Paradigm Academic Press
Studies in Social Science & Humanities
ISSN 2709-7862
MAR. 2026 VOL.5, NO.2

The Origin, Objectives, and Challenges of the European Union's Concept of Digital Sovereignty

Changjie Chen[1] & Shukun Zhang[1]

[1] Shanghai University of Political Science and Law, Shanghai 201701, China

Correspondence: Changjie Chen, Shanghai University of Political Science and Law, Shanghai 201701, China.

doi:10.63593/SSSH.2709-7862.2026.03.003

Abstract

Against the backdrop of intense strategic competition between China and the United States and the profound restructuring of global digital governance, the European Union (EU) has proposed the concept of "digital sovereignty" to seize strategic initiative and safeguard its core interests. The EU's digital sovereignty emerged from a position of relative digital incapacity, manifesting strategic anxiety under the dual pressure of two technological superpowers, as well as internal digital fragmentation. At its core, it emphasizes a trinity of technological autonomy, data autonomy, and institutional autonomy. Guided by this vision, the EU has developed a multi-layered strategy that integrates internal and external policies across multiple institutional circles. This includes a "digital single market" strategy as the inner core, the General Data Protection Regulation (GDPR) and the Gaia-X project as pioneering regulatory instruments in the middle circle, and the European Chips Act and Artificial Intelligence Act as specialized initiatives on the outer edge. However, the construction of EU digital sovereignty faces severe domestic coordination hurdles due to the internal "digital divide" among member states, alongside a strategic dilemma of "de-dependence vs. re-dependence" under US-China competition. Ultimately, the EU's endeavors represent a novel attempt at building sovereignty in the digital era by a regional integration organization, offering critical insights and points of reference for global digital governance and China's own digital sovereignty strategies.

Keywords: European Union, digital sovereignty, global digital governance, US-China-EU competition

1. Introduction

In 2017, French President Emmanuel Macron delivered a speech at the Sorbonne University titled "Initiative for Europe: A Sovereign, United, and Democratic Europe," where he first put forward the concept of a "Sovereign Europe." One of the critical paths to achieving "European Sovereignty" was identified as leading the global digital transformation and promoting a governance model that combines digital innovation with strict regulation worldwide. Following the institutional transition of the European Commission in 2019, "digital transformation" became one of the two core policy pillars initiated by the new Commission led by Ursula von der Leyen, alongside the "green transition" which itself heavily relies on digital infrastructure. In the official documents of previous Commissions, the term "sovereignty" was rarely mentioned due to its inherent logical tension with the process of European regional integration. However, since the von der Leyen Commission took office, this landscape has changed significantly. The word "sovereignty" has witnessed an exponential increase in frequency across various policy texts, and derivative concepts such as "technological sovereignty," "data sovereignty," and "digital sovereignty" have emerged sequentially, becoming central keywords in the EU's governance discourse. As the core hallmark of the modern nation-state since the Westphalian system in 1648, the sudden resurgence of "sovereignty" as the EU's new policy favorite is by no means accidental. It represents both a deep strategic reassessment of the EU's self-positioning and development path in its integration process, and a proactive choice to pursue strategic autonomy and defend its core interests amid the prominent backdrop of US-China strategic

competition. Therefore, a systematic examination of the theoretical core, practical trajectories, and development dilemmas of EU digital sovereignty can not only accurately grasp its essence and evolutionary logic, but also provide critical reference and insights for strategic alignment, risk management, and international cooperation in China's own digitalization process.

2. The Context and Origin of EU Digital Sovereignty

In 1996, John Perry Barlow, a famous American hacker and digital rights advocate, published his monumental "A Declaration of the Independence of Cyberspace" at the Davos Forum, stating: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." At that time, cyberspace, as an emerging sphere of human activity, was highly anticipated to shake off physical constraints and fulfill the ideal of absolute liberty. Network sovereignty was deemed impossible because the internet could directly bypass traditional mechanisms of state control. However, much like the broader transition from idealism to realism within international relations theory, cyberspace gradually revealed its darker facets. Proliferating issues such as cyber fraud, online harassment, and massive data breaches made people in the 21st century realize that digital space is not a detached utopia, but a domain deeply rooted in physical infrastructure. Without robust normative guidelines, catastrophic events threatening human survival and societal order are inevitable. The three-dimensional characteristics of digital space—namely the immediacy of virtual interaction, the boundlessness of data flows, and the transnational nature of infrastructure—confront states not only with the challenge of maintaining exclusive jurisdiction, but also with the necessity to re-establish their authority and positioning in a highly interconnected, blurry-bounded ecosystem.

The EU recognized as early as the mid-1990s that cyberspace was not a lawless terra nullius, but a novel public sphere requiring public authority and regulatory governance. It proactively categorized cyberspace within the scope of public governance under state jurisdiction and drafted matching regulatory instruments. In 1995, the EU enacted the Data Protection Directive (Directive 95/46/EC), marking the first regional consolidation of basic principles for personal data protection, effectively extending the right to privacy into the digital domain. It unified rules across member states regarding data collection, processing, and cross-border transfers. However, because digital infrastructure and regulatory capacities were still in their infancy and distinct national "digital borders" had not fully materialized, regulations during this period remained largely framework-oriented and principled. Specifically, early EU cyberspace governance focused on rights recognition and risk prevention rather than structured institutional layouts for cross-border data routing, platform liabilities, or comprehensive cybersecurity, leaving concrete legislative execution to individual member states. The Directive utilized a harmonized legislative model and advocated independent data protection authorities, which offered strong advantages in safeguarding data subjects' rights but occasionally compromised data liquidity and market efficiency. Nevertheless, against the backdrop of rapid technological iterations and an expanding digital economy, the normative digital philosophies pioneered by the EU in privacy and data protection inevitably generated global ripples, a phenomenon deeply structurally rooted in the EU's geopolitical configuration.

2.1 Inadequacy of Domestic Digital Capacities

The exposure of the NSA's "PRISM" program revealed that the United States government had been systematically wiretapping European political leaders, followed by WikiLeaks disclosures that the US had monitored French presidents over extended periods. In 2021, Danish media exposed that the NSA utilized Denmark's defense intelligence pipelines to access domestic networks between 2012 and 2014, intercepting text messages and call logs of senior officials from Germany, France, Norway, and Sweden. Leaked US military intelligence in 2022 further confirmed ongoing surveillance targeting global leaders and allies, including UN Secretary-General António Guterres, the South Korean President, the Israeli Prime Minister, and the Ukrainian President. This persistent series of wiretapping scandals underscored a sobering reality for the EU: its critical communication nodes and data infrastructures had long been dependent on American tech conglomerates. Concurrently, the EU faced the continuous intrusion of US extraterritorial "long-arm jurisdiction" and structural inconsistencies between US and European privacy frameworks. This double pressure squeezed the EU out of competitive spaces in cross-border data flows and digital security, rendering its sovereign digital walls fragile. This vulnerability in political, economic, and security terms serves as the primary realistic imperative driving the EU to accelerate its digital sovereignty strategies.

2.2 Strategic Anxiety Intensified by US-China Competition

Amidst the global restructuring of the digital economy and technological governance systems, the digital order anchored by the United States and the meteoric rise of China's digital economy have formed a double-squeeze scenario, trapping the EU in a profound fear of marginalization. Backed by first-mover technical advantages and transnational platform monopolies, the US has long dictated global digital rules. Currently, American tech giants like Google, Microsoft, Amazon, and Apple command the apex of the global internet value chain, possessing the

richest data assets, most expansive consumer markets, and most potent digital capabilities. Conversely, China has leveraged its late-mover advantages to cultivate domestic internet titans, seizing vanguard status in specific advanced technology segments. In sharp contrast, the EU finds itself a "toddler" in digital market capitalization but a "giant" in data regulation. Positioned on the periphery of the commercial digital economy, the EU hosts virtually no massive proprietary digital platforms, accounting for a meager 4% of the market value of the world's 70 largest digital platforms (while the US and China command 90%). However, it excels at defining legislative boundaries. The EU continuously projects the "Brussels Effect" in digital regulation, whereby its unilateral market rules become de facto global standards through compliance by multinational entities seeking market access. By establishing digital sovereignty, the EU aims to forge an independent path between the US and China, asserting itself as the third pole in global tech governance to avoid subjection in the digital age.

2.3 Fragmentation of the Internal Digital Market

As the world's most sophisticated regional integration organization, the EU suffers from severe systemic fragmentation within its internal digital domain, which severely hampers its collective digital economy and sovereign cohesion. Articulating digital rules has historically been fragmented: member states enacted disparate data protection, platform regulation, and digital tax laws tailored to localized interests and asymmetric developmental stages. Even following the execution of the General Data Protection Regulation (GDPR), which harmonized data protection rules, pronounced national variations persist regarding digital service oversight, ethical AI frameworks, and cross-border data flow mechanisms. Furthermore, owing to lagging digital infrastructure investments in certain member states that fall below vanguard international benchmarks, the EU has struggled to solidify an integrated, open, and massive unified digital market, prompting an urgent demand for centralized harmonization.

3. The Conceptual Triad of Digital Sovereignty

Although digital sovereignty has risen to become the cornerstone of the EU's contemporary policy agenda, it has lacked a singular, universally codified official definition. In September 2020, Thierry Breton, the EU Commissioner for Internal Market, observed that "European digital sovereignty is based on three inseparable pillars: computing power, control over data, and secure connectivity," emphasizing that "Europe must now take its strategic destiny into its own hands to protect its sovereignty. In an increasingly competitive world, the battle for autonomy is in full swing. Faced with the 'tech war' waged by the US and China, Europe must lay the foundations for its sovereignty for the next 20 years." Synthesizing the EU's institutional practice and governance logic, the concept of digital sovereignty can be deconstructed into three interconnected, progressive dimensions that collectively form its sovereign architecture:

First, Technological Autonomy. This demands that the EU possesses the capabilities to independently develop, deploy, and utilize critical digital technologies, thereby mitigating the monopolistic dominance of American and Chinese tech conglomerates. This requires escalating R&D investments, incubating domestic technological innovation ecosystems, and commanding the discourse on technical standards, ensuring that the EU retains control over its developmental path rather than suffering strategic bottlenecks caused by external supply dependencies.

Second, Data Autonomy. The core objective is to master data, the fundamental production factor of the digital economy. This entails dictating who determines how data flows, how it is processed and commercialized, and how security architectures are configured. Through legislative frameworks, the restriction of cross-border data transfers, and the creation of localized European data spaces, the EU seeks to shield internal data assets from leakages, illegal commercial exploitation, or unauthorized foreign state access, thereby protecting its economic and security interests.

Third, Institutional Autonomy. This reflects the EU's capability to independently formulate digital governance rules and construct regional regulatory architectures rooted in its normative values. The EU seeks to align internal digital rules, dissolve fragmented institutional barriers, and export its regulatory models globally, carving out global digital rules aligned with its interests and securing dominant discourse power in international standard-setting bodies.

4. Policies and Implementation Pathways of EU Digital Sovereignty

To translate these conceptual goals into practice, the EU has engineered a multi-layered, comprehensive policy framework spanning macro strategic roadmaps to micro legislative acts, covering internal market integration and local technical cultivation. The underlying policy logic is to "dismantle before building, while cultivating internal strength and external reach." On one hand, it seeks to eliminate internal fragmentation and external technological dependencies; on the other, it aims to construct digital governance rules and technological systems that serve its own strategic interests.

4.1 The Digital Single Market Strategy

Launched in 2015, the Digital Single Market (DSM) strategy constitutes the foundational architecture of EU digital sovereignty. By facilitating the free movement of data and services and dismantling technical standard barriers among member states, the strategy aims to establish a unified, open internal digital market. On this basis, consolidating resources to amplify the overall competitiveness of the European digital economy serves as the primary task, laying the economic foundation for digital sovereignty.

The DSM strategy rests on three primary pillars: first, ensuring the free movement of digital services by harmonizing e-commerce rules, copyright protections, and consumer safety standards, enabling digital enterprises to operate seamlessly across all member states; second, ensuring the free flow of non-personal data by removing localized data localization barriers while implementing unified data protection rules to balance commercial flows with individual privacy; third, accelerating digital technology innovation and deployment by standardizing network criteria, investing heavily in digital infrastructure, and fostering a region-wide innovation ecosystem.

4.2 The General Data Protection Regulation (GDPR)

Entering into force in 2016, the General Data Protection Regulation (GDPR) represents a crowning achievement in the EU's pursuit of data autonomy, standing as the world's most stringent and influential data protection framework. Its central tenet dictates that personal data is strictly prohibited from arbitrary cross-border export. Beyond saddling data controllers with rigorous obligations and introducing astronomical fines for non-compliance, the regulation features expansive extraterritorial jurisdiction. Through this architecture, the EU created a comprehensive codification of data privacy, effectively exporting its normative privacy values globally to serve as the baseline compliance architecture for global data governance.

The implementation of GDPR has triggered profound global ripples. By January 2023, out of 194 countries globally, more than 130 had enacted dedicated data and privacy protection legislation. Approximately 57% of Asian nations and 61% of African nations passed data protection acts modeled on or influenced by GDPR, including South Korea's Personal Information Protection Act (Amendment), Japan's Act on the Protection of Personal Information (Amendment), and Singapore's Personal Data Protection Act (Amendment). To retain access to the lucrative EU market, multinational corporations have been compelled to overhaul their data architectures, setting up globally unified compliance systems. An estimated 78% of US corporations conducted GDPR gap assessments and revised their privacy policies, with 27% spending over $500,000 to achieve full compliance and avert prohibitive penalties. This manifestation of the "Brussels Effect" demonstrates that the EU, without relying on military or economic coercion, successfully exported its data governance rules globally using its massive market scale and stringent regulations, establishing preliminary institutional autonomy over data.

4.3 The Gaia-X Project: Building Autonomous Digital Infrastructure

Initiated in 2021 under the leadership of Germany and France, the Gaia-X project represents a focal point in the EU's quest for technological autonomy. Operating under the core philosophy of "controlled data sharing," its objective is to engineer a federated European cloud architecture based on open standards, secure trust, unified identity authentication, and transparent data spaces. By interconnecting decentralized data centers across the continent into a trusted, integrated European cloud network, Gaia-X aims to dismantle the monopolistic grip of American hyperscalers and ensure that digital infrastructure remains structurally autonomous and controllable. Utilizing a federated development model, Gaia-X aggregates participation from EU governments, private enterprises, and scientific research institutes. Currently boasting over 300 members, the project has realized its initial milestone targets up to 2025, mapping out the core architecture, connecting cross-border data centers, and launching foundational tools for identity management and secure data exchange pipelines.

4.4 Intensive Legislative Proliferation: Perfecting the Sovereign Legal Architecture

Between 2023 and 2024, the EU sequentially introduced the European Chips Act and the Artificial Intelligence Act, signaling that its digital sovereignty architecture has advanced into a phase of precise execution and comprehensive mobilization. These specialized legislative frameworks target two frontier technological domains—semiconductors and artificial intelligence—using statutory mechanisms to define developmental benchmarks, allocate state subsidies, and outline regulatory boundaries, thereby reinforcing the legal fabric of digital sovereignty.

The core objective of the European Chips Act is to bolster the EU's domestic supply security and technical competitiveness in semiconductor ecosystems. The act mobilizes over €43 billion in public and private capital to fund chip R&D, manufacturing facilities, and supply chain diversification, aiming to elevate the EU's share of global semiconductor production to 20% by 2030 while breaking technological ceilings in advanced node processing and chip design architectures. Funding is directed into three strategic avenues: first, driving R&D through the creation of the "Chips for Europe Initiative," which subsidizes universities and research labs; second, scaling up domestic manufacturing by providing investment subsidies of up to 20% for building or expanding

fabrication plants to attract global foundries; third, strengthening supply chain resilience by engineering a semiconductor monitoring mechanism and establishing strategic stockpiles to buffer against external disruptions.

The Artificial Intelligence Act stands as the world's first comprehensive, omnibus regulatory code for AI, embodying the EU's dual logic of balancing market development with strict normative oversight. The act institutes a tiered, risk-based regulatory matrix: high-risk AI applications (such as deployments in healthcare, education, critical infrastructure, and financial scoring) face rigorous market entry compliance, requiring exhaustive pre-deployment risk assessments, strict data governance, guaranteed algorithmic traceability, clear explainability, and continuous human oversight; medium-risk AI systems (such as facial recognition or emotion analysis) are subject to strict transparency obligations, mandating clear disclosure to end-users; low-risk AI systems (such as entertainment or administrative tools) enjoy light-touch regulation to stimulate market innovation. Crucially, the act enforces absolute prohibitions on AI systems that engage in cognitive behavioral manipulation, untargeted biometric mass surveillance, or predictive policing, firmly defending the normative red lines of European values.

5. Contemporary Challenges to EU Digital Sovereignty

Despite rolling out a robust suite of policy instruments and achieving notable preliminary outcomes, the EU's quest for digital sovereignty faces formidable domestic and external obstacles. Externally, it is subjected to intense competitive pressures from the US and China; internally, deep structural "digital divides" among member states hamper collective synergy, frequently forcing the EU into positions of re-dependence. The road to genuine digital sovereignty remains long and arduous.

5.1 The Internal Digital Divide

The EU comprises 27 sovereign member states with vastly divergent economic and technological capacities. Despite deepening regional integration, internal "digital divides" remain acute, acting as a primary domestic check on the synchronized execution of digital sovereignty strategies. This gap spans digital infrastructure, industrial scale, innovation capabilities, and societal digital literacy, causing uneven policy implementation and diluting collective strategic efficiency. Regarding infrastructure, the EU's Digital Economy and Society Index (DESI) 2022 report highlighted that corporate adoption of advanced technologies like AI and Big Data across the EU remains low, with systemic shortages in advanced digital skills capping future growth prospects and widening regional disparities. Nations like Finland, Denmark, the Netherlands, and Sweden rank as digital frontrunners. In 2021, while 54% of the aggregate EU population possessed basic digital skills, this figure dropped to 29% in Romania, compared to 80% in Finland. Similarly, while 55% of EU small and medium-sized enterprises (SMEs) achieved baseline digital intensity, Sweden recorded 86%, whereas Romania and Bulgaria registered the lowest metrics. Furthermore, stark divides persist between urban hubs and rural zones within individual member states. In 2021, the urban-rural broadband disparity reached nearly 30% across the union; rural broadband coverage exceeded 90% in the Netherlands but hovered around 20% in Greece. This infrastructural asymmetry leads to uneven regional economic development, preventing the Digital Single Market from fully materializing—enterprises in lagging zones struggle to digitize, and unified regulatory rules face friction during local enforcement.

In terms of human capital, citizens' digital literacy varies significantly. According to official Eurostat indicators up to 2023, a massive 46-percentage-point gap in basic digital skills exists between individuals with higher education (80%) and those with low or no formal qualifications (34%). This gap is most pronounced in Portugal (66 points), Greece (63 points), and Malta (59 points), contrasting sharply with minimal gaps in Estonia (12 points), Finland (14 points), and Lithuania (22 points). This disparity caps the consumption potential of the digital market and weakens societal support for digital sovereignty policies—in low-literacy regions, citizens show limited comprehension of or interest in data privacy or algorithmic transparency, occasionally resisting regulatory compliance. Moreover, cultural differences and conflicting national priorities generate political friction when unifying governance rules. This internal divide breeds a Matthew Effect: digitally advanced member states possess the capital and political will to rapidly advance sovereignty goals, while lagging nations fall further behind, fracturing policy outcomes and undercutting the EU's collective global competitiveness. Rectifying this requires massive internal resource rebalancing and delicate interest-compromise mechanisms.

5.2 Strategic Dilemmas Amidst US-China Bipolar Competition

In the global digital landscape, the US and China have formed a powerful bipolar competitive dynamic. Caught in the middle, the EU faces severe external compression, falling into a complex dilemma of "de-dependence vs. re-dependence" that represents its most severe external challenge.

The EU-US relationship embodies a complex, dual-character dynamic of "allies and competitors," which complicates the EU's pursuit of digital sovereignty. Ideologically and normatively, the US and EU share a Western value system, maintaining close arrangements in intelligence sharing and technical standards. The

US-led NATO framework provides the bedrock of European security, and European regulators frequently draw on US market experiences. However, in commercial digital sectors, the US exerts a dominant, monopolistic squeeze on Europe. As of September 2022, Android and iOS commanded a combined 99.24% of the mobile operating system market in the EU. Google held a 91.96% market share in European search, and an estimated 92% of the Western world's data—including Europe's—is stored by US-based corporations. Revelations from the PRISM scandal and subsequent wiretapping leaks highlighted the acute security risks of this lopsided dependence, driving the EU to launch defensive initiatives like Gaia-X and the European Chips Act to "de-Americanize" its digital dependencies. Nonetheless, "de-dependence" faces immense friction: the US leverages frameworks like the "EU-US Data Privacy Framework" and its massive market leverage to extract concessions from the EU, bounding its regulatory freedom. Furthermore, to develop advanced nodes or frontier AI models, the EU remains dependent on US intellectual property, hardware tools, and talent pipelines. The €43 billion mobilized by the European Chips Act, while substantial, is unlikely to disrupt the US semiconductor hegemony in the short term, ensuring that the EU's "de-dependence" remains partial and localized.

Concurrently, the EU's relationship with China features a mix of "cooperation potential and competitive anxiety," which intensifies its strategic dilemma. As the world's second-largest digital economy, China's breakthroughs in 5G, e-commerce, and AI offer the EU valuable alternative pathways. Member states like Germany and Spain initially selected Huawei pipelines to deploy 5G networks, reducing single-source dependencies on US tech; Sino-EU cooperation in logistical networks and cross-border e-commerce oversight has injected vitality into the European market. China's massive market and technological complementarities provide the EU with a useful counterweight against American tech hegemony. However, deep competitive anxieties and external systemic pressures make the EU highly vigilant toward China. The rapid expansion of Chinese tech firms in European markets has triggered domestic protectionist measures—TikTok's dominance in short-video sectors and platforms like AliExpress squeezing local e-commerce led the EU to tighten scrutiny using regulations like the Digital Markets Act. More critically, Washington exerts heavy diplomatic pressure on Brussels to align against Beijing. Categorizing Chinese firms like Huawei as national security threats, the US threatened to restrict intelligence sharing with allies that integrate Chinese 5G kits, forcing countries like Germany and the Czech Republic to restrict cooperation. This geopolitical pressure prevents the EU from deepening its cooperation with China, leaving it oscillating between cooperating to check the US and distancing itself to avoid Washington's pressure, fearing that over-cooperation could result in a "re-dependence" on China.

6. Conclusion and Strategic Insights

The construction of EU digital sovereignty represents a strategic response to accelerating global technology competition and internal governance demands, aimed at protecting its normative values and economic future. By encoding core rights—such as data privacy, democratic oversight, and market fairness—into statutory frameworks like the Digital Single Market strategy, GDPR, Gaia-X, and specialized acts, the EU has charted a distinct path toward achieving a triad of technological, data, and institutional autonomy, offering a valuable blueprint for regional organizations in the digital age.

However, this journey remains fraught with severe internal structural inconsistencies and external systemic pressures. Internally, the persistent digital divide prevents member states from forging a unified force, retarding the growth of an integrated digital market and an autonomous European tech base. Externally, the intense competition between the US and China traps the EU in a "de-dependence vs. re-dependence" bind. Consequently, realizing true digital sovereignty will require prolonged internal resource balancing and complex international norm-negotiation. For China, the EU's trajectory offers vital lessons: establishing robust digital sovereignty must remain a top national priority. While safeguarding its unique digital development path, China should actively engage in global dialogues on digital governance, helping forge a more equitable, balanced, and multilateral global digital order.

References

Bellanova, R., Carrapico, H. and Duez, D. (2022). Digital sovereignty and European security integration: an introduction. *European Security*, *31*.

Cai, C.H. and Zhang, R.Y. (2022). The EU's Digital Transformation Strategy under the Discourse of 'Technological Sovereignty' and 'Digital Sovereignty'. *Journal of International Political Studies*, (01).

Chander, A., Sun, H.C. and Wei, H.B. (2024). Digital Sovereignty: The Double-Edged Nature of Second-Generation Sovereignty. *Digital Law Review*, (02).

Falkner, G., Heidebrecht, S., Obendiek, A. and Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. *Journal of European Public Policy*, *31*.

Feng, S. (2022). The Sovereignty Principle and Its Competitors: Order Construction and Evolutionary Logic of Digital Space. *Russian East European & Central Asian Studies*, (04).

Gong, Y.M. (2022). The Return of the Concept of Sovereignty in the Digital Age and EU Digital Governance. *Chinese Journal of European Studies*, (03).

Jiang, Z.D. (2021). The Logic of the European Union's Construction of 'Digital Sovereignty' and Sino-EU Digital Cooperation. *International Forum*, (04).

Liao, F. (2024). Digital Sovereignty and Global Digital Governance. *Journal of Jinan University (Philosophy and Social Sciences)*, (07).

Liu, J. and Liu, Z.W. (2025). Platform Infrastructure, Digital Sovereignty, and New Geopolitics: A Study Based on Douyin and TikTok. *Journalism & Communication Review*, (02).

Luo, Y.C. (2024). The Transformation of Sovereignty in the Digital Age and the Reshaping of International Security Order. *Global Review*, (06).

Monsees, L. and Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, *31*.

Sun, Y.X. and Liu, Z.Y. (2025). Risk Governance of Digital Sovereignty in the Era of Globalization. *Studies on Globalization*, (01).

Yan, G. and Xin, H. (2023). A Study on the European Union's Strategy of 'Digital Sovereignty' under the Background of US-China-EU Competition. *Journal of International Relations*, (03).

Yuan, M.S. (2025). Theoretical Analysis and Practical Challenges of the Sovereignty Construction in Digital Space. *Asia-Pacific Security and Maritime Affairs*, (02).

Zheng, C.R. and Jin, X. (2022). The Background, Path and Challenges of the European Union's Digital Sovereignty Construction. *Contemporary World and Socialism*, (02).