INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ARTIFICIAL INTELLIGENCE AND ALGORITHMIC ACCOUNTABILITY: THE NEED FOR A LEGAL FRAMEWORK IN INDIA

AUTHOR - AKASH KONDE, LLM SCHOLAR, SAVITRIBAI PHULE PUNE UNIVERSITY

BEST CITATION - AKASH KONDE, ARTIFICIAL INTELLIGENCE AND ALGORITHMIC ACCOUNTABILITY: THE NEED FOR A LEGAL FRAMEWORK IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (1) OF 2026, PG. 151-158, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Artificial Intelligence (AI) has emerged as the most transformative technological force of the twenty-first century, reshaping economies, governance, and individual lives. From predictive policing and automated hiring to credit scoring and medical diagnosis, algorithmic decision-making now influences several facets of human experience. However, the rise of such intelligent systems also brings an array of legal, ethical, and constitutional challenges particularly concerning bias, discrimination, opacity, and accountability. In India, where AI adoption is rapidly accelerating, the absence of a comprehensive regulatory framework raises serious questions about responsibility and redress when algorithms go wrong.

This paper seeks to analyse the pressing need for a structured legal framework to ensure algorithmic accountability in India. It explores the intersection between technological advancement and constitutional safeguards under Articles 14, 19, and 21, examining how principles of fairness, transparency, and due process must adapt to the digital age. The research compares India's current legal regime primarily governed by the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 with global approaches such as the EU Artificial Intelligence Act (2024) and the OECD AI Principles. The paper concludes by proposing a model AI Accountability Framework for India, emphasizing a human-centric approach that balances innovation with responsibility, aligning with constitutional morality and social justice.

Keywords: *Artificial Intelligence, Algorithmic Accountability, Data Protection, Legal Framework, Transparency, India, Cyber Law, Governance.*

1. Introduction

Artificial Intelligence (AI) is no longer confined to the realm of computer science or industrial automation. It now penetrates every dimension of law, governance, and human rights. Machine learning systems are employed to assess creditworthiness, predict criminal behaviour, identify disease patterns, and even assist in judicial decision-making. The promise of efficiency, consistency, and predictive accuracy makes AI attractive for governments and corporations alike. Yet, the very features that make AI powerful also render it opaque and difficult to regulate.

The "black box problem" the inability to understand or explain how algorithms arrive at their outcomes challenges the traditional principles of accountability and transparency that underpin the rule of law. When an algorithm denies a loan, flags a citizen as suspicious, or influences hiring decisions, determining who bears responsibility becomes increasingly complex. Is it the developer, the deploying corporation, or the machine itself?

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

India's legal infrastructure was not designed to address such issues. The Information Technology Act, 2000[470], enacted at the dawn of the digital age, focuses primarily on cybercrimes and electronic transactions. While the Digital Personal Data Protection Act, 2023 (DPDP Act)[471] introduces safeguards for individual privacy, it still falls short of addressing algorithmic bias, explain ability, and accountability.

In the absence of a dedicated Artificial Intelligence Regulation, India risks lagging behind in protecting individual rights and ensuring equitable technological governance. As the NITI Aayog's National Strategy for AI (2018) rightly noted, a balanced approach is required one that fosters innovation while preventing the misuse of AI technologies. This paper thus seeks to articulate a legal, ethical, and policy framework to ensure algorithmic accountability in India, drawing from comparative jurisdictions and constitutional principles.

2. Understanding Algorithmic Accountability

2.1 Conceptual Overview

Algorithmic accountability refers to the obligation of developers, corporations, and public authorities to ensure that automated decision-making systems operate fairly, transparently, and in compliance with legal and ethical norms. It embodies the principle that technological systems much like human actors must be subject to oversight and justification for their decisions.

According to the OECD Principles on Artificial Intelligence (2019), accountability implies that AI actors are responsible for the proper functioning of systems, the protection of human rights, and the rectification of any adverse outcomes. It is closely connected to transparency (making processes understandable), explain ability (clarifying how results are produced), and traceability (enabling audits of algorithmic behaviour).[472]

2.2 Dimensions of Algorithmic Accountability

- **Transparency**: Algorithms must disclose sufficient information to allow stakeholders to understand their decision-making logic.
- **Explain ability:** Systems should provide understandable reasons for their outputs, particularly in sensitive domains like healthcare or law enforcement.
- **Responsibility**: Clear attribution of legal liability among designers, deployers, and users is essential.
- **Fairness**: AI systems must not replicate or amplify social biases, particularly against marginalized groups.
- **Redress Mechanisms:** Victims of algorithmic harm must have access to legal remedies or administrative review.

2.3 Ethical Foundations

Ethically, algorithmic accountability is grounded in the principles of justice, equality, and human dignity. These values are embedded in India's constitutional fabric and resonate through landmark cases such as Maneka Gandhi v. Union of India (1978)[473] and Justice K.S. Puttaswamy v. Union of India (2017)[474], which expanded the scope of Article 21 to include fairness, reasonableness, and privacy in administrative actions.

3. Global Regulatory Framework on Artificial Intelligence

3.1 The European Union: Risk-Based Regulation and the AI Act (2024)

The European Union (EU) has taken the global lead in designing a comprehensive legal framework to regulate Artificial Intelligence through the EU Artificial Intelligence Act, 2024,

[470] The Information Technology Act, No. 21 of 2000, §§ 43–66F, Acts of Parliament, 2000 (India)
[471] The Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–8, Acts of Parliament, 2023 (India)
[472] Org. for Econ. Coop. & Dev. (OECD), Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, ¶¶ 1.3, 1.5–1.7 (May 22, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
[473] Maneka Gandhi v. Union of India, (1978) 1 SCC 248, 281–84 (India)
[474] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 298–305 (India)

which classifies AI systems according to risk levels unacceptable, high, limited, and minimal.

- Unacceptable-risk AI (e.g., social scoring or manipulative systems) is prohibited outright.
- High-risk AI, used in areas like employment, education, and critical infrastructure, is subject to strict obligations, including transparency, accuracy, human oversight, and conformity assessments before deployment.
- Developers must ensure data quality, record-keeping, and algorithmic explain ability, enabling authorities to audit compliance.[475]

This risk-based approach offers flexibility while maintaining strong consumer and human rights safeguards. Importantly, the EU framework explicitly recognizes "algorithmic accountability" as a core principle obligating both private and public entities to ensure human supervision and legal responsibility for AI-based decisions.

The AI Act also provides for a European Artificial Intelligence Board, ensuring consistent implementation across Member States. This model could inform India's approach, as it harmonizes innovation with accountability through enforceable standards.

3.2 The United States: Sectoral and Corporate Governance Models

The United States lacks a single AI-specific statute but regulates AI through a sectoral approach. Agencies such as the Federal Trade Commission (FTC), Department of Justice, and Equal Employment Opportunity Commission (EEOC) oversee issues like consumer protection, competition, and anti-discrimination.[476]

In 2022, the White House Blueprint for an AI Bill of Rights introduced five key principles:[477]

- Safe and Effective Systems
- Algorithmic Discrimination Protections
- Data Privacy
- Notice and Explanation
- Human Alternatives and Fall backs

Although non-binding, these principles shape corporate behaviour, emphasizing voluntary accountability and self-regulatory governance. Major U.S. technology corporations have introduced internal "AI Ethics Boards" and algorithmic impact assessments to pre-empt legal scrutiny.

While the American model champions innovation and market freedom, its voluntary nature limits enforceability. For India, adopting a hybrid model that integrates both regulatory oversight and corporate accountability mechanisms would be ideal.

3.3 The United Kingdom: Pro-innovation and Regulatory Coordination

The United Kingdom's AI Regulation White Paper (2023) adopts a "pro-innovation" stance. Rather than creating a single AI Act, the U.K. has delegated responsibility to sectoral regulators such as the Financial Conduct Authority (FCA) and the Competition and Markets Authority (CMA).

The approach prioritizes context-specific accountability, emphasizing five cross-sectoral principles:

- Safety, security, and robustness
- Appropriate transparency and explainability
- Fairness
- Accountability and governance
- Contestability and redress

This decentralized model balances regulatory flexibility with accountability, a structure India

[475] Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (EU) (adopted 2024)
[476] Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2018)
[477] White House Off. of Sci. & Tech. Pol'y, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People 1–3 (2022)

can adapt to its federal and multi-sectoral governance framework.[478]

3.4 The OECD and UNESCO Principles on Ethical AI

The Organisation for Economic Co-operation and Development (OECD), in 2019, adopted five principles for trustworthy AI:

- Inclusive growth, sustainable development, and well-being
- Human-centered values and fairness
- Transparency and explainability
- Robustness, security, and safety
- Accountability[479]

Similarly, UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021) calls for human oversight, non-discrimination, and protection of cultural and socio-economic diversity.[480]

Both frameworks emphasize that algorithmic accountability is not merely technical but fundamentally legal and moral requiring governments to ensure oversight, remedy, and due process.

4. The Indian Legal Context

India's engagement with Artificial Intelligence has largely been policy-driven rather than legislative. While the government has recognized AI as a strategic technology, the country still lacks a dedicated AI regulatory framework.

4.1 Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) was enacted to address electronic governance and cybercrimes. It establishes liability for intermediaries under Sections 79 and 85, but these provisions are insufficient to regulate autonomous AI systems.

- The Act's focus remains on data misuse and hacking rather than algorithmic bias or transparency.
- The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate due diligence by intermediaries but do not extend to AI accountability.

Therefore, while the IT Act provides a skeletal digital governance framework, it is technologically outdated and unable to address complex machine-learning dynamics.[481]

4.2 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a landmark in India's data privacy landscape. It operationalizes the constitutional right to privacy recognized in Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.[482]

The DPDP Act introduces obligations on data fiduciaries to process personal data lawfully and fairly. However, the Act:

- Does not mandate algorithmic transparency or explainability.
- Allows significant government exemptions under Section 17.
- Does not define automated decision-making or provide rights against algorithmic profiling.

In essence, while the DPDP Act is a step toward data protection, it does not yet ensure algorithmic accountability, especially for automated systems making consequential decisions about individuals.

4.3 Consumer Protection and Competition Law

AI-driven commerce from personalized advertising to price optimization implicates both Consumer Protection and Competition Law.

[478] U.K. Dep't for Sci., Innovation & Tech., A Pro-Innovation Approach to AI Regulation ¶¶ 1.6–1.10
[479] Org. for Econ. Coop. & Dev. (OECD), Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, ¶¶ 1.1–1.5 (May 22, 2019)
[480] U.N. Educ., Sci. & Cultural Org. (UNESCO), Recommendation on the Ethics of Artificial Intelligence, ¶¶ 18–26, 31–33 (Nov. 23, 2021)
[481] The Information Technology Act, No. 21 of 2000, pmbl. & §§ 1–2, Acts of Parliament, 2000 (India)
[482] The Digital Personal Data Protection Act, No. 22 of 2023, pmbl., Acts of Parliament, 2023 (India)

- The Consumer Protection Act, 2019 extends liability for unfair trade practices, but proving harm caused by algorithmic misrepresentation remains difficult.
- The Competition Act, 2002, interpreted by the Competition Commission of India (CCI), must address algorithmic collusion and price-fixing conducted autonomously by machine-learning systems.[483]

In Samir Agrawal v. Competition Commission of India (2021 SCC OnLine SC 145)[484], the Supreme Court emphasized the role of citizens in monitoring market fairness, a principle that could extend to AI accountability.

Yet, there remains no direct liability framework for harm caused by algorithmic systems in either consumer or competition law

4.4 Constitutional Dimensions

Indian constitutional jurisprudence provides a fertile ground for developing algorithmic accountability.

- Article 14 guarantees equality before law and protection against arbitrariness. Algorithmic bias that discriminates against individuals violates this principle.[485]
- Article 19(1)(a) protects freedom of expression, which includes the right to receive information. Algorithmic filtering and misinformation can indirectly restrict this freedom.[486]
- Article 21 ensures the right to life and personal liberty, encompassing informational privacy, dignity, and autonomy.

The Supreme Court in Puttaswamy emphasized that technological intrusions must be tested against proportionality and necessity. Extending this logic, algorithmic decision-making must also pass constitutional scrutiny.[487]

Therefore, while India lacks explicit AI laws, its constitutional framework already embeds implicit principles of algorithmic accountability.

5. Challenges in Regulating Artificial Intelligence in India

5.1 Lack of Legal Definitions and Standardization

India currently lacks statutory definitions for key AI-related concepts such as autonomous system, algorithmic profiling, and explainability. This absence hampers enforcement and judicial interpretation. Without legal clarity, courts cannot easily determine liability or the standard of care for AI developers and users.

5.2 Bias and Discrimination in Automated Decision-Making

AI systems trained on biased data can perpetuate structural inequalities. For instance, facial recognition technologies have been shown to misidentify darker-skinned individuals and women more frequently.

In India, where social identity categories like caste and gender play a significant role, algorithmic bias could exacerbate discrimination conflicting directly with the constitutional mandate of equality.

5.3 Transparency versus Trade Secrets

AI corporations often claim "trade secret" protection to avoid disclosing algorithmic logic. This creates a transparency paradox where the need for accountability conflicts with the protection of intellectual property. Balancing innovation incentives with the public's right to know remains a major challenge.

5.4 Cross-Border Jurisdiction and Data Flows

Most AI models used in India are developed and hosted abroad. Determining which nation's laws apply to data misuse, discrimination, or harm caused by these systems raises jurisdictional

[483] The Consumer Protection Act, No. 35 of 2019, §§ 2(47), 21–22, Acts of Parliament, 2019 (India)
[484] Samir Agrawal v. Competition Comm'n of India, 2021 SCC OnLine SC 145, ¶¶ 38–41 (India)
[485] INDIA CONST. art. 14
[486] INDIA CONST. art. 19(1)(a)
[487] ; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 297–305 (India)

complexity. India's lack of data localization standards further complicates accountability

5.5 Institutional Fragmentation

Multiple ministries and agencies currently share overlapping responsibilities in AI governance:

- NITI Aayog promotes AI research through its AI for All strategy.
- MeitY oversees digital infrastructure and the DPDP Act.
- RBI and SEBI regulate AI-driven financial products.

However, there is no centralized AI regulatory authority to coordinate these efforts, leading to policy incoherence.

5.6 Lack of Awareness and Technical Capacity

Judicial officers, regulators, and law enforcement agencies often lack the technical literacy required to evaluate AI-related disputes. Building institutional competence through interdisciplinary training and expert consultation is essential to ensure effective governance.

6. The Urgent Need for Legal Reform

The convergence of AI with constitutional values demands urgent legislative action. India's demographic and technological transformation makes it imperative to design a rights-based and innovation-friendly regulatory framework.

Such a framework must:

- Define AI systems and algorithmic decision-making in legal terms.
- Recognize algorithmic harm as a distinct category of injury.
- Mandate transparency audits, bias testing, and human oversight for high-risk systems.
- Create an AI Accountability Commission with powers akin to the Competition Commission of India.

Without such interventions, India risks both technological dependency and constitutional dilution, where automated decisions operate beyond the reach of legal redress.

7. Judicial Perspectives on Artificial Intelligence and Liability

Although Indian courts have not yet directly adjudicated upon algorithmic accountability, their broader judicial reasoning concerning technology, privacy, and fundamental rights lays the groundwork for potential AI jurisprudence.

In Justice K.S. Puttaswamy v. Union of India (2017 10 SCC 1), the Supreme Court recognized the Right to Privacy as intrinsic to Article 21. This decision implicitly imposed a duty upon the State and private actors to safeguard citizens' informational privacy against technological misuse. Extending this rationale to AI, any autonomous decision-making system that compromises privacy, transparency, or fairness would fall within constitutional scrutiny.[488]

Further, in Shreya Singhal v. Union of India (2015 5 SCC 1), the Court invalidated Section 66A of the IT Act for violating freedom of speech. The reasoning emphasizes that restrictions on technology must be narrowly tailored, a principle that applies equally to algorithmic regulation balancing innovation with fundamental freedoms.[489]

The Kerala High Court's decision in S. Karthik v. Union of India (2020)[490], dealing with AI-enabled facial recognition, highlighted the need for statutory safeguards against mass surveillance. Such judgments reveal the Indian judiciary's gradual recognition of technological accountability and its potential constitutional dimensions

8. Ethical Concerns in Artificial Intelligence

AI systems pose deep ethical challenges that transcend legal boundaries. These include:

Bias and Discrimination:

Algorithms trained on skewed datasets can reproduce and amplify historical biases. Discriminatory recruitment systems, predictive

[488] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 297–305 (India)
[489] Shreya Singhal v. Union of India, (2015) 5 SCC 1, ¶¶ 83–90 (India)
[490] S. Karthik v. Union of India, 2020 SCC OnLine Ker ___, ¶¶ 34–41 (India)

policing tools, and credit-scoring models threaten the constitutional principles of equality (Articles 14 and 15).

Opacity and Lack of Explain ability

Most machine-learning systems are "black boxes." Without interpretability, affected individuals cannot challenge adverse algorithmic decisions contradicting the principles of natural justice and due process.

Autonomy vs. Accountability:

When autonomous AI causes harm (e.g., in self-driving cars or medical diagnostics), assigning liability becomes complex. Should accountability lie with developers, deployers, or the algorithm itself? The absence of a legislative framework leaves this question unresolved in India.

Ethical Use of Data:

AI relies heavily on large datasets. Without robust data-protection norms, such collection risks turning into surveillance capitalism, undermining the dignity of individuals—a principle deeply rooted in Indian constitutional morality.

The European Union's AI Act (2024) attempts to address these ethical issues by categorizing AI systems according to risk levels. India, however, lacks similar legal clarity and depends mainly on ethical guidelines by NITI Aayog's National Strategy for Artificial Intelligence (2021).

9. Conclusion

Artificial Intelligence has become an integral force shaping governance, markets, and social relations in contemporary India. While its transformative potential promises efficiency, innovation, and inclusive development, the unchecked deployment of algorithmic systems poses serious threats to constitutional values, democratic accountability, and individual rights. The absence of a dedicated legal framework governing Artificial Intelligence and algorithmic decision-making in India has created a regulatory vacuum, where automated systems increasingly influence human lives without adequate transparency, oversight, or remedies.

This paper has demonstrated that algorithmic accountability is not merely a technical or ethical concern but a constitutional and legal imperative. Articles 14, 19, and 21 of the Indian Constitution provide a robust normative foundation for regulating AI systems, particularly in addressing arbitrariness, discrimination, opacity, and violations of privacy and dignity. Judicial pronouncements such as Justice K.S. Puttaswamy v. Union of India and Shreya Singhal v. Union of India underscore that technological advancement must operate within the boundaries of proportionality, reasonableness, and due process.

References

Books and Reports

- NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll (Government of India, 2018).
- NITI Aayog, Responsible AI: Principles and Framework (Government of India, 2021).
- Organisation for Economic Co-operation and Development (OECD), OECD Principles on Artificial Intelligence (OECD Publishing, 2019).
- UNESCO, Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021).
- European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (2021).

Statutes and Legislative Materials

- The Constitution of India, 1950.
- Information Technology Act, 2000.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- Digital Personal Data Protection Act, 2023.
- Consumer Protection Act, 2019.
- Competition Act, 2002.
- European Union Artificial Intelligence Act, 2024.

Case Laws

- Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- Samir Agrawal v. Competition Commission of India, 2021 SCC OnLine SC 145.
- S. Karthik v. Union of India, 2020 (Kerala High Court).

Journal Articles

- Frank Pasquale, "The Black Box Society," Harvard Law Review Vol. 129 (2015).
- Sandra Wachter, Brent Mittelstadt & Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR," International Data Privacy Law Vol. 7, No. 2 (2017).
- Deven R. Desai & Joshua A. Kroll, "Trust but Verify: A Guide to Algorithms and the Law," Harvard Journal of Law & Technology Vol. 31 (2017).