

The European Union's Digital Sovereignty Protection Model in the Big Data Era

Hanyu Ma ^{1, a}, Dr. Md. Zahurul Haq ^{2, b}

¹ School of Law, Universiti Utara Malaysia, 06010 Sintok, Malaysia;

² UUM College of Law, Government and International Studies, Universiti Utara Malaysia, Malaysia.

^a mahanyu1995@gmail.com, ^b md.zahurul@uum.edu.my

Abstract. This article aims to explore the significance of the European Union's digital sovereignty protection model as a representative model in the era of big data, emphasizing the importance of safeguarding national data security and sovereignty in the digital economy. The European Union has constructed a legal protection framework centered around the General Data Protection Regulation (GDPR) and various policy documents, establishing itself as a leader in the global data protection field. The European Union's digital sovereignty protection model revolves around protecting personal data within the framework of the Digital Single Market and operates on two dimensions: internal and external. Internally, it focuses on creating a unified digital market and advancing digital technologies, while externally it aims to reduce dependence on data superpowers and enhance international influence. The European Union's efforts in digital sovereignty protection serve as an important example for global digital governance and personal privacy protection.

Keywords: European Union; Big Data Era; Digital Sovereignty; Digital Economy.

1. Introduction

Entering the era of big data, big data has become one of the most valuable new strategic factors concerning national security and interests. Countries have proposed data-driven development strategies, aiming to maximize the value of data resources while protecting national data security and sovereignty. Due to its massive volume, cross-border circulation, and diverse interests involved, big data has sparked strong concerns about digital sovereignty among nations. Digital sovereignty represents national interests, and different countries have adopted different digital sovereignty protection models based on their socio-economic-cultural backgrounds and interest demands. In 2016, the European Commission passed The General Data Protection Regulation (GDPR), which sparked strong reactions worldwide and became a benchmark in international digital sovereignty protection legislation. This article will delve into the European Union's digital sovereignty protection model, aiming to promote the development of digital sovereignty.

2. The Connotation of Digital Sovereignty

The arrival of the era of big data has ended the era where states exclusively enjoyed "absolute sovereignty." The scope of national sovereignty is no longer confined to the domains of sea, land, and air, but extends to the cyberspace of network information. Existing information sovereignty cannot address the situation where states struggle to control the transmission and aggregation of massive data, thereby catalyzing the emergence of digital sovereignty (Sun & Zhang, 2015). The impact of globalization coupled with the cross-border effects of data means that during the process of data transfer between different countries, national data may be exposed to one or more foreign jurisdictions, and the rules regarding data jurisdiction vary between different countries, sometimes even conflicting (Irion, 2012). As a result of this problem, the idea of digital sovereignty has emerged in several nations, inspiring them to give their own digital sovereignty more consideration.

The concept of digital sovereignty was formally proposed by the European Union (EU) and primarily applies to the digital market within the EU. Digital sovereignty officially appeared in the "European Digital Sovereignty" report published by the EU in July 2020, which highlighted the

risks faced by the EU in the digital field due to excessive reliance on foreign technologies and lack of control over data generated within its borders. Therefore, the report proposed the concept of "digital sovereignty": In this context, 'digital sovereignty' refers to Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation. Meanwhile, Ursula von der Leyen, president of the European Commission, proposed achieving technological sovereignty in key areas. In order to strengthen its strategic autonomy in the digital sphere, the EU has proposed three measures: creating a data structure, encouraging a reliable environment, and enacting laws and regulations. In terms of building a data framework, the EU aims to strengthen its digital sovereignty. To make data gathering, processing, and sharing easier, a data framework must be established. Alternatively, it involves building out data infrastructure and investing more in emerging technologies like blockchain, high-performance computing, artificial intelligence, and quantum technology (Madiaga, 2020). It can be said that the European Union has constructed its digital sovereignty system from dimensions such as data protection and technological development.

Digital sovereignty refers to all actions of the EU in the digital world, including the full cycle of data activities such as collection, flow, and sharing, as well as all activities involving digitization such as digital enterprise competition, industry digitization, cybersecurity, artificial intelligence, and online transactions. It represents the EU's ability to maintain independence in the digital world.

3. European Union's People-Centric Protection Model in the Digital Single Market

The General Data Protection Regulation (GDPR) was passed by the European Parliament on April 14, 2016, and because of its innovative features and stringent data protection guidelines, it helped the EU establish itself as a global leader in data protection. Subsequently, amidst the competition between China and the United States in technology, compounded by the impact of the COVID-19 pandemic, the EU introduced a series of legislative acts, such as the Data Governance Act, Digital Markets Act, Digital Services Act, and Cyber Resilience Act, establishing a comprehensive framework for data sovereignty protection. Overall, the EU's digital sovereignty protection model encompasses both internal and external dimensions. Internally, it promotes the creation of a unified digital market, the advancement of digital technology, and the observance of values that place a premium on safeguarding personal privacy. Externally, it aims to reduce dependence on data superpowers, expand international influence in the digital domain, and become a leader in establishing international data frameworks while respecting international rules.

3.1 Building a European Digital Single Market

To address and eliminate the digital divide and unify the fragmented digital market within the European Union, the EU proposed the "Digital Single Market" strategy. Under the following three circumstances, the term "Digital Single Market" refers to a market in which capital, goods, people, and services can freely flow, irrespective of country or location of residence: (1) ensuring free movement of goods, people, services, and capital; (2) enabling seamless connectivity for residents, individuals, and businesses, with all online activities conducted under fair competition conditions; and (3) ensuring high levels of protection for personal data. On January 19, 2016, the European Commission announced the "Towards a Digital Single Market Act," which proposed three major measures to support the single market: (1) promoting the transformation and upgrading of cross-border digital services to better facilitate consumer and business access to the digital single market. Specific measures include amending cross-border e-commerce rules to protect consumer rights, digitizing cross-border parcel delivery to promote flexibility and innovation in cross-border tracking systems, reducing geographical barriers, supplementing existing e-commerce frameworks, and implementing existing legislation to effectively address unreasonable geo-blocking issues, as well as reducing the VAT burden on cross-border sales and establishing a common consolidated

corporate tax base across the EU; (2) optimizing digital network services by improving existing telecommunications rules to promote innovation and fair competition, creating a new media services framework to protect minors, consumers, and personal data, and enhancing network platform governance to encourage the sharing economy and combat illegal content on the internet; and (3) optimizing the digital economy's growth potential by concentrating on small and medium-sized businesses' digital transformation, enhancing transparency in government services, promoting digital skills among citizens, and increasing awareness of the global nature of the data economy, while ensuring the free and secure flow of data within and outside the EU through high standards of data protection measures.

3.2 Developing Digital Technologies

A significant portion of EU's economic potential is found in digital marketplaces, with the global market for new digital technologies predicted to reach €2.2 trillion by 2025 (ESPAS,2019). To maintain its strategic autonomy and reduce dependence on Chinese and American technology, the EU pays great importance to the development of digital technology. On one hand, it enhances digital infrastructure construction across various sectors. The "European strategy for data," proposes to enhance data technology infrastructure in nine areas including transportation, agriculture, culture, tourism, and healthcare, aiming to foster data-sharing spaces and promote innovation in data products and services. The "Digital Sovereignty for Europe" introduces the Gaia-X project to facilitate the implementation of cloud infrastructure within the EU. On the other hand, it increases investment in technological research and development significantly to reduce reliance on foreign technology. The "White Paper on Artificial Intelligence" suggests an annual investment of over €20 billion in the field of artificial intelligence over the next decade. In the "European Parliament resolution on the EU's Cybersecurity Strategy for the Digital Decade," In order to decrease reliance on foreign technologies and improve cybersecurity leadership and competitiveness throughout the digital supply chain, it suggests leveraging initiatives like the EU Recovery and Resilience Facility, the Digital Europe program, the Horizon Europe program, and processor technologies. These initiatives include data processing and storage in clouds, integrated circuits (chips), ultra-secure connectivity, quantum computing, and the next generation of networks.

3.3 Strict Protection of Citizens' Personal Privacy: A People-Centered Approach

The General Data Protection Regulation (GDPR), which went into force globally on May 25, 2018, had a big impact. Renowned for its strict protection of citizens' privacy, the GDPR mandates all entities, whether private companies or government institutions, to ensure the integrity, security, and accuracy of data when collecting and processing it. It restricts the quantity and purposes of data collection, requires user "informed consent" for data acquisition, and grants users the rights to rectify and delete data. Subsequently, principles regarding the protection of personal data are reflected in various strategic documents in the digital domain. For instance, the Data Act published on April 14, 2023, prohibits the reduction or limitation of individuals' rights to data protection, communication privacy, and confidentiality. The European data strategy mandates comprehensive oversight by data protection agencies over any processing of personal data, ensuring innovation while safeguarding citizen rights. However, GDPR's protection of personal data is not limitless or immutable; it must be balanced with considerations of national security and public safety.

The European Union actively pursues data collaboration and values data diplomacy on the outside. It has ratified framework agreements for digital cooperation with nations including Singapore, South Korea, and China in an effort to collaboratively advance cross-border data flow cooperation. The EU actively encourages digital technology assistance to help developing nations with poorer digital development capacities strengthen their digital capabilities. In addition, the EU consistently convenes summits and talks with other nations and regions to promote the creation and execution of the global digital agenda through digital diplomacy. Regarding data diplomacy, the

European Union seeks to uphold global norms while taking the lead in creating global data frameworks.

Table 1. Digital Sovereignty Strategy Documents of the European Union

Numble	Document	Year of Publication
1	Digital Single Market	2014
2	Towards a Digital Single Market Act	2016
3	The General Data Protection Regulation	2016
4	Data Governance Act	2020
5	European Strategy for Data	2021
6	The EU's Cybersecurity Strategy for the Digital Decade	2021
7	Digital Markets Act	2021
8	Digital Services Act	2022
9	European Declaration on Digital Rights and Principles	2022
10	Data Act	2023
11	Cyber Resilience Act	2024

4. Challenges and Prospects of the European Union Digital Sovereignty Protection Model

The EU's people-centric digital sovereignty protection legal system under the Digital Single Market is undoubtedly one of the world's most representative legal systems. Not only does it strictly protect personal data, but it also tends to perfect the legal system for protecting personal privacy. It attaches importance to the cross-border flow of data, preventing threats to national data security posed by foreign entities controlling data, and further realizes effective governance of data within national territory boundaries or political jurisdictions, ensuring complete digital sovereignty rules. However, the strict digital sovereignty protection model also brings significant challenges to the EU. Complex data regulations and the uneven digital development among member states complicate enforcement in practice. Regarding GDPR, after its enactment, the European Data Protection Committee and individual member states issued different versions of GDPR supplementary guidelines and data compliance standards based on different data governance goals. The guidelines from the European Data Protection Committee mainly focus on extensive issues concerning the entire EU, while those issued by member states vary in emphasis based on their respective digital economic development and data governance differences. The complexity of laws, coupled with different interpretations, has led to the emergence of many novel and uncertain abstract concepts and judgment criteria, affecting the discretionary power of data enforcement agencies and posing challenges for businesses and organizations in compliance (Li,2021).

Additionally, the stringent regulations and standards of digital sovereignty protection may require businesses and organizations to invest significant amounts of funds and human resources to comply with regulatory requirements. This will severely limit the development of small and medium-sized enterprises (SMEs). Compared to large enterprises, SMEs lack advanced digital technology, talent management, and sufficient financial investment to comply with strict digital sovereignty protection regulations, exacerbating their disadvantage in market competition.

In the future development of digital sovereignty, the European Union (EU) needs to focus on addressing the challenges faced by data enforcement agencies in practice. It should clarify enforcement standards, strengthen the technical capabilities of enforcement agencies, and enhance their understanding and application of digital sovereignty protection technologies and methods to better carry out enforcement work. Strengthening cooperation and coordination with other relevant departments and organizations is crucial for collectively addressing challenges in the digital sovereignty protection field and improving enforcement efficiency.

The EU may need to provide more support for the development of local small and medium-sized enterprises (SMEs) by offering financial subsidies, loan support, tax incentives, and other means to provide financial assistance. Providing guidance and training tailored to digital sovereignty protection for SMEs will help them understand regulatory requirements. Moreover, increasing technical guidance for SMEs and encouraging the development and application of new technologies that meet digital sovereignty protection requirements will help maintain the balance of the digital market economy. Given the rapid development of digital trends, the EU's digital sovereignty protection model needs to continuously update and adjust according to changes in the digital environment to adapt to the challenges and changes brought by new technologies.

5. Summary

Entering the era of big data, digital sovereignty has become one of the most concerned issues for countries. Digital sovereignty involves not only individual rights and corporate development but also the operation of society and national sovereignty. As a major participant in the global digital economy, the European Union (EU) bears the responsibility of upholding digital sovereignty. The EU's model of digital sovereignty protection, with its pioneering, strict, and comprehensive characteristics, has set an example for countries to improve their digital sovereignty protection systems. The EU's model not only conforms to European values and legal standards but also reflects its high regard for individual privacy and data security, providing important insights for global digital governance. In the future digital process, the EU must continue to improve its legal framework for digital protection, promote innovation and application of technologies for protecting digital sovereignty, actively engage in digital diplomacy, and collectively address the various challenges brought by digital technologies.

References

- [1] Sun, N., & Zhang, X. (2015). On data sovereignty: An examination based on virtual space gaming and cooperation. *Journal of Pacific Studies*, 2(Issue), 64.
- [2] Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet*, 4(3-4), 40-71.
- [3] Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data Sovereignty: A Review. *Big Data & Society*, 8(1), 205395172098201.
- [4] Madiega, T. A. (2020). Digital sovereignty for Europe.
- [5] ESPAS (European Strategy and Policy Analysis System). (2019, April). *Global Trends to 2030: Challenges and Choices for Europe* (p. 28).
- [6] Li, B. (2021). Protection Modes and Practical Principles of Data Sovereignty. In Shanghai Bar Association (Eds.), *Shanghai Legal Research*, Vol. 4, No. 52 (pp. 183-194). Shanghai Bar Association.
- [7] Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, 31(3), 415–434.