Sovereignty in the Age of Artificial Intelligence: Intensifying Debates and New Directions

VENKATESWARA RAO BOBBILI
data.bobbili@gmail.com

Abstract- Artificial intelligence (AI) is reshaping how sovereignty is understood and practiced. No longer confined to territorial authority, sovereignty now reaches into digital infrastructures, data governance, and collective rights, including those of Indigenous peoples. This paper synthesizes recent developments in policy and scholarship to show how AI simultaneously strengthens state capacity and challenges state authority, how digital sovereignty is becoming a strategic priority for states, and how Indigenous Data Sovereignty (IDS) demands new ethical and legal approaches. The analysis concludes with practical recommendations for policymakers, governance professionals, and Indigenous authorities.

Index Terms- Sovereignty, Artificial Intelligence, Digital Sovereignty, Indigenous Data Sovereignty, Federalism, Regulation, Data Governance

I. INTRODUCTION

The spread of AI technologies requires a fresh appraisal of sovereignty. Where sovereignty was once principally about a state's exclusive authority over territory and population, it now encompasses control over data, algorithmic systems, and the digital architectures that underpin public life. These developments matter not only for interstate relations and national security, but for everyday governance, rights protection, and the power relations between states, corporations, and communities. This paper maps the principal fault lines—state-level surveillance and capacity, digital sovereignty as policy, Indigenous claims over data, and the fragmentation of governance in federal systems—and offers policy-minded recommendations.

II. STATE SOVEREIGNTY AND THE RISE OF AI

2.1. Strengthening capacity, widening vulnerability

AI has amplified state administrative and enforcement capabilities border management, disease surveillance, and criminal-justice tools are now routinely augmented by predictive analytics and automated decision systems. These tools can improve efficiency and responsiveness, but they also create new points of failure and risk: algorithmic bias, opaque decision-making, and the potential for misuse. At the same time, the global architecture of platforms and cloud services allows non-state and transnational actors to operate in ways that can circumvent or dilute state control

Surveillance's rapid expansion and accountability gaps From 2018 onward, many governments have accelerated deployment of AI-enabled surveillance for security and public-health objectives. This expansion frequently outpaces the development of legal safeguards. Where oversight mechanisms are weak or absent, algorithmic systems can erode privacy and civil liberties without clear avenues for redress.

Regulatory reach beyond borders

Recent laws and proposals—most prominently in the European Union and in China's PIPL—illustrate how domestic AI and data laws can have extraterritorial consequences. Companies operating across borders face mounting pressure to adapt their data-handling practices and operational models to comply with multiple, sometimes conflicting, regulatory regimes.

III. DIGITAL SOVEREIGNTY: FROM CONCEPT TO POLICY

3.1. What digital sovereignty means today

Digital sovereignty refers to a polity's capacity to control the digital infrastructure that underpins social and economic life: networks, cloud services, standards, and data flows. It encompasses economic strategy, national security, and normative commitments to rights and governance. In practice, digital sovereignty is both a political claim and a set of policy instruments designed to secure autonomy in the digital domain [3,4].

3.2. Core trade-offs in policy design

Efforts to bolster digital sovereignty often confront three central tensions:

- Dependence versus autonomy: Outsourcing critical services to foreign providers can create vulnerabilities, yet building domestic equivalents is costly and time-consuming.
- Localization versus openness: Data-residency rules can protect control but impede cross-border research and innovation.
- Fragmentation versus harmonization: Nationally divergent rules risk creating a fractured internet "splinternets" that raise costs for businesses and limit the free flow of information.

3.3. How states are acting

Governments have used measures such as cloud regulation, data-residency requirements, and stringent privacy frameworks to operationalize digital sovereignty. Countries including India, Russia, Brazil, and members of the EU have adopted policies that reflect a stronger desire to govern data and digital infrastructure domestically [5–8].

IV. INDIGENOUS DATA SOVEREIGNTY (IDS): RIGHTS AND GOVERNANCE

4.1. Foundations and principles

Indigenous Data Sovereignty centers on the collective right of Indigenous peoples to govern data about their communities, cultures, and lands. Unlike individual-centric data frameworks, IDS emphasizes relational and community-based control, reflecting Indigenous values of stewardship and self-determination [9–11].

4.2. Standards and frameworks

IDS is framed by international norms such as the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) and by practice-oriented frameworks like OCAP® (Ownership, Control, Access, Possession) and CARE (Collective Benefit, Authority to Control, Responsibility, Ethics). These frameworks insist that data governance should deliver meaningful participation and equitable benefit for Indigenous communities [9–12].

4.3. Implementation and friction points

Jurisdictions such as New Zealand and parts of Canada show how Indigenous governance can be integrated into data-policy processes. However, practical challenges remain: limited community resources, misalignment with national legal frameworks, and difficulties reconciling collective governance with dominant individual rights paradigms.

V. FEDERALISM AND FRAGMENTED AI GOVERNANCE

5.1. Local experimentation and innovation

In federal systems, subnational governments often lead in piloting AI regulations and initiatives. This bottom-up experimentation can generate valuable lessons and policy innovation, enabling localized responses to technology's social impacts

5.2. Costs of fragmentation

Divergent subnational standards, however, produce legal complexity and compliance burdens. Companies face higher costs and fragmented enforcement environments, while citizens may experience uneven protections across jurisdictions. Notable examples include Quebec's Law 25 and California's CCPA/CPRA, which can exceed national protections and complicate cross-jurisdictional compliance [13–15].

5.3. Pathways toward coherence

Balancing subnational experimentation with national coherence calls for institutional mechanisms that align baseline protections while allowing local innovation. Approaches could include model rules, coordinated intergovernmental bodies, or federal frameworks that set minimum standards while permitting regional enhancements.

VI. POLICY IMPLICATIONS AND STRATEGIC CONSIDERATIONS

6.1. Managing complexity

Stakeholders must navigate a patchwork of requirements from different levels of governance and from Indigenous authorities. This necessitates more sophisticated governance architectures within both public institutions and private firms.

6.2. Seizing opportunities for resilient governance

Investments in domestic technical capacity, active participation in international standard-setting, and adoption of rights-based approaches to data governance can strengthen both national resilience and ethical AI development. Harmonization efforts—regional or multilateral—can reduce fragmentation while protecting rights [2,4,16].

6.3. Avoiding protectionism and rights erosion

Policymakers should be wary of digital sovereignty measures that slide into protectionism, stifling innovation and cooperation. Likewise, the expansion of surveillance capacities must be accompanied by transparency, independent oversight, and accessible remedies to prevent rights infringements [8,16].

VII. FUTURE WORK

Empirical work is needed to evaluate the effectiveness of different digital sovereignty policies, to document operational models for implementing IDS across legal systems, and to measure the economic and social costs of regulatory fragmentation. Comparative case studies and quantitative analyses of compliance burdens would be particularly useful for policymakers.

VIII. POLICY RECOMMENDATIONS

- Act across scales: Track and shape legal developments at international, national, and subnational levels and anticipate the extraterritorial effects of domestic laws.
- Center Indigenous rights: Embed IDS principles in national data strategies and procurement policies, and ensure meaningful Indigenous participation in governance design.
- Promote harmonization with flexibility: Support regional and multilateral alignment on core standards while allowing subnational experimentation within agreed guardrails.
- Build domestic capacity: Invest in public infrastructure, open-source platforms, and workforce skills to reduce strategic dependence.
- Strengthen accountability: Require transparency, independent audits, and clear remedies for algorithmic systems used by both states and private actors.
- Constrain surveillance: Ensure that security and public-health uses of AI are guided by necessity, proportionality, and robust oversight.

CONCLUSION

Sovereignty in the AI era is plural, layered, and contested. It now extends into infrastructures, algorithms, and the governance of knowledge itself. To manage these shifts, policy must reconcile state-level priorities with the rights of communities and the realities of a global digital ecosystem.

REFERENCES

[1] AdvanceLRF. Vol. 5, No. 2 (2023). https://www.advancelrf.org/wp-content/uploads/2023/04/Vol-5-No.-2-1.pdf

[2] World Economic Forum. "Sovereign AI: what is it and ways states are building." (2024). https://www.weforum.org/stories/2024/04/sovereign-ai-what-is-ways-states-building/

[3] Artefact. "What does AI sovereignty really mean?" https://www.artefact.com/blog/what-does-ai-sovereignty-really-mean/

[4] Sciences Po. "Report — European sovereignty and AI: a competence-based perspective" (2024). https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2024/11/report-european-sovereignty-artificial-intelligence-competence-based-perspective.pdf

[5] World Governments Summit. "Sovereignty in AI and cloud." https://www.worldgovernmentssummit.org/observer/reports/detail/sovereignty-in-ai-and-cloud

[6] Zextras Community. "Digital sovereignty vs. data sovereignty." https://community.zextras.com/digital-sovereignty-vs-data-sovereignty-what-are-the-differences-blog/

[7] Deloitte. "Achieving digital sovereignty." https://www.deloitte.com/lu/en/our-thinking/future-of-advice/achieving-digital-sovereignty.html

[8] IDC. "Digital Sovereignty" (2025). https://www.idc.com/wp-content/uploads/2025/03/D3_4_Digital_Sovereignty_v04_Clean_afGWcBe4lNR1dSYCS9RgVVuNB6E_95774.pdf

[9] Indigenous Data Sovereignty Brief (2022). https://static1.squarespace.com/static/5b3043afb40b9d20411f3512/t/642a53c991c4e1604f3b0b9b/1680495564354/Indigenous+Data+Sovereignty+Brief+2022.pdf

[10] University of Waikato Research Commons. https://researchcommons.waikato.ac.nz/server/api/core/bitstreams/679630a0-77ae-4821-a7f4-b482f65ad39c/content

[11] Concordia University. Data sovereignty research guide (Nov 2024). https://www.concordia.ca/content/dam/library/docs/research-guides/data-sovereignty/datasovinfo_nov2024.pdf

[12] Development Gateway. "Deep Dive on Indigenous Data Sovereignty" (2023). https://developmentgateway.org/wp-content/uploads/2023/02/Deep-Dive-on-Indigenous-Data-Sovereignty_2023.pdf

[13] L. Solum (blog). "Wu on AI governance and federalism" (2025). https://lsolum.typepad.com/legaltheory/2025/04/wu-on-ai-governance-and-federalism.html

[14] Just Security. "AI governance and federalism, moratorium perspectives." https://www.justsecurity.org/113728/ai-governance-federalism-moratorium/

[15] Ave Maria Law. "Navigating federal governance frameworks for emerging technology." https://www.avemarialaw.edu/navigating-federal-governance-framework-for-emerging-technology/

[16] SSRN. "Paper: Sovereign AI and digital governance" (SSRN). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4996387