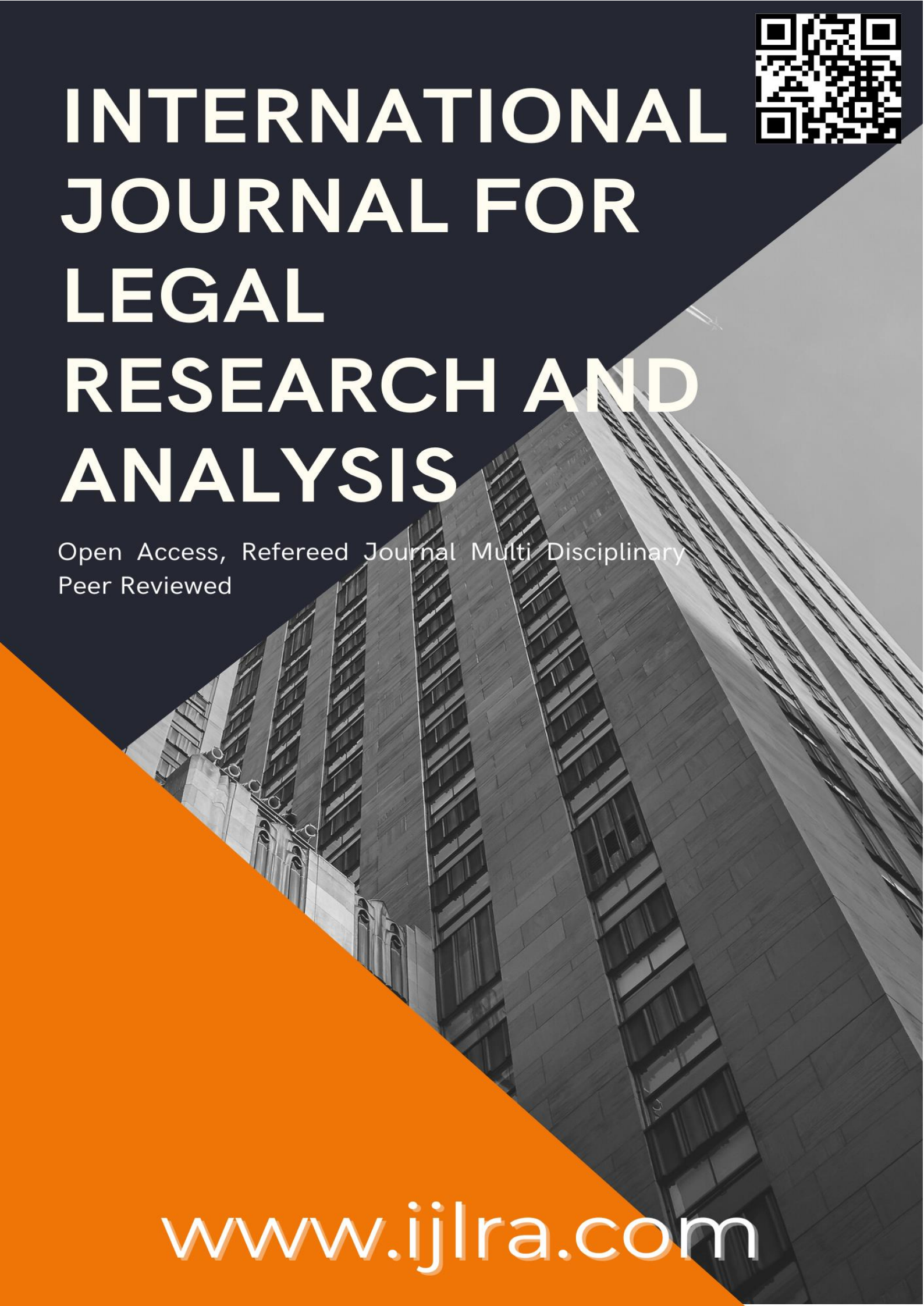
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

AI AND LEGAL RESPONSIBILITY IN INDIA: A STUDY OF LIABILITY AND REGULATORY CHALLENGES

AUTHORED BY - P JASHUVA
Student, Department of Legal Studies, School of Law
Vels Institute of Science Technology and Advanced Studies (VISTAS), Chennai

CO-AUTHOR - DR. SM AZIZUNISAA BEGUM
Assistant Professor, Department of Legal Studies, School of Law
Vels Institute of Science Technology and Advanced Studies (VISTAS), Chennai

Abstract

The rapid proliferation of Artificial Intelligence (AI) technologies across healthcare, finance, law enforcement, transportation, and governance has fundamentally altered the terrain of legal accountability in India. Existing legal instruments the Information Technology Act, 2000, the Indian Contract Act, 1872, the Consumer Protection Act, 2019, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023 were formulated without anticipation of autonomous decision-making systems, and consequently leave significant doctrinal lacunae in matters of tortious liability, contractual responsibility, criminal culpability and regulatory oversight. This paper undertakes a systematic doctrinal and comparative analysis of the legal challenges posed by AI in India, examining the inadequacy of the current legislative framework, the evolution of judicial responses, and the experience of leading international jurisdictions including the European Union, the United States of America, and the United Kingdom. Drawing upon decided Indian case law, statutory provisions, policy documents of the NITI Aayog, and international instruments such as the EU Artificial Intelligence Act 2024 and the UNESCO Recommendation on the Ethics of Artificial Intelligence, the paper argues that India urgently requires a dedicated, risk-stratified AI regulatory statute complemented by a specialised enforcement authority. The paper further contends that judicially developed principles including the absolute liability doctrine articulated in *M.C. Mehta v Union of India* may offer immediate common-law solutions pending legislative action. The paper concludes with concrete recommendations for statutory reform, judicial capacity building, and international regulatory co-operation.

ISSN: 2582-6433

Keywords: Artificial Intelligence; Legal Liability; Regulatory Framework; India; Comparative Law

I. INTRODUCTION

Artificial Intelligence, broadly understood as the capability of a machine to perform cognitive functions ordinarily associated with human intelligence including reasoning, learning, problem-solving, and decision-making has traversed the path from academic theory to pervasive social infrastructure within a remarkably compressed timeline. In India, AI applications have penetrated the delivery of judicial services through the courts Mission Mode Project, medical diagnostics through government-backed digital health platforms, and financial services through algorithmic credit-scoring tools deployed by scheduled commercial banks and non-banking financial companies. The government's National Strategy for Artificial Intelligence, published by NITI Aayog in 2018, projected India as an emerging 'AI garage for the world' and recognised AI as a strategic national priority.[1]

Despite this policy enthusiasm, India's legal infrastructure has not kept pace with technological reality. The Ministry of Electronics and Information Technology (MeitY) released a discussion paper titled 'Responsible AI for All' in 2021, acknowledging the regulatory deficit, yet no dedicated AI statute has been enacted as of April 2026.[2] The Information Technology Act, 2000 defines 'computer resource' and 'computer system' broadly,[3] yet it does not address autonomous decision-making systems that cause harm independent of direct human instruction. The result is a fragmented legal landscape in which victims of AI-inflicted harm whether through biased facial-recognition systems used by police or erroneous automated medical diagnoses face severe difficulties in identifying the legally responsible party and the applicable cause of action.

The problem is not unique to India. Globally, legislatures have struggled to retrofit nineteenth and twentieth-century legal categories developed for human actors with identifiable intentions and foreseeable consequences onto twenty-first-century autonomous systems. The European

[1]NITI Aayog, 'National Strategy for Artificial Intelligence' (2018) <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> accessed 10 April 2026.
[2]Ministry of Electronics and Information Technology (MeitY), 'Responsible AI for All' (2021) <https://www.meity.gov.in> accessed 10 April 2026.
[3]Information Technology Act 2000, s 2(1)(l) (India).

ISSN: 2582-6433

Union's Artificial Intelligence Act, adopted in 2024, represents the most comprehensive legislative attempt to date to establish a risk-based regulatory framework for AI.[4] India must engage critically with this international experience and develop a regulatory model suited to its own constitutional values, developmental priorities, and institutional capacities.

This paper is organised as follows. Part II traces the historical and legislative background, examining how India's existing statutes apply and fail in the context of AI. Part III analyses the doctrinal challenges: liability attribution, the mens rea problem, algorithmic opacity, data protection, and intellectual property. Part IV examines the Indian judiciary's developing jurisprudence on technology-related rights. Part V undertakes a comparative analysis of the regulatory approaches of the European Union, the United States, and the United Kingdom. Part VI states the conclusions, and Part VII sets out legislative and policy recommendations.

II. HISTORICAL BACKGROUND AND LEGISLATIVE FRAMEWORK

2.1 Evolution of AI and Its Legal Implications

The theoretical foundations of artificial intelligence are traceable to the mid-twentieth century work of Alan Turing, whose 1950 paper 'Computing Machinery and Intelligence' posed the foundational question of whether machines could think. The subsequent decades witnessed episodic progress from symbolic AI and expert systems in the 1970s and 1980s, through the 'AI winters' of reduced funding and diminished expectations, to the contemporary renaissance driven by machine learning and deep neural networks. What distinguishes modern AI from its predecessors is the capacity for autonomous adaptation: systems trained on vast datasets can generate outputs that were neither explicitly programmed nor anticipated by their designers. This emergent autonomy is the core challenge for legal systems premised upon human agency and rational choice.

2.2 India's Digital Legislative Framework

India's primary legislative response to the digital economy has been the Information Technology Act, 2000 (IT Act), which was modelled upon the UNCITRAL Model Law on Electronic Commerce. The IT Act established civil and criminal liability for offences such as unauthorised access, data theft, and publication of obscene material in electronic form. The

[4]European Parliament and of the Council, Regulation (EU) 2024/1689 on Artificial Intelligence (EU AI Act) [2024] OJ L 2024/1689.

ISSN: 2582-6433

Digital Personal Data Protection Act, 2023 (DPDPA) introduced data fiduciary obligations, consent mechanisms, and the rights of data principals.[5] The Bharatiya Nyaya Sanhita, 2023 (BNS) replaced the Indian Penal Code, 1860 and introduced updated provisions on cheating, fraud, and economic offences, but contains no express reference to AI-mediated crimes.

The Consumer Protection Act, 2019 (CPA) extended product liability to manufacturers and service providers, with section 2(34) defining 'product liability' as the responsibility of a manufacturer, product service provider, or product seller for any harm caused by a defective product or deficient service. The Supreme Court's landmark decision in *Justice K.S. Puttaswamy v Union of India* recognised privacy as a fundamental right under Article 21 of the Constitution, with profound implications for AI systems that process personal data.[6] However, the doctrinal connection between the constitutional right to privacy and specific AI regulatory obligations remains underdeveloped in Indian jurisprudence.

2.3 Contractual Framework and AI

The Indian Contract Act, 1872 governs contractual transactions in which AI systems are increasingly implicated whether as tools used in contract formation, performance, or as subjects of service agreements. Section 23 of the Indian Contract Act renders void any agreement whose object or consideration is unlawful, opposed to public policy, or immoral.[7] The emergence of smart contracts self-executing code deployed on blockchain platforms raises questions about whether such contracts satisfy the requirements of offer, acceptance, and free consent as understood in traditional contract doctrine. Indian courts have not yet pronounced definitively on the enforceability of autonomous smart contracts, leaving commercial parties in a state of legal uncertainty.

2.4 Consumer Protection and Product Liability

The Consumer Protection Act, 2019 extended liability to cover both defective products and deficient services. An AI system that provides erroneous medical advice or makes a wrongful financial recommendation could constitute a 'defect' under section 2(7) or a 'deficiency' under section 2(9) of the CPA.[8] However, proving that an AI system was 'defective' at the time of manufacture is technically demanding, given the adaptive nature of machine-learning systems: the system may have functioned correctly at deployment but produced a harmful output only

[5]Digital Personal Data Protection Act 2023 (India), s 4.
[6]*Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (Supreme Court of India).
[7]Indian Contract Act 1872 (India), s 23.
[8]Consumer Protection Act 2019 (India), s 2(7) (definition of 'defect') and s 2(9) (definition of 'deficiency').

ISSN: 2582-6433

after retraining on new data. This temporal dimension of AI malfunction is not addressed by existing consumer protection doctrine.

III. ISSUES AND CHALLENGES OF ARTIFICIAL INTELLIGENCE

3.1 Liability Attribution: The Problem of Distributed Agency

The attribution of legal liability for AI-caused harm is complicated by the distributed character of AI development and deployment. A single AI-enabled product may involve a dataset curator, a model developer, an application programmer, a platform operator, and an end-user each of whom contributes to the final output in different ways and to different degrees. Traditional tort law, which requires identification of a specific defendant who owed a duty of care to the claimant, struggled to accommodate multi-party industrial supply chains even before AI; the complexity is now exponentially greater.

In *Shreya Singhal v Union of India*, the Supreme Court struck down section 66A of the IT Act and clarified the scope of intermediary liability, holding that platforms could not be held responsible for third-party content unless they had actual knowledge of the specific unlawful material.[9] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 subsequently imposed enhanced due-diligence obligations on significant social media intermediaries.[10] While these rules address platform liability for user-generated content, they do not address the liability of AI systems that autonomously generate or curate content.

3.2 The Problem of Mens Rea in AI-Related Offences

Criminal liability in both the repealed Indian Penal Code, 1860 and the Bharatiya Nyaya Sanhita, 2023 is predicated upon mens rea a guilty mind. An AI system, being incapable of intention, desire, or knowledge in the legally cognised sense, cannot itself be a criminal. Yet AI systems are increasingly used in fraud, financial manipulation, and cyberattacks. The question of whether the developer or deployer of an AI system that commits what would otherwise be a criminal act can be held vicariously or constructively liable has not been resolved by Indian courts. The BNS provisions on abetment and common intention provide partial assistance, but were not designed to address the intentional deployment of autonomous systems for criminal ends.

[9] *Shreya Singhal v Union of India* (2015) 5 SCC 1 (Supreme Court of India).
[10] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India), r 4.

ISSN: 2582-6433

3.3 Algorithmic Opacity: The 'Black Box' Problem

Machine-learning systems, particularly deep neural networks, operate through layers of mathematical transformations that resist intuitive explanation even by their creators. This algorithmic opacity has been characterised in the literature as the 'black box' problem. Its legal significance is acute: if a claimant cannot demonstrate why an AI system produced a particular output, it becomes practically impossible to establish that the output was caused by a 'defect' in the product or a 'negligent' design decision. The duty of explainability central to the EU AI Act's requirements for high-risk systems has no direct analogue in Indian statute law. The DPDPA, 2023 grants data principals a right to information about automated processing of their personal data but does not establish an enforceable right to algorithmic explanation.

3.4 Data Protection and Privacy

AI systems are data-hungry; their performance is proportional to the volume and quality of training data. This creates structural tension with the right to privacy affirmed in *Puttaswamy* and codified, in part, in the DPDPA, 2023. The DPDPA establishes a consent-based framework for personal data processing but contains limited provisions specifically addressed to AI applications, automated profiling, or the use of personal data for training machine-learning models. Section 16 of the DPDPA restricts processing of personal data of children, which is relevant where AI systems such as educational technology platforms process data of minors. The adequacy of these provisions to address AI-specific data harms, including re-identification of anonymised datasets and inferences drawn from non-sensitive data, remains a significant open question.

3.5 Algorithmic Bias and Discrimination

AI systems trained on historically biased datasets systematically reproduce and amplify societal discrimination. In the Indian context, AI systems used in lending, employment screening, and predictive policing have been documented to produce outputs that correlate with caste, gender, and religion protected characteristics under Articles 14, 15, and 16 of the Constitution of India. The Constitution prohibits discriminatory state action; however, when private entities deploy AI for discriminatory decisions, the horizontal application of fundamental rights is uncertain in Indian constitutional doctrine. The CPA remedy of 'unfair trade practice' under section 2(47) may provide some relief, but is not specifically designed to address algorithmic discrimination.

ISSN: 2582-6433

3.6 Intellectual Property Challenges

Generative AI systems create literary, artistic, musical, and computer-generated works at scale, raising profound questions under the Copyright Act, 1957. The Act vests copyright in 'authors' and recognises computer-generated works but requires a 'human author' for most categories of protected works. When an AI system independently generates a novel work without specific human creative input, the question of authorship and hence ownership of the resulting intellectual property is unresolved. The High Court of Delhi, in *Christian Louboutin SAS v Nakul Bajaj*, observed that technology operators who actively participate in infringing processes bear liability.[11] This principle, extended to generative AI, could impose liability on AI operators for copyright infringement by their systems, but the doctrinal reasoning requires development.

3.7 Regulatory Uncertainty and the Innovation-Accountability Tension

A recurring challenge in AI governance is balancing regulatory certainty necessary for legal compliance, investor confidence, and consumer protection against the need to avoid premature regulatory closure that stifles innovation. India's approach, as articulated in NITI Aayog's policy papers, has tended to favour a 'soft touch' regulatory model relying on industry self-regulation and voluntary codes of conduct.[12] Critics have argued that this approach is structurally incapable of protecting citizens from the harms of AI deployed in high-stakes domains such as health, credit, and criminal justice, where market incentives do not naturally align with user welfare.

IV. ROLE OF THE JUDICIARY IN ADDRESSING ARTIFICIAL INTELLIGENCE

4.1 Judicial Approach to Technological Developments

Indian courts have demonstrated a capacity for creative constitutional interpretation in responding to technological change, although explicit AI-focused jurisprudence remains nascent. The Supreme Court's willingness in *Puttaswamy* to articulate a multi-dimensional conception of the right to privacy encompassing informational privacy, decisional autonomy, and bodily integrity provides a constitutional foundation upon which AI-specific rights could be developed. The Court's methodology of 'constitutional updating' applying timeless

[11] *Christian Louboutin SAS v Nakul Bajaj* (2018) SCC Online Del 12215 (High Court of Delhi).
[12] NITI Aayog, 'Principles for Responsible AI' (2021) <https://www.niti.gov.in> accessed 12 April 2026.

ISSN: 2582-6433

constitutional principles to new factual circumstances has been deployed in areas such as environmental law and reproductive rights, and could equally be applied to AI governance.

4.2 Digital Evidence and Admissibility

The admissibility of digitally generated evidence has been addressed in a series of Supreme Court decisions. In *Anvar P.V. v P.K. Basheer*, the Court held that electronic records were admissible in evidence only when accompanied by a certificate under section 65B of the Indian Evidence Act, 1872 (now section 63 of the Bharatiya Sakshya Adhiniyam, 2023).[13] In *State of Maharashtra v Praful Desai*, the Court permitted the recording of evidence through video-conferencing, acknowledging the legitimacy of technology-mediated judicial processes.[14] The Bharatiya Sakshya Adhiniyam, 2023 updated evidentiary rules for electronic records,[15] but does not specifically address the admissibility of AI-generated outputs such as facial recognition identifications or predictive risk assessments as evidence in civil or criminal proceedings.

4.3 Intermediary Liability and Platform Responsibility

The courts have actively shaped intermediary liability doctrine. In *Google India Pvt Ltd v Visaka Industries*, the High Court of Andhra Pradesh considered the liability of a search engine for defamatory autocomplete suggestions generated by an algorithm.[16] In *MySpace Inc v Super Cassettes Industries Ltd*, the Delhi High Court held that an intermediary which fails to act upon notice of infringing content loses the immunity conferred by section 79 of the IT Act.[17] In *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd*, the Delhi High Court examined the liability of an e-commerce marketplace for products sold by third-party sellers.[18] These decisions, while not directly concerned with AI liability, provide doctrinal building blocks for courts that will be called upon to adjudicate AI-related claims.

4.4 Absolute Liability and AI

The doctrine of absolute liability, developed by the Supreme Court in *M.C. Mehta v Union of India*, imposes strict, non-delegable liability upon enterprises engaged in inherently hazardous

[13] *Anvar PV v PK Basheer* (2014) 10 SCC 473 (Supreme Court of India).
[14] *State of Maharashtra v Praful Desai* (2003) 4 SCC 601 (Supreme Court of India).
[15] Bharatiya Sakshya Adhiniyam 2023 (India), s 63.
[16] *Google India Pvt Ltd v Visaka Industries Ltd* (2020) SCC Online AP 549 (High Court of Andhra Pradesh).
[17] *MySpace Inc v Super Cassettes Industries Ltd* (2017) 236 DLT 478 (High Court of Delhi).
[18] *Amazon Seller Services Pvt Ltd v Amway India Enterprises Pvt Ltd* (2020) SCC Online Del 350 (High Court of Delhi).

ISSN: 2582-6433

activities, without the escape valve of 'act of God' or 'act of third party' that qualifies the common law rule in *Rylands v Fletcher*.[19] AI systems deployed in high-risk environments autonomous surgical robots, self-driving vehicles, automated weapons systems could be characterised as 'hazardous' for the purpose of this doctrine, thereby imposing liability on the enterprise that introduces the AI into commerce, irrespective of whether the specific failure was foreseeable. This approach has been canvassed in academic literature and provides a judicially available tool pending legislative reform.

4.5 Challenges Faced by the Judiciary

Indian courts face institutional constraints in adjudicating AI-related claims. Technical complexity requiring understanding of machine-learning architectures, training methodologies, and statistical evaluation metrics is not within the ordinary competence of judicial officers trained in law. The absence of court-appointed technical experts in AI-related proceedings, the lack of discovery mechanisms tailored to algorithmic systems, and the reliance on adversarial expert witnesses who are often retained by the party with the deepest resources collectively disadvantage claimants with limited means. These structural deficits, combined with the costs and delays of Indian civil litigation, may deter AI-related claims even were meritorious.

V. COMPARATIVE INTERNATIONAL ANALYSIS

5.1 The European Union: Risk-Based Regulation

The European Union's Artificial Intelligence Act, adopted in 2024, is the world's first comprehensive, horizontally applicable AI regulatory statute. Its foundational architecture is risk-stratification: AI systems are classified into four tiers unacceptable risk (prohibited), high risk (subject to ex ante conformity assessment), limited risk (transparency obligations only), and minimal risk (unregulated). Article 6 designates as 'high-risk' AI systems used in critical infrastructure, education, employment, essential private services, law enforcement, migration, and administration of justice.[20] Article 9 requires providers of high-risk AI systems to establish and maintain a risk management system throughout the lifecycle of the system.[21] The EU AI Act also establishes a European AI Office with supervisory and enforcement powers, and creates a right to explanation for individuals adversely affected by high-risk AI decisions an

[19]*MC Mehta v Union of India* (1987) 1 SCC 395 (Supreme Court of India) (absolute liability rule for hazardous activities, per Bhagwati CJ).
[20]EU AI Act (n 4), art 6 (classification of high-risk AI systems).
[21]EU AI Act (n 4), art 9 (risk management system obligations for high-risk AI).

ISSN: 2582-6433

entitlement that, as noted above, has no direct equivalent in Indian law.

5.2 The United States: Sectoral and Decentralised Regulation

The United States has historically adopted a sectoral approach to AI governance, relying upon existing regulatory agencies the Federal Trade Commission, the Securities and Exchange Commission, the Food and Drug Administration to apply their existing mandates to AI applications within their respective domains. President Biden's Executive Order on Safe, Secure, and Trustworthy Development and Use of AI, issued in October 2023, sought to establish cross-agency co-ordination mechanisms and safety standards for AI systems with dual-use potential,[22] though it was subsequently revoked in January 2025. The proposed Algorithmic Accountability Act of 2021 would have required impact assessments for automated decision systems, but was not enacted.[23] The United States' approach reflects a deliberate preference for industry-led innovation and post-deployment enforcement over prescriptive ex ante regulation, a model that critics argue has allowed AI harms to proliferate before regulatory responses are mobilised.

5.3 The United Kingdom: Principles-Based Regulation

The United Kingdom's 2023 AI Regulation White Paper adopted a principles-based, sector-specific approach, declining to create a dedicated AI regulator and instead empowering existing sector regulators the Competition and Markets Authority, the Information Commissioner's Office, the Financial Conduct Authority to apply five overarching principles (safety, transparency, fairness, accountability, and contestability) within their domains.[24] This approach preserves regulatory flexibility and avoids the risks of premature statutory ossification, but has been criticised for creating fragmentation, regulatory arbitrage opportunities, and inadequate protection in sectors with no existing specialist regulator. The UK's post-Brexit divergence from the EU regulatory model creates international inconsistency that may complicate cross-border AI governance.

[22]Executive Order No 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (United States, 30 October 2023), revoked by Executive Order No 14148 (20 January 2025).
[23]Algorithmic Accountability Act (proposed), S 3572, 117th Congress (United States, 2021).
[24]UK Government, 'A Pro-Innovation Approach to AI Regulation' (White Paper, CP 815, 2023) <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach> accessed 12 April 2026.

ISSN: 2582-6433

5.4 International Instruments

At the multilateral level, the OECD Recommendation on Artificial Intelligence (2019) adopted by India as an adherent state establishes non-binding principles including transparency, accountability, robustness, and human oversight.[25] The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021), adopted unanimously by 193 member states including India, calls upon states to establish regulatory frameworks that protect human rights, ensure accountability, and promote AI literacy.[26] These instruments, while non-binding, provide normative foundations for India's domestic regulatory architecture and articulate consensus positions on contested issues such as the prohibition of AI systems that manipulate human behaviour in ways that circumvent autonomy.

5.5 Lessons for India

The comparative survey reveals three significant lessons for India. First, the EU's experience demonstrates that a risk-stratified framework applying rigorous requirements only to high-risk applications while permitting lower-risk innovation to proceed can reconcile regulatory protection with developmental imperatives. Second, the US experience illustrates the inadequacy of relying solely on existing sectoral regulators when AI systems cut across multiple regulatory boundaries; a co-ordinating authority with AI-specific expertise is necessary. Third, the UK's principles-based model, while flexible, creates the risk of regulatory gaps in unregulated sectors.[27] India's constitutional commitment to social justice and substantive equality, reflected in the Directive Principles of State Policy, provides normative guidance for a regulatory model that prioritises protection of vulnerable populations including low-income borrowers subjected to algorithmic credit decisions and marginalised communities subject to AI-powered surveillance.

VI. CONCLUSION

The foregoing analysis demonstrates that India confronts a structural mismatch between the pace of AI deployment and the adequacy of its legal framework. The existing statutory architecture the IT Act, 2000, the DPDPA, 2023, the CPA, 2019, and the BNS, 2023 provides

[25]OECD, 'Recommendation of the Council on Artificial Intelligence' (OECD/LEGAL/0449, 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 12 April 2026.
[26]UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (adopted 23 November 2021) UNESCO Doc SHS/BIO/PI/2021/1.
[27]World Economic Forum, 'AI Governance Alliance: Briefing Paper Series' (2024) <https://www.weforum.org/publications/ai-governance-alliance-briefing-paper-series-2024> accessed 14 April 2026.

ISSN: 2582-6433

fragmentary and largely inadequate responses to the liability, accountability, and governance challenges generated by AI systems operating across critical social domains. The judiciary has developed valuable common-law principles most notably the absolute liability doctrine in *M.C. Mehta* and the privacy jurisprudence of *Puttaswamy* that provide a partial doctrinal foundation, but judicial responses to AI-specific harms remain episodic and insufficiently developed to provide consistent legal protection.

The comparative analysis confirms that India is not alone in confronting these challenges, but also that it is behind the international regulatory frontier. The EU AI Act 2024 represents a decisive legislative intervention that will set the global standard for AI governance and will affect Indian AI developers and deployers operating in European markets. India's strategic interest in maintaining access to international AI markets, attracting foreign investment in its AI sector, and protecting its citizens from AI-inflicted harm converge in favour of enacting a domestic AI regulatory statute that is broadly compatible with international norms while adapted to India's developmental context.

The absence of dedicated AI legislation creates not merely a protective gap for citizens but also a competitive disadvantage for the Indian AI industry, which faces compliance uncertainty when seeking to operate in regulated jurisdictions. A clear, proportionate domestic framework would simultaneously protect Indian citizens and provide Indian AI businesses with regulatory certainty that enhances their international commercial credibility.[28]

India's constitutional values of equality, dignity, and social justice impose affirmative obligations upon the state to ensure that AI technologies are deployed in ways that promote rather than impede fundamental rights. The concentration of AI development capacity in a small number of large technology corporation’s domestic and multinational creates structural power asymmetries that market regulation alone cannot correct.[29] Effective AI governance in India must therefore combine market regulation with fundamental rights enforcement, consumer protection, and active promotion of trustworthy AI in the public sector.

[28]NITI Aayog, 'AI for India 2.0' (Discussion Paper, 2023) <https://www.niti.gov.in> accessed 14 April 2026.
[29]Competition Act 2002 (India), s 4 (abuse of dominant position) — digital market application discussed in CCI v Maruti Suzuki (2021) and CCI orders against Google (2022).

ISSN: 2582-6433

VII. RECOMMENDATIONS

7.1 Enactment of a Dedicated AI Statute

India should enact a comprehensive Artificial Intelligence Regulation Act that establishes a risk-stratified classification system for AI applications, defines the obligations of AI developers, deployers, and users at each risk tier, and creates enforceable rights for persons affected by AI decisions. The Act should expressly address liability attribution in multi-party AI supply chains, providing for joint and several liability of all parties whose negligence contributed to an AI-inflicted harm. The Law Commission of India has previously examined technology-specific liability in the context of autonomous vehicles;[30] its methodology could be adapted for a broader AI liability framework.

7.2 Establishment of a National AI Regulatory Authority

A dedicated National Artificial Intelligence Technology Regulatory Authority (NAITRA) should be established with multi-disciplinary expertise in law, technology, ethics, and economics. NAITRA should be empowered to conduct pre-market conformity assessments for high-risk AI applications, investigate AI-related harms, impose remedies including mandatory recall of defective AI systems, and co-ordinate with sectoral regulators. The Non-Personal Data Governance Framework proposed by the Gopalakrishnan Committee[31] provides a precedent for the kind of multi-stakeholder regulatory body that could be adapted for AI governance.

7.3 Risk-Based Regulatory Framework

Building on the EU AI Act model, Indian AI regulation should adopt explicit risk tiers. Applications that use AI to make consequential decisions in healthcare, criminal justice, credit allocation, and employment should be classified as high-risk, subject to mandatory impact assessments, explainability requirements, human oversight mechanisms, and post-deployment audit obligations. The Motor Vehicles (Amendment) Act, 2019[32] and its compensation scheme for road accident victims provides a precedent for no-fault compensation mechanisms that could be adapted for AI-related harms in high-risk domains.

[30]Law Commission of India, 'Report on Legal Framework: Autonomous Driving' (Report No 270, 2018).
[31]Expert Committee on Non-Personal Data Governance Framework (Kris Gopalakrishnan Committee), Report (Ministry of Electronics and Information Technology, 2020).
[32]Motor Vehicles (Amendment) Act 2019 (India), s 110A (compensation scheme) — applicable to autonomous vehicle scenarios by analogy.

ISSN: 2582-6433

7.4 Strengthened Data Protection

The Digital Personal Data Protection Act, 2023 should be amended to include AI-specific provisions: a right to meaningful explanation for automated decisions with significant effects on data principals, restrictions on the use of personal data for training commercial AI models without explicit consent, and mandatory data impact assessments for AI applications processing sensitive personal data. The existing right to compensation under section 43A of the IT Act[33] for failure to protect sensitive personal data should be extended and clarified in the DPDPA to cover AI-specific data harms.

7.5 Judicial Capacity Building

The National Judicial Academy and State Judicial Academies should introduce structured programmes in AI literacy for judges and court staff, covering the technical fundamentals of machine learning, the legal issues generated by AI evidence, and comparative international AI jurisprudence. Courts should develop protocols for the appointment of neutral technical experts in AI-related proceedings, modelled on the court-appointed expert mechanism used in competition law cases before the Competition Commission of India.

7.6 International Co-operation

India should actively engage with international AI governance mechanisms including the OECD AI Policy Observatory, the Global Partnership on AI, and bilateral AI dialogues with the EU and the United States to ensure that its regulatory framework is interoperable with international norms and that Indian AI developers have clarity regarding cross-border compliance obligations. India's chairmanship of the G20 in 2023 produced the New Delhi Leaders' Declaration affirming commitment to 'safe, secure and trustworthy AI'; this political commitment must now be translated into domestic legislative action.

7.7 Transparency and Explainability Obligations

High-risk AI systems deployed in India should be subject to mandatory transparency obligations, including publication of model documentation, training data sources, performance metrics, and known failure modes. A compulsory algorithmic impact assessment regime modelled on the environmental impact assessment requirement under the Environment Protection Act, 1986 would ensure that AI harms are anticipated and mitigated before

[33]Information Technology Act 2000 (India), s 43A (compensation for failure to protect sensitive personal data).

ISSN: 2582-6433

deployment rather than remediated after damage has occurred.[34] The principle of preventive environmental governance articulated by the Supreme Court offers a normative analogy for precautionary AI governance.

7.8 Addressing Algorithmic Bias

Anti-discrimination provisions under the Constitution and civil rights statutes should be interpreted, and if necessary amended, to expressly cover algorithmic discrimination. AI systems used by government bodies and regulated entities in consequential decisions should be subject to mandatory bias audits conducted by accredited independent auditors. The results of such audits should be disclosed to affected persons and to the regulatory authority.[35] India's experience with reservation policies and anti-discrimination legislation provides a domestic normative framework that can inform the design of AI fairness standards suited to India's social context.

[34]Digital India Programme, notified under Ministry of Electronics and Information Technology, Government of India (2015).
[35]UNCTAD, 'Technology and Innovation Report 2021: Catching Technological Waves — Innovation with Equity' (UN, 2021) UNCTAD/TIR/2021.