

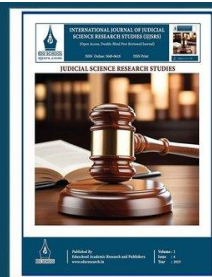


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Artificial Intelligence and Legal Accountability: Frameworks for Algorithmic Governance

Vinothini S

Sathyabama School of Law, Chennai, India

Article information

Received: 29th May 2026

Received in revised form: 13th June 2026

Accepted: 4th July 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0051>

Abstract

The accelerating deployment of artificial intelligence systems in consequential decision-making credit scoring, employment screening, welfare eligibility, criminal justice, and healthcare has outpaced the development of legal accountability frameworks. This paper offers a comparative analysis of emerging regulatory responses to algorithmic harm across three jurisdictions: the European Union's Artificial Intelligence Act 2024, the United States' sectoral and state-law approach, and India's Digital Personal Data Protection Act 2023 and proposed Digital India Act. The analysis constructs a typology of algorithmic harms discrimination, opacity, safety failures, and informational manipulation and evaluates the regulatory tools addressing each type: risk classification, conformity assessment, data-protection impact assessments, transparency obligations, human oversight, and ex post liability. The paper argues that the EU's risk-based horizontal approach and the US sectoral approach each capture different but partial dimensions of algorithmic accountability, while the Indian framework remains under-specified. It proposes a convergent framework combining horizontal transparency obligations with sectoral risk regulation and a sustainable liability regime.

Keywords:- Artificial intelligence, algorithmic accountability, EU AI Act, GDPR Article 22, risk-based regulation, automated decision-making

I. INTRODUCTION

Artificial intelligence systems are increasingly deployed in decisions that have substantial consequences for individual life chances. Credit-scoring models allocate credit; employment-screening tools shortlist candidates; predictive-policing systems influence enforcement resource allocation; automated welfare-eligibility systems determine social-assistance benefits; medical-diagnostic systems inform treatment decisions. The speed and scale at which these deployments have proceeded has produced a growing catalog of algorithmic harms: discriminatory outcomes replicated or amplified from training data, opaque decision processes that preclude meaningful review, safety failures in high-stakes applications, and informational manipulation through recommender systems and content moderation.

Legal and regulatory responses have accelerated in the 2020s. The European Union's Artificial Intelligence Act, adopted in 2024, represents the most comprehensive horizontal framework to date. The United States has pursued a mixed strategy of sectoral regulation, state-level statutes, and executive-branch initiatives, supplemented by the White House Blueprint for an AI Bill of Rights (2022) and Executive Order 14110 (2023). India's Digital Personal Data Protection Act 2023 establishes foundational data-protection rules, with a proposed Digital India Act to supersede the Information Technology Act 2000 expected to introduce AI-specific provisions.

This paper offers a comparative analysis of these three regulatory frameworks with particular attention to the doctrinal instruments they employ, the harms they address, and the gaps they leave. It argues that algorithmic accountability is best conceived as a multi-layered problem requiring horizontal transparency obligations, sectoral risk regulation, and a functional liability regime.

II. ALGORITHMIC HARMS: A TYPOLOGY

Scholarship on algorithmic harm has converged on a rough taxonomy of four categories. First, discrimination, encompassing decisions that produce unjustified disparate impact or disparate treatment against protected groups. Well-documented cases include the ProPublica investigation of the COMPAS recidivism-risk tool (Angwin et al., 2016), gender bias in Amazon's now-abandoned employment-screening system, racial bias in facial-recognition systems (Buolamwini & Gebru, 2018), and disparate mortgage-lending outcomes from automated underwriting.

Second, opacity, referring to the inability of affected persons, decision-makers, or oversight bodies to understand or audit the basis of algorithmic decisions. Pasquale (2015) described the 'black box society' produced by commercial secrecy, technical complexity, and deep-learning architectures that resist interpretation. The resulting accountability gap affects both individual redress and systemic governance.

Third, safety failures, particularly in applications where algorithmic error can cause physical or serious economic harm: medical diagnostic errors, autonomous-vehicle failures, algorithmic trading-driven financial instability. These harms raise issues of product liability, professional responsibility, and regulatory oversight that extend beyond pure algorithmic-governance doctrines.

Fourth, informational manipulation, including recommender-system amplification of misinformation, political microtargeting, and content-moderation decisions that shape public discourse. These harms raise free-speech concerns alongside algorithmic-accountability concerns, creating tensions that complicate regulatory design.

A coherent regulatory framework must address all four categories, though not necessarily with identical instruments. The typology also helps to identify blind spots: for example, most existing regulations focus on discrimination and opacity in individual decisions, with less attention to systemic informational harms and safety failures.

III. THE EU AI ACT: RISK-BASED HORIZONTAL REGULATION

The EU AI Act (Regulation 2024/1689) adopts a horizontal, risk-based framework. AI systems are classified into four risk tiers. Prohibited practices (Article 5) include social scoring by public authorities, untargeted scraping of facial images for recognition databases, emotion-recognition systems in workplaces and schools (with defined exceptions), and certain predictive-policing applications. High-risk systems (Article 6 and Annex III) include biometric identification, critical-infrastructure management, education and vocational training, employment and worker management, access to essential services, law enforcement, migration, administration of justice, and democratic processes. High-risk systems are subject to rigorous obligations: risk-management systems, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, and cybersecurity. General-purpose AI models (Article 51 ff.) face transparency and documentation obligations, with systemic-risk designation triggering additional requirements. Limited-risk systems face transparency obligations (disclosure that the user is interacting with an AI system, disclosure of deep fakes). Minimal-risk systems remain largely unregulated.

The Act's strengths include its horizontal reach, its coverage of general-purpose models, and its integration with existing product-safety and conformity-assessment infrastructure. Its structural weaknesses include the list-based approach to high-risk classification, which may prove insufficiently agile as AI applications evolve; the extended implementation timeline (phased from 2025 through 2027); and the potential for forum-shopping through EU Member State designation of national competent authorities.

The Act interacts with the General Data Protection Regulation. GDPR Article 22 prohibits decisions based solely on automated processing that produce legal or similarly significant effects, subject to exceptions for contractual necessity, authorization by Union or Member State law, or explicit consent; where permitted, safeguards including human intervention, contesting, and explanation must be provided. The 2023 SCHUFA decision of the Court of Justice of the European Union clarified that credit-scoring systems fall within Article 22 even where a human formally implements the output. The AI Act and the GDPR together form the regulatory core, complemented by the Digital Services Act 2022 for online platforms and the proposed AI Liability Directive.

IV. US SECTORAL AND STATE-LEVEL APPROACH

The United States has not enacted a horizontal AI statute. Federal regulation proceeds through sectoral authorities: the Equal Employment Opportunity Commission's 2023 technical assistance on employer use of algorithmic tools; the Federal Trade Commission's unfair-or-deceptive-practices enforcement against algorithmic misrepresentation; the Consumer Financial Protection Bureau's application of the Equal Credit Opportunity Act and Fair Credit Reporting Act to algorithmic lending; the Department of Health and Human Services' Algorithmic Accountability Framework in healthcare; the Securities and Exchange Commission's 2023 proposed rule on predictive-data-analytics conflicts of interest.

Executive Order 14110 of October 2023 directed agencies to implement AI safety testing, red-teaming, critical-infrastructure protection, and immigration-adjacent AI reviews. The order was partially rescinded and replaced by Executive Order 14179 (January 2025), reflecting the administration's preference for lighter-touch regulation while preserving safety-evaluation elements.

State legislation has been active. Illinois' Artificial Intelligence Video Interview Act (2020) requires candidate disclosure of AI use in video interviews. The Colorado Artificial Intelligence Act (2024) imposes duties on developers and deployers of 'high-risk' AI systems affecting consequential decisions. New York City Local Law 144 (2023) requires bias audits of automated employment-decision tools. California's SB 1047 on frontier-model safety was passed and vetoed in 2024, with successor legislation under consideration.

The US approach's strengths include sectoral expertise and regulatory flexibility. Its weaknesses include fragmentation, enforcement gaps where sectoral coverage is thin (notably in political advertising and social-media platforms), and the patchwork burden on multijurisdictional operators. Industry preferences for preemptive federal legislation reflect this concern.

V. INDIAN REGULATORY LANDSCAPE AND THE DPDP GAP

India's current framework for AI governance rests on three instruments. First, the Information Technology Act 2000 and Rules regulate intermediary liability, data-security obligations, and digital-communications offenses, but do not directly address algorithmic accountability. Second, the Digital Personal Data Protection Act 2023 establishes a horizontal personal-data framework with consent-based processing, purpose limitation, data-minimization, and breach notification, but does not contain specific provisions on automated decision-making analogous to GDPR Article 22. Third, the Niti Aayog's Principles for Responsible AI (2021) and subsequent policy papers offer non-binding guidance. The proposed Digital India Act, expected to supersede the IT Act 2000, has been in consultation since 2023 and is anticipated to introduce high-risk AI classifications and online-platform obligations.

The absence of a GDPR-equivalent Article 22 is a particular gap. Indian consumers confronted by algorithmic credit denial, insurance-eligibility determination, or employment screening lack the GDPR's foundational right to contest and obtain human review of solely automated decisions. The Supreme Court's 2017 Puttaswamy decision established privacy as a fundamental right, providing a constitutional basis for future recognition of algorithmic-accountability rights, but statutory specification remains pending.

Additional initiatives include the Ministry of Electronics and Information Technology's 2024 Advisory on AI Platforms (requiring explicit government approval for certain under-tested AI deployments, subsequently softened following industry pushback), the Reserve Bank of India's 2024 guidelines on lending-platform liability, and the Competition Commission of India's 2024 study on algorithmic harms in digital markets. A horizontal framework integrating these developments with the DPDP Act remains the structural next step.

VI. RECOMMENDATIONS

Five reforms would strengthen algorithmic accountability across the comparative landscape. First, horizontal transparency obligations should be specified. A minimum requirement that affected persons be informed when consequential decisions are made by automated systems, together with a right to meaningful explanation and a right to human review, should be common across jurisdictions. GDPR Article 22 provides the base model; India's DPDP Act should be amended or supplemented to incorporate equivalent provisions.

Second, sectoral risk regulation should complement horizontal transparency. High-stakes sectors credit, employment, healthcare, criminal justice, education, welfare should be subject to specific obligations on data governance, testing, and monitoring, as in the EU AI Act's Annex III classification.

Third, liability regimes should be adapted. The EU's proposed AI Liability Directive and the updated Product Liability Directive (2024) extend product-liability concepts to software and AI-system damage; analogous approaches should be considered in the US and India. A 'joint and several' regime for developers and deployers, with appropriate contractual allocation, supports accountability where fault allocation among actors is complex.

Fourth, international coordination is essential to prevent regulatory arbitrage. The OECD AI Principles 2019 and the Council of Europe Framework Convention on Artificial Intelligence 2024 provide coordinating platforms. Mutual-recognition agreements for conformity assessment and shared standards development through IEEE and ISO could reduce compliance burdens while preserving protective standards.

Fifth, enforcement capacity requires investment. Regulators need technical expertise to audit algorithmic systems; affected persons need accessible remedies including class-action or representative mechanisms. Regulatory sandboxes, as provided under Article 57 of the EU AI Act, allow controlled experimentation while preserving accountability.

VII. CONCLUSION

Algorithmic accountability is no longer a theoretical concern; it is a concrete policy domain with established regulatory instruments, growing case law, and rapidly evolving practice. The EU has adopted the most comprehensive horizontal framework; the US has produced a patchwork of sectoral and state-level responses with considerable substantive depth in covered areas; India has established a foundational data-protection statute but lacks specific algorithmic-accountability provisions.

This paper has argued that effective algorithmic governance requires the combination of horizontal transparency obligations, sectoral risk regulation, and a functioning liability regime. Each element addresses distinct accountability concerns; absent any one, the overall framework leaves substantial gaps.

The immediate priority in each jurisdiction differs. In the EU, the priority is effective implementation of the AI Act. In the US, the priority is either comprehensive federal legislation or more systematic coordination of sectoral authorities. In India, the priority is to enact the Digital India Act with clear automated-decision-making provisions and to align DPDP Act rules with algorithmic-accountability requirements. The global convergence of these frameworks will shape how consequential decisions are made, audited, and challenged for decades to come.

REFERENCES

- Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine bias*. ProPublica.
Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. Proceedings of Machine Learning Research, 81, 77–91.
Colorado Artificial Intelligence Act, SB 24-205 (2024).

Council of Europe. (2024). *Framework Convention on Artificial Intelligence* (CM(2024)92-final).

Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, India.

Digital Services Act, Regulation (EU) 2022/2065, [2022] OJ L 277/1.

Executive Order 14110, 88 Fed. Reg. 75191 (2023) (United States).

Federal Trade Commission. (2022). *Aiming for truth, fairness, and equity in your company's use of AI*.

General Data Protection Regulation, Regulation (EU) 2016/679, [2016] OJ L 119/1.

Information Technology Act, No. 21 of 2000, Acts of Parliament, India.

Justiz, SCHUFA Holding AG v. OQ, Case C-634/21, EU:C:2023:957.

K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

NITI Aayog. (2021). *Responsible AI: Approach document for India* (Parts 1 & 2).

New York City Local Law 144 of 2021 (Automated Employment Decision Tools) (effective 2023).

OECD. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449).

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Regulation (EU) 2024/1689 (Artificial Intelligence Act), [2024] OJ L 1689.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*. *International Data Privacy Law*, 7(2), 76–99.

White House Office of Science and Technology Policy. (2022). *Blueprint for an AI Bill of Rights*.