Cosmos Multidisciplinary Research E-Journal
Online Available at www.cmrj.in
Recognized International Peer Reviewed Journal
Impact Factor 5.69
ISSN No. 2456-1665

Digital Age, AI and the Changing Concepts of Sovereignty

Dr. Satish Karad
Associate Professor
Indraraj Arts, Commerce and Science College,
Sillod

Abstract:
The traditional concept of state sovereignty, rooted in territorial and jurisdictional authority, is undergoing a profound transformation. Digital disruption, borderless technologies, the dominance of global tech corporations—often foreign-owned—and cyber threats from hostile states are redefining sovereignty's significance. Geopolitical conflicts, warfare, and global challenges such as climate change, pandemics, and cybercrime further erode conventional notions of sovereign control. This study explores the growing role of Artificial Intelligence (AI) in international relations, focusing on how global leaders exercise authority and pursue digital sovereignty amidst these shifts. This paper examines how AI-enabled technologies reshape social, cultural, economic, and political norms, challenging traditional concepts of sovereignty. It analyzes the interplay between AI and state authority, highlighting how digital advancements disrupt the global state system. The discussion begins with an overview of international relations, sovereignty, and strategic autonomy, followed by an assessment of digital technology's impact on geopolitical dynamics. The study concludes with practical recommendations for crafting public policy to navigate sovereignty in the digital and humanistic era.

Key Words: Digital Age, AI, State Sovereignty

Introduction:.

Sovereignty, traditionally understood as state sovereignty, encompasses the authority of a government over its territory and people. However, individual sovereignty—the rights and agency of citizens—shares a critical relationship with state power. Sovereignty reflects the dynamics of power between governments and their people, where mutual legitimacy is essential. A government rejected by its citizens risks instability, while citizens unsupported by their state face hardship. Democracy and respect for human rights serve as mechanisms to balance this power, forming the foundation of both state and individual sovereignty. These principles align closely with digital humanism, which emphasizes human-centric governance in the digital era. In today's geopolitically charged digital age, sovereignty faces unprecedented strain. Global challenges—cybercrime, pandemics, climate change—alongside geopolitical conflicts and the disruptive influence of digital technologies and multinational tech corporations, transcend national borders, challenging traditional notions of state autonomy (Kello, 2017). These forces disrupt the global state system, potentially heralding a transformative shift. State leaders, grappling with these pressures, have prioritized sovereignty and strategic autonomy since 2017, advocating proactive public policies to preserve and strengthen sovereign control.

This analysis focuses on crafting public policies that address the interplay between sovereignty and digital technology, aligning with the ideals of a human-centric digital era. The central challenge lies in defining sovereignty's possible forms in the digital age, identifying preferred political choices, and understanding the interaction between

technology and society. Neglecting this task risks empowering undemocratic regimes, unaccountable authorities, and unchecked technological growth—outcomes contrary to digital humanism's principles.

The discussion begins with an overview of perspectives on sovereignty, strategic autonomy, and international relations, providing a framework to assess digital technology's impact. It then explores the challenges of formulating public policy for sovereignty, with specific focus on two critical domains: cybersecurity and artificial intelligence (AI). The rise of AI, in particular, poses complex challenges to state sovereignty, with some arguing it undermines governmental authority by reshaping social, economic, and political norms.

- **Digital Technologies and Sovereignty**
  - Traditionally, sovereignty centered on territorial control, but digital technology has expanded this to include intangible assets. National digital identities, domain names (at national, provincial, and municipal levels), health and genetic data, and digital representations of domestic products or smart cities now constitute critical sovereign assets. Cyberspace—comprising servers, data centers, and domestic digital networks—has tangible locations subject to governmental oversight. Yet, transnational networks, cloud-based services, and intangible standards complicate jurisdictional control. Digital services can operate independently of a nation's physical boundaries, challenging traditional sovereignty.
  - A nation's digital literacy is vital for progress. Health and genetic data, often viewed as mere information, are national assets tied to collective identity and economic value, such as innovative pharmaceuticals or wellness programs. Governments increasingly advocate for data localization to assert sovereignty, requiring technological frameworks with defined boundaries. Technologies like homomorphic encryption, which enables secure data processing without compromising privacy, offer potential solutions for maintaining control over these assets. However, such measures raise questions about balancing access, security, and national authority.
  - Digital Technology's Impact on Sovereign Institutions. Digital technologies enhance public services, civic participation, and access to information, strengthening internal legitimacy. E-governance platforms and digital voting systems, for instance, can deepen democratic engagement. However, these technologies also disrupt sovereign institutions beyond their jurisdictions. Originally designed for human interaction, sovereignty struggles to adapt to machine-driven systems, particularly autonomous AI. AI's ability to operate independently poses a paradox: it can protect sovereignty by enhancing security and efficiency but also threaten it by evading human oversight and political accountability.
  - The lack of a technological framework ensuring human control over autonomous AI remains a critical gap. Without such mechanisms, AI risks undermining internal legitimacy, as citizens may perceive diminished governmental authority.

Furthermore, the proliferation of digital technologies necessitates new regulatory entities, which could encroach on sovereignty by imposing external standards or norms.

- Digital technologies reshape power dynamics between states, citizens, and global entities. They empower individuals by facilitating global citizenship, transcending physical borders and political authority. Social media and decentralized platforms amplify voices, fostering collective identities that challenge state-centric sovereignty. However, this empowerment coexists with risks, including digital subjugation through surveillance or unaccountable tech corporations.
- The rise of artificial general intelligence (AGI) intensifies concerns about sovereignty. AGI could disrupt geopolitical stability, potentially sparking technological conflicts that undermine both internal and external legitimacy. States must navigate the tension between leveraging AI for national advantage and mitigating its risks to sovereign control.
- The interplay between digital technology and sovereignty is reciprocal. While technology challenges traditional state authority, it also offers tools to enhance sovereignty. For instance, blockchain-based systems can secure national digital assets, and AI-driven cybersecurity can protect against cyber threats. Conversely, overreliance on technology without robust governance risks eroding sovereignty, as states may cede control to transnational corporations or unregulated AI systems.
- To address these challenges, states must prioritize policies that balance technological innovation with human oversight. This includes investing in digital literacy, developing regulatory frameworks for AI and data governance, and fostering international cooperation to set standards for transnational digital networks. Digital humanism, which emphasizes human agency in technological progress, should guide these efforts to ensure that digital advancements strengthen both state and individual sovereignty.

Sovereignty and International Relations

Sovereignty, a contested concept akin to religion or art (Gallie, 1956), is evolving amidst advancing international relations. While states and governments remain central, international law has progressed to tackle global challenges, despite occasional conflicts (Klabbers, 2021). International collaboration—encompassing civil society, technical standards, industry coalitions, and multi-stakeholder partnerships—plays a critical role in building consensus and driving voluntary initiatives. Entities like ICANN, which governs digital domain names, wield significant economic, social, legal, and democratic influence while adhering to national and international laws.

Sovereignty hinges on internal and external legitimacy (Biersteker, 2012). Internal legitimacy arises when citizens recognize governmental authority, while external legitimacy depends on recognition by other states. Sovereignty encompasses three core elements requiring governance:

Fundamental Sovereignty: The authority to govern, rooted in democratic institutions ensuring free elections and effective public services.

Territorial Sovereignty: Control over physical and digital assets, including geographic resources, demographics, cultural values, and digital identities. Institutional Sovereignty: The framework of economic, social, and democratic structures that sustain state functionality.

These elements underpin both internal and external legitimacy, shaped by power dynamics within and between states. Democratic governance must balance authoritative control with individual autonomy to maintain legitimacy. The concept of "territory" extends beyond physical borders to include resources and assets unique to a state. These encompass natural resources, cultural heritage, demographics, and digital assets like national digital identities and health data. Territorial sovereignty requires both internal authorization (citizen consent) and external validation (recognition by other states). In the digital realm, assets such as domain names and data flows are governed by entities like ICANN, highlighting the need for international cooperation to manage borderless technologies.

Governments often seek extraterritorial jurisdiction to assert control over digital assets, a practice that can spark international disputes (Klabbers, 2021, pp. 106–108). The rise of digital technologies complicates territorial sovereignty, as cloud-based services and transnational networks challenge traditional boundaries. Internal legitimacy links state sovereignty to individual sovereignty, though the two often conflict. When states regulate personal domains—such as health, thoughts, or social choices—within a democratic framework, tensions arise. The COVID-19 pandemic exemplified this, as some citizens viewed state-imposed restrictions as infringements on personal liberties, questioning governmental legitimacy. The regulation of information flows between citizens and the state, particularly through digital citizen identities, further complicates this dynamic. Digital identities, while enhancing governance, raise concerns about privacy and state overreach.

Sovereignty in the Digital Age

Digital technologies amplify the complexities of sovereignty. They enable global collaboration but also challenge state authority by transcending borders. The legitimacy of state actions, both domestically and internationally, depends on balancing control over digital assets with respect for individual autonomy. For instance, data localization policies aim to assert sovereignty but risk stifling innovation or clashing with global standards.

Sovereignty's evolution demands adaptive governance. States must strengthen democratic institutions, foster international partnerships, and regulate digital technologies to preserve legitimacy. This includes ensuring transparent information flows and protecting digital citizen identities while respecting personal freedoms.

Table 1. Illustrative Uses of AI Tools by Public and Private Governors

Domain	Governor	Instrumental Power	Structural Power	Discursive Power
Violence	*Public*	Weapons systems	Mass surveillance	Legitimating violence
	Private	Cyber strikes	Spyware	Crime/terrorism perceptions
Markets	*Public*	Economic revenues	Weaponized interdependence	Neoliberal preferences
	Private	Investments	Monopoly rents	AI hype perceptions
Rights	*Public*	Law enforcement	Risk profiling	Rights consciousness
	Private	Worker quantification	Automation	Surveillance capitalism

Table 2. Illustrative Uses of AI Agents and Three Faces of Power

Domain	Instrumental Power	Structural Power	Discursive Power
Violence	Lethal autonomous weapons	Dehumanization of violence	Hidden violence
Markets	High-frequency trading	Computing resource concentration	Illusion of neutral AI
Rights	AI adjudicated rights	AI personhood claims	Technical rationality claims

(Source: SSRN- AI, Global Governance, and Digital Sovereignty Swati Srivastava∗1 and Justin Bullock2,3,4

1Political Science, Purdue University 2Bush School of Government & Public Service, Texas A&M University

3Convergence Analysis 4Global Governance Institute Draft: Wednesday 23rd October, 2024)

Conclusion:

The rapid advancement of Artificial Intelligence (AI) is reshaping state interactions and citizen relationships, presenting significant challenges to state sovereignty. AI's borderless nature and potential for autonomous decision-making threaten traditional notions of governmental authority, territorial control, and institutional legitimacy. To safeguard sovereignty while harnessing AI's benefits, states must collaborate on responsible AI development and governance. This involves establishing regulations,

promoting transparency, ensuring equitable benefit distribution, and investing in research and development (R&D)

Recommendations:

- International collaboration is essential to establish a consensus on the legal and ethical implications of AI. The collaboration must entail the establishment of standards and regulations that safeguard state sovereignty against the advancement of AI.
- Promoting transparency, accountability, and adherence to human rights must be a priority for both parties.
- Non-state actors and governments must collaborate to guarantee the responsible development and utilization of AI technology.
- Inclusive AI development must encompass a variety of stakeholders, including civil society organizations.
- The academic realm and the private sector. This will facilitate the equitable allocation of AI advantages and avert an Erosion of authority over the political, social, and economic spheres of member states.

References:

1. Ahmadi, M. and Bullock, J. (2023). Government procurement and acquisition: Opportunitiesand challenges presented by artificial intelligence and machine learning. Technical report, IBM Business of Government.
2. Paul Trimmers, Sovereignty in the digital age, Introduction to digital humanism, https://doi.org/10.1007/978-3-031-45304-5
3. Kello, L. (2017). The virtual weapon and international order.
4. Keohane, R., & Nye, J., Jr. (2011). Power & interdependence (4th ed.). Pearson.
5. Klabbers, J. (2021). International law (3rd ed.). Cambridge University Press.
6. Gallie, W. B. (1956). Essentially contested concepts. Proceedings of the Aristotelian Society, 56, 167–198.
7. Biersteker, T., (2012). State, sovereignty and territory. In Handbook of international relations. Sage Publications Ltd. Especially recommended for the issue of sovereignty.
8. Hazrat Usman The Future of State Sovereignty in the Age of Artificial Intelligence Journal of Law & Social Studies (JLSS) Volume 5, Issue 2, pp 142-152- DOI: 10.52279/jlss.05.02.142152.