

 Cite this article as: Sharifi Poor Bgheshmi, M. S., & Sharajsharifi, M. (2025). Managing the Crisis: AI and the Demise of National Sovereignty? *Journal of World Sociopolitical Studies*, 9(4), 853-886. <https://doi.org/10.22059/wsps.2025.396021.1522>

Managing the Crisis: AI and the Demise of National Sovereignty?^{*}

Mohammad Sharif Sharifi Poor Bgheshmi¹, Mahsa Sharajsharifi²

1. M.A in Civil Engineering-Structural Engineering, Islamic Azad University, Gheshm, Iran (Mohammad.sharifi@ut.ac.ir)  0009-0006-4437-4989
2. M.A. in Architectural Engineering, Islamic Azad University, North Tehran Branch, Iran (mahsa.sharajsharifi@ut.ac.ir) (Corresponding Author)  0009-0006-8053-5313

(Received: Apr. 05, 2025 Revised: Jun. 03, 2025 Accepted: Jul. 21, 2025)

Abstract

This study investigates the evolving crisis of national sovereignty in the context of artificial intelligence and the expanding power of transnational technology corporations. Drawing from over thirty peer-reviewed academic and policy sources published between 2018 and 2025, this paper critically examines how traditional concepts of sovereignty—particularly data, digital, technological, and normative sovereignty—are being redefined by global AI infrastructures and the algorithmic authority of private firms. Employing a qualitative, interdisciplinary methodology grounded in law, political theory, and ethics, the research reveals growing asymmetries between state authority and corporate influence over digital infrastructures, data governance, and regulatory norms. Our findings highlight divergent policy responses, including efforts to reassert sovereign control through data localization, the pursuit of strategic autonomy, and emerging international cooperation frameworks. The study also evaluates normative debates surrounding legitimacy, democratic oversight, and algorithmic accountability. The study concludes that sovereignty in the AI era must be reconceptualized beyond territorial jurisdiction to include infrastructural and ethical dimensions, necessitating hybrid governance models that integrate states, civil society, and corporations, while prioritizing democratic legitimacy and public interest.

Keywords: Algorithmic Power, Artificial Intelligence Governance, Data Localization, Digital Sovereignty, Transnational Technology Firms

^{*} The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in this manuscript.

Journal of World Sociopolitical Studies | Vol. 9 | No. 4 | Autumn 2025 | pp. 853-886

Web Page: <https://wsps.ut.ac.ir/> Email: wsps@ut.ac.ir

eISSN: 2588-3127

PrintISSN: 2588-3119

This is an open access work published under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0), which allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use (<https://creativecommons.org/licenses/by-sa/4.0/>)



1. Introduction

The concept of national sovereignty, long anchored in territorial integrity and juridical independence, is undergoing unprecedented stress in the digital era. The rapid expansion of AI and the consolidation of power by transnational technology corporations have introduced structural disruptions that challenge the authority of states to govern data, infrastructure, and algorithmic systems within their borders. At the core of this crisis is a reconfiguration of sovereignty itself, now contoured not solely by geography or public law, but by control over digital infrastructures and the capacity to define normative frameworks for AI governance. Governments increasingly find their legislative and regulatory efforts constrained by the infrastructural dominance and global reach of private firms such as Google, Meta, Amazon, and Microsoft, whose algorithmic systems operate across jurisdictions with limited public oversight or democratic accountability (Zuboff, 2019; Kelton et al., 2022).

This study critically examines the evolving discourse on sovereignty in the age of AI, with a specific focus on the contested dynamics between state authority and corporate influence. It explores how various forms of sovereignty—data, digital, technological, and normative—are being redefined in response to the infrastructural power and normative ambitions of global technology platforms. The analysis is situated within an interdisciplinary framework that draws on legal theory, political science, ethics, and international relations. It interrogates whether the legal and normative tools traditionally employed by states remain adequate to assert democratic control over AI-driven systems and transboundary data flows, or whether new paradigms are required to address these shifts.

By synthesizing insights from more than thirty peer-reviewed

sources and policy analyses, the study identifies core tensions that underpin the current sovereignty crisis: the extraterritoriality of digital governance, asymmetries in public and private power, and the erosion of democratic legitimacy in algorithmically mediated societies. The analysis also assesses various proposed policy responses, including data localization measures, strategies aimed at achieving strategic autonomy, multilateral governance approaches, and regulatory models grounded in human rights principles. In doing so, the research aims to clarify the conditions under which sovereignty can be meaningfully reasserted in the digital age—or whether the concept itself must be fundamentally reconceptualized.

2. Methodology

This study adopts a qualitative, interpretive methodology grounded in an extensive literature review of peer-reviewed academic articles, policy reports, and institutional analyses spanning the fields of digital governance, international law, political theory, and artificial intelligence ethics. The research employs a critical hermeneutic approach to evaluate how various conceptualizations of sovereignty—namely data, digital, technological, and normative sovereignty—are being challenged and redefined by the proliferation of AI and the global influence of transnational technology firms. Textual analysis was conducted on over thirty scholarly and policy sources published between 2018 and 2025, selected through purposive sampling to ensure topical relevance and disciplinary diversity. The sources were systematically coded for recurring themes such as jurisdictional conflicts, state-corporate power asymmetries, and regulatory responses to platform capitalism. This method allowed for a multi-perspectival mapping

of the evolving discourse, emphasizing contested interpretations of sovereignty and identifying normative tensions between democratic governance and algorithmic authority. The methodology is inherently interdisciplinary, drawing insights from law, political science, ethics, and international relations to construct an integrative framework suitable for analyzing the crisis of sovereignty in the AI era.

3. Findings

The findings presented in this section synthesize a wide-ranging body of academic and policy literature that addresses the reconfiguration of national sovereignty under the influence of artificial intelligence and the expanding authority of transnational technology corporations. Rather than offering a source-by-source summary, the analysis identifies recurrent themes and contrasts among governance models, normative justifications, and geopolitical strategies. Across diverse jurisdictions and disciplines, the reviewed materials reveal a convergence on the erosion of state control over digital infrastructures, coupled with diverging interpretations of what digital sovereignty entails and how it should be reclaimed or redefined. This section is structured to foreground key conceptual shifts, explore thematic clusters in the literature, and elucidate areas of consensus, conflict, and unresolved tension regarding the future of sovereignty in the AI age.

Woods (2018) explored the complex legal and geopolitical tensions surrounding national sovereignty over digital data, particularly in the context of cross-border internet governance. He examined a body of emerging case law that he termed “data-sovereignty litigation”, encompassing disputes where national

governments and large internet firms clash over regulatory authority, jurisdiction, and compliance with domestic laws. Examples include Google's resistance to global enforcement of Europe's "right to be forgotten", Microsoft's challenge to U.S. government attempts to access emails stored overseas, and litigation concerning the extraterritorial application of takedown or delisting orders.

Woods (2018) argued that these disputes reveal a central jurisdictional dilemma: how courts can respect one state's sovereign interest in governing internet activity within its borders without infringing upon the sovereignty of others. He posited that comity—a legal principle of mutual respect among sovereigns—offers a framework for navigating these tensions. Contrary to common assumptions, he contended that comity doctrines do not categorically prohibit extraterritorial jurisdiction; rather, they frequently enable it by recognizing the legitimacy of foreign sovereign interests, especially when no global governance mechanism is in place.

As a solution, Woods (2018) advocated for a policy of "sovereign deference", urging courts to balance competing sovereign claims pragmatically rather than defaulting to internet exceptionalism or isolationism. He further called for coordinated approaches across legislative, executive, and judicial domains, warning that failure to accommodate sovereign claims could lead states to forcibly localize data and assert control over internet infrastructure—threatening global connectivity, innovation, and rights.

Latonero (2018) proposed a human rights-based framework for the governance of AI, emphasizing the need to align AI

development and deployment with globally recognized human dignity principles. He argued that, although AI systems are capable of great social benefit, they already present risks to fundamental rights—including nondiscrimination, equality, political participation, privacy, and freedom of expression. Notably, the report critiqued the de facto sovereignty of technology companies over digital infrastructure, highlighting how Big Tech's algorithmic systems can infringe on rights across jurisdictions without adequate regulatory oversight.

While not focused solely on national sovereignty in the traditional sense, the report critically assessed the inability or unwillingness of states to assert sovereign authority over AI impacts on their populations. It called for states to fulfill their duty to protect rights in national AI strategies and regulations, thereby reasserting a form of normative digital sovereignty grounded in international human rights law.

To address these challenges, Latonero (2018) offered several actionable recommendations. These included conducting Human Rights Impact Assessments (HRIAs) throughout the AI lifecycle, fostering cross-sector collaboration to operationalize rights in technical design, and advocating for global governance structures (e.g., through the UN) that reflect shared human dignity values. The report also highlighted the role of civil society, academia, and intergovernmental organizations in monitoring AI systems and promoting accountability mechanisms, especially in contexts where national governance is insufficient or co-opted.

In the *Spotlight on Sustainable Development 2019* report, Alemany & Gurumurthy (2019) express a critical view of the erosion of national sovereignty over data, particularly in light of the growing influence of transnational digital corporations. The report

argues that current regulatory and institutional frameworks are inadequate to safeguard civic, political, economic, and cultural rights from being undermined by opaque algorithmic systems controlled by private actors. The report emphasizes the need for governments to reclaim regulatory authority and ensure that digital governance serves the public interest rather than being dictated by corporate agendas. It warns against the dominance of platform companies in data ownership and AI development, portraying these entities as assuming quasi-sovereign roles over digital infrastructure and decision-making.

In terms of proposed solutions, the report advocates for a paradigm shift in global digital governance. It calls for stronger regulatory frameworks at the national level to address rights violations, enforce accountability, and realign data and AI governance with international human rights standards. Importantly, it argues for a multilateral, human rights-based approach to digital governance under the auspices of the United Nations, with inclusive participation that resists corporate capture. Specific policy tools include mandating data sharing with public agencies for essential services, enforcing digital rights, and advancing the communitization of the digital realm to ensure that data governance is not merely driven by market logic, but is rooted in democratic accountability and social justice.

Timmers (2019) analyzed the ethical and strategic implications of AI and cybersecurity in the context of national sovereignty and strategic autonomy. He observed that sovereignty is increasingly under threat due to digital transformation, rising cyber incidents, and global geopolitical tensions. Timmers (2019) framed this challenge through three policy responses—risk management, strategic partnerships, and the global common good—and

examined how each approach intersects with ethical concerns and national sovereignty.

In the risk management model, states attempt to mitigate threats to critical infrastructures through AI-enabled detection and resilience. However, Timmers (2019) highlighted ethical dilemmas related to surveillance, algorithmic opacity, and loss of human agency, as well as the political cost of failing to ensure national legitimacy and security.

The strategic partnership approach emphasizes cooperation among like-minded states and firms to retain control over key digital technologies. This includes ethically aligned initiatives like Europe's GAIA-X cloud infrastructure. Timmers (2019) discussed the emerging role of "strategic ethics", whereby ethical standards (such as the EU's AI guidelines) may double as geopolitical tools, potentially viewed as barriers to trade or sovereignty.

The global common good model, while less widely adopted, advocates treating cyberspace as a shared resource governed by inclusive, international norms. According to Timmers, this requires overcoming institutional and technical challenges, but presents a compelling alternative to sovereignty-based fragmentation. He proposed that states prioritize AI tools that uphold privacy, transparency, and distributed control. Timmers (2019) concluded that sovereignty in the AI era is not only about control, but legitimacy, and that ethical governance frameworks are essential to preserving democratic values, while managing cyber risks.

Zuboff (2019) introduced the concept of *surveillance capitalism* to describe a novel economic logic, in which private companies claim ownership over behavioral data derived from individuals' digital activities. She argued that this model represents

a significant usurpation of democratic sovereignty, as dominant tech firms (notably Google, Facebook, and Microsoft) unilaterally appropriate personal data without meaningful consent, process it through proprietary AI systems, and monetize predictive analytics for profit. In doing so, they accumulate a form of *instrumentarian power*—a new mode of governance through algorithmic influence, behavioral modification, and control of digital infrastructure.

In Zuboff's (2021) view, these corporate practices constitute a “coup from above” against both individual autonomy and democratic institutions. She described how states have failed to regulate or even fully comprehend the depth of this privatized data regime, effectively allowing companies to operate as *extra-democratic sovereigns* that set their own norms for data use, surveillance, and algorithmic decision-making. This results in a fundamental erosion of the state's ability to fulfill its responsibilities to protect citizens' rights, ensure transparent governance, and maintain epistemic authority in the public sphere.

Zuboff (2021) did not advocate for co-sovereignty with Big Tech. Instead, she called for a comprehensive regulatory rebuke akin to the antitrust responses to industrial monopolies in the 20th century. Her solutions included banning the commercial trade in personal data, establishing democratic oversight of algorithmic systems, reinforcing legal rights to privacy and data self-determination, and reclaiming the digital commons for public benefit. She emphasized that true digital sovereignty must be grounded in democratic rule-making, not in corporate dominance or technical capability.

Aktoudianakis (2020) assessed the European Union's (EU) evolving strategy to establish digital sovereignty, presenting it as a

central pillar of broader strategic autonomy. The paper argued that Europe's overreliance on foreign technologies—particularly in data infrastructure, AI, cloud services, and 5G networks—has compromised its ability to assert sovereignty over data generated within its borders. This dependency undermines privacy protections, creates vulnerabilities in public infrastructure, and allows dominant non-EU technology firms to act as *de facto* data sovereigns.

The EU's response, according to the report, should rest on three strategic pillars: (1) Bracing—reducing dependencies and strengthening technological resilience; (2) Empowering—removing internal market barriers, investing in SMEs, digital skills, and data infrastructure; and (3) Engaging—leveraging the EU's regulatory power to shape global rules for digital technologies. Key policy initiatives include the Digital Services Act, Digital Markets Act, and the Data Governance Act, all intended to rein in excessive “data power” of Big Tech and promote fairer competition.

A notable solution proposed is the Gaia-X initiative, a European cloud infrastructure project aimed at enhancing sovereignty over data storage and processing. The report also stressed the importance of interoperable “Common European Data Spaces”, public funding for digital innovation, and the creation of a European digital identity. While supporting global cooperation, the paper emphasized that such engagement must occur on terms defined by European values and interests, not those of foreign corporate actors.

Wood et al. (2020) explored the evolving and contested landscape of digital sovereignty by analyzing its interpretation and implications for states, enterprises, and citizens. It defined digital sovereignty as the ability to exert control over digital assets—such

as data, digital infrastructure, and content—and framed it as a multidimensional issue shaped by surveillance concerns, technological dependency, online harms, and economic interests.

The report found that states interpret digital sovereignty differently. For example, China enforces a tightly controlled digital ecosystem under its concept of cyber-sovereignty, while the U.S. favors an open internet with multistakeholder governance, and though its CLOUD Act, extends jurisdiction over global data held by U.S. firms. Countries like France, Germany, India, and Brazil occupy intermediate positions, advocating for stronger domestic control, data localization, and regulatory frameworks like the GDPR and national AI strategies to assert sovereignty while fostering innovation.

Beyond state actors, the report emphasized enterprises' concern with data control and legal compliance, coining the term “enterprise data sovereignty” to describe firms' strategies for managing and monetizing proprietary data. Meanwhile, citizens and civil society increasingly demand personal data sovereignty, advocating for greater transparency, consent, and accountability, particularly in the wake of scandals such as Snowden and Cambridge Analytica.

To address these overlapping claims, the report warned of increasing internet fragmentation and legal conflict unless multilateral approaches can be forged. It called for interoperable, rights-based regulatory frameworks that balance national interests, private sector innovation, and citizen rights across jurisdictions.

Feijóo et al. (2020) critically examined the geopolitical tensions and sovereignty dilemmas arising from the global race for AI dominance. The paper highlighted that AI is reshaping national

power structures, and driving what the authors termed a “new industrial revolution”, with significant risks of global fragmentation driven by techno-nationalism and protectionism. States, especially the U.S., China, and the EU, are pursuing divergent strategies reflecting their institutional values and strategic goals—ranging from market-driven models to state-led techno-socialism.

The authors argued that this AI arms race exacerbates digital sovereignty concerns, particularly for states lacking domestic AI capacity. They warned that such states risk becoming “data colonies”—dependent on foreign firms and infrastructures that control data processing, storage, and analytics. These dynamics threaten national sovereignty by enabling digital platforms to act as transnational actors with greater *de facto* control than some governments.

As a response, the paper introduced the concept of “new technology diplomacy”—a multi-stakeholder, polycentric model of international AI governance. It called for inclusive, cross-border cooperation focused on shared human rights, safety standards, and ethical AI deployment. Key proposed mechanisms included global norms for AI safety, transparent governance of data flows, ethical AI principles, and coordinated policy dialogues. The authors emphasized that preventing abusive or fragmented governance regimes requires collaborative engagement between states, corporations, and civil society, ideally culminating in a flexible, international AI governance charter.

Bauer and Erixon (2020) critically assessed the European Union's evolving narrative on technology sovereignty, arguing that its current trajectory risks conflating strategic autonomy with protectionism. The paper defined technology sovereignty as the EU's capacity to independently influence digital and technological

developments in line with its economic and societal values. However, the authors warned that some interpretations—particularly those pushed by France and Germany—tend toward state-led industrial policy and digital protectionism, which may fragment the Single Market and impair competitiveness.

The report acknowledged legitimate concerns around dependence on foreign technologies and the need for greater European capacity in areas like cloud infrastructure, data governance, and AI. However, it challenged the idea that Europe should pursue technological independence through subsidized national champions or exclusionary data policies. Notable critiques were leveled against the Gaia-X initiative and data localization policies, which the authors argued would do little to enhance resilience and more to stifle innovation by duplicating already functional global solutions.

Instead, Bauer and Erixon (2020) proposed a model of “technological openness with sovereignty”—advocating for regulatory harmonization within the EU, stronger integration of the Single Market, investment in human capital and digital infrastructure, and strategic partnerships with trusted global allies (e.g., the U.S. and OECD countries). They concluded that Europe's real path to sovereignty lies not in erecting digital barriers, but in scaling innovation and regulatory excellence across borders to influence global norms.

Timmers (2021) critically examined the evolving tensions between AI, national sovereignty, and democratic values. He argued that AI poses both opportunities and threats to state sovereignty, especially concerning the legitimacy of public service delivery, internal and external recognition, and the preservation of

democratic institutions. The article highlighted that while AI can bolster state capacity—for example, in cybersecurity and predictive public service applications—it can also lead to erosion of trust in governance when applied without accountability or fairness, as demonstrated in case studies from Austria, the UK, and the Netherlands. In these instances, AI systems embedded discrimination or produced unreliable outputs, undermining the state’s legitimacy.

Timmers (2021) emphasized that sovereignty over data and AI technologies is increasingly contested, particularly as global tech corporations shape norms and values through investment and lobbying. He pointed to the EU’s proposed AI Act as a regional response that categorizes AI risks and attempts to assert normative sovereignty, notably through proposed bans on mass surveillance and facial recognition in public spaces. Nevertheless, he acknowledged that such legal mechanisms face practical limitations due to the rapid and opaque evolution of AI systems.

To address these sovereignty concerns, Timmers (2021) proposed a multifaceted approach: enhancing end-to-end accountability and transparency in AI systems, fostering international cooperation to govern AI ethically, and integrating technical, legal, and societal measures to ensure democratic oversight. He concluded that maintaining sovereignty in the AI era requires reconciling technological development with the evolving social constructions of democracy and law.

Roumate (2021) investigated the evolving notion of sovereignty in the age of AI, emphasizing how traditional state-centered sovereignty is being contested by powerful transnational technology corporations. The paper distinguished among data sovereignty, cyberspace sovereignty, and technological

sovereignty—arguing that these forms are becoming essential to understanding geopolitical power in the digital era. Data sovereignty, as defined by UNESCO, refers to the right of states to regulate data generated within their territories. Cyberspace sovereignty extends legal and political autonomy to the digital realm, while technological sovereignty encompasses a state's capacity to independently access, develop, and govern critical technologies, including AI.

Roumate (2021) contended that the COVID-19 pandemic accelerated the entrenchment of AI in all aspects of societies, thereby intensifying competition between states and big tech firms over control of digital infrastructures and data. She emphasized that the goals of states (peace and security) diverge from those of corporations (profit), necessitating a recalibration of international public law and ethical governance frameworks. The article critiqued the dominance of big tech in shaping digital norms, and called for clearer definitions and international consensus on key terms like “digital sovereignty”.

As a response to these sovereignty challenges, Roumate (2021) advocated for multilevel strategies: national policies to ensure data protection and democratic integrity, regional efforts, such as the EU's single data market initiative, and global frameworks like UNESCO's draft recommendation on AI ethics. She concluded that effective governance of AI must recognize and integrate transnational corporate actors into international regulatory structures, while reinforcing the ethical and legal authority of states.

Elms (2021) examined the increasingly prominent global discourse around digital sovereignty, exploring how national efforts

to assert control over digital data intersect with broader economic and geopolitical dynamics. The report defined digital sovereignty as a government's claim to jurisdictional authority over the data generated within its territory, and analyzed the policy implications of this stance across Asia-Pacific countries, the European Union, and major economies like India and China.

The study emphasized that the push for data sovereignty is often framed as a response to under-regulated digital environments and the perceived dominance of foreign tech firms over domestic digital infrastructures. While intended to promote privacy and security, such regulations frequently take the form of data localization, cross-border data restrictions, and expanded governmental access to user data. Elms (2021) argued that, despite their protective aims, these policies often serve as *de facto* protectionist tools, benefiting domestic firms at the expense of foreign competitors and open digital trade.

The paper critiqued this trajectory as potentially counterproductive, particularly for smaller or less technologically advanced countries, which may lack the infrastructure or technical expertise to comply with or benefit from restrictive data regimes. Conversely, larger markets like China and India may be better positioned to absorb the economic costs, while leveraging digital sovereignty to boost domestic industries. As a solution, Elms (2021) urged a careful balance between the desire for national autonomy and the economic necessity of cross-border data flows. She concluded that uncoordinated digital sovereignty measures risk fragmenting the global internet, raising compliance burdens, and exacerbating global digital inequality.

Aaronson (2021) analyzed how growing claims of national data sovereignty are reshaping global data governance and digital trade.

She argued that countries such as China, India, and increasingly the U.S. and EU are asserting sovereignty over data under the justification of protecting national security, promoting economic development, and securing individual rights. However, Aaronson (2021) warned that these assertions can often lead to state overreach, lack of reciprocity, and fragmentation of the global digital economy.

The paper provided detailed case studies on India, China, and the U.S., illustrating different rationales for sovereign data control—ranging from social stability and human rights (India) to state supremacy over corporate data holdings (China) and national security (U.S.). In many cases, governments exempt themselves from the very privacy protections they impose on private actors, undermining trust and consistency.

Aaronson (2021) critiqued the absence of enforceable global norms, noting that while many digital trade agreements endorse free cross-border data flows, they include broad “public policy” exceptions. These loopholes enable governments to assert sovereignty, while circumventing interoperability or shared standards. The paper concluded that unilateral approaches to data control risk suppressing the generativity and public benefits of data, especially when data is hoarded or withheld from collaborative use.

To address these tensions, Aaronson (2021) proposed several solutions: strengthening multilateral cooperation through forums like the WTO, OECD, and APEC; developing a model law under UN auspices to harmonize cross-border data governance; and encouraging transparent, rights-based data policies that prioritize the public good over national or corporate self-interest.

Moerel and Timmers (2021) offered a detailed exploration of the multifaceted concept of digital sovereignty, arguing that it extends beyond state control over digital systems and data to encompass strategic autonomy in economic, societal, and democratic dimensions. They identified three primary threats to digital sovereignty: dependence on a few dominant foreign technology providers, rising cybersecurity threats, and extraterritorial legal claims from foreign powers (e.g., through the U.S. CLOUD Act). The authors highlighted that European states, particularly the Netherlands, increasingly lack autonomous control over cloud infrastructure, data storage, and critical AI applications, putting national security and democratic integrity at risk.

The study presented digital sovereignty as involving control not only over the data itself, but also over the infrastructures and standards through which data flows. This includes the resilience of cyber-physical systems, the control of economic ecosystems (especially in areas like AI and quantum computing), and the maintenance of public trust in democratic institutions. Moerel and Timmers (2021) discussed cases such as the GAIA-X cloud project, the NIS Directive, and European e-ID systems to illustrate existing gaps in the EU's ability to enforce digital sovereignty.

As a solution, the paper proposed stronger integration and central coordination at both national and EU levels. It advocated for a designated national digital affairs coordinator, improvements in EU treaties to expand sovereignty-related competences, as well as investments in secure, interoperable, and sovereign-by-design digital infrastructure. The authors concluded that digital sovereignty should be operationalized as strategic autonomy that supports democratic governance and national resilience in an increasingly interconnected and contested digital world.

Kelton et al. (2022) explored the concept of "virtual sovereignty", focusing on the growing infrastructural power of U.S.-based digital platforms and its implications for state sovereignty. The article argued that major tech firms—such as Google, Meta, Amazon, and Microsoft—have amassed sovereign-like authority by controlling the digital stack: the layers of software, hardware, data infrastructure, and networked services that mediate nearly all online interactions. These platforms exercise “extractive” and “transformative” power, traditionally associated with the state, shaping public opinion, social behavior, and even geopolitical influence through algorithmic control and data commodification.

The authors described how U.S. digital platforms construct and manage a vast array of global physical infrastructures (e.g., undersea cables, satellites, cloud services), enabling them to command critical data flows and connectivity. They warned that this infrastructural dominance challenges the U.S. state's ability to regulate these actors, weakening its traditional capacities to secure national interests and project global influence. This shift creates a form of sovereignty decoupled from legal recognition or democratic legitimacy, grounded instead in the commercial logic of platform capitalism.

Although the article does not prescribe concrete policy solutions, it highlights the urgent need for reasserting state control over the digital realm, noting the inadequacy of existing antitrust and data protection measures. The authors called for critical rethinking of sovereignty, legitimacy, and infrastructural power in light of the profound transformations wrought by digital capitalism and its potential to outstrip traditional state authority.

Usman et al. (2023) examined the multifaceted challenges that AI poses to traditional conceptions of state sovereignty, emphasizing the disruptive effects of AI across legal, economic, security, and geopolitical domains. The authors traced the evolution of sovereignty from the Peace of Westphalia to the present, framing it as the foundational principle of international relations. They argued that AI-enabled technologies—such as autonomous weapons, predictive algorithms, and digital surveillance tools—are increasingly transcending territorial borders, thereby eroding the state's monopoly on authority and control.

The paper offered a nuanced view, acknowledging that AI both challenges and reinforces state sovereignty. On the one hand, AI empowers non-state actors and global technology firms to wield influence previously reserved for states, undermining traditional legal and political authority. On the other hand, AI is also deployed by states to bolster internal governance, particularly through surveillance, border control, and predictive decision-making. The authors discussed how these dynamics are reshaping national security paradigms and altering global power structures.

As a solution, the authors emphasized the importance of international cooperation in developing legal and ethical standards for AI. They advocated for inclusive governance frameworks involving states, civil society, and the private sector to ensure accountability, transparency, and the protection of fundamental rights. The paper concluded by calling for the creation of globally accepted norms to regulate AI in a manner that preserves democratic values and reinforces legitimate sovereignty.

Roberts et al. (2023) examined the interplay between digital sovereignty, digital expansionism, and the feasibility of global AI governance. They analyzed how these geopolitical trends influence

the development of international AI regulatory frameworks. The authors conducted a comparative case study focusing on China, the European Union (EU), and the United States (US), evaluating each region's approach to digital sovereignty and expansionism. Their findings indicate that the extraterritorial nature of policies and competitive narratives, especially from the US, may hinder effective global cooperation on AI governance. Nonetheless, the study identifies emerging areas of potential alignment, such as data governance and technical standards, which could serve as foundational elements for building trust in multilateral forums like the G20 or the United Nations.

Fischer (2023) provided an in-depth legal analysis of the relationship between national data sovereignty and e-governance, examining how varying legal frameworks shape the operation and security of digital government systems. The article defined data sovereignty as the principle that data is governed by the laws of the country in which it resides, highlighting the tensions this creates in a globalized digital environment. The author argued that while data sovereignty is essential for ensuring national security, economic competitiveness, and individual privacy, it also poses challenges for cross-border data flows and international cooperation.

Through comparative case studies of jurisdictions including the European Union, the United States, China, India, Brazil, and Russia, Fischer (2023) illustrated the diversity of approaches to data regulation. These ranged from stringent data localization laws (e.g., China and Russia) to more fragmented or open regimes (e.g., the U.S.). Each model presented trade-offs between national control and operational efficiency in e-governance. For instance, strict localization bolsters security, but may hinder innovation,

while lenient regimes facilitate global integration, but risk weakening sovereign oversight.

The article proposed several legal and policy recommendations to navigate these tensions. Key among them were the harmonization of international legal standards, adoption of adaptive national laws that keep pace with emerging technologies (e.g., AI, blockchain, and cloud computing), and stronger protections for citizen rights through comprehensive data protection and cybersecurity laws. Fischer concluded that effective e-governance in the digital age hinges on a dynamic legal architecture that upholds national sovereignty while accommodating global data interdependence.

Roumate (2024) examined the transformation of sovereignty in the age of AI, focusing on the mounting tension between state authority and the influence of transnational technology corporations. The chapter differentiated between technological, digital, and data sovereignty, presenting them as emerging pillars of political autonomy that are increasingly threatened by the growing power of big tech. Technological sovereignty was described as a state's ability to independently access, develop, and control critical technologies without external dependency, while data and digital sovereignty pertain to control over data flows and digital infrastructures, respectively.

The chapter argued that the competitive dynamic between states and corporations for dominance over these sovereignties has intensified, particularly as big tech's role in shaping global digital infrastructure and AI development outpaces that of many governments. Roumate (2024) highlighted how this imbalance poses risks to democratic governance and international legal norms, framing it as a form of "digital dictatorship". In response, she

advocated for a reassessment of international public law and a reinforcement of ethical AI governance structures that prioritize human rights and state-led accountability over corporate profit motives.

Ultimately, Roumate (2024) called for a recalibration of the global order to reassert the normative role of states in governing AI technologies. She emphasized that while corporations may lead technological development, the responsibility for ensuring peace, security, and ethical compliance must remain with states and international institutions.

Chen (2024) provided a comprehensive analysis of the emerging concept of AI sovereignty, emphasizing its increasing importance as nations seek to assert control over artificial intelligence technologies amidst rapid global proliferation. The article defined AI sovereignty as a state's right to regulate and direct AI development, deployment, and governance within its borders in alignment with national values, interests, and laws. Drawing parallels with cyber sovereignty, the study explored six key connotations of AI sovereignty: control over AI development and deployment, data sovereignty, economic competitiveness, national security imperatives, ethical and cultural dimensions, and technological independence.

Chen (2024) conducted a critical analysis of the debates surrounding AI sovereignty, highlighting key tensions between national autonomy and the need for global cooperation. The study underscored concerns about the rise of technological protectionism and the potential for sovereignty-driven approaches to infringe upon human rights and privacy. A central issue identified was the risk that rigid assertions of sovereignty could obstruct international collaboration, lead to fragmented AI governance, and deepen global

disparities in access to AI resources, skilled personnel, and technological infrastructure. To address these issues, the article proposed a multifaceted international governance framework. Core recommendations included fostering multilateral cooperation and standard-setting, implementing transparency and accountability mechanisms, developing ethical guidelines with strong human rights protections, and establishing platforms for technology transfer and capacity building. Additionally, the article emphasized the need for effective dispute resolution and enforcement protocols to support the legitimacy and functionality of global AI governance structures.

Chen (2024) concluded that while AI sovereignty is a legitimate and necessary goal, it must be balanced with global solidarity and ethical integrity to ensure a fair and sustainable AI future for all nations.

Gu (2024) examined the evolving dynamics between Big Tech corporations and state sovereignty in the digital era. The study posited that major technology firms have emerged as *de facto* data sovereigns, leveraging their vast data repositories and computational capabilities to influence global affairs and challenge traditional notions of state authority. These corporations not only disseminate their values and ideologies, they also play a significant role in international relations, effectively transforming into new forms of Leviathans.

The article argued that the unprecedented access and control over data by Big Tech firms have led to a deconstruction of conventional sovereignty concepts. This shift has resulted in a complex symbiotic relationship between states and technology companies, wherein governments must navigate the dual realities of reliance on these firms for technological advancement and the need to maintain regulatory control. The study highlighted the

tension between the exclusivity of state sovereignty and the transnational operations of Big Tech, emphasizing the challenges in asserting traditional sovereign powers in the face of borderless digital influence.

Gu (2024) concluded that the rise of Big Tech necessitates a re-evaluation of sovereignty frameworks, urging policymakers to consider new governance models that address the unique challenges posed by digital platforms. The article called for a balanced approach that recognizes the technical advantages of Big Tech, while safeguarding the principles of state sovereignty and democratic accountability.

Roberts (2024) introduced a normative framework for interpreting digital sovereignty, particularly in relation to artificial intelligence, by reframing it from a descriptive focus on control to a principle-based emphasis on legitimate authority. He argued that while various actors—including states, corporations, and others—compete for dominance over digital technologies, such control should be assessed in terms of legitimacy, specifically, whether it is supported by public consent and aligned with broader societal values. Drawing on the example of Big Tech firms' dominance in AI development, Roberts illustrated how these companies function as quasi-sovereigns due to their substantial influence over digital infrastructure, algorithms, and data. However, he contended that despite their considerable power, these entities often lack both input legitimacy (such as democratic engagement and transparency) and output legitimacy (such as equitable public outcomes and accountability). This legitimacy deficit raises ethical concerns about their authority and challenges the validity of their sovereign claims. To address this, Roberts (2024) called for an approach to digital sovereignty that includes states, private

companies, and civil society, but holds each actor accountable to normative criteria of legitimacy. He proposed mechanisms such as third-party audits, improved transparency, and participatory governance to close the “legitimacy gap”. The goal is to develop governance structures that are responsive, inclusive, and reflective of public interest—ensuring digital control serves democratic rather than corporate imperatives.

Ofilu et al. (2024) addressed the growing significance of data sovereignty within the U.S. national security strategy, emphasizing the role of cloud innovation in enhancing cybersecurity and digital warfare readiness. The article defined data sovereignty as the assertion of legal and jurisdictional control over data, particularly data stored or processed within national borders. It highlighted the strategic importance of retaining national control over digital infrastructures in the face of adversarial cyber operations, foreign surveillance, and global legal asymmetries.

The authors identified the challenges posed by multinational cloud infrastructures, where cross-border data flows complicate regulatory enforcement. To counter this, they advocated for the deployment of sovereign cloud frameworks—cloud infrastructures that enforce strict domestic legal control and integrate advanced encryption, real-time monitoring, and Zero Trust security models. These frameworks aim to reduce jurisdictional conflicts and protect sensitive data from foreign access.

The paper also emphasized the integration of AI-driven threat intelligence systems capable of real-time anomaly detection and predictive analysis. Coupled with offensive cyber capabilities, these systems enable proactive defense and cyber deterrence. In addition to proposing quantum-safe encryption and automated attack surface reduction, the authors stressed the strategic need for

public-private partnerships and regulatory clarity to ensure interoperability, compliance, and innovation.

Ultimately, the study called for a cohesive national policy framework that balances sovereign control with collaborative global cybersecurity norms. The authors concluded that securing U.S. digital sovereignty is critical not only for national defense, but also for maintaining strategic advantage in the emerging landscape of AI-augmented cyber warfare.

Dezeure et al. (2024) presented a provocative argument that digital sovereignty—particularly for the European Union (EU)—cannot be achieved without strategic cooperation with Big Tech firms. The article framed digital sovereignty as control over national digital infrastructures, critical data, and AI systems, which is presently undermined by Europe's dependency on a few dominant U.S. cloud and AI providers (notably Amazon, Microsoft, and Google). These corporations control the vast majority of European data and infrastructure, contributing to vendor lock-in, reduced interoperability, and external influence over democratic institutions.

Rather than proposing traditional regulatory responses, the authors advocated for a counterintuitive solution: embracing Big Tech as partners in safeguarding digital sovereignty. They called for the EU and U.S. governments to initiate self-regulatory dialogues with Big Tech to implement default baseline cybersecurity measures across digital infrastructures. This includes automated patching, encrypted data management, secure configurations, and telemetry-based threat detection—offered by default rather than as premium services. The goal is to leverage Big Tech's scale and resources to protect all users, including under-resourced sectors, thereby increasing systemic cyber resilience.

The authors acknowledged potential drawbacks: reinforcing Big Tech monopolies, increased dependency, and legal liability concerns. Nonetheless, they argued that the benefits of this cooperative model—greater cybersecurity, reduced inequality in digital capabilities, and more effective cyber defense—outweigh these risks. Their proposal positioned Big Tech not as adversaries of sovereignty, but as essential co-guardians of secure digital ecosystems.

George (2025) critically examined how the escalating geopolitical race between the United States and China for AI supremacy undermines consumer data privacy and reconfigures notions of sovereignty. The study highlighted how both nations have prioritized the advancement of national AI champions—such as OpenAI’s ChatGPT and DeepSeek’s Xiao-Ice—by permitting aggressive and often opaque data harvesting practices. George (2025) documented that major AI systems collect expansive personal information, including behavioral metadata, browsing histories, and biometric inputs, often without informed user consent. The research demonstrated that while Chinese models like DeepSeek are disproportionately scrutinized in Western discourse, American counterparts engage in similarly intrusive data collection under the guise of innovation and national security.

The paper argued that both governments have strategically aligned with corporate actors, enabling data accumulation to further national interests in AI development. Legal and regulatory frameworks in both regimes, such as China’s Cyber Security Law and the U.S. Consumer Privacy Bill, were critiqued for offering generous carve-outs that prioritize technological advancement over individual rights. George (2025) observed that this convergence on surveillance-oriented data policies blurs the line between

democratic and authoritarian approaches to digital governance, effectively marginalizing citizen agency.

As a policy response, the paper advocated for a rebalancing of AI innovation imperatives with stronger consumer protections. Proposed solutions included enforcing transparent data governance, creating interoperable yet privacy-preserving AI infrastructures, and encouraging participatory policymaking that centers on individual rights rather than institutional control. George (2025) concluded that redefining technological leadership in terms of ethical governance and global equity is critical to preventing the normalization of mass surveillance as the price of progress.

4. Discussion and Conclusion

The literature reviewed converges on a central insight: sovereignty in the AI age can no longer be understood solely through the lens of territorial jurisdiction or legal authority. Instead, it must be reconceptualized as a hybrid construct encompassing infrastructural control, normative legitimacy, and geopolitical strategy. This reconceptualization is essential to address the growing asymmetries between state power and the algorithmic governance capacities of transnational technology corporations.

Thematically, the scholarship clusters around three dominant models of governance. First, state-centric regulatory sovereignty is typified by efforts to reclaim control through legal instruments such as data localization, digital services legislation, and national AI strategies. Studies from Fischer (2023), Aktoudianakis (2020), and Ofili et al. (2024) articulate how states attempt to operationalize sovereignty by securing domestic data infrastructure, enforcing jurisdictional authority, and enhancing cybersecurity. These

approaches emphasize strategic autonomy, but often risk fragmenting the digital commons and obstructing global interoperability.

Second, multilateral and normative frameworks highlight sovereignty as a function of democratic legitimacy, human rights adherence, and participatory governance. Authors such as Latonero (2018), Roberts (2024), and Chen (2024) argue that algorithmic systems must be subject to ethical scrutiny and collective oversight that transcends national borders. Their vision promotes AI governance rooted in shared values, transparency, and legitimacy, suggesting that sovereignty must be earned through normative alignment rather than asserted through coercive control. This approach converges with calls for “technology diplomacy” (Feijóo et al., 2020) and global AI governance charters that treat AI as a transnational common good.

Third, platform-based and infrastructural sovereignty reflects the shifting power locus from states to corporations. Zuboff’s (2019) account of “surveillance capitalism” and Kelton et al.’s (2022) theory of “virtual sovereignty” underscore the structural influence of platform firms over digital infrastructure, data flows, and epistemic authority. While some scholars, such as Dezeure et al. (2024), propose pragmatic collaboration with Big Tech to enhance systemic cybersecurity, others—most notably Zuboff (2019) —warn that such cooperation risks legitimizing corporate rule and eroding democratic agency. The tension between these perspectives reveals a profound epistemological divide: whether Big Tech should be treated as adversarial sovereigns or indispensable partners.

Geopolitically, the sources diverge in how sovereignty is asserted across regions. The EU positions itself as a normative regulator, the U.S. oscillates between market liberalism and

strategic protectionism, and China enforces a statist model of digital authoritarianism (Wood et al., 2020; Roberts, Hine & Floridi, 2023). This heterogeneity hampers global cooperation, raising the specter of a “splinternet” divided by competing sovereignty regimes. At the same time, common ground exists: many authors recognize the inevitability of interdependence and call for coordinated regulatory standards that reconcile national autonomy with global functionality.

Unresolved tensions persist. Legal efforts to assert sovereignty—such as through the CLOUD Act or GDPR—frequently conflict with technological realities of cloud computing and cross-border data exchange. Ethical aspirations toward inclusive governance are undermined by resource asymmetries and enforcement gaps. Calls for democratization of AI systems must contend with entrenched monopolies and opaque algorithms. Furthermore, sovereignty claims are often co-opted for nationalist or protectionist purposes, challenging the balance between local control and universal rights.

References

- Aaronson, S. A. (2021). *Data is Disruptive: How Data Sovereignty is Challenging Data Governance*. Hinrich Foundation. <https://www.hinrichfoundation.com/research/wp/digital-technology/data-is-disruptive>
- Aktoudianakis, A. (2020). *Fostering Europe's Strategic Autonomy: Digital Sovereignty for Growth, Rules and Cooperation*. European Policy Centre & Konrad-Adenauer-Stiftung. <https://www.epc.eu/en/publications/Fostering-Europes-Strategic-Autonomy--A-new-Agenda-for-Trade-and-Inv~357f50>

- Aleman, C., & Gurumurthy, A. (2019). Governance of Data and Artificial Intelligence. In *Spotlight on Sustainable Development 2019* (pp. 86–94). Global Policy Forum. [https://www.2030spotlight.org/en/book/1730/chapter/v-governance-data-and-artificial-intelligence:contentReference\[oaicite:0\]{index=0}](https://www.2030spotlight.org/en/book/1730/chapter/v-governance-data-and-artificial-intelligence:contentReference[oaicite:0]{index=0})
- Bauer, M., & Erixon, F. (2020). *Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls*. ECIPE Occasional Paper (No. 02/2020). <https://hdl.handle.net/10419/251089>
- Chen, Y. (2024). *AI Sovereignty: Navigating the Future of International AI Governance*. Philpapers. <https://philpapers.org/rec/CHEASN-2>
- Dezeure, F., Moerel, L., & Webster, G. (2024). Digital Sovereignty Is Impossible Without Big Tech. *Atlantisch Perspectief*, 48(1), 30–35. <https://www.jstor.org/stable/10.2307/48761751>
- Elms, D. (2021). *Digital Sovereignty: Protectionism or Autonomy?*. Hinrich Foundation. <https://www.hinrichfoundation.com/research/wp/digital-technology/digital-sovereignty-protectionism-or-autonomy/>
- Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing Artificial Intelligence (AI) to Increase Wellbeing for All: The Case for a New Technology Diplomacy. *Telecommunications Policy*, 44(6), 101988. <https://doi.org/10.1016/j.telpol.2020.101988>
- Fischer, A. (2023). Data Sovereignty and E-Governance: The Legal Implications of National Laws on Digital Government Systems. *Legal Studies in Digital Age*, 2(4), 1–12. <https://jlsda.com/index.php/jlsda/article/view/39/41>
- George, A. S. (2025). AI Supremacy at the Price of Privacy: Examining the Tech Giants' Race for Data Dominance. *Partners Universal Innovative Research Publication*, 3(1), 26–42. <https://doi.org/10.5281/zenodo.14909763>

- Gu, H. (2024). Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*, 29(15), 591–612. <https://doi.org/10.1007/s11366-023-09855-1>
- Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual Sovereignty? Private Internet Capital, Digital Platforms and Infrastructural Power in the United States. *International Affairs*, 98(6), 1977–1999. <https://doi.org/10.1093/ia/iiaa226>
- Latonero, M. (2018). *Governing Artificial Intelligence: Upholding Human Rights and Dignity*. Data & Society. <https://datasociety.net/library/governing-artificial-intelligence>
- Moerel, L., & Timmers, P. (2021). *Reflections on Digital Sovereignty*. EU Cyber Direct. <https://ssrn.com/abstract=3772777>
- Ofil, B. T., Ezeadi, S. C., & Jegede, T. B. (2024). Securing U.S. National Interests with Cloud Innovation: Data Sovereignty, Threat Intelligence and Digital Warfare Preparedness. *International Journal of Science and Research Archive*, 12(1), 3160–3179. <https://doi.org/10.30574/ijrsra.2024.12.1.1158>
- Roberts, H. (2024). Digital Sovereignty and Artificial Intelligence: A Normative Approach. *Ethics and Information Technology*, 26(4), Article 70. <https://doi.org/10.1007/s10676-024-09810-5>
- Roberts, H., Hine, E., & Floridi, L. (2023). Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance. In M. Timoteo, B. Verri, & R. Nanni (Eds.), *Quo Vadis, Sovereignty?* (pp. 51–75). Springer. https://doi.org/10.1007/978-3-031-41566-1_4
- Roumate, F. (2021). Ethics on AI and Technological Sovereignty. *Communication. Media. Design*, 6(4), 139–151. <https://cmd-journal.hse.ru/article/view/13766/13406>

- Roumate, F. (2024). AI and Technological Sovereignty. In *Artificial Intelligence and the New World Order* (pp. 59–65). Frontiers of Artificial Intelligence, Ethics and Multidisciplinary Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-50312-2_5
- Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, 29(4), 635–645. <https://doi.org/10.1007/s11023-019-09508-4>
- Timmers, P. (2021). AI Challenging Sovereignty and Democracy. *Turkish Policy Quarterly*, 20(4), 45–55. https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias3959692&context=SearchWebhook&vid=32KUL_KUL:Lirias&search_scope=lirias_profile&adaptor=SearchWebhook&tab=LIRIAS&query=any,contains,staffnr_u0147461&sortby=date&offset=0
- Usman, H., Nawaz, B., & Naseer, S. (2023). The Future of State Sovereignty in the Age of Artificial Intelligence. *Journal of Law & Social Studies*, 5(2), 142–152. <https://doi.org/10.52279/jlss.05.02.142152>
- Wood, S., Hoffmann, S., McFadden, M., Kaur, A., Wongsaroj, S., Schoentgen, A., Forsyth, G., & Wilkinson, L. (2020). *Digital Sovereignty: The Overlap and Conflict between States, Enterprises and Citizens*. Plum Consulting & Oxford Information Labs. <https://plumconsulting.co.uk/publications/digital-sovereignty>
- Woods, A. K. (2018). Litigating Data Sovereignty. *The Yale Law Journal*, 128(2), 328–406. <https://www.jstor.org/stable/45389445>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
- Zuboff, S. (2021). The Coup We Are Not Talking About. *The New York Times*. <https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html>