

Artificial Intelligence Governance and Legal Regulation: Emerging Trends and Challenges

Manindra Singh Hanspal

Assistant Professor, School of Law, Presidency University, Bengaluru, Karnataka

ARTICLE INFO

*Correspondence:

mhanspal21@gmail.com

Assistant Professor,
School of Law,
Presidency University,
Bengaluru, Karnataka

Dates:

Received: 25-04-2026

Accepted: 28-05-2026

Published: 30-06-2026

Keywords:

artificial intelligence,
AI governance, AI
regulation, EU AI
Act, algorithmic
accountability, data
protection, India
DPDP Act, risk-based
regulation.

How to Cite:

Hanspal, M.S. (2025)
Article Title. DME
Journal of Law, 7(1),
45-55.
doi: 10.53361/dmejl.
v7i01.05

Abstract

Artificial intelligence (AI) has become an integral part of governance, economics and law. Governments employ algorithmic technologies for taxes, social welfare, law enforcement and health care, and private platforms control information and labour markets. This growth has led to a regulatory challenge. Technological innovation proceeds through processing data, training algorithms. Legislative regulation progresses through more time-consuming regulatory mechanisms. This paper explores the field through a doctrinal analysis of legal and regulatory initiatives, such as the European Union AI Act, OECD AI Principles, US executive model and the Indian position under the DPDP Act and NITI Aayog. The paper highlights four recurring issues of accountability and responsibility, bias and discrimination, data governance and regulatory fragmentation. The paper links empirical research trends to legal issues. Richness in the use of ethics and governance terms and scantiness in the doctrinal work on liability and enforcement is noted. The paper recommends a comprehensive regulatory approach with a chain of risk-based classification, impact assessments and sectoral regulatory measures. The novelty is the combination of bibliometric analysis and legal analysis to offer regulators, academics and practitioners an overview of the state of AI governance and its direction.

INTRODUCTION

Artificial intelligence systems now decide who gets a loan, which job applications reach human reviewers, how diseases are screened, and how content spreads online.¹ The shift from research labs to everyday infrastructure has happened within a short span. With the release of large generative models from late 2022 onward, public attention to AI risks rose sharply.² Governments responded with proposals, executive orders, and binding statutes. AI governance refers to the set of rules, institutions, and processes used to steer the design, deployment, and oversight of AI systems. It covers law, technical standards, internal corporate

1 Brandao, P. R. (2025). The impact of artificial intelligence on modern society. *AI*, 6(8), 190.

2 Hutson, J., & Plate, D. (2025). *The case against disclosure: Defending creative autonomy in the age of AI*. Common Ground Research Networks.

controls, and international coordination.³ Legal regulation forms one part of this wider field. It sets binding duties on developers and deployers, creates rights for affected persons, and assigns enforcement powers to public authorities.⁴ The importance of AI governance rests on three points. First, AI systems scale decisions in ways older tools do not. A flawed credit model affects millions of applicants in a single deployment.⁵ Second, many systems are opaque. Users and regulators often cannot inspect how outputs are produced. Third, harms tend to fall on people with the least power to push back, including job seekers, welfare claimants, and members of historically disadvantaged groups. The problem this article addresses is the gap between the speed of AI deployment and the maturity of legal frameworks. Rules drafted in 2021 are being asked to cover technologies released in 2025 and 2026. Different jurisdictions are heading in different directions. The European Union has built a comprehensive risk-based statute. The United States, after a change in administration, has shifted toward a deregulatory federal stance with active resistance to state-level rules. India has taken a soft-law route grounded in existing statutes. Companies operating across all three face conflicting expectations. The objective of this article is to map the field as it stands in 2026. The article asks four questions. What are the research trends in AI governance over the last decade? What is the conceptual scope of AI governance, and why is regulation needed? Where do the main

legal frameworks stand today? What are the open challenges for researchers and policymakers to resolve?

The article uses public regulatory texts, recent bibliometric reviews, and policy analyses from law firms, academic journals, and government bodies. It does not propose a new model. It synthesizes work done by others and points to the open questions. The scope is limited in three ways. First, the article focuses on civilian AI governance and does not cover military AI in detail. Second, it gives most attention to three jurisdictions, with shorter notes on others. Third, it treats technical issues at the level needed to understand legal questions, not at the level of model engineering. Two background points help frame the rest of the article. First, AI is not one technology. Rule-based expert systems, narrow predictive models, large language models, and autonomous agents raise different risks and need different rules. Many AI laws use technology-neutral definitions to keep up with change, but the choice creates its own interpretive problems.⁶ Second, AI risks fall on a spectrum. Some are immediate and individual, like a wrongful denial of a loan. Some are diffuse and systemic, like changes to information markets caused by AI-generated content. Governance has to address both.⁷

Research Trends In Ai Governance

This section presents an overview of research output on AI governance and regulation within Law and Legal Studies. The data was retrieved from the Dimensions database on 28 April 2026 using the search query: “artificial intelligence governance” OR “AI governance” OR “artificial intelligence regulation” OR “AI regulation” OR “AI policy”, restricted to Field of Research code 48 (Law and Legal Studies) under the ANZSRC 2020 classification. The query returned 2,077 publications across the years 2017 to 2026. The

3 Mukherjee, B. N. (2025). Navigating AI Governance: National and International Legal and Regulatory Frameworks. In *Navigating the Intersection of AI Policy, Technology, and Governance* (pp. 201-224). IGI Global Scientific Publishing.

4 Osifo, E. O., Omumu, E. S., & Alozie, M. (2025). Evolving contractual obligations in construction law: Implications of regulatory changes on project delivery. *World J. Adv. Res. Rev.*, 25(3), 1315-1333.

5 Abbas, S. K. (2025). Lending by algorithm: Fair or flawed? An information-theoretic view of credit decision pipelines. *SN computer science*, 6(6), 679.

6 Ojanen, A. (2025). Technology neutrality as a way to future-proof regulation: the case of the Artificial Intelligence Act. *European Journal of Risk Regulation*, 1-16.

7 Fan, L., & Wu, M. (2025, October). Social Impacts, Risks, and Governance Framework of Generative Artificial Intelligence Applications. In *2025 International Conference on Algorithms, Software and Network Security (ASNS)* (pp. 41-48). IEEE.

Table 2: Principal keyword clusters in the AI governance corpus

Rank	Keyword Cluster	Frequency Tier	Indicative Themes
1	Artificial intelligence / AI	Very high	Core subject term across all clusters
2	Governance	High	Public administration, oversight, institutional design
3	Regulation / Law	High	EU AI Act, sectoral rules, national frameworks
4	Ethics	High	Fairness, principles, responsible AI
5	Data protection / Privacy	Medium	GDPR, personal data, consent, profiling
6	Algorithmic decision-making	Medium	Automated systems, ADM, public sector use
7	Bias / Discrimination	Medium	Fairness audits, equality, protected groups
8	Accountability / Liability	Medium-low	Civil liability, redress, responsibility gaps
9	Risk-based regulation	Medium-low	Risk classification, impact assessments
10	Generative AI / Large language models	Rising	Foundation models, content moderation, copyright

broad governance and regulation terms, followed by ethics-oriented vocabulary. Terms tied to operational legal mechanisms, including accountability, liability, and risk classification, appear less frequently. Generative AI and large language models are a rising cluster from 2023 onwards.

Figure 2 shows a co-authorship network for the corpus, generated using VOSviewer. Several distinct clusters appear, organized around scholars working on EU AI regulation, ethics-led governance, fundamental rights, and platform regulation. The network density confirms that the field is no longer a small group of contributors but a connected scholarly community with multiple sub-communities. The largest nodes correspond to authors with sustained output across the period and indicate the consolidation of recognizable research programmes within AI law and regulation.

Figure 3 presents a tighter sub-network of the most frequently co-citing authors. The compact structure of this map indicates a core group of contributors whose work is regularly engaged across the broader literature. This pattern is consistent with an early-stage but rapidly maturing field, where a small set of authors anchors the doctrinal conversation.

Thematic Insights

The trend data points to three thematic concentrations within legal scholarship on AI governance. The first is ethics. Work in this stream addresses fairness, transparency, autonomy, and human dignity. It draws on the high-level expert group reports of the European Commission,

UNESCO instruments, and the OECD AI Principles. Ethical writing dominates the early years of the corpus and continues to influence the framing of later legal work. The strength of this stream explains why ethics terms remain among the most frequent in the keyword data. The second concentration is governance. Publications under this theme examine institutional design, multi-stakeholder oversight, and the role of standard-setting bodies. They address how AI systems are managed within organizations, how risks are assessed, and how external oversight is structured. Governance writing has grown particularly fast since 2022. Several contributions focus on the operational use of impact assessments, audits, and registers of high-risk systems. This stream connects directly with the EU AI Act and with similar national frameworks under development in the United Kingdom, Canada, and Brazil. The third concentration is regulation. Publications under this

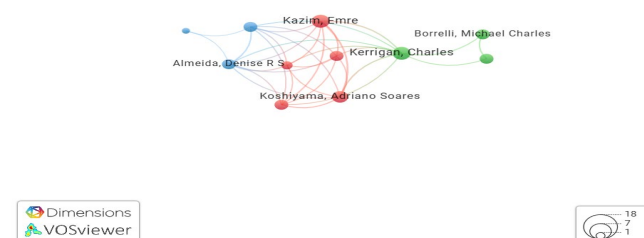


Figure 3: Core sub-network of frequently co-cited authors in the AI governance corpus. Source: Dimensions data analysed in VOSviewer.

theme cover specific statutory instruments, sectoral rules, and enforcement mechanisms. The EU AI Act, the General Data Protection Regulation, and competition rules feature prominently. Indian work focuses on the Digital Personal Data Protection Act, 2023, and on sectoral guidance from the Reserve Bank of India and the Securities and Exchange Board of India. United States writing addresses the 2023 executive order on AI and a patchwork of state-level statutes, such as those of Colorado and Illinois. Regulation-focused work has expanded rapidly since 2024 but remains lighter than ethics and governance writing on questions of liability, enforcement design, and judicial review.

Conceptual Framework Of Ai Governance

Governance in this context refers to the set of rules, institutions, and practices through which decisions about AI systems are made and enforced.⁸ It includes formal sources, such as legislation, regulations, and case law, and informal sources, such as standards, codes of conduct, and organizational policies. Governance is broader than regulation. Regulation is one instrument of governance, applied through binding rules issued by a public authority. Governance also includes self-regulation, co-regulation, technical standards, and procurement requirements.⁹ The OECD describes AI governance as the structures and processes that ensure AI systems align with public values and rights, including transparency, accountability, and respect for human oversight.¹⁰

Law plays a specific role within this structure.

8 Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: a systematic literature review. *AI and Ethics*, 5(3), 3265-3279.

9 McGuinness, M., Wallace, A., Dollery, B., & Kortt, M. (2025). Regulatory dark matter: How unofficial rules shape policy outcomes in the Australian regulatory environment. *Australian Journal of Public Administration*.

10 Lund, B., Orhan, Z., Mannuru, N. R., Bevara, R. V. K., Porter, B., Vinaih, M. K., & Bhaskara, P. (2025). Standards, frameworks, and legislation for artificial intelligence (AI) transparency. *AI and Ethics*, 5(4), 3639-3655.

It provides the binding rules that shape rights and duties, the institutional arrangements for oversight, and the remedies available when harm occurs.¹¹ Law also sets the conditions under which softer instruments, including standards and codes, become enforceable. In the AI context, law operates at three levels. The first is general law, including constitutional protections, data protection statutes, anti-discrimination law, consumer protection law, and tort or civil liability rules. The second is sectoral law, covering financial services, healthcare, employment, transport, and law enforcement. The third is dedicated to AI law, of which the European Union AI Act is the leading example.

Regulation is needed for four reasons. First, AI systems can produce decisions with legal effect, including denial of credit, refusal of welfare benefits, surveillance, and removal of online content.¹² These decisions need to be subject to lawful authority, due process, and effective remedies. Second, AI systems carry risks that are not equally borne. Errors and bias often fall on already disadvantaged groups, including minorities, women, migrants, and people with disabilities. Regulation is needed to allocate these risks fairly and to require systematic testing and mitigation. Third, AI systems involve complex supply chains that include data providers, model developers, deployers, and users.¹³ Without clear rules, responsibility moves along the chain in ways that leave affected persons without an addressable counterparty. Fourth, the technology has cross-border effects. A model trained in one

11 Al-Dulaimi, A. O. M., & Mohammed, M. A. A. W. (2025). Legal responsibility for errors caused by artificial intelligence (AI) in the public sector. *International Journal of Law and Management*.

12 Omotoso, O. (2025). Financial Exclusion in Modern Banking: A Legal Analysis of Accountability and the Right to Explanation in AI-Driven Decision Systems. *Available at SSRN 5743224*.

13 Handa, R. (2025). Securing the Intelligent Software Supply Chain: Vulnerability Detection and Exploit Pathways in AI-Integrated Systems. *Journal of Computational Analysis & Applications*, 34(12).



jurisdiction can be deployed in many others. Regulation is needed to enable interoperability, mutual recognition, and consistent enforcement.¹⁴ Three regulatory design choices shape the field. The first is the unit of regulation. Some frameworks regulate AI systems directly, by classifying them according to risk and imposing obligations on providers and deployers. Others regulate the underlying activities, such as automated decision-making affecting individuals, regardless of the technology used.¹⁵ The European Union AI Act primarily regulates systems by risk class. The General Data Protection Regulation regulates the activity of automated decision-making.¹⁶ The second design choice is between prescriptive and outcome-based rules. Prescriptive rules set specific technical or procedural requirements, including documentation, logging, and human review. Outcome-based rules require the controller to achieve a defined result, such as non-discrimination or accuracy, and leave the means to the regulated entity.¹⁷ The third design choice is the institutional architecture. Some jurisdictions create dedicated AI authorities. Others rely on existing regulators to apply general rules to AI use within their sector. India largely follows the second model.¹⁸

LEGAL AND REGULATORY DEVELOPMENTS

The legal picture in 2026 shows three distinct paths. The European Union is rolling out a binding, comprehensive statute. The United States has shifted toward federal preemption and lighter rules. India is using guidelines built on existing laws, with a soft-law preference. The differences are significant for any company operating across borders.

European Union

The European Union AI Act, formally Regulation (EU) 2024/1689, entered into force on 1 August 2024. It is the first comprehensive AI statute in any major jurisdiction.¹⁹ Prohibitions on certain practices and AI literacy obligations applied from 2 February 2025. Rules for general-purpose AI models and the governance structure became applicable on 2 August 2025. Most remaining provisions are set to apply from 2 August 2026, including the bulk of high-risk system obligations and the transparency rules in Article 50.²⁰

In November 2025, the European Commission proposed a Digital Omnibus on AI to simplify implementation. As of April 2026, trilogue negotiations between the Commission, Council, and Parliament were ongoing.²¹ The high-risk category covers AI systems used in biometrics, critical infrastructure, education, employment, essential public and private services, law enforcement, migration and border control, and the administration of justice. Conformity assessments, EU declarations of conformity, and CE marking apply before placing on the market. Registration in the EU database is also

19 European Commission. (2024, August 1). *AI Act enters into force*. https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en

20 Future of Life Institute. (n.d.). *EU Artificial Intelligence Act: Deadlines & implementation timeline*. <https://www.artificial-intelligence-act.com/>

21 European Parliamentary Research Service. (2026, March). *Digital omnibus on AI* (Briefing No. PE 782.651). European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2026\)782651](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2026)782651)

14 Khan, M. N. I. (2025). Cross-border data privacy and legal support: a systematic review of international compliance standards and cyber law practices.

15 Kumari, P. (2025). Legal Frameworks for AI Regulation: A Comparative Study. *Advances in Consumer Research*, 2(2).

16 Mouggiakou, E., Papadimitriou, S., Chrysafiadi, K., & Virvou, M. (2025). Artificial intelligence in educational games and consent under general data protection regulation. *Intelligent Decision Technologies*, 19(2), 670-686.

17 Markova, V. (2025). Toward Fair and Interpretable AI: A Regulation-Aware Framework for Detecting Bias and Mitigating Unfairness.

18 Dave, E., Mishra, R., & Yadav, A. (2025). AI Regulation and Governance: Comparative Analysis of Legal Frameworks Across Jurisdictions.

required.²² General-purpose AI rules form a separate track. Providers of general-purpose AI models must publish a summary of training content using a Commission template, comply with European Union copyright rules, and maintain technical documentation.²³ Providers of models presenting systemic risk face additional duties around model evaluation, risk mitigation, and incident reporting. The Code of Practice on general-purpose AI is the central operational document, developed through a multi-stakeholder process led by the AI Office.²⁴

United States

The United States approach has moved sharply since January 2025. President Trump signed Executive Order 14179 on 23 January 2025, revoking the prior administration's AI executive order.²⁵ America's AI Action Plan was released in July 2025, focused on speeding deployment and reducing rules. On 11 December 2025, the President signed Executive Order 14365, Ensuring a National Policy Framework for Artificial Intelligence.²⁶ The order directs the Attorney General to set up an AI Litigation Task Force to challenge state AI laws inconsistent with federal policy. It directs the Department of Commerce to evaluate state AI laws and to condition non-deployment Broadband Equity, Access, and Deployment funding on states either not enacting conflicting AI laws or agreeing not to enforce them. It directs the Federal Trade Commission to

issue a policy statement on preemption of state laws requiring alterations to truthful AI outputs. It directs the Federal Communications Commission to consider a federal reporting and disclosure standard for AI models. Sector-specific federal oversight remains active. The Equal Employment Opportunity Commission applies anti-discrimination rules to AI in hiring. The Federal Trade Commission applies consumer protection rules to deceptive AI claims. The Food and Drug Administration regulates AI in medical devices. There is no comprehensive federal AI statute on the model of the European Union AI Act.

India

India released the India AI Governance Guidelines on 5 November 2025, issued by the Ministry of Electronics and Information Technology under the IndiaAI Mission.²⁷ The document is a soft-law framework. It does not introduce a new AI statute. Instead, it works through existing laws, including the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, the Copyright Act 1957, and sector-specific regulations issued by bodies like the Reserve Bank of India and the Securities and Exchange Board of India. The framework rests on seven guiding principles, called sutras: trust as the foundation, people first, innovation over restraint, fairness and equity, accountability, understandable by design, and safety, resilience, and sustainability. Recommendations are organized across six pillars in three domains. The enablement domain covers infrastructure and capacity building. The regulation domain covers policy frameworks and risk mitigation. The oversight domain covers accountability and institutions. Two new bodies are central. The AI Governance Group is an inter-ministerial coordinator. The AI Safety Institute, working on a hub-and-spoke model, is to test AI systems, advise regulators, and develop standards. A Technical and Policy Expert Committee supports both bodies. The Reserve Bank of India released its own Framework for Responsible and Ethical Enablement of Artificial Intelligence in August 2025,

22 Delaney, H. (Ed.). (2008). *Guide to EU standards and conformity assessment*. DIANE Publishing.

23 Popa, A. Ş. (2025). COPYRIGHT PROTECTION IN THE CONTEXT OF THE PROVISION OF AI MODELS FOR GENERAL USE. *Challenges of the Knowledge Society*, 453-463.

24 Lim, E. C. N., & Lim, C. E. D. (2025). Polycentric AI Governance: A Multi-Stakeholder Approach to Distributed Responsibility and Ethical Technology Management. *International Journal of Advanced AI Applications*, 1(4), 77-97.

25 Gray, C. (2026). AI governance under the second Trump administration: implications for labour. *Global Political Economy*, 1-12.

26 Howell, J. R. Preemption: The White House AI Framework's Real Design.

27 Jain, M. A., & Thakur, M. K. About: White Paper Series Emerging Policy Priorities for India's AI Ecosystem.



with seven sutras and 26 recommendations across six pillars for the financial sector.²⁸ India's stance rests on the view of existing laws covering most AI risks today. Targeted legal amendments will follow if real gaps appear. This light-touch approach pairs with heavy investment in AI infrastructure, including more than 38,000 GPUs onboarded under the IndiaAI Mission and the AIKosh dataset platform.²⁹ The trade-off is between regulatory speed and innovation room. India has chosen room. The first major test will come as the AI Safety Institute begins operations and as sectoral regulators issue domain-specific rules.³⁰

The phased action plan has short, medium, and long-term elements. Short-term priorities include setting up the AI Governance Group and Technical and Policy Expert Committee, developing India-specific risk frameworks, conducting regulatory gap analyses, and promoting voluntary industry commitments.³¹ Medium-term priorities include piloting regulatory sandboxes for testing AI under supervision, and resourcing the AI Safety Institute for safety testing and standards.³² Long-term

priorities include continuous horizon scanning, an AI Incidents Database, and consideration of targeted legal amendments where soft law is not enough.³³ India's approach also draws on its Digital Public Infrastructure model. State-backed datasets, open compute access, and identity infrastructure are used as enablers for responsible AI practice. The Data Empowerment and Protection Architecture for AI Training is one example, aimed at giving people control over how their data is used in model training. The combination of soft-law guidelines, sectoral regulation, and public infrastructure is distinct from both the European Union and the United States approaches.

KEY CHALLENGES IN AI REGULATION

Four challenges recur across the literature and across legal systems. They are accountability, bias, data governance, and regulatory gaps. Each is examined in turn.

Accountability

The accountability challenge concerns the allocation of legal responsibility for outcomes produced by AI systems.³⁴ AI development and deployment involve multiple actors. Data is collected by one entity, used to train a model by another, integrated into a product by a third, deployed in a service by a fourth, and used by an end-customer who interacts with the output. When harm occurs, including financial loss, discrimination, defamation, or physical injury, it is often unclear which actor is liable, on what doctrinal basis, and to what extent. The literature describes this as the responsibility gap. Existing tort and contract doctrines fit poorly with systems whose behaviour emerges from

28 Sundar, A. (2026). Governing Compounding Risk: The Case for a Simultaneity-Aware Architecture for Resilience, Oversight and Accountability in AI-Driven Financial Services. *Oversight and Accountability in AI-Driven Financial Services* (March 14, 2026).

29 Jain, M. A., & Thakur, M. K. About: White Paper Series Emerging Policy Priorities for India's AI Ecosystem.

30 Arora, S., Chavali, D., & Reddy, N. S. (2025). Innovating Responsibly: AI Regulation, Sustainable Developments and Challenges. *International Journal on Advanced Computer Theory and Engineering*, 14(1), 1-11.

31 Garg, M., & Lanka, S. N. (2025). Automating the State: Public Sector AI in India and the Challenge of Rights-Based Regulation. *Indian Journal of Law and Technology*, 21(1), 5.

32 Joshi, S. (2026). A Comprehensive National Framework for Federal AI Adoption: Governance, Standards, and Implementation Pathways for Agentic and Generative Systems. *Standards, and Implementation Pathways for Agentic and Generative Systems* (February 01, 2026).

33 Ray, P. P. (2026). A Review of TRiSM Frameworks in Artificial Intelligence Systems: Fundamentals, Taxonomy, Use Cases, Key Challenges and Future Directions. *Expert Systems*, 43(3), e70213.

34 Biswas, B., & Sarkar, S. (2026). Responsible agentic artificial intelligence governance: Risk, safety, and ethical challenges in autonomous systems. *International Journal of Applied Resilience and Sustainability*, 2(2), 142-167.

data and is updated continuously. The European Union has addressed parts of this gap through the revised Product Liability Directive of 2024 and the proposed AI Liability Directive.³⁵ The Product Liability Directive treats software, including AI systems, as a product, allows defectiveness to be inferred from non-compliance with safety rules, and eases the evidentiary burden on claimants.³⁶ India has not undertaken comparable reform. Liability for AI harm in India falls back on the Consumer Protection Act, 2019, the Indian Contract Act, 1872, and general tort principles, none of which were designed for algorithmic systems.

Algorithmic Bias and Discrimination

Bias in AI systems arises from training data, model design, deployment context, and feedback loops.³⁷ Documented examples include credit scoring systems with disparate outcomes by gender or caste-correlated proxies, hiring tools that disadvantage women, predictive policing models that concentrate enforcement in already over-policed areas, and facial recognition systems with higher error rates for darker-skinned individuals. The legal challenge is twofold. The first is detection. Discrimination produced by AI systems is often statistical and indirect, and is difficult to identify without access to the model, the training data, and the outcome data.³⁸ The second is a remedy. Anti-discrimination law in most jurisdictions, including

India, has been built around individual claims and direct evidence. It is not well-suited to claims based on patterns of automated outputs across thousands of decisions.³⁹ The European Union AI Act addresses bias through the data governance requirements for high-risk systems, including representativeness, accuracy, and the testing of training data.⁴⁰ India's anti-discrimination framework, anchored in Articles 14, 15, and 16 of the Constitution and in sector-specific rules, has not yet been adapted to algorithmic decision-making.⁴¹

Data Governance

AI systems depend on data, and data governance, therefore, sits at the centre of AI regulation.⁴² The challenges include lawful basis for processing, purpose limitation in a context where models are reused across applications, data minimization in the face of incentives to collect at scale, the handling of special categories of data, the rights of data subjects to access and explanation, and cross-border transfers. The European Union addresses these issues through the General Data Protection Regulation, the Data Act, the Data Governance Act, and the AI Act.⁴³ India addresses them primarily through the Digital Personal Data Protection Act, 2023, supplemented by sectoral rules. Open issues

39 Johari, B. (2026). Dual erosion of equality and remedy in algorithmic decision systems. *Discover Artificial Intelligence*.

40 Niemiec, E., Davis, P. A., & Hauglid, M. K. (2026). Will the EU AI Act help to mitigate dataset bias in medical AI?. *Journal of Law and the Biosciences*, 13(2), Isag001.

41 Solanki, S., Sharma, K., Pandey, V. D., Kapila, M., Sinha, R., Singh, S., & Verma, V. (2026). AI Corporate Governance and Legal Accountability: Comparative Indian–International Frameworks. In *Legal Challenges of AI Across Interdisciplinary Sectors* (pp. 1-42). IGI Global Scientific Publishing.

42 Qiu, Y., & Hu, Z. (2026). Construction of a Theoretical Framework for Scientific Data Governance. *Scientific Data*.

43 Ledendal, J. (2026). AI Data Governance: Overlaps Between the AI Act and the GDPR. *Law, Innovation and Technology*.

35 Mutlu İpek, B., & Akıncı, E. (2026). WHO is responsible? Towards the normativity of AI-driven BCI technologies in product liability in healthcare. *AI & SOCIETY*, 1-22.

36 Nguyen, S. T. (2026). The applicability of product liability to artificial intelligence systems. *The Sydney Law Review*, 48, 1-32.

37 Lazaros, K., Vrahatis, A. G., & Kotsiantis, S. (2026). Human-in-the-Loop Artificial Intelligence: A Systematic Review of Concepts, Methods, and Applications. *Entropy*, 28(4), 377.

38 Park, K., & Yang, J. (2026). Attributional Ambiguity in AI-Mediated Harm: How Perceived AI System Limitations Shape Forgiveness and Regulatory Demand. *Journal of Broadcasting & Electronic Media*, 1-29.



include the status of synthetic data, the lawful basis for training on publicly available content, the treatment of inferences as personal data, and the obligations associated with model outputs that reveal information about identifiable individuals. The Indian framework requires further development on each of these points, including detailed rules under the DPDP Act and clarification on the scope of consent and legitimate uses.⁴⁴

Regulatory Gaps and Fragmentation

The fourth challenge is the fragmentation of regulation across jurisdictions and sectors. AI systems are global, but rules are national or regional. A model developed in the United States, trained on data drawn from many countries, and deployed in India is subject to overlapping legal regimes.⁴⁵ Fragmentation produces three problems. The first is forum-shopping, where actors locate activities in jurisdictions with the lightest rules. The second is compliance cost, especially for small and mid-sized firms that cannot bear the burden of multiple regimes. The third is enforcement weakness, where regulators lack the technical capacity, jurisdictional reach, and information-sharing arrangements required to act on cross-border AI harms. Even within a single jurisdiction, sectoral fragmentation arises. In India, AI use in financial services is overseen by the Reserve Bank of India, in capital markets by the Securities and Exchange Board of India, in telecommunications by the Telecom Regulatory Authority of India, and in personal data processing by the Data Protection Board of India.⁴⁶ There is

no horizontal coordinating mechanism. The result is overlapping or inconsistent guidance, gaps in coverage for cross-sector use cases, and limited capacity to address systemic risks from foundation models.

CONCLUSION

Artificial intelligence governance has moved from policy discussion to legal regulation. The volume of scholarly output has risen sharply since 2022, with 945 publications in 2025 alone within Law and Legal Studies under the search terms used in this paper. The European Union has produced the first comprehensive statute. The United States has shifted toward federal pre-emption and lighter rules. India has chosen a soft-law route grounded in existing statutes. The OECD, UNESCO, and G20 provide reference points but no binding cross-border regime. Common ground exists across the three jurisdictions reviewed. All three rely on risk-based thinking. All three call for human oversight, transparency, and accountability. All three are building dedicated institutions, including AI offices and safety institutes. The differences lie in legal form. The European Union uses binding law with hard penalties. The United States favors executive action and sector-specific federal rules with limited state involvement. India favors guidelines built on existing laws. Gaps remain. Generative AI continues to outrun rules drafted for earlier systems. Cross-border enforcement is unproven. Audit practices are immature. Bias mitigation tools work in narrow settings but not as a general solution. Regulators face capacity limits. Coverage of low and middle-income countries in research and standards-setting bodies is thin. Future work should focus on four directions. First, comparative empirical research on enforcement, including how often penalties are issued, which actors are sanctioned, and what changes in industry behaviour follow. Second, technical standards for AI audits, including independence, qualification, and method. Third, governance models for general-purpose AI and frontier systems, including pre-deployment evaluation regimes. Fourth, inclusion of voices from

44 Hanspal, M. S. (2026). Artificial intelligence governance and legal regulation: Emerging trends and challenges. *DME Journal of Law*, 7(1), xx-xx. <https://doi.org/10.53361/dmejl.v7i01.00>

45 Sharma, A. K., & Sharma, R. (2024). Comparative analysis of data protection laws and AI privacy risks in BRICS nations: A comprehensive examination. *Global Journal of Comparative Law*, 13(1), 56-85.

46 Yoganandham, G. (2025). Trends, Challenges, and Opportunities in India's Financial Sector: Policy Shifts, AI Integration, and Financial Stability—An Empirical Assessment. *GIS Science Journal*,

outside the Global North, both in research and in standards bodies. AI is not waiting. The aim of governance is not to stop the technology. The aim is to make sure that as AI scales, the benefits reach widely and the harms fall on no one in particular by accident. Closing the gap between deployment speed and regulatory maturity is the central task for the next phase of work.

