The American Journal of Interdisciplinary Innovations and Research
ISSN 2642-7478 | Open Access

Type Original Research
PAGE NO. 32-42
DOI 10.37547/tajiir/Volume07Issue08-03

AI Governance for Multi-Cloud Data Compliance: A Comparative Analysis of India and the USA

Yashvardhan Rathi
Truist Financial Services, USA

OPEN ACCESS

SUBMITED 17 July 2025
ACCEPTED 24 July 2025
PUBLISHED 06 August 2025
VOLUME Vol.07 Issue 08 2025

CITATION
Yashvardhan Rathi. (2025). AI Governance for Multi-Cloud Data Compliance: A Comparative Analysis of India and the USA. The American Journal of Interdisciplinary Innovations and Research, 7(8), 32–42. https://doi.org/10.37547/tajiir/Volume07Issue08-03

Abstract- Multinational companies that manage data across jurisdictional boundaries are having trouble integrating artificial intelligence systems with multi-cloud architectures. This is especially true since over 90% of businesses use multiple cloud providers and deal with complicated AI governance frameworks. This paper examines how well AI governance frameworks in India and the US deal with multi-cloud data residency compliance issues through a systematic literature evaluation based on PRISMA standards and thematic analysis of 26 publications, including academic articles, government policy papers, and industry reports published between 2020 and 2025. The study points out significant cross-border regulatory coordination problems and examines whether existing bilateral strategies need more ways to work together. The thematic analysis identified trends in regulatory frameworks and compliance problems, revealing "regulatory incommensurability" as a central theme—meaning that following one jurisdiction's rules goes against the basic ideas behind another's procedures. The Digital Personal Data Protection Act in India has a permission-by-default approach, which is very different from the USA's restriction-by-default approach. This leads to impossible compliance situations instead of coordination problems. Organizations face systemic inefficiencies because of duplicate infrastructure and multiple governance systems that do not provide the same level of AI safety or data security. For example, 35% of data breaches include "shadow data" not covered by existing frameworks. The results show that traditional working methods cannot settle significant disagreements between AI governance frameworks.

This means that new theoretical approaches are needed that acknowledge valid regulatory differences while making it easier for multinational companies to use AI systems in both jurisdictions.

Keywords: AI Governance, Data Sovereignty, Multi-Cloud Compliance, Digital Personal Data Protection Act (DPDPA) ,NIST AI RMF, India-USA Regulatory Comparison, Regulatory incommensurability

1. Introduction

Using AI systems and multiple cloud architectures has completely changed how multinational businesses send and receive data across borders. Things have become more difficult in the middle of technological growth and following the rules. Over 90% of companies now use more than one cloud provider. It is becoming even more important for governments worldwide to set up AI oversight systems and comprehensive data security rules (Tata Communications, 2024) for multi-cloud data residency.

Two significant places have different rules about how to handle these new tools. This shows how hard it is to follow the rules when not in the same place. Two important laws that affect how companies handle AI systems and data across borders are India's Digital Personal Data Protection Act (DPDPA) of 2023 and the US's new AI governance framework based on the NIST AI Risk Management Framework (Bahl et al., 2024; Cloud Security Alliance, 2021). India and the US are working together more on technology while these changes to the rules are happening. This makes it even more important for companies from different countries to work together on their rules.

However, the current AI governance frameworks make it hard for companies that use multi-cloud architectures in different countries to follow the rules and run their businesses, even with these unified policy efforts. International companies have different breach notice rules based on where the data is stored, where the company is based, and where the client lives (Mathew, 2024). A study shows that these companies have "overlapping notification duties." It is hard for companies that do business between India and the US to be sure of anything because AI control methods differ. 31% of data leaders say that cross-cloud security boundaries are a big worry regarding applications (Atlan, 2023).

This is made worse by problems with technology. This practical complexity shows that there is even less written on this subject. Many studies have been done on the rules for AI governance in different countries and on cloud compliance rules in general. However, we still do not fully understand how AI governance works with multi-cloud data residency compliance when it goes both ways (Roberts et al., 2024). It is essential to fill this study gap because the current ways of governing AI and ensuring that cloud data is safe are not enough to handle the complicated issues businesses face when doing business in multiple places.

This study looks at how AI governance frameworks in India and the US handle the issue of multi-cloud data residency compliance. It also finds specific gaps or conflicts in cross-border regulatory coordination. It decides if new ways are needed to ensure that companies that run AI systems in both countries follow the same rules. The results come at a good time because international efforts are still being made to make clear rules for AI control. It helps with academic research and policy-making, where good governance is needed to keep an eye on the rules and encourage international cooperation in technology.

2. Literature Review

2.1. Fragmented National AI Governance Approaches

The academic literature reveals significant concern about the fragmented nature of global AI governance and its implications for cross-border operations. Research demonstrates that "the centrality of AI to interstate competition, dysfunctional international institutions, and disagreement over policy priorities problematizes substantive cooperation" in global AI governance (Shulan & Mengting, 2024). This fragmentation is particularly evident in comparative studies highlighting contrasting regulatory approaches across key regions (Alibašić, 2025).

The India-USA divergence represents more than policy variation—it reflects fundamentally contradictory philosophical approaches to AI governance that create irreconcilable compliance conflicts for multinational organizations. India's regulatory philosophy emphasizes pragmatic adaptation, with policymakers arguing that "existing laws can address many of the anticipated risks of AI, and a gap analysis is required to identify areas where new rules are required" (Mohanty & Sahu, 2024; Joshi, 2024). This "light touch approach" contradicts emerging US approaches that increasingly favor prescriptive, risk-categorized frameworks.

The most significant contradiction emerges in approaches to AI system accountability and liability. While India's framework emphasizes organizational self-assessment and compliance through existing legal structures, the US approaches seek to impose specific "duty of care" requirements on AI developers with mandatory safety protocols (CCPA, 2024; Electronics & Information Technology, 2023). This fundamental disagreement over whether AI governance should be adaptive and organization-led versus prescriptive and government-mandated creates "compliance impossibility" scenarios for organizations operating across both jurisdictions.

2.1.1. Synthesis Implication

This philosophical contradiction suggests that bilateral harmonization efforts focusing on technical standards will be insufficient. Instead, successful India-USA AI governance coordination requires addressing the underlying disagreement about the appropriate roles of government and industry in AI oversight.

2.2. Multi-Cloud Data Governance Complexity

The literature extensively documents challenges organizations face when implementing data governance across multiple cloud environments, revealing the inadequacy of current theoretical frameworks. Research demonstrates that "given its intrinsic distributed nature, regulations and laws may differ and customers and cloud providers must find a way to balance increasing compliance pressures with cloud computing benefits" (Brandis et al., 2019; Al-Ruithe et al., 2019).

Tata Consultancy Services' "Distributed Data Management Solution" exemplifies these issues. It was designed to address the challenges of cross-border compliance, stating that "there is no unified framework for cross-border data flow," which "complicates the implementation and enforcement of data privacy policies" (TCS, 2024). IBM's 2024 Cost of a Data Breach Report indicates that organizations facing compliance challenges across borders incur an average expenditure of $4.9 million on data breaches. 35% of breaches pertain to "shadow data," defined as material not encompassed by existing governance systems (IBM, 2024).

The technical issues extend beyond merely increasing the workload; they also influence fundamental architectural decisions. Cloud providers possess varying compliance architectures not because of necessity, but due to the prevailing ambiguity surrounding the transnational movement of AI training data. 31% of data executives identify data retention within its designated cloud as a primary implementation challenge (Atlan, 2023).

2.2.1. Synthesis Implication

The proliferation of jurisdiction-specific compliance infrastructures represents systematic inefficiency in global AI governance that undermines innovation and security, suggesting that current approaches prioritize regulatory sovereignty over effective governance outcomes.

2.3. Data Residency and Cross-Border Transfer Divergence

The literature reveals stark differences in how India and the United States approach cross-border data transfers, exposing fundamental contradictions in their conceptualization of data sovereignty. India's DPDPA "adopts a blacklisting approach that enables cross-border transfer of personal data from India without any hurdles, unless the transfer is proposed to be made to a territory or country that is 'blacklisted'" (Securiti, 2024). This permissive framework operates on the principle that data flows should be unrestricted unless explicitly prohibited.

In direct contradiction, US approaches emphasize restrictive, sector-specific controls, assuming data transfers require explicit authorization rather than general permission. FISMA requirements create a presumption against cross-border data flows unless specifically authorized (CISA, 2024). This fundamental disagreement—permission-by-default versus restriction-by-default—creates "regulatory incommensurability" where compliance with one framework structurally violates assumptions underlying the other.

Recent analysis reveals that regulatory ambiguity compounds these contradictions, as "the Act and Rules are also silent on the implementation of any regulation for 'Binding Corporate Rules'" and "lack specific details on mechanisms for such assessments" (Lexology, 2025).

2.3.1. Synthesis Implication

The contradiction between permission and restriction illustrates conflicting theories of digital sovereignty, which cannot be resolved through technical means. This necessitates new approaches to bilateral AI governance that address the fundamental philosophical differences regarding data flows and national sovereignty (Batool et al., 2025).

2.4. Research Gaps and Limitations

Current research fails to adequately address fundamental incompatibilities between India and the USA's approaches to AI governance and multi-cloud compliance. Instead, regulatory differences are treated as technical coordination challenges rather than structural conflicts requiring new theoretical frameworks. The literature's focus on technical coordination solutions fails to address underlying philosophical contradictions about government oversight roles, data sovereignty presumptions, and fundamental approaches to AI risk management.

2.4.1. Gap Statement

While existing studies focus on individual national AI governance frameworks and general cross-border data transfer challenges, they fail to address fundamental regulatory incommensurabilities between India's permission-by-default and the USA's restriction-by-default approaches to cross-border AI data governance, perpetuating policy solutions that address symptoms of regulatory fragmentation while ignoring structural causes that make traditional harmonization mechanisms insufficient.

3. Methodology

This study employs a secondary qualitative comparative document analysis design utilizing systematic literature review methodology following PRISMA guidelines to ensure comprehensive and transparent document selection and analysis. Document analysis is particularly valid for this research as AI governance frameworks and multi-cloud compliance requirements are primarily codified in formal policy documents, regulatory texts, and scholarly analyses representing authoritative sources of regulatory intent and implementation guidance.

A comprehensive search strategy was employed across multiple databases, including Google Scholar, IEEE Xplore, PubMed, and Web of Science, complemented by government repositories and industry sources. Following PRISMA guidelines, the systematic review process began with 227 initial search results. After removing 28 duplicates, 199 unique documents underwent screening, excluding 164 documents outside the 2020-2025 timeframe or lacking relevance to AI governance or India-USA contexts. This yielded 35 full-text articles for detailed review, of which 23 were subsequently excluded due to insufficient detail on regulatory frameworks or inadequate bilateral relevance. The final corpus comprised 26 documents, including 12 academic papers from peer-reviewed journals, 3 government policy documents covering India's DPDPA and USA frameworks, and 11 industry reports from recognized organizations published between 2020 and 2025 (Figure 1).

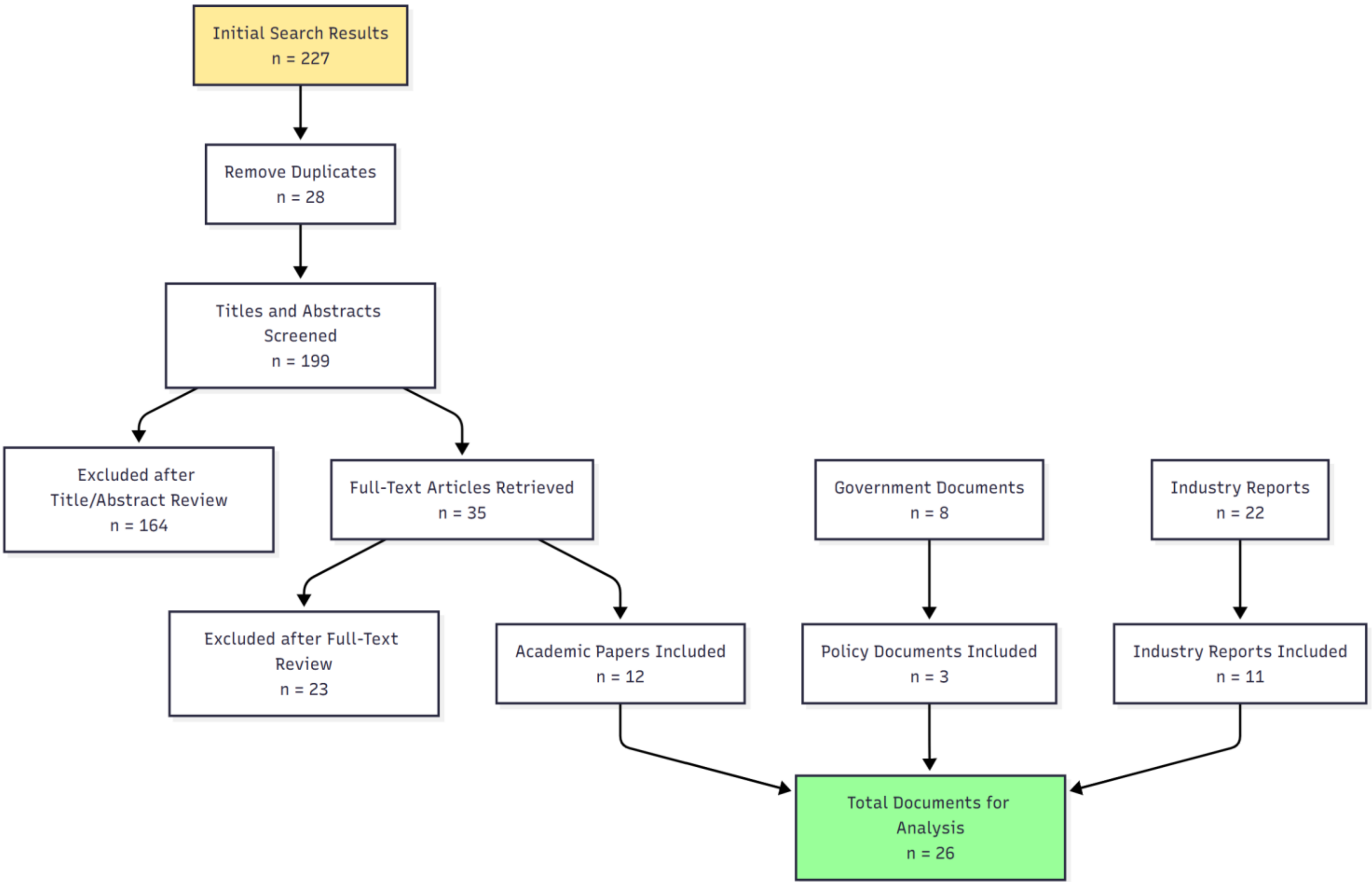
Initial Search Results
n = 227
Remove Duplicates
n = 28
Titles and Abstracts Screened
n = 199
Excluded after Title/Abstract Review
n = 164
Full-Text Articles Retrieved
n = 35
Government Documents
n = 8
Industry Reports
n = 22
Excluded after Full-Text Review
n = 23
Academic Papers Included
n = 12
Policy Documents Included
n = 3
Industry Reports Included
n = 11
Total Documents for Analysis
n = 26

Figure 1 - PRISMA Analysis of Documents

Documents were analyzed using thematic analysis following Braun and Clarke (2006), focusing on identifying convergences and divergences between India and the USA approaches, compliance challenges faced by multinational organizations, and harmonization opportunities. The analysis employed a structured coding approach that examined six primary thematic categories: regulatory philosophy and approach (encompassing governance philosophy, risk assessment models, and accountability mechanisms), cross-border data transfer frameworks (including transfer permissions, data residency requirements, and blacklisting versus whitelisting approaches), multi-cloud compliance challenges (covering technical implementation barriers, operational complexity, and shadow data issues), bilateral coordination mechanisms (examining existing frameworks, harmonization opportunities, and structural conflicts), industry impact assessment (analyzing compliance costs, innovation effects, and competitive disadvantages), and regulatory incommensurability (identifying philosophical contradictions, implementation impossibilities, and sovereignty conflicts). This coding framework enabled systematic identification of text segments related to each category, followed by iterative refinement to capture emerging themes and sub-patterns within the established analytical structure.

Quality assurance measures included systematic documentation, standardized data extraction templates, and cross-referencing findings across multiple document types to enhance validity through triangulation. The methodology acknowledges limitations inherent in relying on secondary documents, including gaps in understanding informal coordination mechanisms and rapidly evolving regulatory frameworks. Ethical considerations are minimal given exclusive reliance on publicly available documents without human participants or confidential information.

4. Results

The systematic analysis of 26 documents revealed significant regulatory divergences and operational challenges in India-USA AI governance coordination, organized around three primary themes: regulatory framework incompatibilities, multi-cloud compliance complexities, and bilateral coordination gaps.

4.1. Regulatory Framework Incompatibilities

The analysis revealed systematic contradictions between India's DPDPA and the USA's AI governance frameworks, creating irreconcilable compliance scenarios. Table 1 presents a comparative analysis of key regulatory dimensions.

Table 1: Comparative Analysis of India DPDPA vs USA AI Governance Frameworks

Regulatory Dimension	India DPDPA 2023	USA Framework (NIST AI RMF + FISMA)
Data Transfer Approach	Permission-by-default (blacklisting)	Restriction-by-default (authorization required)
AI Oversight Philosophy	Self-assessment, gap analysis	Prescriptive risk categorization
Compliance Mechanism	Organizational adaptation to existing laws	Mandatory technical safeguards
Enforcement Model	Reactive, penalty-based	Proactive, prevention-based
Cross-border Coordination	Bilateral blacklisting agreements	Sector-specific authorization
Implementation Timeline	Phased rollout 2023-2025	Variable by sector and state
Penalty Structure	Up to ₹500 crore ($60M)	Varies by sector, loss of federal contracts
Data Residency Requirements	Permissive unless blacklisted	Restrictive for government/critical sectors

***Sources: Bahl et al. (2024), CISA (2024), Securiti (2024),* Electronics & Information Technology (2023)**

The documentary evidence revealed that these differences represent competing paradigms rather than implementation variations. India's framework assumes existing laws can address AI risks through gap analysis, while the US approaches favor prescriptive, risk-categorized frameworks with mandatory technical implementations (Kohler, 2025).

4.2. Multi-Cloud Compliance Operational Challenges

The analysis identified systematic inefficiencies in organizational responses to regulatory divergence, with evidence of substantial infrastructure duplication and administrative overhead. Figure 2 illustrates the compliance challenge categories identified across industry documentation.

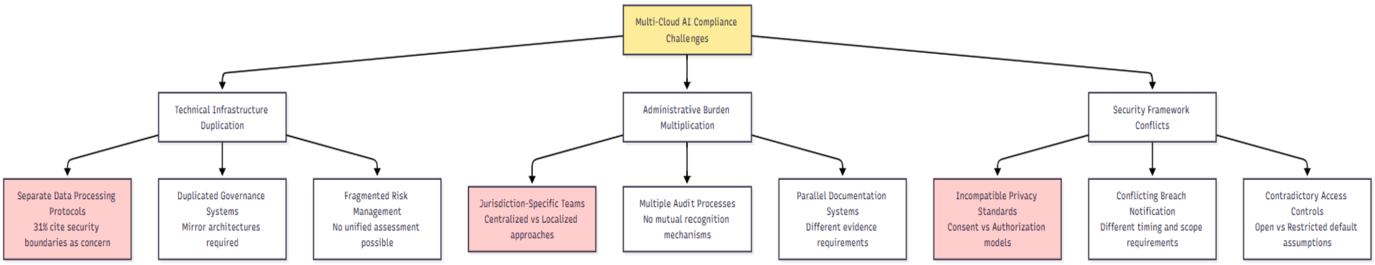
Multi-Cloud AI Compliance Challenges
Technical Infrastructure Duplication
Administrative Burden Multiplication
Security Framework Conflicts
Separate Data Processing Protocols
31% cite security boundaries as concern
Duplicated Governance Systems
Mirror architectures required
Fragmented Risk Management
No unified assessment possible
Jurisdiction-Specific Teams
Centralized vs Localized approaches
Multiple Audit Processes
No mutual recognition mechanisms
Parallel Documentation Systems
Different evidence requirements
Incompatible Privacy Standards
Consent vs Authorization models
Conflicting Breach Notification
Different timing and scope requirements
Contradictory Access Controls
Open vs Restricted default assumptions

Figure 2 – Multi-cloud AI compliance challenges

Source: Synthesized from Atlan (2024), Matthew (2024), Tata Communications (2024)

Industry documentation revealed specific examples of operational inefficiencies, including TCS's development of distributed data management solutions specifically addressing the reality that "there is no common framework for cross-border data flow" (TCS, 2024).

IBM's analysis found 35% of breaches involve "shadow data" existing outside formal governance frameworks, with organizations facing average breach costs of $4.9 million, challenges particularly acute for multi-jurisdictional AI deployments (IBM, 2024). The Cloud Security Alliance documented that organizations face pressure to implement "adaptable, modular compliance strategies," yet 31% of data leaders cited securing cross-cloud data boundaries as major implementation concerns (Cloud Security Alliance, 2025).

4.3. Bilateral Coordination Gaps

The analysis revealed systematic gaps in existing bilateral coordination mechanisms, with evidence that current harmonization efforts address technical coordination rather than paradigmatic conflicts. Table 2 summarizes identified coordination gaps.

Table 2: Bilateral Coordination Gaps in India-USA AI Governance

Coordination Aspect	Current Status	Identified Gap	Operational Impact
Policy Alignment Forums	Ad hoc summits	No permanent mechanism	Reactive coordination
Technical Standards	Industry-led initiatives	No government endorsement	Limited enforcement
Data Transfer Agreements	Sectoral arrangements	No comprehensive framework	Case-by-case negotiations
Mutual Recognition	Limited pilots	No systematic process	Duplicated certification
Dispute Resolution	Traditional channels	No specialized mechanism	Lengthy timelines

Sources: Stimson Center (2025), ITU (2024), Mohanty & Sahu, 2024)

Literature analysis revealed that emerging bilateral cooperation efforts remain limited in scope and enforceability. The Cloud Security Alliance noted emerging India-US technology collaborations focus on harmonizing AI standards, but these initiatives lack binding commitments or systematic implementation mechanisms (Cloud Security Alliance, 2025).

4.4. Regulatory Incommensurability and Implementation Barriers

The synthesis revealed "regulatory incommensurability"—situations where compliance with one jurisdiction's framework structurally violates foundational assumptions of another's approach. Cross-border compliance represents a "significant challenge for organizations operating globally," requiring "comprehensive risk assessment" and "localization of compliance programs" (TrustCloud, 2024). However, evidence suggests such localization approaches institutionalize regulatory fragmentation by creating parallel governance systems that cannot achieve unified risk management objectives.

The analysis found that traditional harmonization mechanisms prove insufficient for addressing philosophical contradictions about appropriate government oversight roles, data sovereignty presumptions, and fundamental approaches to AI risk management (Walter, 2024). Organizations have developed automated systems to "identify regulatory obligations and map legal requirements to risk governance frameworks," but these technical solutions cannot resolve underlying paradigmatic conflicts (IBM, 2025).

5. Discussion

5.1. Fundamental Regulatory Incommensurability

The results show that the AI governance frameworks in India and the US are based on fundamentally different philosophical ideas. This leads to "regulatory incommensurability," which means that following one jurisdiction's framework would structurally violate the fundamental assumptions that underlie the other jurisdiction's approach. This means global companies must deal with impossible compliance situations instead of complicated coordinating problems.

The obligations for notifying people about data breaches are a clear example. India's DPDPA emphasizes that organizations do their assessments and notify people of harm. In contrast, new US approaches require organizations to have specific technical safeguards and set timetables, believing organizations cannot self-govern. When multinational AI systems have security problems in both countries, companies cannot simultaneously follow India's harm-based self-assessment and the US's prescriptive mandatory reporting rules. This is because the two sets of rules make different assumptions about how well organizations can do their jobs and how much government oversight they should have.

These conclusions differ from what other research has said about regulatory discrepancies being coordination problems that need technical harmonization. Our research shows that these kinds of technical fixes cannot solve deeper philosophical problems like how to balance encouraging innovation with keeping people safe, or giving organizations freedom while the government controls them.

5.2. Systemic Inefficiencies in Multi-Cloud Compliance

The findings indicate that organizational responses to regulatory divergence create systematic inefficiencies that undermine innovation and security objectives rather than enhance protection or performance. This suggests that current approaches create deadweight losses—resources consumed in regulatory navigation that produce no corresponding benefit in AI safety, data protection, or operational efficiency.

The fact that big IT companies need to duplicate their systems shows how inefficient this is. It is not that companies keep their AI model training environments and data governance systems separate for different reasons, like different technology security needs. The rules for data sovereignty and AI supervision do not work well together. Investors are not making these purchases because of real technical or security needs; they are doing so because regulations are getting messy.

By showing that goals of regulatory sovereignty might not always lead to good government, these new ideas could change how policies are made in the future. Policymakers might want to consider whether having different national ways is good for the country or makes it harder to develop new ideas and keep people safe.

5.3. Limitations of Traditional Bilateral Cooperation

The results show that the current ways of working together on two sides are not good enough to settle profound differences between AI governance frameworks because they only focus on making the systems work together technically and not on ensuring they agree on what is right. Traditional diplomatic methods like mutual recognition deals and technical working groups cannot fix problems built into the system.

India and the US are working together on the idea that different rules about AI are just different ways of doing things, not deep disagreements about what the government should do to control AI. There is a big difference between India's "permission-by-default" policy and the US's "restriction-by-default" framework. The two are based on different ideas about how new technology affects national security.

They show that countries need to settle philosophical differences about digital sovereignty, risk tolerance, and the right amount of government control before they can try to make technical changes. This could change how countries work together in the future.

5.4. Study Limitations

The study is limited by reliance on publicly available documents, which may not capture the full complexity of informal coordination mechanisms or internal organizational decision-making processes. The rapidly evolving nature of AI governance frameworks means regulatory developments may outpace the publication of analytical documents. The India-USA bilateral focus may limit generalizability to other jurisdictional pairs with different philosophical approaches to technology governance.

5.4.1. Future Research Directions

Future studies should examine the lived experiences of compliance professionals through cross-jurisdictional surveys to understand how theoretical regulatory conflicts translate into practical decision-making challenges. Research should investigate compliance simulation studies modeling operational impacts of different harmonization scenarios. Longitudinal studies tracking organizational responses to regulatory changes would provide insights into adaptation strategies. Comparative analysis extending beyond India-USA contexts could test whether regulatory incommensurability applies to other jurisdictional pairs.

6. Conclusion

This study examined how AI governance frameworks in India and the US deal with problems with data residency compliance in multiple clouds. It did this by looking at the specific gaps and conflicts in cross-border regulatory coordination that make it hard for multinational companies to use AI systems in both countries. The research aimed to determine if the current bilateral approaches need new ways to make things more consistent or standard practices for good AI governance across borders. The study found a basic idea of "regulatory incommensurability," which means that following one jurisdiction's rules would structurally break the basic assumptions of another's approach. India's permission-by-default philosophy in the DPDPA is the opposite of the USA's restriction-by-default approach. This makes it impossible to follow the rules, which makes coordination more difficult. This difference in philosophy goes beyond how data is transferred to include fundamental disagreements about the right amount of government oversight, the right amount of freedom for organizations to develop AI, and the right balance between encouraging innovation and preventing risk. The proof shows that multinational companies have systematic inefficiencies and spend much money managing regulatory differences by duplicating infrastructure and setting up parallel governance systems that do not make AI safer or better protect data.

These results have important consequences for many people trying to figure out how to deal with the changing AI governance landscape. The study shows that cloud providers like AWS, Microsoft Azure, and Google Cloud must quickly redesign their architectural approaches to deal with regulatory conflicts that are too big to be solved with one-size-fits-all compliance solutions. Data Protection Officers and compliance teams in multinational companies should know that the current ways of coordinating between two countries are not enough to deal with the underlying philosophical differences. This means that adaptive governance frameworks need to be created that can handle contradictory regulatory assumptions at the same time. When technology startups try to grow their businesses in India and the US, they face many problems because they do not have the same resources as bigger companies to keep up with two compliance rules. This shows that they need new business models and compliance strategies that consider that regulations are not always compatible from the start, instead of trying to fix things later.

The bigger picture includes the structure of global AI governance itself. The study suggests that the current path toward fragmented national AI governance frameworks creates compliance burdens that are too high to be sustainable and may ultimately hurt the safety and innovation goals these frameworks are meant to achieve. Both sets of policymakers should consider whether keeping different philosophical approaches to AI governance is in the best interests of their countries or makes it harder to manage risks effectively. The study shows that to make bilateral AI governance work, we need new theoretical frameworks for dealing with paradigm conflicts that consider the fact that different countries have different ways of doing things, making it easier for multinational companies to do business.

Future research should focus on empirical studies that look at the real-life experiences of compliance professionals through surveys and interviews across jurisdictions. This will help us understand how theoretical regulatory conflicts turn into real-life decision-making problems. Compliance simulation studies that model the effects of different harmonization scenarios on operations could see if proposed bilateral cooperation mechanisms would lower compliance costs or move them around. Also, a comparative study examining more than just the India-USA relationship could show whether regulatory incommensurability is a common problem in global technology governance or just something in this one relationship. As both jurisdictions continue to improve their AI governance methods, long-term studies examining how organizations adapt will be important for making future policies that balance regulatory sovereignty and operational effectiveness in an AI ecosystem that is becoming more connected worldwide.

References

1. Alibašić, H. (2025). Harmonizing artificial intelligence (AI) governance: A comparative analysis of Singapore and France's AI policies and the influence of international organizations. *Global Public Policy and Governance*, 1-21.
2. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, 23, 839-859.
3. Atlan. (2023, December 23). Multi-cloud data governance: Five rules for success. https://atlan.com/know/data-governance/multi-cloud-data-governance/
4. Bahl, R., Bagai, R., & Sumi, K. (2024, March 13). India: Digital Personal Data Protection Act, 2023 part three – data transfers. AZB Partners. https://www.azbpartners.com/bank/india-digital-personal-data-protection-act-2023-part-three-data-transfers/
5. Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: a systematic literature review. *AI and Ethics*, 1-15.
6. Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, risk, and compliance in cloud scenarios. *Applied Sciences*, 9(2), 320.
7. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.
8. CCPA. (2024). California Consumer Privacy Act. https://www.oag.ca.gov/privacy/ccpa
9. CISA. (2024). Federal Information Security Modernization Act. https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act
10. Cloud Security Alliance. (2025, April 22). AI and privacy: Shifting from 2024 to 2025. https://cloudsecurityalliance.org/blog/2025/04/22/ai-and-privacy-2024-to-2025-embracing-the-future-of-global-legal-developments
11. Electronics and Information Technology. (2023). Digital Personal Data Protection Act. https://www.dpdpa.in/
12. IBM. (2024). Cost of a data breach report 2024. IBM Security. https://www.ibm.com/reports/data-breach
13. IBM. (2025). IBM WatsonX Platform: Compliance obligations to controls mapping. https://www.ibm.com/products/blog/ibm-watsonx-platform-compliance-obligations-to-controls-mapping
14. ITU. (2024). Key findings on the state of global AI governance. https://www.itu.int/hub/2024/07/key-findings-on-the-state-of-global-ai-governance/
15. Joshi, D. (2024). AI governance in India – law, policy and political economy. *Communication Research and Practice*, 10(3), 328-339.

16. Kohler, S. (2025). Technology federalism: US states at the vanguard of AI governance. Carnegie Endowment for International Peace.

17. Lexology. (2025, January 21). Cross border data transfers under India's proposed data protection regime. https://www.lexology.com/library/detail.aspx?g=d5715e1d-4b25-40b2-a817-38966662c69f

18. Mathew, A. (2024). Cloud data sovereignty governance and risk implications of cross-border cloud storage. Information Systems Audit and Control Association.

19. Mohanty, A., & Sahu, S. (2024). India's advance on AI regulation. Carnegie India.

20. Roberts, H., Hine, E., Taddeo, M., & Floridi, L. (2024). Global AI governance: barriers and pathways forward. *International Affairs*, 100(3), 1275-1286.

21. Securiti. (2024, October 29). Cross-border data transfer requirements under India DPDPA. https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdpa/

22. Shulan, Y., & Mengting, L. (2024). Global AI governance: Progress, challenges, and prospects. *China International Studies*, 109, 48.

23. Stimson Center. (2025). Shaping inclusive AI governance – Reflections on Paris and opportunities for the India AI Summit. https://www.stimson.org/2025/shaping-inclusive-ai-governance-reflections-on-paris-and-opportunities-for-the-india-ai-summit/

24. Tata Communications. (2024). 7 best practices for multi-cloud governance & compliance. https://www.tatacommunications.com/knowledge-base/best-practices-for-multi-cloud-governance-and-compliance/

25. TCS. (2024). Data privacy management: Distributed data management solution. TCS White Paper.

26. TrustCloud. (2024). Cross-border compliance: Navigating globalization challenges in 2024. https://community.trustcloud.ai/article/cross-border-compliance-navigating-globalization-challenges-in-2024/

27. Walter, Y. (2024). Managing the race to the moon: Global policy and governance in artificial intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*, 4(1), 14.