight, incident investigation, and international coordination.
- **Amend the DPDP Act** to introduce rights against purely automated decision-making with significant effects, a right to explanation of algorithmic decisions, and specific provisions for the lawful processing of personal data for AI training purposes.
- **Enact a dedicated Text and Data Mining exception** in the Copyright Act to provide legal clarity for AI training activities while preserving the rights of copyright holders through appropriate remuneration mechanisms.
- **Introduce an AI Liability framework** — whether as part of a dedicated AI Act or as amendments to the Consumer Protection Act — that specifies standards of care, allocates liability across the AI supply chain, and introduces evidentiary presumptions that address the information asymmetry between AI developers and harmed individuals.
- **Legislate a Facial Recognition Governance Act** that establishes the legal basis, permissible purposes, technical standards, oversight mechanisms, and individual redress rights for state and private use of biometric surveillance technology.
- **Invest in AI regulatory capacity** across existing sector regulators — particularly the RBI, SEBI, IRDAI, and the proposed National Health Authority — through dedicated technical units, training programmes, and inter-agency coordination mechanisms.
- **Engage proactively in international AI governance** through the OECD, G20, the Council of Europe Framework Convention on AI, and bilateral regulatory cooperation agreements, ensuring that Indian interests and values are reflected in emerging global standards.

India's legal conundrum of AI is ultimately not a technical problem to be solved by lawyers in isolation. It is a governance challenge that requires collaboration between legal scholars, technologists, policymakers, civil society organisations, and the communities most affected

by AI systems. The urgency is real: every day that AI systems operate in India without adequate legal governance is a day on which fundamental rights may be violated, markets may be distorted, and harms may be caused that prove difficult or impossible to remedy after the fact.

But the opportunity is equally real. India has the legal tradition, the constitutional framework, the institutional capacity, and the democratic commitment to build an AI governance architecture that is not merely adequate but exemplary — one that demonstrates to the world that ambitious AI adoption and the rigorous protection of human rights are not in tension but are, properly understood, mutually reinforcing. The challenge is to summon the political will to make it so.

REFERENCES

1. Bhatia, G. (2019). *The transformative constitution: A radical biography in nine acts*. HarperCollins India.
2. Chandrashekhar, R. (2022). India's approach to AI governance: Principles and practice. *Journal of Information Technology & Politics*, 19(3), 245-261.
3. Consumer Protection Act, 2019. No. 35 of 2019. Government of India.
4. Copyright Act, 1957. No. 14 of 1957. Government of India.
5. Digital Personal Data Protection Act, 2023. No. 22 of 2023. Government of India.
6. European Parliament and Council. (2024). Regulation (EU) 2024/1689 on a European approach for artificial intelligence (EU AI Act). *Official Journal of the European Union*.
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Ministry of Electronics and Information Technology, Government of India.
8. Justice K.S. Puttaswamy (Retd.) v. Union of India. (2017). (10) SCC 1. Supreme Court of India.
9. Khanna, A., & Pal, M. (2023). Towards an AI governance framework for India: Challenges and prospects. *National Law School of India Review*, 35(1), 78-114.
10. M.C. Mehta v. Union of India. (1987). (1) SCC 395. Supreme Court of India.
11. MEITY. (2024). Advisory for intermediaries and platforms on generative AI and LLMs. Ministry of Electronics and Information Technology, Government of India.
12. NITI Aayog. (2018). National strategy for artificial intelligence #AIforAll. Government of India.
13. NITI Aayog. (2021). Responsible AI for all: Adopting the framework. Government of India.
14. Pant, M. (2024). AI and competition law in India: Algorithmic collusion and data dominance. *Competition Commission of India Working Paper Series*, No. 12.
15. Patents Act, 1970. No. 39 of 1970. Government of India.
16. Raghavan, S. (2023). Artificial intelligence, liability, and Indian law: A doctrinal vacuum. *Indian Law Review*, 7(2), 189-224.
17. Schwartz, P. M. (2021). Global data privacy: The EU way. *New York University Law Review*, 94(4), 771-818.
18. Shreya Singhal v. Union of India. (2015). (5) SCC 1. Supreme Court of India.
19. Singh, J., & Sahai, R. (2024). Facial recognition surveillance and constitutional rights in India. *Economic and Political Weekly*, 59(8), 34-42.
20. Thatcher, J., & Dalton, C. M. (2023). Data colonialism and the global south: AI governance implications for emerging economies. *Global Policy*, 14(3), 412-425.
21. UK Department for Science, Innovation and Technology. (2023). A pro-innovation approach to AI regulation. HMSO.