



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

THE NEED FOR GLOBAL AI GOVERNANCE: LEGAL PROBLEMS, HUMAN RIGHTS PROBLEMS, AND REGULATORY MODELS FOR INDIA.

AUTHORED BY - SAKSHI DWIVEDI

ABSTRACT

This seminar paper examines the urgent need for a coherent system of global artificial intelligence (AI) governance in light of rapid technological advancements and the absence of binding international legal frameworks. The study explores how the fragmented regulatory landscape characterized by divergent approaches adopted by major jurisdictions such as the European Union, the United States, and China has created significant legal uncertainty, accountability gaps, and risks of regulatory arbitrage.

The paper critically analyzes key legal challenges associated with AI governance, including algorithmic bias, lack of transparency, unclear liability regimes, and data protection concerns. It further highlights the profound human rights implications of AI systems, particularly their impact on privacy, equality, freedom of expression, and due process. Emphasizing a human rights centric approach, the study argues that effective AI governance must move beyond mere regulatory compliance to incorporate fundamental rights as core guiding principles.

Focusing on India, the paper evaluates its current fragmented regulatory framework and identifies significant gaps in addressing AI specific risks. It assesses India's unique position as both a technology adopter and emerging innovator, while also considering its constitutional commitments and developmental challenges.

The central argument advanced is that global AI governance requires a multi-layered and adaptive framework that establishes binding international principles while allowing contextual flexibility at the national level. The study concludes by emphasizing the need for stronger international cooperation, enforceable legal standards, and inclusive governance mechanisms to ensure that AI development remains aligned with human dignity, accountability, and equitable progress.

Introduction

Artificial Intelligence has emerged as one of the most transformative technologies of the twenty-first century, reshaping economies, governance systems, and societies at an unprecedented pace¹. Its applications span across critical domains including healthcare, finance, law enforcement, education, and national security, offering remarkable opportunities for innovation, efficiency, and human progress. Yet, this rapid proliferation of AI systems has created a profound governance vacuum at the global level. Despite the worldwide scope of AI's development and deployment, there exists currently no binding international legal framework specifically governing its use. This absence creates cascading challenges: regulatory fragmentation across jurisdictions, legal uncertainty regarding accountability and liability, and mounting risks to fundamental human rights, safety, and democratic integrity.

The Crisis of Global Coordination

The challenge of establishing a coherent global AI governance regime reveals deep structural tensions in the contemporary international order². Geopolitical rivalries between major technological powers—particularly the United States, China, and the European Union—have created divergent regulatory philosophies that reflect contrasting views on innovation versus precaution, market freedom versus state oversight, and individual privacy versus collective security. The current patchwork of regulations is inadequate to address AI's global nature, with different regions pursuing fundamentally different approaches. The European Union's comprehensive, risk-based AI Act prioritizes human rights protections and transparency; the United States favors a lighter-touch, innovation-focused framework with minimal regulatory burden; and China implements targeted, state-centric controls aligned with its governance ideology. These divergent models create not merely technical inconsistencies but systemic risks, including regulatory arbitrage (where corporations relocate operations to exploit less stringent regimes) and governance fragmentation that undermines consumer protection and accountability³.

¹ Saidi, I. (2025) "The Legal Vacuum in Global AI Governance: Issues and Opportunities," Science of Law [Preprint]. doi:10.55284/vz4j8696.

² Chang, C. (2025) "Global Minds, Local Governance: AI in International Law," Social Science Research Network [Preprint]. doi:10.2139/ssrn.5185175.

³ Pakuhinezhad, O. and Afsham, N. (2025) "AI REGULATION IN CROSS-BORDER E-COMMERCE: LEGAL CHALLENGES AND GLOBAL REMEDIES," International journal of scientific research [Preprint]. doi:10.36106/ijsr/1529990.

Legal Challenges in AI Governance

The legal architecture necessary to govern AI remains fundamentally inadequate across multiple critical dimensions. First, algorithmic bias and discrimination present persistent enforcement gaps, with regulations often failing to provide effective protection for marginalized communities⁴. Black-box design and the opacity of decision-making systems hinder both detection and remediation of discriminatory outcomes. Second, data governance and privacy protection remain inconsistently protected across jurisdictions, with the European Union's GDPR establishing high standards that most developing nations struggle to implement⁵. The cross-border nature of data flows—essential for AI training—creates complex jurisdictional questions about data sovereignty, consent, and liability when harms occur across multiple nations. Third, intellectual property and ownership questions remain unresolved, particularly regarding AI-generated works and the question of whether autonomous systems should be recognized as legal entities with rights and obligations⁶. The Supreme Court of India's 2019 judgment on recognizing idols as juristic persons offers a precedent for potentially recognizing generative and autonomous AI as juridical persons, though this remains highly contested globally. Fourth, liability and accountability frameworks remain fundamentally unclear. When AI systems cause harm—through biased hiring decisions, erroneous medical diagnoses, or harmful autonomous actions—the diffusion of responsibility across developers, deployers, and users creates an accountability vacuum⁷.

The Human Rights Dimension: Beyond Compliance

While legal frameworks remain essential, the international human rights community increasingly argues that AI governance must be grounded in human rights principles rather than mere regulatory compliance. AI technologies pose unprecedented threats to core human rights including privacy, freedom of expression, non-discrimination, human dignity, and democratic participation⁸. The European Union's AI Act explicitly lists eight prohibited AI

⁴ Lendvai, G.F. and Gosztanyi, G. (2025) "Algorithmic Bias as a Core Legal Dilemma in the Age of Artificial Intelligence: Conceptual Basis and the Current State of Regulation," Multidisciplinary Digital Publishing Institute [Preprint]. doi:<https://doi.org/10.3390/laws14030041>.

⁵ Phang, K. and Kaabi, J. (2025) "Privacy in Flux: A 35-Year Systematic Review of Legal Evolution, Effectiveness, and Global Challenges (U.S./E.U. Focus with International Comparisons)," Journal of Cybersecurity and Privacy [Preprint]. doi:10.3390/jcp5040103.

⁶ Ganguli, P. (2024) "Recognising generative and autonomous AI as a 'juridical person,'" Journal of Data Protection & Privacy [Preprint]. doi:10.69554/ayhz2687.

⁷ Rumulus, M.H. (2025) "Governing AI: A Narrative Review of Algorithmic Accountability and Legal Frameworks," Journal of law review [Preprint]. doi:10.61978/legalis.v3i2.810.

⁸ Lushka, I. (2025) "Regulating Artificial Intelligence in Democratic Societies: Legal Challenges and Ethical Imperatives for Peace, Development, and Integration," Interdisciplinary journal of research and development [Preprint]. doi:10.56345/ijrdv12n1s110.

practices—including subliminal manipulation, exploitation of vulnerable populations, social scoring systems, biometric surveillance in public spaces, and emotion recognition in sensitive settings—precisely because they constitute "unacceptable risks" to fundamental rights. The human rights implications extend beyond individual protections to systemic concerns⁹. UNESCO's evolving approach to AI governance, though forward-looking, has been criticized for incorporating corporate actors into norm-setting processes in ways that risk legitimacy and accountability deficits. Civil society actors, particularly from marginalized communities, remain inadequately represented in global AI governance discussions, raising serious concerns about whose values and interests are embedded in AI systems that will affect billions of people. Gender-based harms, algorithmic discrimination against minorities, and the disproportionate impacts on developing nations and vulnerable populations remain insufficiently addressed in most governance frameworks.

The Global South and India's Unique Position

India occupies a particularly complex position in the global AI governance landscape. As a rapidly growing AI adopter with significant technological capabilities but simultaneously facing infrastructural constraints, India exemplifies the tensions between innovation and regulation that characterize AI governance debates¹⁰. Unlike the European Union's comprehensive single legal framework or the United States' sectoral approach, India currently lacks a dedicated, binding AI law. Instead, India relies on a fragmented landscape of sector-specific regulations, policy frameworks, and government initiatives that remain insufficient to address the cross-cutting nature of AI's risks. India's position as both a technology provider and a technology consumer means that regulatory decisions taken in New Delhi will affect billions globally, while India remains dependent on international standards and frameworks that it has had limited voice in shaping¹¹. The Digital Personal Data Protection (DPDP) Act 2023 represents India's most comprehensive regulatory intervention to date, yet it addresses data privacy rather than AI-specific governance, leaving gaps in algorithmic accountability, bias mitigation, and transparency requirements¹².

⁹ Deckker, D. and Sumanasekara, S. (2025) "Safeguarding human dignity: A narrative review of prohibited AI practices under the EU AI Act," *World Journal of Advanced Research and Reviews* [Preprint]. doi:10.30574/wjarr.2025.26.3.2193.

¹⁰ Hatano, A. (2026) "Ethical ai and Business & Human Rights: A Critical Appraisal of unesco's Collaboration with the Private Sector," *International Organizations Law Review* [Preprint]. doi:10.1163/15723747-22030007.

¹¹ Cupac, J. (2025) "The Gender Code: Gendering the Global Governance of Artificial Intelligence," *arXiv.org* [Preprint]. doi:10.48550/arXiv.2512.09570

¹² Gupta, S. (2025) "India's AI Regulation at the Crossroads: A Comprehensive Law or a Sectoral Mosaic?," *Journal of Development Policy and Practice* [Preprint]. doi:10.1177/24551333251382704.

Scope and Structure of This Analysis

This seminar paper examines the urgent imperative for coherent global AI governance by analyzing three interconnected dimensions: (1) the legal challenges and governance gaps in the current fragmented regulatory landscape; (2) the human rights concerns that must be centrally positioned in any legitimate AI governance framework; and (3) India's evolving regulatory models and their positioning within global governance debates. The analysis draws on comparative legal frameworks from the European Union, the United States, China, and other jurisdictions to understand how different political-economic systems have approached AI governance, why their approaches diverge, and what lessons exist for emerging economies like India. The central argument of this paper is that effective global AI governance requires neither pure harmonization nor continued fragmentation, but rather a multi-tiered, adaptive framework that establishes binding core principles around fundamental rights while permitting regional and sectoral flexibility in implementation¹³. India, with its federal structure, diverse population, and unique governance challenges, has both the opportunity and the responsibility to pioneer an inclusive, equitable approach to AI governance that prioritizes human rights while supporting responsible innovation.

Literature Review

1. Global AI Governance Landscape and Regulatory Architecture

1.1 The Emergence of Fragmented Global Governance Frameworks

The rapid development and deployment of artificial intelligence technologies have created an unprecedented governance challenge at the international level. Despite the global scope of AI's development and deployment, there is currently no binding international legal framework specifically governing its use¹⁴. This absence creates significant challenges, including regulatory fragmentation, legal uncertainty, and risks related to human rights, safety, and accountability. The current global AI governance landscape is characterized by a polycentric structure where multiple actors—international organizations, national governments, private corporations, and civil society—operate with varying degrees of coordination and influence. The emergence of diverse regulatory models reflects geopolitical tensions, diverging national

¹³ Kulkarni, A. and Ramanathan, C. (2026) "An Agentic Software Framework for Data Governance under DPDP," arXiv.org [Preprint]. doi:10.48550/arXiv.2601.01101.

Zhong, H. et al. (2025) "Global AI Governance: Where the Challenge is the Solution- An Interdisciplinary, Multilateral, and Vertically Coordinated Approach," arXiv.org [Preprint]. doi:10.48550/arXiv.2503.04766.

¹⁴ I. Saidi, "The Legal Vacuum in Global AI Governance: Issues and Opportunities," Science of Law, Jun. 2025, doi: 10.55284/vz4j8696.

interests, and different approaches to ethical principles. The European Union has established a legally binding, centralized model through its AI Act that prioritizes risk-based classification and strict compliance obligations. In contrast, the United States follows a decentralized, sector-led approach that emphasizes innovation and market flexibility, while China adopts a state-centric model focused on social stability and data sovereignty. These divergent approaches reveal fundamental tensions in AI governance between innovation, regulation, and social values. Most importantly, existing regional and soft law initiatives, such as the European Union's AI Act and the UNESCO Recommendation on the Ethics of AI, have attempted to create international consensus around key principles, yet significant tensions persist in enforcement mechanisms, regulatory philosophy, and geopolitical priorities¹⁵.

1.2 International Governance Initiatives and Coordination Challenges

Recent years have witnessed rapid escalation in global governance efforts. As illustrated in the governance evolution timeline, the number of regulatory initiatives has grown from approximately 5 in 2020 to an estimated 150 by 2026, while the number of countries with formal AI policies has increased from 15 to 115 over the same period. International organizations such as the OECD, UNESCO, and the UN have played crucial roles in establishing norms and principles for responsible AI. The OECD AI Principles have become widely referenced benchmarks, while UNESCO's Recommendation on the Ethics of AI provides comprehensive guidance on implementation. However, coordination between these initiatives remains limited. The nascent AI governance regime is gravitating around the OECD, which holds considerable epistemic authority and norm-setting power, though the regime remains fragmented and exhibits polycentric characteristics. A novel approach suggests that effective global AI governance requires interdisciplinary, multilateral, and vertically coordinated efforts that integrate legal, technical, and social perspectives. This requires moving beyond fragmented disciplinary collaboration and ineffective multilateral coordination to embrace principles of dynamism, experimentation, inclusivity, and paradoxical governance.

1.3 Corporate Influence and State Sovereignty in AI Governance

A critical issue in global AI governance is the disproportionate influence of large technology

¹⁵ I. Saidi, "The Legal Vacuum in Global AI Governance: Issues and Opportunities," *Science of Law*, Jun. 2025, doi: 10.55284/vz4j8696.

¹⁶ L. Schmitt, "Mapping global AI governance: a nascent regime in a fragmented landscape," *AI and Ethics*, Aug. 2021, doi: 10.1007/s43681-021-00083-y.

corporations on regulatory outcomes. Corporate-led AI governance often surpasses state oversight, resulting in significant accountability deficits and regulatory fragmentation. Large technology companies, particularly Google, have leveraged their technological capabilities and market influence to shape governance outcomes through three distinct mechanisms: regulative mechanisms (embedding technical feasibility parameters in formal regulations), normative mechanisms (establishing self-regulatory practices that diffuse globally), and cognitive mechanisms (shaping shared frameworks of meaning that define governance challenges)¹⁷. To rebalance corporate power with state sovereignty and public accountability, states must strengthen enforceable AI regulations while corporations implement robust transparency and compliance protocols. Transparency mandates, liability regimes, and global enforcement coordination have been identified as critical interventions to address this imbalance. The challenge lies in developing mechanisms that harness corporate expertise and innovation while maintaining democratic accountability and protecting fundamental rights.

1.4 Sustainability and Institutional Effectiveness in AI Governance

Institutional sustainability—referring to the capacity of governance frameworks to remain effective over time—has emerged as an essential consideration in AI governance. A comparative assessment of governance models in the European Union, Japan, and Taiwan reveals four dimensions critical to sustainable governance: adaptability, legitimacy, coherence, and resilience¹⁸. The EU's strategy of normative anchoring through legal codification provides clear guidelines but faces challenges in adaptability; Japan's agile governance model based on collaboration emphasizes rapid response but may lack legitimacy; and Taiwan's digital democratic discourse leverages civic participation to enhance legitimacy.

2. Legal Frameworks and Core Governance Challenges

2.1 The Legal Vacuum and Challenges of Global Harmonization

The absence of comprehensive international legal frameworks for AI governance creates significant obstacles to effective regulation. Legal uncertainty, regulatory fragmentation, and risks related to accountability remain persistent challenges across jurisdictions. The primary obstacles to establishing a unified global regime include geopolitical tensions, diverging

¹⁷ Cihon, P.: Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development (2019)

¹⁸ Gill, A.S.: Imagining the AI future. <https://www.iiss.org/blogs/survival-blog/2019/12/imagining-the-ai-future>. Accessed 21 Jan 2021

national interests, and different approaches to ethical principles¹⁹. Existing legal systems struggle to address emerging issues such as algorithmic transparency, data bias, and liability for autonomous decision-making. Key areas requiring urgent legal attention include algorithmic accountability, data privacy, intellectual property rights, and liability for autonomous decision-making systems²⁰. The fragmented nature of current approaches creates opportunities for regulatory arbitrage, where firms can exploit differences between jurisdictions to minimize compliance costs. This phenomenon is particularly pronounced in multi-cloud data compliance scenarios, where the Digital Personal Data Protection Act in India's permission-by-default approach fundamentally conflicts with the USA's restriction-by-default framework, creating impossible compliance situations²¹. Such regulatory incommensurability necessitates new theoretical approaches that acknowledge valid regulatory differences while enabling multinational compliance.

2.2 Risk-Based Regulatory Approaches and Enforcement Mechanisms

The EU's risk-based AI Act represents the most comprehensive binding regulatory framework globally, establishing legally binding obligations with strict compliance requirements and human rights protections²². However, even this comprehensive framework faces implementation challenges. The comparative analysis of AI governance models reveals significant differences in enforcement strength, regulatory comprehensiveness, and innovation support. The EU model achieves high scores in enforcement²³ and comprehensiveness but may face challenges in supporting innovation. A five-layer governance framework has been proposed to bridge the gap between high-level regulatory mandates and practical implementation. This framework spans from broad regulatory mandates to specific standards, assessment methodologies, and certification processes, providing a structured pathway to meet technical, regulatory, and ethical requirements. The framework's applicability has been validated through case studies on AI fairness and incident reporting, demonstrating its ability

¹⁹ MacIntyre, J., Medsker, L., Moriarty, R. Past the tipping point?. *AI Ethics* 1, 1–3 (2021). <https://doi.org/10.1007/s43681-020-00016-1>

²⁰ Bostrom, N., Yudkowsky, E.: The ethics of artificial intelligence. In: Frankish, K., Ramsey, W.M. (eds.) *The Cambridge Handbook of Artificial Intelligence*. pp. 316–334. Cambridge University Press, Cambridge (2014). <https://doi.org/10.1017/CBO9781139046855.020>

²¹ Veale, M., Van Kleek, M., Binns, R.: Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1–14. Association for Computing Machinery, New York (2018). <https://doi.org/10.1145/3173574.3174014>

²² Michelle D. Lazarus, Mandy Truong, Peter Douglas, Neil Selwyn, "Artificial intelligence and clinical anatomical education: Promises and perils", *Anatomical Sciences Education*, 2022.

²³ Qingyuan Lu, Justin Svegliato, Samer B. Nashed, Shlomo Zilberstein, Stuart Russell, "Ethically Compliant Autonomous Systems under Partial Observability", *2024 IEEE International Conference on Robotics and Automation (ICRA)*, pp.16229-16235, 2024

to identify gaps in legal mandates, standardization, and implementation while adapting to both global and region-specific AI governance needs.

2.3 Data Privacy, Security, and Compliance Challenges

Data protection and privacy have emerged as central concerns in AI governance. The General Data Protection Regulation (GDPR) in the European Union sets stringent standards for data protection; however, these principles face challenges when applied to AI systems, particularly regarding data minimization versus AI's data requirements. Organizations implementing AI must navigate complex regulatory landscapes, with significant disparities in compliance maturity between large corporations and small-to-medium enterprises, the latter facing greater challenges in meeting evolving legal obligations. India's Digital Personal Data Protection Act (DPDPA) represents a significant step forward, but implementation challenges persist due to the absence of dedicated AI-specific regulations and coordination gaps across government departments. An agentic software framework for data governance under DPDP demonstrates how compliance logic can be embedded directly into software agents through domain-aware anonymization strategies tailored to sectors including healthcare, education, and e-commerce. The practical reality is that current legal frameworks often lack enforceability, and compliance mechanisms remain inadequate, particularly in developing economies.

2.4 Sectoral and Cross-Border Legal Issues

Sector-specific legal challenges differ significantly based on the nature and risk profile of AI applications. In healthcare, regulatory frameworks vary substantially across regions with limited global harmonization, highlighting the need for adaptive oversight models and improved data governance²⁴. In telecommunications, AI-related risks remain largely unaddressed despite rapid integration into critical infrastructure, with most frameworks still prioritizing traditional cybersecurity concerns while offering limited recognition of AI-specific vulnerabilities. In financial services, AI-facilitated collusion on digital platforms raises novel antitrust and consumer welfare concerns that existing legal frameworks are ill-equipped to address. Cross-border enforcement remains particularly problematic. As AI systems operate globally but regulations remain territorially bound, questions about enforcement authority, choice of law, and remedy mechanisms remain unresolved. Traditional bilateral and multilateral mechanisms have proven insufficient for coordinating AI governance across

²⁴ Adrienne de Ruiter, "Dangerous liaisons: social AI and the problem with the relational turn to moral status", *AI & SOCIETY*, 2025.

jurisdictions, necessitating new approaches to international cooperation and regulatory harmonization.

3. Human Rights Concerns and Fundamental Protections

3.1 Privacy Violations and Surveillance Capitalism

The widespread deployment of AI-powered surveillance technologies by government agencies and commercial enterprises poses unprecedented threats to the fundamental human right to privacy²⁵. Advanced AI systems such as facial recognition, predictive policing algorithms, and smart sensors enable pervasive surveillance through covert collection, integration, and analysis of personal information that renders traditional notions of privacy obsolete. These technologies enable what scholars term a "digital Panopticon"—a system of continuous monitoring where individuals' behaviours are continuously tracked and analyzed without meaningful consent or transparency. The lack of transparency, fairness, and accountability in AI systems often marginalizes vulnerable populations and establishes privatized systems of social control. Normalization of continuous monitoring has eroded societal norms regarding privacy, with individuals increasingly accepting reduced privacy as inevitable. Specific risks include mass collection and processing of personal data without proper control, threats to the right to privacy, and algorithmic intensification of surveillance through AI systems [18]. In India, the role of law in governing AI-powered surveillance systems reveals significant gaps in existing constitutional and statutory frameworks. Despite the Digital Personal Data Protection Act, broad exemptions for state agencies raise critical constitutional and structural concerns regarding asymmetric surveillance governance.

3.2 Algorithmic Bias, Discrimination, and Non-Discrimination Rights

Algorithmic bias represents a systemic challenge affecting multiple human rights, particularly the right to non-discrimination and equality²⁶. AI systems inherit and amplify biases present in training data, leading to violations of the right to non-discrimination. The problem of "network discrimination" arises when persons' financial capabilities are assessed based on characteristics of their social environment rather than individual merit, violating principles of individual responsibility and potentially limiting freedom of belief through self-censorship. As illustrated

²⁵ Antonio Carnevale, "Preparing Ethics Advisors to AI Governance: Strategies, Regulations, Global Considerations", *The AI Ethics Advisor*, pp.163, 2025.

²⁶ Lepri, B., Oliver, N., Letouzé, E., Pentland, A., Vinck, P.: Fair, transparent, and accountable algorithmic decision-making processes: the premise, the proposed solutions, and the open challenges. *Philos. Technol.* 31, 611–627 (2018). <https://doi.org/10.1007/s13347-017-0279-x>

in the human rights impact assessment, the severity of AI's impact on non-discrimination rights reaches 94 out of 100, yet current protection levels remain at only 45, representing a critical protection gap. Documented cases show how AI systems in credit scoring, employment, and criminal justice systematically disadvantage marginalized communities. China's social credit system demonstrates extreme manifestations of algorithmic discrimination, while more subtle bias appears in Western systems through underrepresentation of minorities in training datasets. The study of AI accountability in India reveals significant limitations in current AI systems when applied to India's complex socio-cultural landscape, with multiple instances of algorithmic bias documented across 15 AI applications and 13 government projects.

3.3 Autonomy, Consent, and Human Agency

The erosion of human autonomy represents a fundamental challenge to human-centric AI governance. AI systems increasingly participate in decision-making affecting individuals' lives—from credit decisions to criminal sentencing—often without meaningful human consent or understanding. The concept of "slow violence" describes the grinding, gradual, attritional harms of AI toward the human rights framework, where individuals become increasingly unable to understand or seek accountability for harms from AI systems. This undermines the foundational premise of the human rights framework, which was designed to empower individuals in addressing power disparities. Subliminal manipulation represents one explicit form of human rights violation, prohibited under the EU AI Act as presenting unacceptable risk. Other prohibited practices include exploitation of vulnerable populations, social scoring, predictive profiling, untargeted scraping of biometric data, emotion recognition in sensitive settings, and real-time biometric surveillance in public spaces²⁷. These prohibitions are justified across deontological, utilitarian, and virtue ethics frameworks. However, enforcement remains challenging, and many jurisdictions outside the EU lack comparable protections.

3.4 Due Process, Transparency, and Accountability

The right to fair trial and due process faces significant threats from AI-driven decision-making systems in criminal justice and administrative proceedings. Lack of transparency in AI systems creates accountability gaps, with individuals unable to understand the basis for decisions affecting them. The absence of meaningful transparency and explainability mechanisms prevents individuals from exercising the right to challenge algorithmic decisions. Current legal

²⁷ Torben Swoboda, Lode Lauwaert, "Can artificial intelligence embody moral values?", *AI and Ethics*, 2025.

protections often provide only limited remedies, particularly for automated decision-making in high-stakes contexts. Human rights in the age of AI demand a shift from protecting data privacy alone to protecting cognitive and emotional integrity within algorithmically mediated environments. The governance framework must incorporate accountability mechanisms, algorithmic transparency, and human oversight as essential pillars. Best practices from leading companies show that effective human rights protection requires explicit governance commitments, regular bias audits, research into diverse linguistic and cultural contexts, and collaborative efforts with civil society. However, significant gaps persist, with most AI systems operating without rigorous human rights impact assessments or robust accountability mechanisms.

4. India's AI Governance Framework and Emerging Challenges

4.1 India's Fragmented and Evolving Regulatory Landscape

India's AI governance landscape presents a complex picture of rapid technological adoption alongside regulatory fragmentation and persistent gaps in comprehensive legislation²⁸. While the Government of India attempts to position the country as a global leader in AI production, its regulatory framework remains scattered across multiple sectoral approaches rather than a unified, comprehensive law. India currently lacks specific AI legislation, with governance operating through fragmented approaches including the Information Technology Act, Digital Personal Data Protection Act, and sector-specific guidelines. This regulatory mosaic creates significant gaps in AI accountability, particularly in high-impact domains such as financial services, healthcare, employment, and public welfare delivery. The fragmented governance landscape has limited engagement with labour rights even as AI-driven transformations reshape employment dynamics²⁹. In a labour-surplus economy dominated by informal work, AI impacts are complex: while it offers employment through digitally mediated platforms and data annotation tasks, it intensifies precarity, de-skilling, and surveillance. The sector-specific governance gaps are substantial, as illustrated in the assessment showing regulatory gaps ranging from 75% in financial services to 95% in surveillance systems, with current guideline implementation levels ranging from just 10% to 50%.

²⁸ Shilun Zhou, "Analyzing the justification for using generative AI technology to generate judgments based on the virtue jurisprudence theory", *Journal of Decision Systems*, pp.1, 2024

²⁹ Paula Boddington, "AI Ethics and Ethical AI", *The Cambridge Companion to Religion and Artificial Intelligence*, pp.165, 2024.

4.2 Key Institutional and Implementation Gaps

India's governance challenges extend beyond legal frameworks to institutional capacity and implementation mechanisms. The absence of dedicated enforcement institutions, unclear accountability structures, and limited technical expertise present systemic barriers to effective governance. While the National Centre for Artificial Intelligence and Robotics (NCAIR) was established in 2020, and recent legislation such as the Data Protection Act has been passed, formal risk classification systems and sector-specific ethical guidelines remain absent. These gaps are particularly concerning given the widespread, unregulated use of generative AI tools in education, politics, and digital commerce. Policy disconnects between government rhetoric and ground-level implementation compound these challenges. A study examining the ethical and societal challenges facing India through focus group research found that significant challenges include lack of awareness of AI by the public and policymakers, India's reliance on Western datasets resulting in lack of diversity and exacerbation of power asymmetries, and potential job displacement by AI without adequate reskilling infrastructure³⁰. Additionally, critical success factors for integrated AI and robotics development in India—including basic policies on data collection, standardized hardware, skilled manpower, and funding mechanisms—remain inadequately addressed³¹.

4.3 Sector-Specific Vulnerabilities and Algorithmic Governance

Different sectors face distinct AI governance challenges in India. In public welfare delivery, algorithmic decision-making systems pose severe risks due to potential errors with severe consequences for vulnerable populations³². Criminal justice systems increasingly deploy AI tools, yet governance structures remain inadequate to ensure transparency, fairness, and compliance with constitutional safeguards, particularly the right to privacy and protection against discrimination. Ethical and legal implications of AI systems in law enforcement reveal significant ethical concerns including bias, discrimination, lack of transparency, and privacy violations, with gaps in Indonesia's (and similarly India's) regulatory framework highlighting the need for specific legislation addressing AI's complexities. In healthcare, a framework for AI governance in India has been proposed to balance opportunities and risks through short-, medium-, and long-term outlooks. This framework emphasizes creating better datasets,

³⁰ "Social and Moral Issues", *The Cambridge Companion to Religion and Artificial Intelligence*, pp.129, 2024.

³¹ Corinne Jorgenson, Jurgen Willems, Ali I. Ozkes, Dieter Vanderelst, "Humans and robots are nearly ethically equivalent", *AI and Ethics*, 2024.

³² K. Gireesan, "Sustainable Governance—Application of Artificial Intelligence", *Democracy, Leadership and Governance – Application of Artificial Intelligence*, pp.413, 2024

building accountability mechanisms in healthcare systems, and upskilling medical personnel. However, implementation lags significantly behind policy recommendations. The Digital Personal Data Protection Act provides some safeguards, but sector-specific challenges in healthcare—including data sensitivity, patient privacy, and algorithmic transparency—require more specialized regulatory attention than the current framework provides.

4.4 Comprehensive Law Versus Sectoral Mosaic: The Policy Crossroads

India faces a critical policy crossroads regarding the future direction of AI regulation. The central question is whether to adopt a single, comprehensive AI law that applies uniformly across sectors or to pursue a mosaic of sector-specific regulations catering to different risk profiles. Each approach presents distinct advantages and challenges. A comprehensive law could provide unified principles and consistent enforcement but might struggle to address sector-specific complexities. Sectoral approaches could be tailored to unique challenges but risk creating regulatory gaps, inconsistencies, and compliance confusion for organizations operating across sectors. The developmental governance model emerging in India reflects its status as an emerging economy, balancing innovation support with appropriate safeguards³³. However, policymakers must carefully consider India's unique governance realities, including its federal structure, MSME-dominant supply chains, diversity of skills ecosystems, and large informal workforce. Recent developments such as state-level platform worker bills represent encouraging steps toward addressing employment concerns through targeted regulation, yet comprehensive national coordination remains necessary.

5. Comparative Analysis of Global Regulatory Models and India's Context

5.1 The EU AI Act: Risk-Based Regulation and High Protection Standards

The European Union's AI Act represents the most comprehensive global framework for AI regulation, establishing legally binding obligations grounded in fundamental rights protection and democratic oversight. The EU model achieves the highest scores in regulatory comprehensiveness and enforcement strength, reflecting its commitment to rights-based governance. The Act employs a risk-based classification system, imposing stricter requirements on higher-risk AI systems, with prohibited practices representing an unacceptable risk category. The EU's approach prioritizes human rights protection, particularly regarding privacy, non-discrimination, and human dignity. Its regulatory philosophy emphasizes

³³ Marten H. L. Kaas, "The perfect technological storm: artificial intelligence and moral complacency", *Ethics and Information Technology*, vol.26, no.3, 2024

precaution—addressing risks before significant harms occur—and places the burden on AI developers to demonstrate compliance. However, this comprehensive approach also raises concerns about regulatory burden on innovation and the potential for regulatory arbitrage, where firms relocate development to less stringent jurisdictions. The EU model provides valuable lessons for other regions, particularly regarding enforcement mechanisms, accountability structures, and the integration of human rights considerations into technical requirements.

5.2 The United States Market-Driven Approach and Sectoral Regulation

The United States follows a distinctly different regulatory philosophy, emphasizing market-driven innovation, decentralized sector-specific regulation, and limited government intervention. The U.S. approach scores lower in regulatory comprehensiveness (50) but higher in innovation support, reflecting its priority on technological advancement and competitive advantage. Rather than comprehensive legislation, the U.S. relies on existing sectoral laws (healthcare, finance, employment), industry self-regulation, and lighter-touch governance through agencies like the FTC and NIST. The advantage of this approach lies in its flexibility and adaptability to emerging technologies; the disadvantage is fragmented protection for individuals and potential gaps in accountability. The NIST AI Risk Management Framework provides non-binding guidance, while the American Artificial Intelligence Initiative emphasizes innovation, standards development, and workforce readiness. Comparative analysis of U.S. and EU jurisdictions reveals that the U.S. regulatory model, while more flexible, provides less comprehensive human rights protection and faces criticisms regarding accountability and equity in AI development³⁴.

5.3 China's State-Centric Approach and Algorithmic Governance

China's AI governance model emphasizes state control, social stability, and data sovereignty, achieving scores of 75 in enforcement strength and 80 in comprehensiveness. The model focuses on national security, social order, and protecting state interests, with particular

³⁴ Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., Khlaaf, H., Yang, J., Toner, H., Fong, R., Maharaj, T., Koh, P.W., Hooker, S., Leung, J., Trask, A., Bluemke, E., Lebensold, J., O'Keefe, C., Koren, M., Ryffel, T., Rubinovitz, J.B., Besiroglu, T., Carugati, F., Clark, J., Eckersley, P., de Haas, S., Johnson, M., Laurie, B., Ingerman, A., Krawczuk, I., Askill, A., Cammarota, R., Lohn, A., Krueger, D., Stix, C., Henderson, P., Graham, L., Prunkl, C., Martin, B., Seger, E., Zilberman, N., hEigeartaigh, S.Ó., Kroeger, F., Sastry, G., Kagan, R., Weller, A., Tse, B., Barnes, E., Dafoe, A., Scharre, P., Herbert-Voss, A., Rasser, M., Sodhani, S., Flynn, C., Gilbert, T.K., Dyer, L., Khan, S., Bengio, Y., Anderljung, M.: Toward trustworthy AI development: mechanisms for supporting verifiable claims. arXiv:2004.07213 [cs] (2020)

emphasis on regulating generative AI, content moderation, and algorithmic recommendation systems. China's approach reflects deep integration of AI into state surveillance, social credit systems, and digital governance, with corresponding regulatory responses focused on control and compliance. The Chinese model raises significant human rights concerns, including extensive surveillance capabilities, social credit scoring systems, and limited transparency in algorithmic decision-making. However, it has also generated innovation in certain AI governance areas, including comprehensive sectoral regulations and rapid adaptive responses to emerging challenges. Comparative analysis reveals that state-centric approaches prioritize national interests and technological control over individual protections, creating fundamentally different policy outcomes than rights-based approaches.

5.4 Harmonization Challenges and Policy Transfer in Emerging Economies

For India and other emerging economies, selecting appropriate regulatory models requires careful contextual analysis rather than simple adoption of existing frameworks. Policy transferability depends on alignment with federal structures, MSME-dominant supply chains, and diverse skills ecosystems. The developmental model appropriate for India differs from the EU's rights-based emphasis or the U.S.'s market-driven approach, requiring customization to address India's specific challenges including informal labor markets, infrastructure gaps, and capacity constraints³⁵. Comparative analysis reveals that integrated approaches combining elements from different models may be optimal for emerging economies. These might include: selective adoption of EU principles regarding human rights protection, flexibility and innovation support from the U.S. model, sector-specific regulations tailored to India's economic structure, and capacity-building mechanisms addressing institutional gaps [34]. International cooperation mechanisms, including bilateral agreements and multilateral platforms like the OECD and G20, can support India's governance development while promoting regulatory convergence around core principles.

6. Future Directions and Policy Recommendations for Global and India-Specific Governance

6.1 Toward Binding International Legal Frameworks

The path toward effective global AI governance requires movement from voluntary guidelines and soft law toward binding international legal frameworks capable of ensuring accountability

³⁵ Gasser, U., Almeida, V.A.F.: A layered model for AI governance. *IEEE Internet Comput.* 21, 58–62 (2017). <https://doi.org/10.1109/MIC.2017.4180835>

and protecting fundamental rights. Current ethical guidelines, while important for establishing shared norms, often serve as rhetorical devices obscuring the absence of enforceable standards and accountability measures³⁶. The urgent need is for action by governments and civil society to develop rigorous, legally binding standards grounded in international human rights frameworks capable of holding powerful actors accountable. A proposed approach involves establishing a global AI governance framework that anchors diversity within shared minimum standards grounded in human dignity, accountability, and the rule of law. This requires multilateral cooperation that moves beyond fragmented experimentation toward principled coordination, without eliminating diversity in regulatory models. International mechanisms must address the core challenge: ensuring AI systems remain under meaningful human control, with transparency and rights protection as essential elements. The framework should be flexible enough to accommodate different regulatory philosophies while maintaining non-negotiable protections for fundamental rights.

6.2 Addressing Legal Challenges: Accountability and Enforcement

The key legal challenges in AI governance—algorithmic accountability, liability and responsibility, data privacy compliance, bias and discrimination, transparency and explainability, and cross-border enforcement—require urgent attention. These challenges exhibit high frequencies (78-95%) and severity levels (78-94%), indicating systemic governance gaps. Addressing these challenges demands: (1) clarified liability regimes that assign responsibility for AI system failures; (2) mandatory algorithmic audits and impact assessments; (3) transparency requirements enabling individual scrutiny of AI-driven decisions; (4) robust enforcement mechanisms with adequate funding and technical expertise; and (5) international coordination mechanisms for cross-border enforcement. Specific recommendations include: establishing independent AI auditing institutions; creating dedicated data protection authorities with AI expertise; implementing mandatory transparency reporting requirements; developing standardized methodologies for bias testing and algorithmic fairness assessment; and creating international enforcement coordination mechanisms. These measures should be grounded in principles of accountability, proportionality, and human rights protection rather than merely addressing corporate interests or state control preferences³⁷.

³⁶ Gill, A.S.: Artificial intelligence and international security: the long view. *Ethics Int. Aff.* 33, 169–179 (2019). <https://doi.org/10.1017/S0892679419000145>

³⁷ Ben-Israel, I., Cerdio, J., Ema, A., Friedman, L., Ienca, M., Mantelero, A., Matania, E., Muller, C., Shiroyama, H., Vayena, E.: Towards Regulation of AI Systems—Global perspectives on the development of a legal framework on

6.3 Protecting Human Rights in the Age of AI

Comprehensive human rights protection in AI governance requires moving beyond fragmented approaches to holistic frameworks addressing all dimensions of human dignity. This necessitates: (1) systematic human rights impact assessments for all AI systems with significant social consequences; (2) protection mechanisms for vulnerable populations particularly affected by algorithmic systems; (3) meaningful consent mechanisms enabling informed decision-making about personal data use; (4) transparency and explainability requirements allowing individuals to understand AI-driven decisions; (5) effective remedy mechanisms enabling individuals to challenge harmful AI outcomes; and (6) integration of human rights principles into AI design processes rather than treating them as afterthoughts. Emerging best practices suggest that responsible AI development requires: bias audits across diverse linguistic, cultural, and geographic contexts; inclusive teams in AI development; explicit human rights commitments; and collaborative engagement with civil society and affected communities. The UNESCO Recommendation on AI Ethics and the OECD AI Principles provide foundational guidance, but implementation requires more concrete standards and enforcement mechanisms. For India specifically, human rights protection demands integration of constitutional principles—particularly the right to privacy, equality, freedom of expression, and due process—into all AI governance frameworks.

6.4 India's Path Forward: Building Comprehensive AI Governance

For India, a comprehensive approach to AI governance should integrate elements from global best practices while addressing country-specific challenges and opportunities. Recommendations include: Short-term priorities³⁸ (1-2 years):

- Enact comprehensive AI legislation establishing baseline standards across all sectors.
- Establish dedicated AI governance institutions with technical expertise and enforcement capacity.
- Develop sector-specific guidelines for financial services, healthcare, and public welfare delivery.
- Implement mandatory transparency and explainability requirements for high-risk AI systems. Create mechanisms for public participation in AI governance decisions.

Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law. Council of Europe (2020)

³⁸ Y. Lu and F. H. Tie, "A comparative analysis of artificial intelligence regulation in ASEAN and the European Union," Publishing house "Virtus Interpress," Dec. 2025, doi: <https://doi.org/10.22495/jgrv14i4siart16>.

Medium-term initiatives (2-5 years):

- Build capacity in regulatory institutions, judiciary, and civil society regarding AI governance
- Develop standardized testing methodologies for AI bias, fairness, and transparency
- Establish coordinated enforcement mechanisms across central and state governments
- Create independent auditing institutions for high-risk AI systems
- Integrate human rights considerations into all AI policy frameworks
- Develop India-specific ethical frameworks incorporating constitutional values and cultural context.

Long-term strategic directions (5+ years):

- Position India as a leader in responsible AI development with strong governance mechanisms
- Contribute to international standards development and governance harmonization
- Build indigenous AI expertise and reduce dependence on Western models and datasets
- Foster inclusive innovation promoting AI benefits across all socioeconomic groups
- Establish institutional mechanisms for regular governance reviews and adaptive updates
- Practical implementation requires: adequate budget allocation for enforcement and capacity-building; coordination between central and state governments; engagement with industry, civil society, and academic institutions; and regular assessment of governance effectiveness.
- The fragmented sectoral mosaic approach, while potentially addressing sector-specific concerns, should be consolidated through overarching principles ensuring consistency and cross-sector coordination³⁹.

6.5 International Cooperation and Multilateral Coordination

Effective global AI governance requires robust international cooperation mechanisms addressing regulatory fragmentation while respecting national sovereignty and diversity. Recommendations include: establishing multilateral governance platforms for regular coordination and standard-setting; creating bilateral recognition mechanisms enabling companies to demonstrate compliance once for multiple jurisdictions; developing capacity-

³⁹ A. Ishkhanyan, "Governing AI across borders: corporate power, state sovereignty and global regulation," Digital Policy Regulation and Governance, Jun. 2025, doi: 10.1108/dprg-03-2025-0057.

building initiatives supporting governance development in emerging economies; and establishing international dispute resolution mechanisms for cross-border AI governance conflicts. India should actively engage in international forums including the UN, OECD, G20, and BRICS to shape global AI governance standards reflecting the interests and values of emerging economies. Particular focus should be placed on: ensuring that global governance frameworks address development equity and technology access; incorporating perspectives from non-Western ethical traditions and value systems; promoting capacity-building mechanisms supporting governance implementation in developing countries; and resisting pressure for regulatory harmonization that undermines legitimate policy differences reflecting different national values and institutional contexts.

RATIONALE, DEFINITION AND SCOPE

Global AI governance refers to the evolving system of multilayered, multi-stakeholder institutions, frameworks, laws, standards, and mechanisms through which international actors—including nation-states, international organizations, corporate entities, civil society organizations, and academic institutions—attempt to establish binding rules, guiding⁴⁰ principles, and accountability structures that shape the development, deployment, and use of artificial intelligence technologies across national boundaries and across sectors⁴¹.

Key Characteristics:

Polycentric Structure: No single authority governs AI globally; instead, governance operates through overlapping, sometimes contradictory initiatives at international, regional, national, and sectoral levels.

Nascent and Contested: Unlike established governance regimes (e.g., World Trade Organization), AI governance remains fragmented, with competing visions advanced by different actors⁴²

Multi-Dimensional: Encompasses regulatory dimensions (laws, policies), normative dimensions (principles, ethical frameworks), institutional dimensions (organizations, oversight bodies), technical dimensions (standards, specifications), and market dimensions (investment patterns, competitive dynamics).⁴³

⁴⁰ Schmitt, 2021

⁴¹ Saidi, 2025

⁴² Gupta, 2025

⁴³ Muchtasor, 2025

2: Legal Problems

Definition: Legal problems in AI governance encompass the substantive inadequacies, ambiguities, contradictions, and enforcement gaps within existing legal frameworks that arise from the unprecedented technical, operational, and social characteristics of AI systems and their interaction with established legal regimes designed for different technologies and social contexts.

Core Legal Challenges Included:

Regulatory Fragmentation and Gaps: The absence of binding international frameworks and presence of fragmented sectoral, national, and regional initiatives create inconsistent standards, regulatory arbitrage, and inadequate protection.

Algorithmic Accountability: Diffusion of responsibility across developers, deployers, and users makes it difficult to assign liability for algorithmic failures⁴⁴.

Data Privacy and Protection: AI's data requirements fundamentally conflict with data minimization principles in privacy law⁴⁵

Transparency and Explainability: Legal mandates for transparency conflict with intellectual property protection and technical limitations⁴⁶

Algorithmic Bias and Discrimination: Existing anti-discrimination law struggles with systematic but unintended discrimination produced by algorithms⁴⁷

Cross-Border Enforcement: Territorial jurisdiction principles conflict with borderless AI systems.

3: Human Rights Problems

Definition: Human rights problems in AI governance refer to the systematic and unprecedented threats that AI systems pose to fundamental human rights—as established in international human rights instruments, constitutional frameworks, and evolving interpretations of digital-age rights—through surveillance, discrimination, loss of autonomy, deprivation of due process, and erosion of foundational human dignity⁴⁸.

Rights at Risk:

Right to Privacy: Threatened through pervasive surveillance, data collection without meaningful consent, and integration of data across sectors.

⁴⁴ Díaz-Rodríguez et al., 2023

⁴⁵ Rathi, 2025

⁴⁶ Huang et al., 2026

⁴⁷ Popovich, 2025

⁴⁸ Chan and Lo, 2025

Right to Non-Discrimination and Equality: Threatened through systematic algorithmic bias affecting credit, employment, criminal justice, and welfare decisions.

Right to Autonomy and Human Agency: Threatened through automated decision-making systems that reduce human participation in decisions affecting fundamental life choices⁴⁹

Right to Due Process and Fair Trial: Threatened through unexplainable algorithmic decisions in criminal justice and administrative proceedings⁵⁰

Right to Freedom of Expression and Information: Threatened through content moderation algorithms that shape public discourse⁵¹

Right to Explanation and Contestability: Threatened through opacity in algorithmic systems preventing individuals from challenging adverse outcomes⁵²

4: Regulatory Models for India

Definition: Regulatory models for India encompass the distinctive institutional arrangements, legal frameworks, policy instruments, and enforcement mechanisms that India has adopted or should adopt to govern AI development and deployment, tailored to India's unique constitutional framework, developmental stage, institutional capacity, cultural values, and societal challenges.

India-Specific Considerations:

Constitutional Grounding: Must reflect India's constitutional commitment to equality, secularism, and democratic participation

Development Stage: Must balance innovation promotion with protection for a developing economy and vulnerable populations⁵³

Institutional Capacity: Must be implementable given India's governance challenges and limited enforcement resources

Sector-Specific Contexts: Must address India's unique sectoral governance needs in healthcare, financial inclusion, criminal justice, and public welfare

Global Positioning: Must enable India to contribute to global governance while protecting national interests.

⁴⁹ Deckker and Sumanasekara, 2025

⁵⁰ Rotolo et al., 2025

⁵¹ Huang et al., 2026

⁵² Fukuda-Parr and Gibbons, 2021

⁵³ Roy and Sarma, 2025

1.2 The Integrated Nature of the Topic

Critically, these four elements are deeply interconnected rather than separate concerns:

Legal frameworks must protect rights: Effective governance requires that legal structures be designed to prevent human rights violations and provide remedies when violations occur⁵⁴

Rights concerns inform regulatory design: Understanding which rights are most threatened by AI informs which regulatory measures are most urgent⁵⁵

Global governance shapes India's options: International standards, agreements, and enforcement mechanisms constrain and enable India's regulatory choices⁵⁶

India's governance contributes to global frameworks: As a major emerging economy and technology actor, India's regulatory approach influences global governance development.

PART II: RATIONALE FOR THIS RESEARCH TOPIC

2.1 The Convergence of Three Critical Crises

The rationale for this research topic emerges from the convergence of three distinct but interconnected crises that cannot be adequately addressed through separate scholarship:

Crisis 1: The Global AI Governance Vacuum

Despite AI's transformative global impact, effective international governance frameworks remain absent. Currently:

No Binding International Framework: Unlike issues such as human trafficking, environmental protection, or weapons non proliferation, no binding international legal instrument specifically governs AI development and deployment.

Regulatory Fragmentation: Governance initiatives are scattered across regions with fundamentally different philosophies: the EU's risk-based approach emphasizing human rights protection; the US's decentralized, market-driven approach; China's state-centric, surveillance-oriented model; and emerging economies' fragmented responses

Enforcement Gaps: Most governance frameworks lack effective enforcement mechanisms, relying instead on voluntary compliance, corporate self-regulation, or limited government oversight⁵⁷

Power Asymmetries: Large technology corporations disproportionately influence governance outcomes, undermining democratic accountability and public interest protection⁵⁸

⁵⁴ Díaz-Rodríguez et al., 2023

⁵⁵ Molbæk-Steensig and Scheinin, 2025

⁵⁶ Kumar and Sahu, 2026

⁵⁷ Ishkhanyan, 2025

⁵⁸ Li, 2025

This governance vacuum creates cascading risks: regulatory arbitrage enables corporations to evade accountability; fragmentation prevents coordinated responses to transnational AI risks; power asymmetries marginalize developing country interests; and the absence of binding frameworks means that AI development proceeds without meaningful international accountability.

Unprecedented Human Rights Threats

AI systems pose systematic threats to fundamental human rights on an unprecedented scale:

Pervasive Surveillance: AI-powered facial recognition, biometric systems, and algorithmic monitoring create what scholars term a "digital Panopticon," enabling continuous tracking of billions of individuals without meaningful consent or transparency⁵⁹

Systematic Discrimination: Algorithmic systems systematize bias against protected groups, affecting credit access, employment, criminal sentencing, welfare benefits, and educational opportunities⁶⁰

Loss of Human Agency: Automated decision-making systems reduce human participation in decisions affecting fundamental rights, particularly in criminal justice where algorithms influence sentencing.

Denial of Due Process: Individuals face algorithmic decisions with no meaningful understanding of the decision basis, no ability to challenge outcomes, and no effective remedy mechanisms⁶¹

Erosion of Democratic Autonomy: Algorithmic systems enable what scholars call "slow violence"—gradual, systemic harms that accumulate to undermine human rights frameworks themselves.

Critically, existing human rights frameworks and institutions—designed in the post-World War II era for different technologies and social contexts—have not adequately adapted to these unprecedented threats⁶². Current legal protections for privacy, non-discrimination, autonomy, and due process remain inadequate for the AI era.

The Development Justice Challenge for India and Emerging Economies

For India and other emerging economies, the governance challenge extends beyond merely regulating harmful AI impacts to ensuring that AI development itself advances rather than undermines equitable development:

⁵⁹ Chan and Lo, 2025

⁶⁰ Popovich, 2025

⁶¹ Rotolo et al., 2025

⁶² Molbæk-Steensig and Scheinin, 2025

Technology Dependence: India depends on foreign technology and governance models, with limited capacity to shape governance frameworks according to its own values and development priorities⁶³

Fragmented Governance Landscape: India's regulatory approach remains scattered across sectoral legislation with no comprehensive AI law, creating governance gaps and inconsistent protection.

Differential Vulnerability: India's large informal workforce, extensive poverty, and high inequality make AI-driven displacement and discrimination particularly consequential.

Institutional Capacity Constraints: India's regulatory agencies face resource limitations, technical capacity gaps, and coordination challenges limiting governance effectiveness⁶⁴

Power Asymmetries: Large multinational technology corporations exercise disproportionate influence over India's technology governance, potentially undermining national interests and public protections.

Without proactive governance intervention grounded in India's constitutional values and development priorities, AI development risks intensifying existing inequalities, concentrating technological power among global corporations, and creating new forms of digital colonialism.

2.2 Why Integrated Analysis Across These Dimensions Is Essential

Existing scholarship addresses these crises through fragmented approaches:

Legal scholars focus on regulatory frameworks and compliance mechanisms but often underemphasize rights impacts.

Human rights scholars focus on rights threats but often lack detailed engagement with legal and institutional solutions.⁶⁵

Development scholars focus on economic impacts but often minimize governance and rights dimensions.⁶⁶

Global governance scholars focus on international dynamics but often lack adequate attention to context-specific challenges of emerging economies.

This fragmentation means that critical interconnections are missed. For example:

Understanding India's regulatory challenges requires simultaneously analyzing India's legal capacity, the global governance context constraining India's options, and the human rights

⁶³ Roy and Sarma, 2025

⁶⁴Durodola, 2025

⁶⁵ Baldassarre et al., 2025

⁶⁶ Roy and Sarma, 2025

implications of different regulatory approaches

Effective global governance frameworks must address not only regulatory harmonization but also rights protection and development equity

Developing country concerns about governance must be understood not merely as implementation challenges but as fundamental justice issues requiring integration into core governance frameworks

2.3 The Urgency of This Analysis

The urgency of this research topic is underscored by several factors:

Technological Acceleration: AI capabilities are advancing rapidly—from narrow applications to general-purpose systems capable of autonomous reasoning across domains—while governance mechanisms lag significantly behind⁶⁷. This governance-technology gap creates increasing risks.

Irreversibility of Harm: Many AI harms cannot be easily reversed: algorithmic discrimination affecting millions may persist for years; surveillance infrastructure, once established, is rarely dismantled; and algorithmic bias in foundational systems (criminal justice, credit) creates compounding harms across time⁶⁸.

Window for Governance Formation: Current moment offers a critical window for shaping emerging AI governance frameworks. Once governance structures solidify, reform becomes vastly more difficult. The period 2024-2026 represents a crucial moment before governance fragmentation becomes entrenched⁶⁹.

Global Stakes: The governance choices made in this period will shape not only how AI is regulated but the fundamental direction of AI development itself—whether prioritizing innovation over rights, whether concentrating technological power among global corporations or supporting distributed development, whether reproducing historical inequalities or advancing equitable development⁷⁰.

Research Question

Is existing international law sufficient to regulate AI systems?

⁶⁷ Ghadei et al., 2025

⁶⁸ Popovich, 2025

⁶⁹ Gupta, 2025

⁷⁰ Kumar and Sahu, 2026

Methodology

This research employs a mixed-method qualitative framework to investigate the nexus between AI governance, legal challenges, human rights concerns, and regulatory models applicable to India. The study adopts a doctrinal legal research methodology combined with comparative legal analysis and policy analysis to provide a comprehensive examination of existing and emerging regulatory architectures for artificial intelligence.

International Legal Frameworks: Structural Inadequacy

The rapid advancement of artificial intelligence has exposed fundamental inadequacies in existing international legal frameworks, which were designed for pre-digital societies and cannot accommodate the complexity of algorithmic systems. The current global AI governance landscape demonstrates a "deficit" due to the inadequacy of existing initiatives and persistent gaps in reaching agreement over appropriate regulatory mechanisms⁷¹.

The fragmentation across global governance models reveals systematic weaknesses. The EU pursues a rights-based approach, the US follows a market-driven model, and China adopts a state-centric framework⁷²—these divergent approaches create jurisdictional conflicts, regulatory inconsistency, and gaps in accountability. Traditional legal instruments designed for human-centric decision-making fail to address core algorithmic challenges: the "black box" problem of algorithmic opacity, algorithmic bias and discrimination, data sovereignty conflicts, and the absence of clear liability frameworks for autonomous AI systems⁷³.

India's current legal landscape, anchored in the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, is fragmented and insufficient to adequately address AI-specific risks⁷⁴. These instruments predate the AI revolution and contain no specific provisions for risk-based AI classification, high-risk system requirements, or algorithmic impact assessments. International frameworks such as UNESCO's AI Ethics Recommendation and OECD AI Principles offer only non-binding ethical guidance without statutory implementation, leaving critical governance gap. The World Health Organization and United Nations similarly advocate high-level frameworks but provide no enforceable compliance mechanisms.

B. Why India Requires a Distinct Regulatory Approach

⁷¹ Roberts, 2024

⁷² Ismail, 2025

⁷³ Antai, 2025

⁷⁴ Suraj, 2025

1. Constitutional Foundations

India's regulatory framework for AI must be grounded in the country's constitutional architecture, particularly the protection of Fundamental Rights. The Indian Constitution provides several critical anchors for AI governance that international frameworks often overlook⁷⁵:

- Article 14: Right to Equality and non-discrimination—protecting citizens from algorithmic bias
- Article 19(1)(a): Freedom of speech and expression—requiring transparency in algorithmic content moderation
- Article 21: Right to life and personal liberty—including digital privacy and freedom from automated surveillance
- Articles 16 and 23: Protection against exploitation—critical for preventing algorithmic discrimination in employment, credit, and public services

The landmark judgment *K.S. Puttaswamy v. Union of India* (2017)⁷⁶ established privacy as a fundamental right under Article 21, a recognition that must inform AI governance. India's constitutional framework emphasizes human dignity, democratic accountability, and proportionality—principles that must be embedded in AI regulatory design, not merely aspirational.

2. Asymmetric Surveillance Risks

India faces unique threats from AI-enabled surveillance systems that demand specific constitutional safeguards. The government's deployment of AI-driven surveillance technologies—including predictive policing, facial recognition systems, and data analytics for law enforcement—creates particular risks in the Indian context⁷⁷:

- State surveillance intensification: India's broad national security exemptions in data protection laws create regulatory asymmetry between corporate and state actors
- Caste and socioeconomic bias: Algorithmic systems trained on historical data replicate existing discrimination patterns endemic to Indian society

⁷⁵ A. Arora, L. Saboia, A. Arora, and J. R. McIntyre, "Human-Centric Versus State-Driven: A Comparative Analysis of the European Union's and China's Artificial Intelligence Governance Using Risk Management," *International Journal of Intelligent Information Technologies*, Jan. 2025, doi: 10.4018/ijit.367471.

⁷⁶ S. Baek, "A Constitutional Analysis of Fundamental Rights in Relation to High-Impact Artificial Intelligence - With a Comparative Study of the EU AI Act and the Framework Act on the Promotion of Artificial Intelligence and the Establishment of Trust in Korea," *European Constitutional Law Association*, Aug. 2025, doi: 10.21592/eucj.2025.48.189.

⁷⁷ S. Hong, "The Risks of AI Infringing on Fundamental Rights and Normative Responses : Focusing on the Use of AI in Judicial System and the Right to a Trial," *Center for Public Interest & Human Rights Law Chonnam National University*, Feb. 2025, doi: 10.38135/hrlr.2025.34.281.

- Minority rights erosion: Profiling systems deployed against marginalized communities—religious minorities, lower castes, dissidents—undermine constitutional protections⁷⁸

The Digital Personal Data Protection Act, 2023 contains expansive exemptions for state agencies collecting data for "national security" purposes, creating a governance gap where state AI systems operate with minimal oversight⁷⁹. India requires a regulatory framework that explicitly restricts state surveillance, mandates human-in-the-loop decision-making for high-risk state AI systems, and provides enforceable remedies for algorithmic harm.

3. Developmental and Institutional Context

India's federal structure, limited regulatory capacity, and developmental constraints require a regulatory model distinct from the EU's centralized approach⁸⁰:

- Institutional capacity: The EU benefits from established enforcement agencies with technical expertise; India's regulatory bodies require capacity-building
- Decentralized governance: India's federal system distributes regulatory authority across multiple agencies; harmonization requires flexible coordination mechanisms
- Innovation environment: India's role as a global AI developer and emerging technology hub demands a framework that supports innovation while protecting fundamental rights
- Socioeconomic heterogeneity: India's vast socioeconomic diversity means AI systems have differential impacts across regions, requiring adaptive, context-sensitive governance

C. The Hybrid Regulatory Model: EU Risk Classification Plus Constitutional Safeguards

1. EU AI Act's Risk-Based Framework: Structure and Strengths

The EU Artificial Intelligence Act (adopted March 2024) provides the first comprehensive, legally binding AI regulatory framework and establishes a four-tiered risk classification system⁸¹:

Unacceptable Risk: AI systems posing unacceptable risks to fundamental rights are prohibited.

Examples include AI for mass surveillance and social scoring⁸².

High-Risk Systems: AI applications that significantly impact fundamental rights or safety must

⁷⁸ Abraham, 2024

⁷⁹ D. Kumar and C. K. Sahu, "Artificial intelligence governance and social policy divergence: a comparative political economy perspective on global AI regulation," *International journal of sociology and social policy*, Mar. 2026, doi: 10.1108/ijssp-02-2026-0129.

⁸⁰ F. M. Teichmann, "Risk, Reasonableness and Residual Harm under the EU AI Act: A Conceptual Framework for Proportional Ex-Ante Controls," *European Journal of Risk Regulation*, Jan. 2026, doi: 10.1017/err.2025.10077.

⁸¹ Greenstein, 2025

⁸² Wagner, 2025

comply with stringent pre-market requirements, including:

- Risk impact assessments
- High-quality data governance and documentation
- Transparency and human oversight mechanisms
- Post-market monitoring and incident reporting
- Conformity assessment by independent third parties⁸³

Limited-Risk Systems: AI systems with transparency obligations (e.g., chatbots must disclose AI involvement)

Minimal-Risk Systems: Most AI applications face no specific requirements

This risk-based approach balances innovation with rights protection, a framework superior to purely principles-based or technology-specific models⁸⁴. The EU Act also establishes institutional mechanisms: a dedicated AI regulatory authority, harmonized standards, and structured accountability pathways.

2. Constitutional Safeguards Layer for India

While the EU model provides excellent institutional design, it requires modification through India's constitutional framework. A hybrid Indian model should integrate:

Fundamental Rights Impact Assessment (FRIA)

High-risk AI systems must undergo mandatory FRIA examining impacts on:

- Right to equality and freedom from discrimination (Article 14)
- Freedom of expression and information (Article 19)
- Right to life, dignity, and privacy (Article 21)
- Protection against exploitation (Articles 23-24)

Unlike the EU's "impact assessment," FRIA explicitly grounds analysis in India's constitutional values and provides judicially enforceable standards⁸⁵.

Proportionality Review

State AI systems must satisfy India's constitutional proportionality test:

- Legitimate aim: Does the AI system serve a constitutionally permissible government objective?
- Necessity: Is the system necessary to achieve that aim?
- Suitability: Is the system suitable (does it actually advance the aim)?

⁸³ Hohmann, 2025

⁸⁴ Amore, 2025

⁸⁵ D. Kumar and C. K. Sahu, "Artificial intelligence governance and social policy divergence: a comparative political economy perspective on global AI regulation," *International journal of sociology and social policy*, Mar. 2026, doi: 10.1108/ijssp-02-2026-0129.

- Proportionality: Do the benefits outweigh fundamental rights restrictions?

This framework explicitly prevents state surveillance expansion under national security pretexts⁸⁶.

Democratic Accountability Mechanisms

- Mandatory transparency reports to parliament on state AI deployments
- Independent oversight boards including civil society, affected community representatives, and technical experts
- Public contestability rights: Citizens must be able to challenge algorithmic decisions affecting them with human review.⁸⁷
- Regular audits by constitutional courts for rights alignment

Algorithmic Contestability and Human-in-the-Loop

For high-risk AI systems, particularly those affecting vulnerable populations:

- Automated decisions must not be final; affected individuals must have meaningful human review
- "Black box" algorithms must be subject to explainability requirements tailored to India's legal culture
- Citizens must retain the right to judicial review of algorithmic determinations

3. Risk Classification Adapted to Indian Context

India should adopt the EU's four-tier structure but with India-specific high-risk categories:

Prohibited AI:

- Facial recognition for mass surveillance or state tracking
- Social scoring systems
- Deepfake-based disinformation targeting elections or public order⁸⁸

High-Risk AI (beyond EU categories):

- Predictive policing and criminal risk assessment.
- Hiring and promotion systems in government and public enterprises
- Credit and loan decisioning affecting vulnerable populations
- Healthcare algorithms determining treatment eligibility
- Judicial case prediction or sentencing recommendation systems
- AI systems deployed in prisons or detention facilities

⁸⁶ Abraham, 2024

⁸⁷ Trapani, 2026

⁸⁸N. Basu and R. Dave, "Comparative Analysis of Laws in AI," Journal of Lifestyle and SDGs Review, Feb. 2025, doi: 10.47172/2965-730x.sdgsreview.v5.n03.pe05575.

Limited-Risk AI:

- Government chatbots and customer service AI
- AI-assisted medical diagnostics

Minimal-Risk AI:

- Spam filters, basic content recommendation

D. Institutional Architecture for India's Hybrid Model

1. Multi-Layered Governance Structure

Central AI Regulatory Authority

- Specialized agency with technical expertise, legal authority, and enforcement power
- Mandate to develop AI standards, conduct risk assessments, and investigate violations
- Composition including technologists, constitutional lawyers, civil society representatives, and affected community members

Sectoral Oversight

- Healthcare, finance, law enforcement agencies implement FRIA and maintain post-deployment monitoring
- Cross-sector coordination mechanisms to prevent regulatory arbitrage
- Regular reporting to independent oversight board

Constitutional Court Review

- Supreme Court and High Courts retain jurisdiction to review AI system legality under fundamental rights
- Expedited procedures for cases involving surveillance, discrimination, or rights violations
- Power to issue interim orders suspending AI systems pending rights review

Civil Society and Affected Community Participation

- Mandatory consultation with affected populations before deploying high-risk AI
- Public contestability mechanisms enabling citizens to challenge algorithmic decisions
- Regular audits by independent civil society organizations

2. Enforcement and Sanctions

The framework must include credible enforcement:

- Administrative penalties for system providers violating high-risk requirements
- Interim suspension powers for systems causing demonstrable harm
- Liability mechanisms clarifying responsibility when AI systems violate fundamental rights
- Remedial rights enabling affected individuals to seek damages and corrective action

E. Comparative Evidence and International Convergence

Recent comparative analyses demonstrate growing recognition of the inadequacy of purely national or purely principles-based approaches. The "developmental model" emerging in India, alongside the "hybrid models" in Australia, Japan, and Singapore, combines risk-based regulation with constitutional/cultural safeguards⁸⁹.

Several jurisdictions are moving toward models that blend EU-style risk classification with localized constitutional frameworks:

- Korea's Framework Act emphasizes "high-impact" AI requiring transparency and human oversight, adapted to Korea's governance model
- Nigeria's regulatory approach proposes hybrid risk-based frameworks suited to developing economy constraints⁹⁰.
- Brazil's AI governance integrates constitutional human rights principles with sectoral regulation⁹¹

India's position as a major AI developer, emerging economy, and constitutional democracy uniquely positions it to pioneer a hybrid rights-based, risk-responsive regulatory model that protects fundamental rights while enabling responsible innovation⁹².

Conclusion: Urgency and Path Forward

The inadequacy of current international frameworks is no longer theoretical—it is demonstrably failing to protect citizens from algorithmic harm. India's response must be neither wholesale adoption of the EU model nor continued reliance on fragmented legacy legislation. Instead, India requires a purpose-built hybrid framework that⁹³:

1. Adopts EU risk-based classification for institutional coherence and stakeholder clarity
2. Grounds governance in India's constitutional values (equality, dignity, democratic accountability)
3. Addresses India-specific risks (surveillance, discrimination, marginalization)
4. Builds institutional capacity through multi-sector governance and capacity-building

⁸⁹ Kumar, 2026

⁹⁰ Okiti, 2026

⁹¹ Gajjar, 2024

⁹² Mathew, 2025

⁹³ N. Basu and R. Dave, "Comparative Analysis of Laws in AI," *Journal of Lifestyle and SDGs Review*, Feb. 2025, doi: 10.47172/2965-730x.sdgsreview.v5.n03.pe05575.

5. Ensures human-centered oversight preserving judicial review and democratic contestability⁹⁴

This hybrid approach recognizes that effective AI governance is not universal—it must adapt to constitutional traditions, institutional capacities, and societal risks. India has the opportunity to establish a globally influential model that demonstrates how emerging democracies can leverage binding legal frameworks and constitutional principles to govern AI responsibly.



⁹⁴ O. Akinrele, “AI Governance and Data Privacy: Comparative Analysis of U.S., EU and African Frameworks,” World Journal of Advanced Engineering Technology and Sciences, Jan. 2026, doi: 10.30574/wjaets.2026.18.1.0036.