SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Artificial Intelligence, Governance, and Polity: A Comprehensive Literature Review

Ms. Simranpreet Kaur[1], Ms. Shivi[2], Dr. Pooja Puri[3], Ms. Gurinderjeet Kaur[4], Ms. Navjot Kaur[5]

[1]Assistant professor, Department of Management Studies, CKD Institute of Management and Technology, Tarn Taran, Punjab.
E-mail: Kaursimranpreetsach@gmail.com, Orcid: 0009-007-1855-5505
[2]Assistant professor, Department of Commerce, CKD Institute of management and technology, Tarn Taran, Punjab.
E-mail: shivikapila08@gmail.com.
[3]Professor, Management Studies, Centre for Research and Innovation (CRI), Amritsar Group of Colleges, Amritsar, Punjab (India).
E-mail: poojapuri251979@gmail.com
[4]Assistant professor, Department of Commerce, CKD Institute of management and technology, Tarn Taran, Punjab.
E-mail: gurindergindu8@gmail.com
[5]Assistant professor, Department of Hotel Management, CKD Institute of management and technology, Tarn Taran, Punjab.
E-mail: navjotkaur61992@gmail.com

ABSTRACT

Background: As public institutions embed Artificial Intelligence (AI) into administration, governing is shifting from conventional bureaucratic routines toward algorithm-driven decision systems. AI can enhance administrative effectiveness, support decision making and delivery of services, but also poses challenging questions around human rights, transparency, democratic accountability, and social fairness.

The review will consist of an overview of the multi-faceted landscape of AI governance, based on over 40 peer-reviewed studies and policy documents. It critically explores global regulatory approaches, the internal logic of policy design, barriers to implementation, standards for good regulation, policy use in public services and broader political-economic implications.

Key Findings:

Divergent regulation: Models differ significantly between jurisdictions from the EU's rights-based, tiered approach (EU AI Act/GDPR), to a piecemeal, sectoral model in the United States, a state-led programme in China, to a patchy style of regulation that is still developing in Asia-Pacific and Global South.

Weak structural integration: The challenge is not the absence of policy content, rather, the lack of structural integration, as evidenced by the lack of balance in the temporal planning horizon, coordination across government tiers and practical instruments of implementation.

Practical application of ethics: Using explainability, algorithmic fairness, and human oversight requires good architectures for risk management (e.g. NIST AI RMF), ongoing bias audits, privacy-preserving techniques like federated learning, and mechanisms to prevent regulatory capture.

While AI development is set to become a public-domain change, with three generations of automation, personalisation and prediction, if it is not designed and implemented inclusively with citizen involvement, it will create new digital divides and administrative opacity.

Implications: Polycentric governance arrangements involving multiple stakeholders are required to realize effective governance of AI. Future policy should focus on developing institutional capacity, on creating coherence across policy levels and on creating safeguards for vulnerable groups based on evidence, in such a way that AI deployment is compliant with democratic values, public values and human dignity.

Keywords: Artificial Intelligence Governance, Algorithmic Polity, Public Sector Digital Transformation, Policy Structural Consistency, Ethical AI, AI Regulations.

1. Introduction And Landscape Of Ai Governance

Artificial intelligence fundamentally changed the world of public governance and global economic management in general; it is becoming a general-purpose technology that is reshaping state capacities and the way in which the economy is managed over a global scale. This development of AI into government processes represents a paradigm shift from traditional bureaucracy to algorithmic government, with unprecedented potential for improving administrative efficiency and challenging new ethical, legal and political issues.

The use of AI in public sector management is evident from differing approaches around the globe, with developed economies placing greater focus on ethical governance, transparency and human-centric values, while emerging economies tend to focus more on the upgrading of technology and industrial transformation (Zhang et al., 2026). This division of governance has resulted in a global environment with a wide variety of regulatory frameworks, institutional mechanisms, and the ways in which they are implemented (Dharmansyah et al., 2026), presenting vulnerable populations in less-regulated parts of the world with high governance risks.

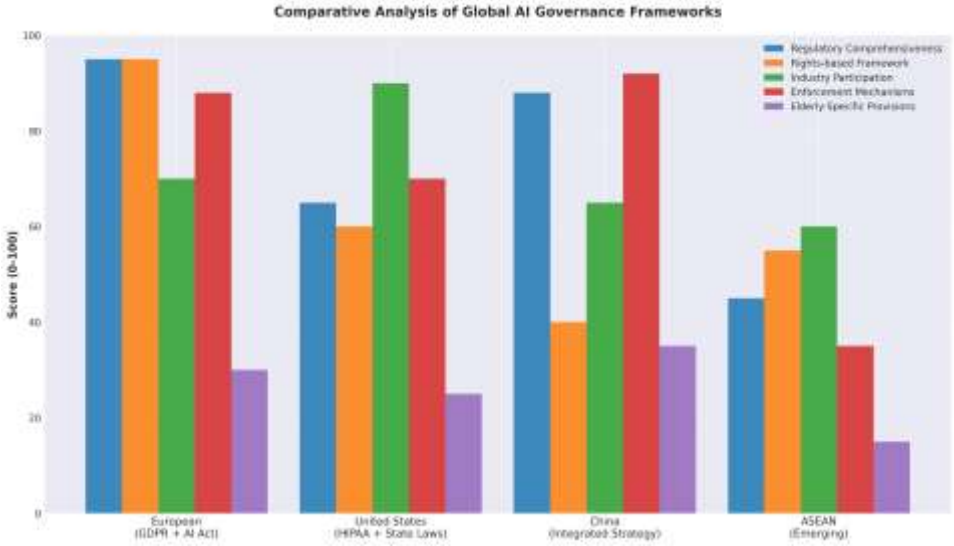

Figure 1: Comparative analysis based on regulatory frameworks documentation across EU GDPR/AI Act, US HIPAA/state laws, China's central-level policies, and ASEAN regulatory landscape (Dharmansyah et al., 2026), (Zhang et al., 2026)

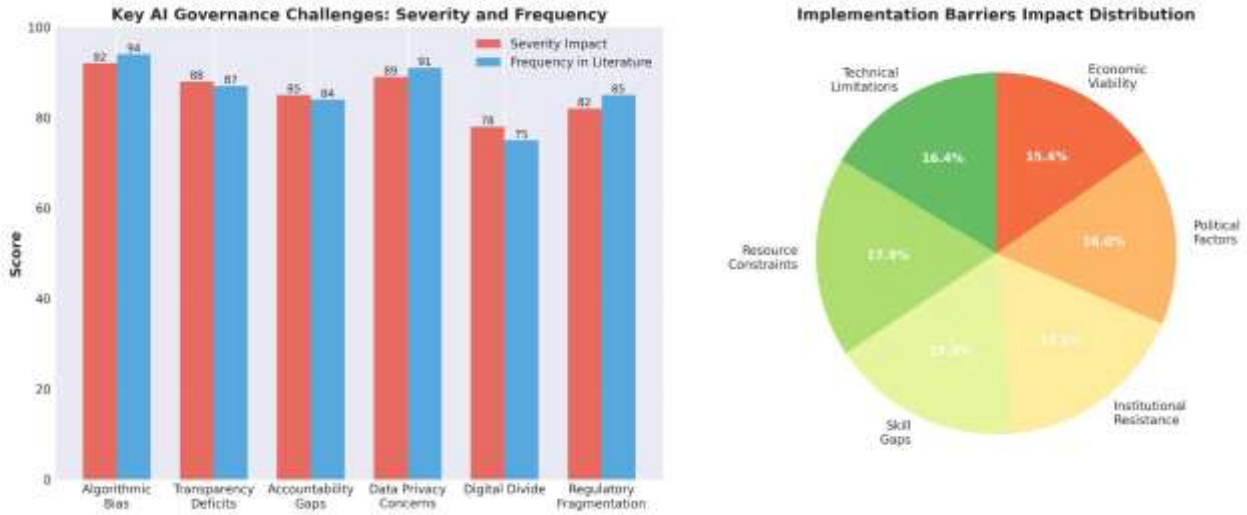

Figure 2: Challenge severity aggregated from peer-reviewed literature addressing algorithmic bias, transparency, accountability, privacy, digital divide, and fragmentation issues

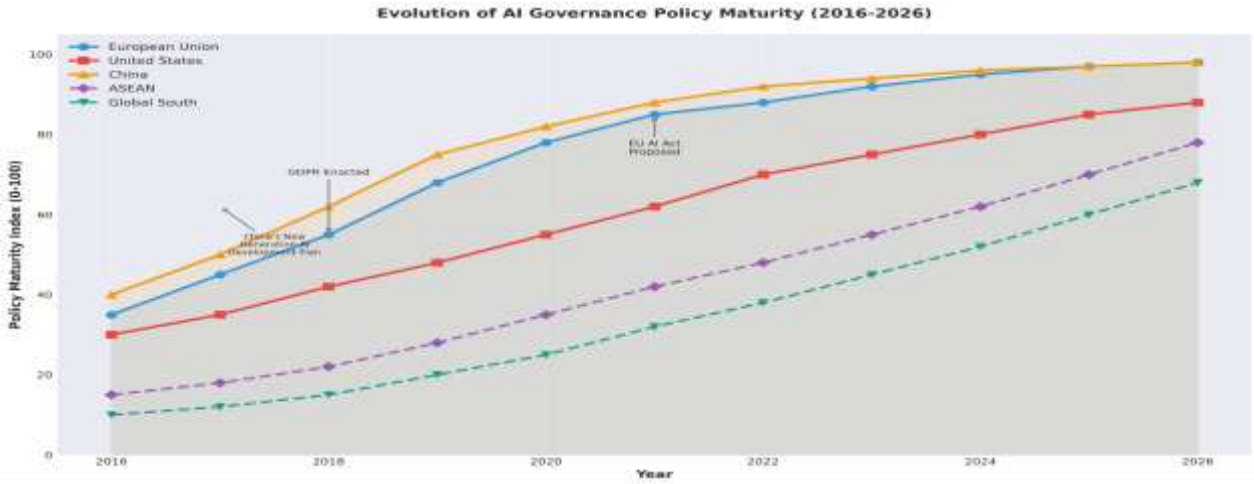

Figure 3: Policy maturity evolution tracking GDPR enactment (2018), EU AI Act proposal and implementation (2021-2024), China's New Generation AI Development Plan (2017), and ASEAN development trajectories

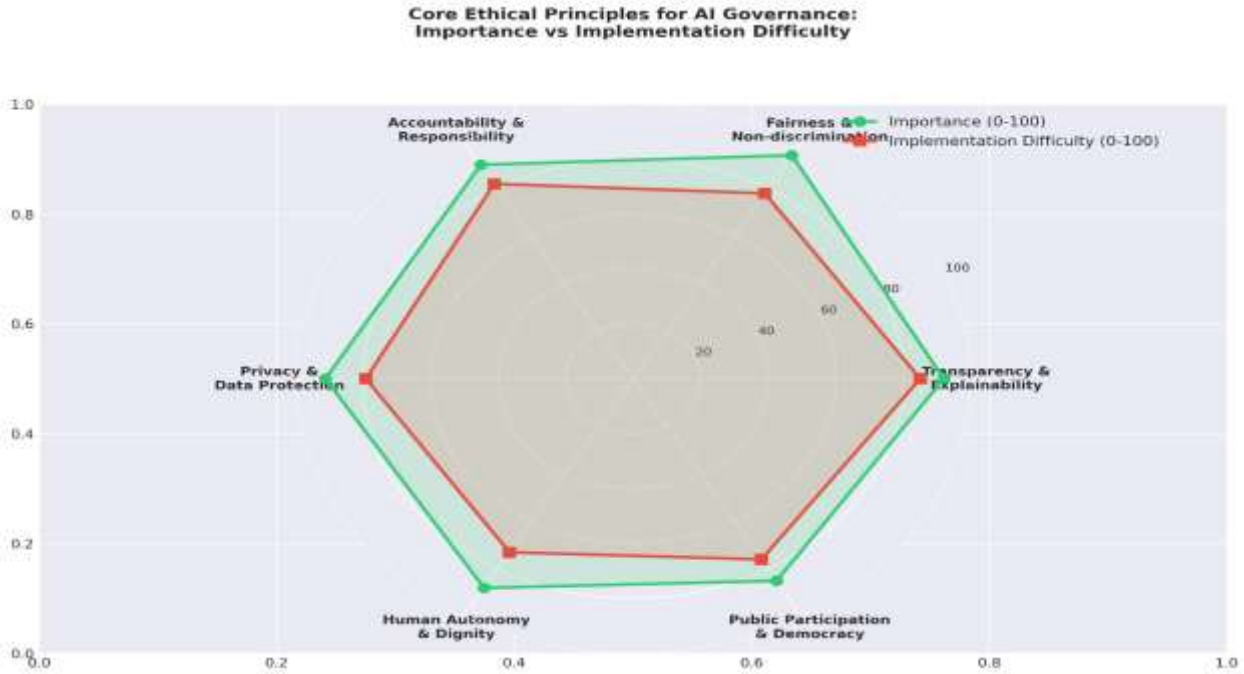

Figure 4: Ethical principles framework based on core principles identified across governance literature including transparency, fairness, accountability, privacy, autonomy, and democratic participation

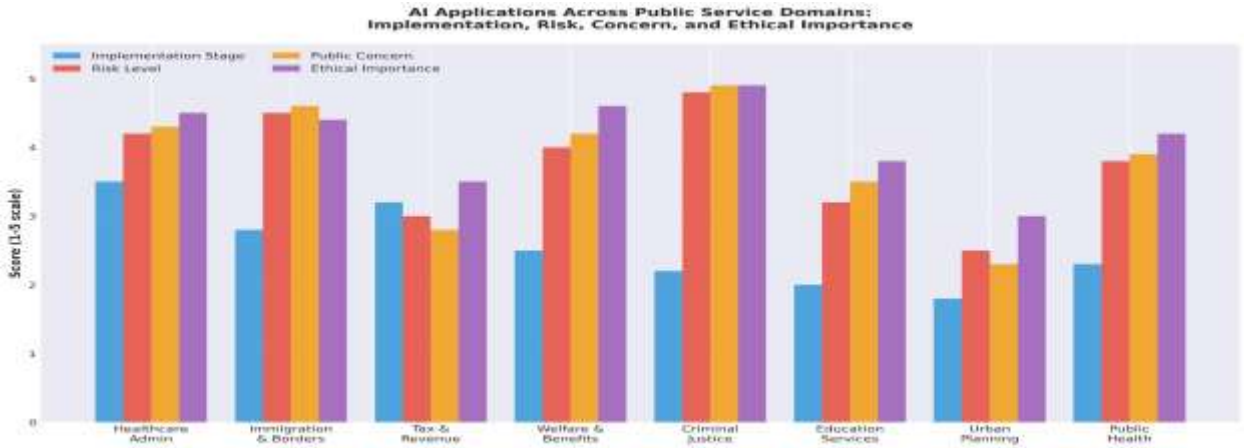

Figure 5: AI applications assessment across public service domains based on implementation stage, risk levels, public concern, and ethical importance ratings from domain-specific literature

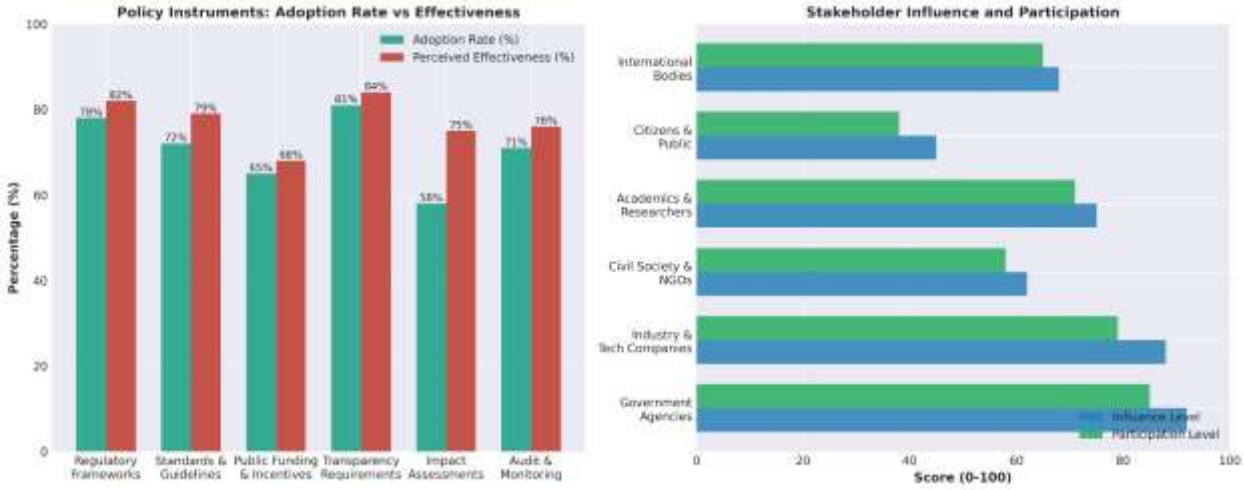

Figure 6: Policy instruments adoption and stakeholder engagement patterns synthesized from governance implementation studies and regulatory effectiveness assessments

While the issue of AI governance is present in each policy document, it is also present in the aggregation of key policy dimensions in concert (Zhang et al., 2026). This literature review aims to draw on more than 40 peer-reviewed research papers and policy documents to explore the multi-faceted nature of AI governance, the political implications of its use and the institutional frameworks needed for responsible public sector implementation.

2.GLOBAL AI GOVERNANCE FRAMEWORKS: COMPARATIVE ANALYSIS

2.1European Union: Rights-Based Regulatory Approach

The General Data Protection Regulation (GDPR) and the EU AI Act (Dharmansyah et al., 2026) are two regulations that have been integrated into the EU regulatory framework for AI related to the rights of individuals.The EU has developed the most comprehensive rights-based regulatory framework for the governance of AI through the integration of the General Data Protection Regulation (GDPR) and the EU AI Act (Dharmansyah et al., 2026). Under the GDPR, biometric and health information is considered a special category of personal data for which stricter guidelines for explicit consent, transparency, and strong user rights, such as access, correction, and deletion, apply, making it crucial to consider the implications for any AI system handling such data (Dharmansyah et al., 2026). The EU AI Act, which will go into effect in August 2024, will establish a risk-based classification that explicitly includes "AI systems intended for medical use" among those subject to third-party conformity assessment, data governance and record-keeping requirements, transparency and human oversight obligations (Dharmansyah et al., 2026).

This is a rights-based approach to governance which is rooted in protecting individual autonomy and dignity with democratic accountability (Fan, 2025). However, challenges to implementing the regulations in practice do exist, particularly for smaller companies where the process of conformity testing can be costly, and some wellness related applications remain in the high-risk applications (grey area) category (Dharmansyah et al., 2026).

2.2United States: Sectoral and Fragmented Approach

The United States regulatory environment is highly fragmented, meaning that regulatory governance is distributed among various regulatory agencies and jurisdictions (Dharmansyah et al., 2026). HIPAA regulations only apply to the care of health information by covered entities, and the FDA only has jurisdiction over devices that claim to be medical, leaving a regulatory void for wellness-oriented consumer wearable devices (Dharmansyah et al., 2026). The National Institute of Standards and

Technology (NIST) offers voluntary frameworks for managing AI risks that have no authority, and the Federal Trade Commission (FTC) deals with deceptive practices, though it does not have jurisdiction over healthcare.The National Institute of Standards and Technology (NIST) offers voluntary guidelines and frameworks for the management of AI risks without any enforcement authority, while the Federal Trade

Commission (FTC) has jurisdiction over deceptive practices but not over healthcare.

This sectoral perspective has fostered quick technology uptake and innovation in the industry, but it has also led to ongoing questions of data ownership, algorithmic accountability, and user rights (Dharmansyah et al., 2026). A fragmented patchwork of state privacy laws such as Colorado's regulations and California's Consumer Privacy Act complicates compliance for multistate businesses and results in inconsistent privacy protection from state to state.

2.3China: Integrated State-Led Strategy

China has taken a holistic, more integrated stance in AI governance, and has integrated AI into a growing part of national development plans (Zhang et al., 2026). The policies at the central level in the country from 2016-2025 illustrate both a drive to promote technological innovation and industrial upgrading, as well as a focus on setting up regulatory frameworks and implementation mechanisms (Zhang et al., 2026). However, the structural consistency analysis shows that the orientation of the Chinese AI policy system is relatively stable with a central theme of technological development, expanded application, and governance support (Zhang et al., 2026).

The Policy Modeling Consistency Index analysis further reveals that China's AI policy exhibits a sound strategic focus and field of application, but its temporal planning, intergovernmental coordination, and incentive design remain significant weak points (Zhang et al., 2026). The evidence of limited long-term policy supply, underdeveloped vertical coordination mechanisms and partially configured policy instruments across the main policy support dimensions shows that there is a need for policy improvement in the future, primarily in strengthening medium- and long-term policy planning and developing the vertical coordination mechanisms.

2.4Asia-Pacific and Global South: Nascent and Emerging Frameworks

The Asia-Pacific region has the most diverse regulatory environment (Dharmansyah et al., 2026), from an established environment, such as Singapore and Japan, to an emerging one, such as Malaysia and Indonesia. The Personal Data Protection Act (Singapore) is the most advanced framework and incorporated the principles of healthcare-specific guidelines, and active compliance audits, while Personal

Data Protection Law (Indonesia) classified health data as sensitive personal data but faced implementation

challenges (Dharmansyah et al., 2026). Despite the progress ASEAN has made in enacting personal data protection laws, there are still significant differences in scope, what information is considered sensitive, and the conditions of transfer of it across borders, with laws specifically for IoT still not existing for several Asian countries (Dharmansyah et al., 2026).

In addition, regulatory diverges and differences pose major compliance issues for global wearable device manufacturers, as devices sold across jurisdictions are subject to fundamentally different consent models, data processing rules, and enforcement regimes (Dharmansyah et al., 2026). This disintegration results in differential protection levels, with users in less regulated jurisdictions being much more exposed to governance risks.

3.STRUCTURAL CONSISTENCY AND POLICY IMPLEMENTATION CHALLENGES

3.1Coherence in Policy Architecture

One of the most significant insights from recent policy studies on AI is that the primary governance challenge is not just about the lack of policy content but also about the varying structural embeddings of policy time horizons, governance hierarchy, and implementation linkage (Zhang et al., 2026). A significant number of national AI strategies highlight the strategic vision and policy engagement on the discursive level, but fail to show structural balance in the design of support tools and the design of governance influence (Zhang et al., 2026).

The structural analysis of AI policies shows that policies have not been supported equally on various dimensions, and inter-policy transmission of policy influence is still structurally uneven, spanning inter-national, inter-regional, inter-industrial and inter-enterprise layers (Zhang et al., 2026). This means that policy coherence cannot be realized with just a single policy document, it needs to encompass several aspects of policy, such as policy nature, policy timeliness, policy content, policy incentive arrangements, target groups of policy, and levels of policy influence.

3.2Implementation Barriers and Gaps

The analysis of the challenges to implementation shows that AI governance is not just about policy declarations but also about the institutional coherence and operational feasibility of policy systems (Zhang et al., 2026). Research indicates that while AI practitioners tend to have a functional view of AI, policymakers are more likely to think of AI in anthropomorphic terms, which can cause a disconnect between the perception of AI in policy and its actual use, with the focus often being on future visions rather than on the systems currently in place (Zhang et al., 2026).

Ambiguous concepts, lack of implementation details, limited evaluation mechanisms, accountability and transparency challenges, risk management shortcomings and unclear institutional roles and responsibilities are key implementation barriers (Zhang et al., 2026). When it comes to AI adoption, these constraints are especially acute in emerging and developing areas, where access to technological infrastructure, the lack of specialized expertise, and a shortage of financial resources can impede the growth and use of AI.

3.3Regulatory Capture and Industry Influence

One of the big governance issues is the role of actors in the AI industry and their strong influence in the regulatory discussion, especially in developed markets (Wei et al., 2024). Although participation of industry is critical to the policy process, it can lead to regulatory capture, where industry undermines the public good by capturing the regulatory system to favour private over public interest. The AI policy experts identified five main pathways by which industry can influence policy, with concerns over
'capture' (strong policy goals that outweigh others or that are weak) and 'information management' (information that is managed by industry) being most prevalent (Wei et al., 2024).

4.ETHICAL GOVERNANCE FRAMEWORKS AND RESPONSIBLE AI

4.1Core Ethical Principles for AI in Government

To ensure the applications are in line with fundamental democratic values, emerging issues related to algorithmic governance need to be addressed in the application of AI technologies in governmental functions (Fan, 2025). Ethical principles that underpin responsible governance of AI encompass transparency and explainability, fairness and non-discrimination, accountability and responsibility, privacy and data protection, human autonomy and human dignity, and public participation and democratic legitimacy (Fan, 2025).

Transparency and explainability solve the "black box" problem of algorithmic governance, where citizens or individuals that are impacted by machine decisions have very limited capacity to challenge decisions that are opaque or exist beyond their comprehension (Fan, 2025). In the example of AI Welfare Qualification Review System in Germany, 83 percent of applicants who were rejected were not able to understand why they were rejected, which resulted in an increase in administrative lawsuits by 300 percent (Fan, 2025). In governmental settings, explainable AI (XAI) is also a technical solution that can help address transparency issues and create methods to explain how algorithmic systems work, but implementing XAI requires considerations of how transparent a system is, given the nature of the decision at stake and the complexity of the model.

Algorithmic bias is one of the most ethically significant issues with government use of AI technologies (Fan,

2025). There are four basic sources of bias, which are related to the scope of the data, the algorithm itself, the context in which it's used, and any dysfunction of the supervisory control system (Fan, 2025). They are synthesized to form a general picture of outcome bias in terms of outcome allocation bias, outcome representational bias, and service level outcome bias (Fan, 2025).
A specific concern with historical data bias is that AI systems trained with historical government data can further reinforce or exacerbate existing discriminatory practices in government systems (Fan, 2025).
Mitigation calls for explicit testing for biases and inequitable recommendations, such as reporting performance by subgroups, language-access evaluation, and prohibiting race-based medicine heuristics unless they are explicitly evidence-based and up-to-date (Khanna, 2026).
There will need to be operational controls that will translate ethical principles into action in order to ensure responsible deployment of AI systems (Khanna, 2026). The NIST Artificial Intelligence Risk Management Framework offers a structure that focuses on governance, identifying risks, tracking progress, and risk management throughout the lifecycle, including accountability and ongoing monitoring (Khanna, 2026). Governance should include multidisciplinary teams such as clinicians, informatics specialists, legal/compliance officers, privacy experts, cybersecurity professionals and patient representatives, and have outcomes like acceptable-use policies, risk-tier frameworks, vendor due diligence standards, and incident response procedures (Khanna, 2026).
Human oversight needs to be put in place with interface design that allows for simple and easy review, identifies points of uncertainty, provides a structured review of contraindications, and does not create false confidence (Khanna, 2026). Federated learning and differential privacy can be used to adhere to privacy-preserving analytics, and least-privilege tool access, prompt injection testing, and input/output filtering are possible solutions for securing against adversarial attacks (Khanna, 2026).

4.2Algorithmic Bias and Fairness Concerns

Algorithmic bias is one of the most ethically significant issues with government use of AI technologies (Fan, 2025). There are four basic sources of bias, which are related to the scope of the data, the algorithm itself, the context in which it's used, and any dysfunction of the supervisory control system (Fan, 2025). They are synthesized to form a general picture of outcome bias in terms of outcome allocation bias, outcome representational bias, and service level outcome bias (Fan, 2025).
A specific concern with historical data bias is that AI systems trained with historical government data can further reinforce or exacerbate existing discriminatory practices in government systems (Fan, 2025). Mitigation calls for explicit testing for biases and inequitable recommendations, such as reporting performance by subgroups, language-access evaluation, and prohibiting race-based medicine heuristics unless they are explicitly evidence-based and up-to-date (Khanna, 2026).

4.3Responsible Deployment Framework

There will need to be operational controls that will translate ethical principles into action in order to ensure responsible deployment of AI systems (Khanna, 2026). The NIST Artificial Intelligence Risk Management Framework offers a structure that focuses on governance, identifying risks, tracking progress, and risk management throughout the lifecycle, including accountability and ongoing monitoring (Khanna, 2026). Governance should include multidisciplinary teams such as clinicians, informatics specialists, legal/compliance officers, privacy experts, cybersecurity professionals and patient representatives, and have outcomes like acceptable-use policies, risk-tier frameworks, vendor due diligence standards, and incident response procedures (Khanna, 2026).
Human oversight needs to be put in place with interface design that allows for simple and easy review, identifies points of uncertainty, provides a structured review of contraindications, and does not create false confidence (Khanna, 2026). Federated learning and differential privacy can be used to adhere to privacy-preserving analytics, and least-privilege tool access, prompt injection testing, and input/output filtering are possible solutions for securing against adversarial attacks (Khanna, 2026).

5.AI APPLICATIONS IN PUBLIC SERVICE DOMAINS

5.1Government Digital Transformation and Service Delivery

AI's infusion into government services shifts the dynamics between the government and citizens, moving beyond mere digitization to systems that are responsive, personalized, proactive, and resource-efficient (Fan, 2025). The applications of AI in the government can be divided into three different stages: First Generation – Intelligent Services for automation of routine clerical tasks using digital interfaces; Second Generation – Intelligent Services for personalisation, based on data and machine learning, to provide profile-specific services; Third Generation – Intelligent Public Services, where AI anticipates citizens' needs before they even express them (Fan, 2025).
AI has a variety of applications within the healthcare sector, the tax system, administration of welfare benefits, immigration, and the criminal justice system, each with its own set of opportunities and challenges (Fan, 2025). The sectors dealing with healthcare and transportation have reached relatively higher stages of

implementation while sectors dealing with education and social services are in earlier stages of development. While all the benefits are good, each one comes with its own set of technical, ethical and organizational issues (Fan, 2025).

5.2Intelligent Decision Support Systems

Government digital transformation is a crucial advancement that brings together AI and conventional decision support systems (DSSs) to assist decision-makers in enhancing the quality of their outcomes.One of the most significant developments in the realm of government digital transformation is the Intelligent Decision Support Systems (IDSS), which integrates AI capabilities with traditional DSSs to improve the effectiveness of decision-making (Fan, 2025). Unlike traditional IDSS that are mainly based on structured data and predefined models, a modern IDSS can be used to handle a wide range of data, learn from past decisions, adapt to new situations, and offer advanced recommendations (Fan, 2025).

Governance challenges for IDSS in government include integration with legacy systems, data privacy policies and inter-departmental silos (Fan, 2025). Administrators need to grasp the rationale behind their decisions, which AI systems need to provide, and how, but their responsibility also involves bounded innovation and accountability within a broader governance framework (Fan, 2025).

5.3Public Participation and Transparency Enhancement

AI technologies have the potential to enhance government transparency, expand public engagement and effectively address information needs (Fan, 2025). A set of tools are available for automated report generation that enable real-time transparency in government information disclosures, improve timeliness, accuracy and completeness of information updates (Fan, 2025). Despite the aforementioned lack of reliability, governments can use sentiment analysis and opinion mining technologies to collect and analyze public sentiment and perception regarding issues on unprecedented scales and technologies can help facilitate rather than replace democratic discourse.

As seen in practical applications, AI can improve the participation process by making it possible for citizens to follow algorithmic processes in local government decision-making with interpretive feedback interfaces, and by using AI to identify consensus points in citizens' proposals and collaboratively constructing policies (Fan, 2025). A tool developed in Finland, named "AI Assistant for Public Consultation," enables the active retrieval of feedback from political documents, thus making it possible to participate in the consultation process for a wider population.

6.CONTEMPORARY POLICY ISSUES AND POLITICAL DIMENSIONS

6.1Data Governance and Sovereignty

Data collection and management are integral to all AI technologies, and accuracy, timeliness, completeness, and consistency are important data quality issues that can affect the outcomes of AI. In the context of AI governance in India, policymers have addressed various aspects of AI production, including provisioning public infrastructure, to stimulate market-driven production of AI, and the nationalisation of data, to facilitate the use of Big Data in AI. This is a general trend of conflicts between data sovereignty issues and open data ecosystems .

The policy of AI has been seen to reinforce a world hegemonic paradigm of informational capitalism; in which the construction of data as a productive resource for information-based economic production is both a precondition and a legitimization of the harmful effects of the AI system, which are to be self-regulated by the AI system itself. Governments try to understand the nature of AI markets through legislation and investment in infrastructure to have good hands in control and to encourage private sector innovation.

6.2Democratic Accountability and Public Value

In the governance aspect, AI ethics should prioritize human welfare, dignity, and autonomy over efficiency, and technologization is not the main concern of public services (Fan, 2025). These principles should counteract deep-rooted inequalities in government-citizen relations that algorithmic governance can reinforce, deepen or weaken depending on the design of the system and its use (Fan, 2025).

Ongoing problems with democratic accountability stem from the lack of responsibility clarity concerning multiple actors involved in algorithmic processes, without clear accountability structures (Fan, 2025). Without adequate oversight, due to poor audit checks and flawed feedback loops, there are opportunities for bias to accumulate over time, which necessitates ongoing bias maintenance and bias rectification from the design stage onwards (Fan, 2025).

6.3Digital Divide and Social Inclusion

The use of AI technologies by government raises important questions concerning digital inequalities and social inclusion (Fan, 2025). The use of automated systems in government services, fueled by AI, could further reinforce socioeconomic inequalities that may be caused by disparities in distribution and access to technologies, such as disparities in social competencies, availability of relevant technologies, and algorithmic representation bias (Fan, 2025).

Individuals who are at the bottom of social hierarchy experience further obstacles in accessing the government services, such as older people, Language Minority populations, Persons with disabilities, and the economically disadvantaged (Fan, 2025). A broad approach is needed to enhance access for everyone, in different ways of accessing systems, at various levels of digital literacy, and by focusing on community-based gatekeepers (Fan, 2025). Social equity concerning technology must integrate into the administrative justice paradigm, as governance upholds democratic legitimacy of contemporary politics (Fan, 2025)

7.RESPONSIBLE AI GOVERNANCE FRAMEWORK AND IMPLEMENTATION

7.1Structural Elements of Responsible Governance

Responsible AI governance covers structural, relational and procedural practices throughout the AI lifecycle as they become part of the organizational decision-making process. We find different precursors of responsible governance identified in literature: organizational commitment to ethical principles, stakeholder engagement mechanisms and institutional capacity for oversight. Benefits of good governance include higher legitimacy of the organization, trust from stakeholders and better match between technical implementation and societal values.

Embedding ethics within institutional settings, in the technical process of AI development and in internal processes and decision making frameworks, is key to the institutionalization of responsible AI governance and is central to the conceptual framework. This means transcending from principle-based to concrete measures with policies, processes and accountability mechanisms.

7.2Multi-Stakeholder Collaborative Governance

The key to good AI governance in the public sector is cross-sectoral collaboration, involving government, technologists, civil society groups, academics and citizen representatives (Fan, 2025). To ensure broad oversight and to avoid regulatory capture, polycentric governance structures should be used, in which local ethics review bodies as well as national specialized technical bodies and other interested parties can play a role. (Fan, 2025)

The use of contracting processes and procurement requirements can help progress ethical AI governance by ensuring transparency, fairness, and privacy commitments before entering into relationships with public administration systems (Fan, 2025). These structures should include differentiated supervision in accordance with the risk level assessments, and most severe measures for those with higher risk to fundamental rights or key resources applications (Fan, 2025).

7.3Institutional Arrangements for Accountability

The collective and individual approaches of actors in AI governance should be integrated into comprehensive frameworks for clear allocation of responsibilities across actors in AI governance (Fan, 2025). Effective mechanisms for the establishment of responsibility should be put in place before deployment, clear standards and control processes should be set, algorithmic impact assessments should be carried out in advance, and multi-stage tests should be performed (Fan, 2025).

Institutions are to be given permission for continuous monitoring, audit trail, validation, operational control, time bound review systems, significant powers of the controller, and responsibility for system failures (Fan, 2025). The legal and regulatory environment should support the use of public sector AI applications in various settings, while introducing a benchmark for assessing the impact of algorithms, robust and powerful bodies of review and clear mechanisms for accountability (Fan, 2025).

8.CRITICAL GAPS AND FUTURE DIRECTIONS

8.1Knowledge and Research Gaps

Despite the escalating scholarly interest in AI governance, profound research deficiencies persist within the existing literature. Significant limitations remain regarding the empirical validation of ethical framework efficacy and the operational translation of high-level principles into tangible governance mechanisms. Furthermore, there is a distinct scarcity of longitudinal evidence concerning the socio-political impacts of implementation across diverse jurisdictional landscapes. A critical omission in contemporary regulatory regimes involves the absence of specialized provisions tailored to the unique vulnerabilities of elderly populations, representing a substantial protection gap
(Dharmansyah et al., 2026).

Current discourse has predominantly emphasized thematic mining, instrument typologies, and isolated policy effectiveness, while largely neglecting the structural consistency and internal coordination requisite for holistic policy systems (Zhang et al., 2026). Rigorous quantitative analyses examining the coherence of policy architectures—spanning timeliness, content support, and inter-institutional synergy—remain notably underdeveloped in the current literature (Zhang et al., 2026).

8.2Implementation and Capacity Challenges

There are significant barriers to the implementation of governance frameworks. Technology infrastructure is

still underdeveloped, and specialized skills are rare in Global South countries, as are financial resources to support development of AI. Lack of comprehensive national AI policies can expose these countries to unregulated imports of AI technologies, posing concerns regarding data sovereignty and privacy.
To build institutional capacity for responsible AI governance, technical capacity in government and civil society needs to be built, a new autonomous funding mechanism should be provided, transparency and ethics requirements must be strengthened, more scope for civil society participation in policy-making, and procedural safeguards must be put in place (Wei et al., 2024). Capacity building should be tailored to varied political-economic and institutional environments and levels of development in jurisdictions.

8.3Future Research Priorities

There are several opportunities for further research, such as: empirical testing of integrative governance frameworks in varying regulatory and cultural environments; longitudinal studies of the effects of governance intervention on outcomes and trust; governance provision development of AI-specific provisions for vulnerable populations in ASEAN and Global South jurisdictions; research on new technologies for privacy in resource-constrained environments, and; co-design studies that involve affected populations in the governance mechanism.Some opportunities for further research include: empirical testing of integrative governance frameworks in varying regulatory and cultural environments; longitudinal studies of the effects of governance intervention on outcomes and trust; governance provision development of AI-specific provisions for vulnerable populations in ASEAN and Global South jurisdictions; research on new technologies for privacy in resource-constrained environments, and; co-design studies that involve affected populations in the governance mechanism.
Research is also needed to explore how governance frameworks evolve in response to the unprecedented speed of technology change, especially given the new risks and opportunities emerging from generative AI systems (Khanna, 2026). Studies are needed to consider governance technical, ethical and regulatory aspects together with person-centered governance aspects to show evidence bases for policy refinement (Tornimbene et al., 2026).

9.Conclusion

The governance of AI is a policy challenge that is unique to our times and has to be coordinated along technical, ethical, legal and political lines. The evidence shows that the regulatory environment is quite fragmented globally, with the presence of comprehensive rights-based approaches in developed jurisdictions, very early stages of the development of rights-based approaches in emerging economies, and limited provision in Global South countries (Dharmansyah et al., 2026).
To achieve effective AI governance, there is a need to shift beyond policy documents to structurally robust governance frameworks that incorporate the elements of policy into various aspects (Zhang et al., 2026). This demands putting the ethical principles into operation, with clear mechanisms such as explainability requirements, bias detection protocols, human oversight systems and accountability frameworks. At the same time, governance needs to tackle the twofold challenge of facilitating the positive use of AI and safeguarding fundamental rights, democracy and social equity (Fan, 2025).
Existing and future options require multi-stakeholder cooperation, as the government, technology developers, civil society, academics and affected communities need to work together to develop context-appropriate governance models (Fan, 2025). As AI grows in capability and influence, adaptive governance systems that can learn and evolve, yet remain grounded in essential ethical obligations will be crucial to the movement of AI toward promoting human dignity and democratic principles, and not threatening them.

References

1. Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012
2. Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (pp. 610–623). Association for Computing Machinery. https://doi.org/10.1145/3442188.3445922
3. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 77–91.
4. Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.
5. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
6. Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio,

Y. (2014). Generative adversarial nets. In Advances in neural information processing systems 27 (pp. 2672–2680). Curran Associates.
7. High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. Publications Office of the European Union.
8. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2
9. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539
10. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence, August 31, 1955. AI Magazine, 27(4), 12–14. https://doi.org/10.1609/aimag.v27i4.1904
11. Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. ACM Computing Surveys, 54(6), 1–35. https://doi.org/10.1145/3457607
12. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21. https://doi.org/10.1177/2053951716679679
13. OECD. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
14. O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.
15. Russell, S. J., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
16. Turing, A. M. (1950). Computing machinery and intelligence. Mind, 59(236), 433–460. https://doi.org/10.1093/mind/LIX.236.433
17. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137
18. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. In Advances in neural information processing systems 30 (pp.
19. 5998–6008). Curran Associates.
20. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005
21. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.