

Digital Sovereignty and the Reconstruction of State Power in the Era of Generative AI: An Interpretation Based on the Reconstruction of State Capacity

Jinxin Qu

Zhongnan University of Economics and Law, Wuhan, China
389409223@qq.com

Abstract. The rapid development of generative artificial intelligence is driving a shift in the logic of power competition among states. The established judgment that digital technology would weaken state capacity has not been verified in practice. Instead, countries have reconsolidated their presence in the digital space through the institutional arrangements of "digital sovereignty". On the one hand, generative artificial intelligence provides new technological carriers and capacity support for foreign exchanges; on the other hand, it introduces new risk variables into the national security system. This study argues that data, algorithms and computing power, as core strategic resources in the era of artificial intelligence, are highly dependent on the institutional environment and cannot be effectively allocated by the market mechanism alone, which provides intrinsic motivation for the state to re-engage in digital governance. In this sense, digital sovereignty is not only an extension of the sovereignty principle in the digital field, but also an institutional channel for reshaping state capacity. Based on the theoretical framework of state capacity, this paper examines how changes in the structure of digital resources promote state re-engagement and how this process drives the reconstruction of state capacity, so as to explain the evolution logic of state power in the era of generative artificial intelligence.

Keywords: digital sovereignty, generative artificial intelligence, state capacity, technological competition, data governance

1. Introduction

Over the past two decades, a prevailing judgment has existed in digital politics research: internet technology, due to its transnational mobility and decentralized nature, would exert a weakening effect on state power and push toward a trend of "denationalization". From the late 1990s to the early 2000s, Western academia represented by American scholars held optimistic expectations, believing that the internet could promote the free flow of information, dissolve traditional national borders and accelerate globalization. In 1996, John Barlow argued in *A Declaration of Cyberspace* that governments have no substantive meaning within cyberspace. Such views treat technology as a depoliticized neutral tool, yet ignore the power structure and interest distribution embedded in the process of technology application.

Since the rise of generative artificial intelligence, a gap has emerged between this theoretical presupposition and reality. In recent years, the United States has incorporated artificial intelligence into its national security strategy framework and implemented chip export control measures. The European Union has adopted the *Artificial Intelligence Act*, seeking to build a regulatory system through risk classification. China has continuously improved its institutions in data security and algorithm governance, and successively enacted laws including the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law. Meanwhile, multiple countries have put forward policy concepts such as "digital sovereignty" and "data sovereignty" one after another. Judging from these developments, the state has not withdrawn from the digital space, but re-entered it in new institutional forms. The United States keeps increasing the weight of artificial intelligence in its national security strategy; the European Union advances digital governance based on a risk-oriented regulatory approach; China builds an institutional framework for data governance through legislation, and promotes the development of artificial intelligence on this basis.

The arena of great power competition has shifted to the digital space. The logic of competition unfolds along two parallel tracks: technological breakthroughs and rule-making. The question thus arises: as technological globalization deepens, why has state power not been weakened, but instead strengthened through the mechanism of digital sovereignty? International competition in the field of artificial intelligence reflects both technological contests and changes in the global power structure. From the perspective of state capacity, this paper proposes an analytical framework. Data, algorithms and computing power constitute strategic resources; changes in their structure drive the state to re-engage, ultimately realizing the institutionalization of digital sovereignty and the reconstruction of state capacity.

2. Structure of digital resources and state re-engagement

Data, algorithms and computing power form the foundational resources of generative artificial intelligence. Their common features are high institutional dependence and infrastructure attributes, making it impossible for them to be fully allocated spontaneously by the market mechanism.

2.1. Strategic attributes of core resources

Although data is called "the oil of the new era", its strategic value surpasses that of traditional oil resources. As an information resource, data concerns national security, economic development and governance capacity. The acquisition and distribution of data resources are uneven, and this imbalance further shapes a new pattern of competition among states.

Algorithms are more than technical tools; they are also carriers of power. Algorithms filter, rank, recommend and make decisions on information, directly affecting social cognition, public opinion trends and resource allocation. After the emergence of generative artificial intelligence, the influence of algorithms has expanded further, and their role has shifted from information screeners to content producers.

The development of artificial intelligence relies on computing power support at the material level. The level of computing power determines the degree of artificial intelligence development, and also relates to national industrial competitiveness and technological security.

2.2. Necessity of state re-engagement

Data, algorithms and computing power involve national security, public interests and infrastructure construction. It is difficult to allocate these resources effectively through the market mechanism alone, so the state has once again become the core actor in digital governance [1]. Both data and algorithms have the attributes of public goods and private goods. Their externalities make it hard for the market to balance public interests, requiring the state to coordinate through legal, regulatory and policy tools. On this basis, industrial policies in key areas such as chips and artificial intelligence have been continuously strengthened, aiming to enhance long-term technological capacity and national security rather than pursue short-term market gains.

2.3. Institutionalization of digital sovereignty

Digital sovereignty redraws the state's boundaries in the digital space through legal and policy systems, enabling the state to exercise institutionalized management over data flow, algorithm operation and computing power layout [2]. As algorithmic power keeps expanding, countries have incorporated digital sovereignty into their national strategies. The main paths include fostering independent and controllable artificial intelligence technological capabilities, strengthening supervision of cross-border data flow, and improving algorithm governance rules.

The institutionalization of digital sovereignty is reflected in three dimensions. The technical dimension involves key technology research and development, standard setting and supply chain security building. The regulatory dimension includes the improvement of laws and regulations, the construction of regulatory systems and the improvement of law enforcement mechanisms. The organizational dimension covers the establishment of digital governance institutions, the promotion of international cooperation and the development of capacity building. The core of standard competition is rule competition, and the ownership of technical standard-setting power will shape the future direction of the digital order.

3. Four-dimensional reconstruction of state capacity

3.1. Resource organization capacity

The state needs to reintegrate scattered digital resources and bring data, algorithms and computing power into a unified governance framework. Sovereignty in the physical world takes territory as its core carrier, while the digital world is constituted by technological elements rather than territory. The distribution of technological elements shows marked inequality.

The distribution characteristics of data resources determine the difficulty of integration. Data sources are relatively scattered, involving different actors such as government departments, enterprises, social organizations and individuals. Data formats are also inconsistent, lacking unified standards and interface specifications. There are also disputes over how to define data ownership. Some scholars propose that data rights can be split into three separate components—ownership right, use right and usufruct—for separate normative design [3].

The integration of computing power resources needs to take into account multiple factors such as geographical distribution, energy supply and network conditions. In recent years, multiple countries have launched national-level computing infrastructure construction, improving the allocation efficiency of computing power resources through overall planning, so as to strengthen the foundational support for artificial intelligence development.

3.2. Risk governance capacity

Artificial intelligence brings risks such as algorithmic bias, data leakage and information manipulation, and the state must establish a new governance system. Generative artificial intelligence has large-scale data collection capabilities and can acquire all kinds of information over a wide range. If diverted for other purposes without protective measures, it will undermine the security foundation of national data sovereignty.

Traditional risk governance usually responds after problems occur. Risks in the era of artificial intelligence are more complex, requiring the risk identification link to move further forward [4]. The EU *Artificial Intelligence Act* classifies artificial intelligence applications into four categories according to risk level: unacceptable risk, high risk, limited risk and low risk, and implements differentiated supervision for each category. Artificial intelligence technology is highly professional, so regulatory authorities need to continuously improve their professional capabilities and build a more scientific and systematic governance system.

3.3. Technological autonomy capacity

The focus of artificial intelligence competition is shifting to chips, large models and basic software capabilities. A state's external dependence on technology has become a strategic risk. Chips are the foundational support for artificial intelligence development. Large model capability reflects a country's innovation level in the field of artificial intelligence.

Supply chain security is also an important part of state capacity building. The global supply chain is undergoing restructuring, and countries are continuously strengthening the layout of key technologies to enhance industrial chain resilience. Technological autonomy does not mean closed development, but seeks a balance between open cooperation and security and controllability. It is necessary to maintain international cooperation while reducing the risk of being constrained by others in key areas.

3.4. International rule-shaping capacity

Artificial intelligence governance is entering the stage of rule competition. The power to set standards and design governance frameworks is becoming a new source of power. International rules not only affect the development direction of artificial intelligence technology, but also relate to a country's discourse power in the global digital governance system.

As digital governance deepens, international competition has expanded from technological competition to rule competition. Actively participating in international standard setting, improving the capacity for international institutional supply, and enhancing participation in global governance constitute important components of state capacity building in the digital age.

4. Empirical observation: the practical development of digital sovereignty

4.1. Data dimension

Countries strengthen data boundary management through data localization, restrictions on cross-border flow and data classification. The European Union has established a strict data protection system based on the GDPR, which has given rise to the "Brussels effect" and exerted extensive influence on international data governance rules. Centered on the Data Security Law and the Personal Information Protection Law, China has established a classified and graded data governance

system, promoting digital economy development while ensuring data security. The institutional differences between different governance models have led to a certain degree of fragmentation in the global digital space.

4.2. Algorithm dimension

Algorithm governance has risen from an internal management issue of enterprises to a national regulatory agenda. Model filing, algorithm review and generated content supervision are being gradually incorporated into the digital governance system. Digital technologies such as artificial intelligence and the metaverse are being used by countries as tools for geopolitical competition, and their influence has expanded to political, economic, social and national security fields [5]. China has set up an algorithm filing mechanism, with relevant systems including the *Provisions on the Administration of Algorithmic Recommendation in Internet Information Services*, and the generative artificial intelligence governance system is also being continuously improved.

4.3. Computing power dimension

Computing power infrastructure has been incorporated into the national industrial capacity system, involving links such as chip manufacturing, energy supply and data center layout. At present, high-end chip manufacturing capacity is concentrated in a small number of countries and enterprises, and the trend of supply chain concentration has intensified international competition and security risks. Around the chip industry and computing infrastructure construction, countries keep strengthening policy support to promote a safer and more stable foundation for artificial intelligence development.

5. Transformation of the logic of state competition

In traditional international relations, competition among states mainly revolved around factors such as natural resources, population and capital. After entering the digital age, the focus of competition has gradually shifted to digital resources such as data, algorithms and computing power, and the way state power is generated has changed accordingly.

Data, algorithms and computing power are the core factors of production in the digital age. Compared with traditional resources, these factors have stronger replicability, higher mobility and more prominent economies of scale. Countries with advantages in data resources, algorithm capabilities and computing infrastructure are more likely to build competitive edges in the digital economy and artificial intelligence, and translate such advantages into comprehensive national strength.

Against the background of deepening resource competition, the power to make rules has become the core of state competition. Dominating technical standards, rule design and international agenda setting is the key for a country to gain an upper hand in the future digital order. Rule competition has become a higher-level form of competition above resource competition. Digital sovereignty is the core mechanism connecting the technological system and state power. Through the construction of the digital sovereignty system, the state can improve digital governance capacity and international competitiveness.

6. Conclusion

The development of generative artificial intelligence has pushed state power competition into a new stage. This paper holds that digital sovereignty is not a mere technical governance tool, but a

mechanism for state capacity reconstruction. Data, algorithms and computing power have become new strategic resources, and the state participates in digital space governance through legal systems, industrial policies and governance systems.

State capacity is embodied in four dimensions: resource organization, risk governance, technological autonomy and international rule-shaping. Digital sovereignty strengthens the state's institutional control over digital resources and drives the evolution of governance capacity toward the digital age. At present, artificial intelligence competition has shifted from purely technological competition to a parallel pattern of resource competition and rule competition. Digital sovereignty is the institutional foundation for the state to safeguard security, promote innovation and participate in global governance, and also a key variable in the reconstruction of the global digital order.

The era of artificial intelligence has not weakened state power; it has only changed its organizational form and operation mechanism. With the continuous evolution of technology in the future, the interaction between digital sovereignty and state capacity will be further deepened, and balancing technological innovation, security governance and international cooperation will become the core issue.

References

- [1] Zhang, J. (2024). Reflections and prospects on the embedding of generative AI into digital government construction: From the perspective of strong artificial intelligence. *Research on Financial and Economic Issues*, (7), 36–47. DOI:10.19654/j.cnki.cjwtyj.2024.07.003.
- [2] Liu, H. (2025). What is data sovereignty? A perspective of elastic sovereignty in the global digital rule game. *Journal of Peking University (Philosophy and Social Sciences)*, 62(6), 115–126.
- [3] Chen, M., Li, Q., & Gao, Y. (2026). Distribution of data factors: Theoretical analysis, international practice and institutional innovation. *Research on Financial and Economic Issues*, (4), 20–37. DOI:10.19654/j.cnki.cjwtyj.2026.04.002.
- [4] Wu, P. (2025). Identification and regulation of criminal risks of artificial intelligence. *Journal of Political Science and Law*, 42(4), 52–61.
- [5] Huang, R., & Yao, H. (2023). A reshaped world? New features of artificial intelligence and national security amid the rise of ChatGPT. *Journal of International Security Studies*, 41(4), 82–106+158–159. DOI:10.14093/j.cnki.cn10-1132/d.2023.04.004.