Society, 13 (3), 1194-1205, 2025
P-ISSN: 2338-6932 | E-ISSN: 2597-4874
https://societyfisipubb.id

Analysis of the Government's Political Will to Achieve Data Sovereignty Through National Data Center Development Policies

Muhammad Prakoso Aji *, and Putrawan Yuliandri
Universitas Pembangunan Nasional Veteran Jakarta, South Jakarta 12450, Indonesia
* Corresponding Author: prakosoaji@upnvj.ac.id

ARTICLE INFO

Publication Info:
Research Article

How to cite:
Aji, M. P., & Yuliandri, P. (2025). Analysis of the Government's Political Will to Achieve Data Sovereignty Through National Data Center Development Policies. Society, 13(3), 1194–1205.

DOI: *10.33019/society.v13i3.932*

Received: August 27, 2025;
Accepted: November 23, 2025;
Published: December 26, 2025;

ABSTRACT

Data sovereignty has become an increasingly strategic issue in the digital era, as data now constitutes a critical asset shaping national security, economic competitiveness, and governance capacity. In response to growing concerns over fragmented data governance and recurring data breaches, the Indonesian government initiated the development of the National Data Center (Pusat Data Nasional/PDN) as a key infrastructure for strengthening national data sovereignty. This study examines the extent to which political will supports the realization of data sovereignty through the PDN development policy. Using a qualitative descriptive approach, this research analyzes policy documents, regulatory frameworks, and secondary data related to Indonesia's data governance initiatives. The analytical framework is based on Brinkerhoff's concept of political will, which identifies seven key components: government initiative, policy selection, stakeholder mobilization, public commitment and resource allocation, credible sanctions, sustainability of efforts, and learning and adaptation. The findings reveal that Indonesia's political commitment toward data sovereignty remains partial and uneven. While several components of political will, such as government initiative, policy formulation, stakeholder mobilization, resource allocation, and continuity of policy efforts, have begun to emerge, other crucial elements, particularly credible sanctions and institutional learning mechanisms, remain underdeveloped. The absence of comprehensive implementing regulations under the Personal Data Protection Law and the delayed establishment of an independent data protection authority further weaken the institutional foundation for national data sovereignty. This study argues that strengthening political will is essential to accelerate the implementation of the National Data Center and to build an integrated national data governance system.

Without stronger regulatory commitment and institutional coordination, Indonesia risks lagging behind other countries in securing digital sovereignty and protecting strategic national data in the evolving global digital economy.

Keywords: *Cybersecurity Policy; Data Sovereignty; Digital Governance; National Data Center; Political Will*

1. Introduction

The rapid development of technology has significantly transformed the structure of social and political life within modern states. Several years ago, data sovereignty had not yet become a critical issue. However, alongside global technological developments, the capacity for data sovereignty has increasingly come to reflect a state's sovereignty in cyberspace. Data sovereignty refers to the concept that data must comply with the laws and regulations of the country where the data is physically stored (Hummel et al., 2021). In order to achieve strong data sovereignty, substantial political will from the government is required, particularly in cyberspace, to safeguard and protect data which has now become a highly valuable commodity. Moreover, the realization of data sovereignty requires the development of various infrastructures, which in turn demands strong political commitment from the government in terms of policy formulation, governance arrangements, and substantial budget allocations. Various policies and regulations related to cyber sovereignty and cybersecurity include several legal frameworks that have previously been enacted, such as Law Number 27 of 2022 concerning Personal Data Protection (PDP) and Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) (Fitriati, 2018).

In the effort to build data sovereignty, Indonesia inevitably faces numerous challenges. One of the major problems lies in the fragmentation of government data storage, which has not yet been centralized within a unified national data infrastructure. In addition, there is still an absence of comprehensive policies governing national data management and governance to ensure proper protection of these data assets. Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE) indicates that government expenditures on Information and Communication Technology (ICT) between 2014 and 2016 reached approximately IDR 12.7 trillion annually, with continuous increases each year. However, around 65 percent of this budget was allocated to software or applications that often served similar functions, indicating inefficiencies in digital governance and data management systems.

According to data from the Ministry of Communication and Informatics in 2018, the Indonesian government possessed approximately 2,700 data centers distributed across 630 government institutions at both central and regional levels. Ironically, the utilization rate of these data centers reached only around 30 percent of their maximum capacity. This condition reflects the fragmented policies adopted by individual government institutions regarding data storage. As a result, data security cannot be fully guaranteed because each institution manages its own data and stores it in separate data centers. From the perspective of data sovereignty, this fragmented and unintegrated data storage system weakens the protection of national data. Consequently, Indonesia has experienced numerous cases of large-scale data breaches in recent years, which have caused significant harm to the nation.

https://doi.org/10.33019/society.v13i3.932

In response to these challenges, the Ministry of Communication and Informatics has planned the establishment of four National Data Centers (Pusat Data Nasional/PDN) designed to meet global standards of digital governance infrastructure. The first PDN is planned to be built in the Greater Jakarta area, specifically within the Deltamas Industrial Estate, due to its proximity to the national administrative center. The second PDN will be located in Batam, particularly in Nongsa Digital Park, which has strategic access to support western Indonesia. The estimated budget required for the Batam PDN alone reaches approximately IDR 2.3 trillion. Another PDN is planned to be built in Balikpapan, East Kalimantan Province, due to its proximity to Indonesia's new capital city. The final PDN will be developed in Labuan Bajo to support the eastern region of Indonesia. The connectivity infrastructure supporting these PDNs will be integrated through the Palapa Ring national fiber-optic network. These National Data Centers are expected to connect the 2,700 data centers currently dispersed across various government institutions. Through the development of a centralized national data infrastructure, data that is currently fragmented will be integrated into a single system. Ministries and government institutions will be able to access the data they require in accordance with their respective functions and responsibilities. Furthermore, the security of these data assets can be better ensured through centralized management. Philosophically, the objective of this initiative is to establish a nation that possesses sovereignty over its data, which in turn would strengthen its geopolitical and economic position in the global digital landscape.

Data breaches may also occur because the security of national data is closely linked to whether data centers are located within a country's territorial jurisdiction or outside it. This problem becomes even more severe if a country lacks the capability to secure data stored in data centers located abroad. In the private sector, major technology companies operating platforms such as Instagram, Facebook, WhatsApp, Twitter, and Google often do not place their data centers within the territorial jurisdiction of the countries where their users reside. This situation weakens the legal authority of those countries to protect the data of their citizens from misuse under the framework of data sovereignty law. Such conditions represent a fundamental issue within the field of cyber law.

In reality, societies in many developing countries primarily act as consumers of digital applications developed by global technology corporations. However, these corporations frequently do not establish data centers within the territories of the countries where their services are widely used. Consequently, developing countries often lack sufficient legal leverage when confronting potential misuse of their citizens' data. This condition is also evident in Indonesia. Many global social media platforms, including Instagram, Facebook, and WhatsApp, have not fully located their data centers within Indonesian territory. In some cases, these multinational technology companies also lack permanent representative offices in Indonesia. From a political perspective, this situation could pose a significant obstacle if Indonesia were to face a digital crisis that requires direct negotiation or legal confrontation with foreign technology corporations.

Sudibyo (2019) describes how the integration of a nation into the global digital landscape generates both constructive and destructive consequences. Platforms such as Facebook, Google, and Amazon operate simultaneously as social institutions that contribute to democratic values and as economic institutions whose primary motivation is commodification. Social media applications are not provided entirely free of charge; fundamentally, they are business products designed for economic gain and data instrumentalization. Social media platforms, search engines, and digital marketplaces continuously record the digital activities of their users in order to generate behavioral data about internet users. The more frequently individuals access these platforms, the more behavioral data is collected and stored by the companies operating them.

https://doi.org/10.33019/society.v13i3.932

This user behavior data constitutes the primary raw material for the business models of new media corporations. Such data serves as the foundation for developing increasingly sophisticated algorithms and artificial intelligence systems that can approximate human intelligence. In addition, this behavioral data forms the basis of targeted digital advertising capable of penetrating deeply into users' private spaces. The monetization of behavioral data therefore generates enormous economic profits.

Therefore, the research question of this article concerns how the government's political will contributes to the realization of data sovereignty through the policy of developing the National Data Center (PDN). Strong political commitment from the government is essential to achieve national data sovereignty. This study aims to analyze the government's political will in this context. Data sovereignty is a fundamental issue in the contemporary digital era. From a political perspective, a sovereign nation is one that exercises sovereignty not only over its territory but also over the data owned by its citizens and institutions.

2. Literature Review

2.1. Political Will

A study entitled *Indonesian Cyberspace Expansion: A Double-Edged Sword* written by Paterson from the Australian National University (2019) employed a qualitative approach. The study explains the phenomenon of the rapidly expanding digital economy in Indonesia. This development has led to changes in societal behavior, with people becoming increasingly active in cyberspace. Such developments require appropriate policy responses. However, low levels of digital literacy among Indonesian society often lead to the spread of disinformation, which can create social unrest. Therefore, various emerging issues in cyberspace require a clear regulatory framework in order to prevent potential problems. On the other hand, if regulations are formulated in ways that restrict democratic values and public freedoms, they may also generate new challenges.

According to Brinkerhoff, as cited in Abazovic and Mujkić (2015), *political will* refers to the commitment of actors to undertake actions aimed at achieving certain goals and to bear the associated costs of those actions over time. This definition is based on an analytical concept that distinguishes seven components of political will. These components include: (1) government initiative, (2) policy selection, (3) stakeholder mobilization, (4) public commitment and resource allocation, (5) credible sanctions, (6) sustainability of efforts, and (7) learning and adaptation. Based on these seven components, this study analyzes the government's political will in realizing data sovereignty by examining the extent to which these components have been implemented within the context of national data governance policies.

2.2. Data Sovereignty

Previous research conducted by Patrik Hummel, Matthias Braun, Max Tretter, and Peter Dabrock (2021) entitled *Data Sovereignty: A Review* discusses the development of data-based technologies, which provide numerous benefits but also involve various stakeholders who face challenges in maintaining control over data. The objective of this study was to clearly describe the concept of data sovereignty, given that there are still many differing interpretations of what data sovereignty entails. To address this issue, the researchers reviewed 341 publications that analyzed different frequencies of the concepts of data sovereignty, digital sovereignty, and cyber sovereignty. The study employed a quantitative approach in which the object of analysis consisted entirely of literature from these 341 publications. The findings reveal considerable variation and, in some cases, a lack of conceptual clarity regarding the meaning of data

https://doi.org/10.33019/society.v13i3.932

sovereignty and cyber sovereignty, which creates challenges in understanding these concepts. The various interpretations found in the literature relate to different forms of control, ownership, and claims over data articulated by different actors, ranging from individuals to states. In this context, data sovereignty also involves inclusive deliberation processes and the recognition of fundamental rights related to data subjects.

Another study was conducted by Maggie Walter, Tahu Kukutai, Stephanie Russo Carroll, and Desi Rodriguez-Lonebear (2021). This research is particularly interesting because it was conducted across several countries. The study predominantly employed a qualitative approach, while also utilizing quantitative data as secondary sources to support the analysis. The research focuses on the impact of data policies in several countries on indigenous societies. Data-related issues become a key reference point in the formulation and implementation of state policies toward their citizens. In this regard, indigenous societies often become disadvantaged groups because states frequently lack comprehensive data concerning communities that are often considered marginalized. Conducted across multiple countries, the study highlights differences in how data policies are implemented in each national context. The aim of this research is to ensure that data can be utilized for the benefit of all segments of society, including indigenous communities.

Another study that serves as a reference for this research is conducted by Louise Amoore (2016), entitled *Cloud Geographies: Computing, Data, Sovereignty*, published in *Progress in Human Geography*. This research explains how cloud computing architecture has become increasingly intertwined with geopolitics. Examples include intelligence data sharing, border control, immigration decisions, and drone operations. The study examines the geographical characteristics of cloud computing through two distinct paradigms. The first paradigm, referred to as "Cloud I" or the geography of cloud forms, relates to the identification and spatial location of data centers where the cloud is materially realized. In this perspective, the cloud is understood through a historical framework of observation in which abstract and seemingly invisible infrastructures can be made visible and comprehensible. The second paradigm, "Cloud II" or the analytical geography of the cloud, conceptualizes the cloud as a set of experimental algorithmic techniques operating at the threshold of perception. Similar to twentieth-century airspace, contemporary cloud computing involves processes that render visible and actionable phenomena that would otherwise remain beyond human observation. Amoore proposes three elements of correlative cloud reasoning that demonstrate their significance for contemporary geopolitics: condensing traces, pattern detection, and archiving the future. In this geopolitical context, cloud computing becomes fundamentally important because it can shape and influence sovereignty.

Another study referenced in this research was written by Igor Calzada (2021) entitled *Data Co-operatives through Data Sovereignty*. This study proposes an alternative conceptual framework, interpretations, and networks of smart cities aimed at challenging prevailing forms of data capitalism through existing practical cases. The researcher compares data governance and data justice within the context of current trends and challenges in smart cities. The study seeks to develop a new approach promoted by the United Nations Human Settlements Programme (UN-Habitat), namely the concept of "People-Centered Smart Cities." The research highlights the interconnected ideas related to the technopolitical dimensions of people-centered smart city approaches. Data cooperatives emerge as mechanisms for sharing data through peer-to-peer (P2P) repositories, while data sovereignty can be claimed as a digital right of communities and citizens. Consequently, the study aims to open new avenues for research related to people-centered smart city approaches and demonstrates how collaborative data governance through data sovereignty can support community and citizen development.

https://doi.org/10.33019/society.v13i3.932

Finally, another study used as an academic reference was conducted by Prabowo, Wisnu Handi, Satriya Wibawa, and Fuad Azmi (2020), entitled *Cyber Personal Data Protection in Indonesia*. This research employs a qualitative method to analyze and explain the issues related to data protection. The study utilizes human security theory as its primary analytical framework, supported by concepts in cybersecurity. The research discusses cyber data protection in Indonesia from a security perspective. The findings indicate that Indonesia's position in terms of cyber sovereignty remains relatively weak because many foreign technology companies have not established their data centers within Indonesian territory. Communities with limited cybersecurity capabilities are particularly vulnerable and are more likely to be disadvantaged in matters of cyber sovereignty. According to this study, data protection represents a vital core that must be safeguarded to ensure national security and societal well-being.

3. Research Methodology

This study employs a qualitative research approach using a descriptive analytical method to examine the government's political will in realizing data sovereignty through the development of the National Data Center (PDN) policy in Indonesia. A qualitative approach was chosen because this research aims to understand policy dynamics, institutional commitment, and governance processes related to data sovereignty. Through qualitative analysis, the study seeks to interpret policy developments, regulatory frameworks, and institutional responses associated with national data governance.

The data used in this study consist of both primary and secondary sources. Primary data were obtained through observations and interviews with relevant stakeholders involved in data governance and digital policy, particularly actors associated with ministries or institutions responsible for cybersecurity, digital governance, and national data management. These primary sources were used to gain insights into the implementation and challenges of the National Data Center policy.

Secondary data were collected from various sources, including academic journal articles, books, government policy documents, official regulations, reports, and relevant publications related to data sovereignty and cybersecurity governance. In addition, data were also obtained from credible media reports and institutional publications that discuss developments in Indonesia's national data infrastructure and cybersecurity policies. These sources provide contextual understanding and support the interpretation of empirical findings.

To analyze the data, this study employs qualitative analytical techniques through literature review and policy analysis. The analytical framework is based on the concept of political will developed by Brinkerhoff, which identifies seven key components: government initiative, policy selection, stakeholder mobilization, public commitment and resource allocation, credible sanctions, sustainability of efforts, and learning and adaptation. These components serve as the analytical lens for evaluating the extent to which the Indonesian government demonstrates political will in implementing the National Data Center policy as part of its broader strategy to achieve data sovereignty.

The unit of analysis in this research focuses on ministries and government institutions involved in the formulation and implementation of national data governance policies. By examining the roles, commitments, and institutional coordination among these actors, this study seeks to assess the degree of political will demonstrated in strengthening Indonesia's data sovereignty.

To ensure the credibility of the findings, the study applies data triangulation by comparing information obtained from different sources, including interviews, policy documents, academic

https://doi.org/10.33019/society.v13i3.932

literature, and media reports. This triangulation process helps strengthen the reliability of the analysis and provides a more comprehensive understanding of the political dynamics surrounding Indonesia's efforts to establish national data sovereignty.

4. Results and Discussion

A Data Center is a strategic facility designed to manage, organize, and provide integrated Information and Communication Technology (ICT) services. This facility is supported by physical and digital infrastructure that includes connectivity systems, management mechanisms, governance frameworks, and resource allocation aimed at ensuring continuous service availability, maintaining operational reliability, and protecting ICT assets from various potential threats. In general, a Data Center consists of a set of server devices, communication networks, data storage media, as well as security protocols and management procedures that are organized according to specific standards. As a central point for the implementation of ICT services, the existence of a Data Center is a vital component for the sustainability of information systems, both in the operationalization of services and in providing access for relevant stakeholders. The strategic position of a Data Center is further strengthened by its function as the main repository for storing and managing data and information, which represent valuable and crucial assets for organizations and for the state (Riasetiawan, 2016).

Considering Indonesia's geographical characteristics as a vast archipelagic country and the complexity of its national life, the potential users of the National Data Center are highly diverse and significant in number. This diversity is reflected in the different needs and benefits across regions and sectors. Indonesia, with a population of more than 240 million people and more than 70 million digital connectivity users, represents a very large market for National Data Center services. These users are connected through various connectivity service channels, both from telecommunications companies and internet service providers, to access data centers and information systems. The National Data Center will not only support commercial-scale internet connectivity needs but will also encourage the development of connectivity infrastructure, both general and specialized. The demand for internet services that is widely distributed across various regions of Indonesia will be collected through connectivity nodes that ultimately integrate with the National Data Center. As the purchasing power of society toward digital devices increases and the volume of available data and information grows, the number of Data Center users is projected to continue increasing significantly. The availability of relevant content and services within Data Centers will become a major driving factor in the growth of the digital user base in Indonesia (Riasetiawan, 2016).

The National Data Center (PDN) plays an important role in supporting the establishment of an integrated electronic government system. Currently, many government institutions and regional governments still operate data centers separately and in closed systems according to their respective needs. The absence of a National Data Center has resulted in the existence of numerous heterogeneous data center infrastructures and the creation of "information islands" scattered across various institutions and regions. The primary objective of the PDN is to provide data center services that support the sustainability of e-government implementation. With the existence of PDN, the public will receive more integrated and reliable services, while government agencies and other institutions will gain access to more stable systems. The implementation of e-government requires trust in reliable services, which can only be achieved through high-quality data center support. The PDN will also serve as a bridge toward the implementation of a single identity system (single ID), data and information integration, and the establishment of a single source of national data. The existence of PDN will create an e-government service model that is

https://doi.org/10.33019/society.v13i3.932

well-organized and managed in an integrated manner. Furthermore, PDN enables service collaboration among institutions, agencies, and regional governments, thereby strengthening synergy and collaboration to promote efficiency, effectiveness in government business processes, and sustainable bureaucratic reform (Riasetiawan, 2016).

The Director General of Informatics Applications (Aptika) of the Ministry of Communication and Informatics stated on June 12, 2023, that the development of the PDN in Bekasi is targeted to be completed and inaugurated in October 2024, while the PDN in Batam is expected to be completed in 2025. Meanwhile, the development of PDN facilities in Manggarai Barat and Balikpapan is still in the planning stage, and the tender process for the Batam PDN is currently ongoing. At present, the development of the National Data Center has not yet been completed, so national data is temporarily stored in the Temporary National Data Center system (PDNS). Prior to the existence of PDN, government data was scattered across various institutions with non-uniform systems, making the integration and analysis of data difficult. This fragmentation has resulted in low operational efficiency and has hindered rapid and accurate decision-making. Under these circumstances, the Ministry of Communication and Informatics initiated the development of PDN as an effort to unify and manage government data in a more integrated and efficient manner (Gabriel, 2024).

Several countries have been identified as the main contributors to cyberattacks occurring in Indonesia, as illustrated in the following table.

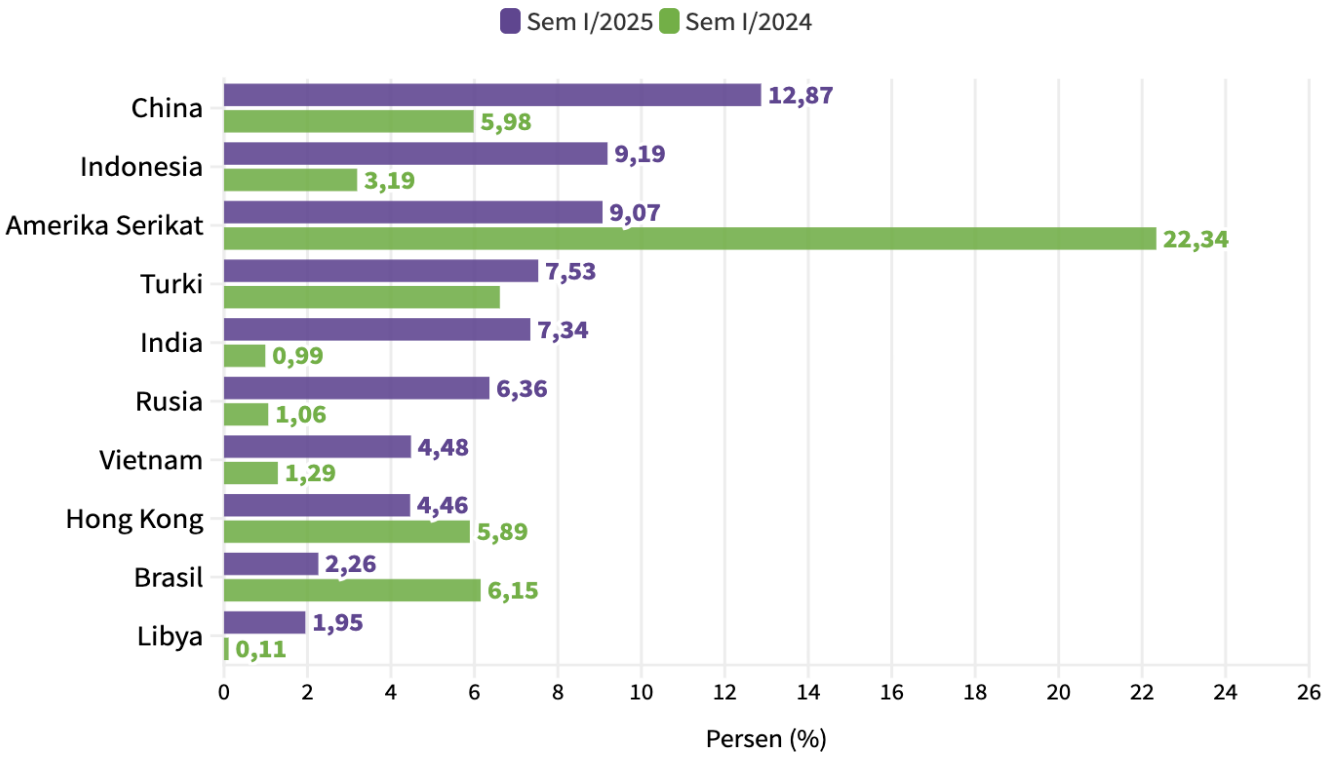

Figure 1. Major Contributor Countries of Cyber Attacks in Indonesia
(Semester I/2024 and Semester I/2025)
Source: AwanPintar.id in DataIndonesia.id (2025)

On June 20, 2024, a large-scale data breach incident occurred due to a LockBit 3.0 ransomware attack on the Temporary National Data Center (PDNS), in which the attackers demanded a ransom of USD 8 million to restore access to the encrypted data. This incident emphasizes the

https://doi.org/10.33019/society.v13i3.932

urgency of implementing criminal law mechanisms in efforts to protect personal data. The data breach incident at PDNS exposed weaknesses in Indonesia's national data security system and raised concerns regarding the effectiveness of legal protection for data in Indonesia. Millions of personal data records involved in the breach have the potential to be exploited for criminal activities, thereby emphasizing the importance of strengthening the legal framework governing data protection. Although Indonesian criminal law, including Law Number 27 of 2022 concerning Personal Data Protection, has regulated aspects of data management and protection, its implementation in practice still faces various obstacles (Gabriel, 2024). Therefore, strong political will from the government is required to realize national data sovereignty.

The political will of the government and the House of Representatives (DPR) regarding data sovereignty can be analyzed using the concept of political will proposed by Brinkerhoff as cited in Abazovic and Mujkic (2015), which defines political will as the commitment of actors to undertake actions aimed at achieving certain goals and to bear the associated costs over time. This definition is based on an analytical concept that distinguishes seven components of political will: (1) government initiative, (2) policy selection, (3) stakeholder mobilization, (4) public commitment and resource allocation, (5) credible sanctions, (6) sustainability of efforts, and (7) learning and adaptation. Based on these seven components, this research finds that within the context of the National Data Center development policy, only five of the seven components have been implemented. These five components include: (1) government initiative, (2) policy selection, (3) stakeholder mobilization, (4) public commitment and resource allocation, and (5) sustainability of efforts.

Political will can primarily be analyzed through the presence of regulations necessary for building data sovereignty. In this regard, Law Number 27 of 2022 concerning Personal Data Protection has not yet been followed by implementing regulations. In fact, such implementing regulations should have been completed no later than two years after the enactment of the law (in 2024). The law also mandates the establishment of a Personal Data Protection Authority (LOPDP), which has not yet been clearly realized. Therefore, stronger political commitment is required before establishing new institutional bodies. This research finds that political will has not yet been sufficiently strong to provide the regulatory foundation necessary to realize data sovereignty, particularly through the policy of developing the National Data Center. This analysis reinforces the argument that the government and the DPR have not yet demonstrated sufficient commitment to building a strong and integrated national data center infrastructure, despite the urgent necessity of such infrastructure in the current cyber era.

In the context of government initiative in building the National Data Center (PDN), there are indications of commitment to strengthening Indonesia's data sovereignty capacity. This initiative is also supported by the government's policy selection through several regulatory frameworks related to data sovereignty and personal data protection. However, these efforts cannot yet be considered optimal because various necessary regulations have not yet been established, including the implementing regulations of Law Number 27 of 2022 concerning Personal Data Protection. The government has also attempted to mobilize various stakeholders, including central government institutions, regional governments, private sector actors, and society, all of whom play important roles in strengthening national data sovereignty. Public commitment has also been encouraged through various forms of socialization and collaboration with educational institutions. These efforts collectively represent continuity in establishing an optimal national data sovereignty governance system. However, the component related to credible sanctions has not yet been clearly implemented due to the absence of implementing regulations under the Personal Data Protection Law and the delay in establishing the mandated data protection

https://doi.org/10.33019/society.v13i3.932

authority. Consequently, the evaluation conducted in this study indicates that greater attention from the government and the DPR is still required in strengthening data sovereignty. Furthermore, the processes of learning and adaptation remain suboptimal because the development of the National Data Center is still ongoing, and the former Minister of Communication and Informatics who initiated this policy has been implicated in a corruption case, which further weakens the representation of the government's political will in realizing national data sovereignty.

When compared with neighboring countries such as Malaysia, the latter appears to demonstrate stronger political will regarding data sovereignty. Malaysia has developed data protection mechanisms through the implementation of policies, procedures, and guidelines focusing on data security, public key infrastructure, and electronic information management. These efforts are manifested through the formulation of policies and guidelines related to data protection, as well as the implementation of the National Cryptography Policy, which outlines methods and strategies for the use and development of cryptographic algorithms and products in order to protect confidential information of strategic importance to national interests. In addition, the management capacity of Computer Emergency Response Teams (CERTs) has been strengthened through improvements in the functions and restructuring of the National Cyber Security Incident Response Teams (CSIRT), including Sectoral CSIRT and Organizational CSIRT (National Security Council of Malaysia, 2020).

Malaysia's Cybersecurity Act 2024 came into force on August 26, 2024. Together with four implementing regulations, this law aims to strengthen Malaysia's cyber defense and enhance the country's resilience against emerging threats through the implementation of necessary measures. A key concept introduced in this law is the National Critical Information Infrastructure (NCII). This concept refers to computer systems or infrastructures that, if disrupted, would negatively affect critical national and governmental functions, public safety, or public order in Malaysia. The law also outlines the roles and responsibilities of Sector Leads for NCII and NCII Entities, as well as licensing requirements for cybersecurity service providers (Chan, 2024). Based on this comparison, stronger political will is still required for Indonesia to align itself with neighboring countries in terms of data sovereignty protection.

An analysis of the various factors contributing to data breaches, as observed in several government websites in Indonesia, indicates the necessity of a multidimensional approach in addressing these issues. Several policy recommendations can be proposed, including improving public literacy regarding cybersecurity, strengthening regulations related to personal data protection, developing more reliable and secure technological infrastructure, and increasing human resource capacity in cybersecurity fields. Through these measures, the risks of data breaches can be minimized in the future and public trust in digital systems can be enhanced. Comprehensive efforts are required to strengthen cybersecurity governance in Indonesia, including regulatory reinforcement, increased awareness of the importance of information security, and investments in developing competent cybersecurity experts. In addition, periodic security audits of government information systems should be conducted in order to identify and address existing vulnerabilities (Dachlan et al., 2025).

The government's political will related to data sovereignty must also be strengthened. Sectoral ego can no longer be maintained because it will become a major obstacle in developing an integrated national data governance system. In the context of the National Data Center development policy, this study finds that sectoral ego still exists among government institutions whose authorities intersect in the domain of data governance. These conflicts arise from issues related to institutional authority, budget allocation, organizational structures, personnel

https://doi.org/10.33019/society.v13i3.932

arrangements, and positions that may be affected by changes in authority, particularly when such changes involve the redistribution of budgetary resources.

5. Conclusion

Data sovereignty has become a highly fundamental issue in the contemporary cyber era. Data has evolved into an extremely valuable commodity, not only in the present but also in the future. Therefore, it has become the responsibility of the government to safeguard national data security. The data owned by Indonesian citizens should ideally provide benefits for the Indonesian nation. In this context, strong political will from the government is essential in order to realize data sovereignty. A crucial policy in this regard is the development of the National Data Center (Pusat Data Nasional/PDN), which is planned to serve as the foundational infrastructure for national data sovereignty.

The political will of the government and the House of Representatives (DPR) regarding data sovereignty was analyzed using the concept of political will proposed by Brinkerhoff as cited in Abazovic and Mujkic (2015). Based on this analytical framework, this study finds that within the context of the National Data Center development policy, only five of the seven components of political will have been implemented. These five components include: (1) government initiative, (2) policy selection, (3) stakeholder mobilization, (4) public commitment and resource allocation, and (5) sustainability of efforts.

The acceleration of political will related to the development of the National Data Center policy is therefore urgently needed to ensure that Indonesia does not fall further behind other countries that already possess more established regulatory frameworks and infrastructure supporting data sovereignty. The state must play an active role in protecting the data owned by its citizens as well as the data held by government institutions. The policy for the development of the National Data Center must be implemented with a firm commitment that this infrastructure will serve as a cornerstone of the nation's digital economy in the future.

6. Acknowledgment

The authors would like to express their sincere gratitude to all individuals and institutions who have contributed to the completion of this research. Special appreciation is extended to colleagues and academic peers who provided valuable insights and constructive discussions during the research process.

7. Declaration of Conflicting Interests

The authors declare that they have no financial or personal affiliations that could have influenced the research or findings presented in this article.

References

Abazović, D., & Mujkić, A. (Eds.). (2015). *Political will: A short introduction case study – Bosnia and Herzegovina*. Friedrich-Ebert-Stiftung.

Amoore, L. (2018). Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography, 42*(1), 4–24. https://doi.org/10.1177/0309132516662147

Baezner, M., & Robin, P. (2018). *Cyber sovereignty and data sovereignty*. Center for Security Studies (CSS), ETH Zürich.

https://doi.org/10.33019/society.v13i3.932

Calzada, I. (2021). Data co-operatives through data sovereignty. *Smart Cities, 4*(2), 558–580. https://doi.org/10.3390/smartcities4020032

Chan, C. (2024). Cybersecurity Act 2024: A new era of cybersecurity in Malaysia. PricewaterhouseCoopers.

Dachlan, A. A., et al. (2025). Pertanggungjawaban hukum pemerintah dalam kebocoran data pribadi pada penyelenggaraan pusat data nasional. *Jurnal Hukum Samudera Keadilan, 20*(1).

Fitriati, R. (2018). *Membangun model kebijakan nasional keamanan siber dalam sistem pertahanan negara*. Universitas Pertahanan Indonesia.

Gabriel, A. (2024). Perlindungan hukum atas data pribadi dalam kasus kebocoran data Pusat Data Nasional Sementara (PDNS) dalam perspektif hukum pidana. *Seminar Nasional Hukum dan Pancasila*, 3.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1), 1–17. https://doi.org/10.1177/2053951720982012

National Security Council. (2020). *Malaysia cyber security strategy 2020–2024*. Prime Minister's Department of Malaysia.

Paterson, T. (2019). Indonesian cyberspace expansion: A double-edged sword. *Journal of Cyber Policy, 4*(2), 216–231. https://doi.org/10.1080/23738871.2019.1627476

Prabowo, W. H., Wibawa, S., & Azmi, F. (2020). Perlindungan data personal siber di Indonesia. *Padjadjaran Journal of International Relations, 1*(3).

Riasetiawan, M. (2016). *Pusat data untuk pemerintahan*. Universitas Gadjah Mada.

Romaniuk, S. N., & Manjikian, M. (Eds.). (2021). *The Routledge companion to global cyber security strategy*. Routledge.

Sudibyo, A. (2019). *Jagat digital: Pembebasan dan penguasaan*. Kepustakaan Populer Gramedia.

Walter, M., Kukutai, T., Carroll, S. R., & Rodriguez-Lonebear, D. (2021). *Indigenous data sovereignty and policy*. Routledge.

About the Authors

1) Muhammad Prakoso Aji is a senior lecturer in the Department of Political Science at the Faculty of Social and Political Sciences, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia. He completed his higher education at the University of Indonesia. His academic interests include cyberpolitics, strategic and global studies, and political communication. In his research, he frequently employs qualitative research methods, particularly case study and phenomenological approaches. He has authored numerous scholarly publications, including books and articles in academic journals.
Email: prakosoaji@upnvj.ac.id

2) Putrawan Yuliandri is a lecturer in the Department of Communication Studies at Universitas Pembangunan Nasional Veteran Jakarta, Indonesia. He completed his undergraduate studies at Padjadjaran University and obtained his master's degree from the University of Indonesia. His research interests include political communication, big data analysis, and intelligence communication. He has published various articles in academic journals and conference proceedings.
Email: putrawanyuliandri@upnvj.ac.id

https://doi.org/10.33019/society.v13i3.932