Volume X Issue X (2025) 106-120
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.46799/jlsp.v3i2.71
https://jolastic.id/index.php/jlsp

Journal of Law & Social Politic

Digital Sovereignty and The Right To Data: A Comparative Study Between Indonesia, The European Union, and The United States

Rahayudin Rahayudin[1*], Muchammad Naseer[2], Nova Agustina[3], Antonio Guterres[4]
[1]Universitas Sehati, Indonesia
[2]Universitas Teknologi Bandung, Indonesia
[3]Universitas Teknologi Bandung, Indonesia
[4]Universidade Oreintal Timor Lorosa'e, Timor Leste
Corresponding Author: ayudrahayudin90@gmail.com[1], naseer@utb-univ.ac.id[2], antonioguterres85@gmail.com[4]

ABSTRACT
This study aims to analyze and compare the principles of digital sovereignty and the right to personal data in Indonesia, the European Union, and the United States, while assessing their legal implications for the national policies of each jurisdiction. The research method used is comparative juridical with a descriptive qualitative approach, using a statutory approach to examine relevant laws and regulations, a comparative approach to compare the implementation of data sovereignty across jurisdictions, and a conceptual approach to examine theoretical concepts regarding the right to data and digital sovereignty. The results show that Indonesia emphasizes state control over data and the obligations of electronic system administrators, the European Union prioritizes comprehensive protection of data subjects' rights through the GDPR, while the United States implements more flexible sectoral regulations oriented towards private sector innovation. These differences in paradigms impact variations in the level of data protection, the effectiveness of oversight, and cross-border data transfer mechanisms. The scientific contribution of this study lies in the formulation of a comparative framework that integrates the concepts of digital sovereignty with the right to data as a basis for evaluating national policies in the era of the global digital economy. The legal implications of this study emphasize the urgency of regulatory harmonization, strengthening oversight capacity, and designing safe and equitable cross-border data transfer mechanisms for Indonesia.

Keywords: Digital sovereignty, data rights, comparative law, national policy, Indonesia

INTRODUCTION
Nearly every aspect of human life today relies on the use and processing of data, driven by the rapid development of information and communication technology (ICT), from social communication and economic transactions to access to public services and participation in digital platforms, which generate vast data footprints. This presents an

opportunity for governments to improve service efficiency and encourage the growth of the digital economy, while simultaneously posing serious challenges in the management, security, and protection of sensitive and potentially misused personal data. In this context, the concept of digital sovereignty becomes increasingly relevant as a state's capacity to regulate, control, and protect data and digital infrastructure within its jurisdiction, including cybersecurity regulations and oversight of cross-border data storage and transfer. Therefore, digital sovereignty demands a legal and policy framework that balances the protection of personal data rights with the use of digital technology for public service and economic development. (Hummel, Braun, Tretter, & Dabrock, 2021).

The European Union has solidified its position as a global leader in data protection regulation through the implementation of the General Data Protection Regulation (GDPR), which grants comprehensive rights to data subjects and requires strict compliance by businesses, including in the collection, processing, storage, and transfer of data across borders. This regulation establishes high standards of protection through the recognition of rights to access, rectification, and deletion of data, as well as mandatory reporting of data breaches. In contrast, the United States has adopted a more sectoral and adaptive approach through regulations such as the California Consumer Privacy Act (CCPA), which provides limited protection and varies across states, creating fragmented data protection. Meanwhile, Indonesia, as a developing country with growing internet users and an increasingly complex digital ecosystem, is developing a legal framework through the Personal Data Protection Law (PDP Law) and electronic systems regulations. However, Indonesia still faces challenges in consistent implementation, oversight capacity, and harmonization with international standards. Therefore, a policy strategy that balances the protection of personal data rights with the development and innovation of the national digital sector is needed (Houtan, Hafid, & Makrakis, 2020).

As technology advances and the volume of personal data increases, countries face challenges in protecting individuals' rights to data without hindering the growth of the digital economy. Differences in priorities and regulatory capacity have led Indonesia, the European Union, and the United States to adopt diverse approaches to regulating digital sovereignty and data protection. The European Union, through the GDPR, emphasizes strict compliance and comprehensive protection of data subjects' rights, while the United States tends to implement more flexible sectoral regulations. Indonesia, through its Personal Data Protection Law (PDP Law) and electronic system regulations, continues to refine its legal framework. This diversity of models presents complex legal challenges, particularly regarding cross-border data transfers, policy harmonization, and effective law enforcement. Therefore, a comprehensive comparative analysis is needed to identify best practices and regulatory gaps, as well as to form the basis for formulating contextual policy recommendations to strengthen digital sovereignty and the protection of personal data rights in Indonesia (Bühler et al., 2023).

The effectiveness of regulations in protecting individual rights to personal data, digital sovereignty mechanisms put in place in different jurisdictions, and harmonization between national regulations and international standards—particularly with regard to interoperability, data security, and the obligations of cross-border electronic system

organizers—are some of the specific issues that are of primary concern in this research (Calzada, 2021).

Recent research shows a global trend of increasing personal data breaches, indicating that the implementation of privacy-by-design principles and data protection from the early stages of technology development remains suboptimal. Despite the enactment of various regulations, data management practices in many sectors often fall short of adequate protection standards, thus maintaining a high risk of data breaches. In Indonesia, a study by (Fajri, 2023) identified inconsistent regulatory implementation and weak oversight of electronic system providers as key factors in the rise in data breaches in both the public and private sectors, as digital services increasingly process citizens' sensitive data. Conversely, international research shows that the European Union, through the GDPR, has successfully strengthened the protection of data subjects' rights, such as the right to access, correct, and delete data, and requires businesses to implement strict protection standards. However, the implementation of the GDPR also poses significant challenges for international businesses, particularly regarding cross-border compliance, the adjustment of information technology systems, and international data transfer mechanisms (Bradford, 2020).

The literature on digital sovereignty emphasizes the importance of regulating cross-border data transfers, protecting national digital infrastructure, and controlling data stored and processed domestically to maintain national security and sovereignty amidst digital globalization. This concept encompasses legal and policy aspects that enable states to control, monitor, and enforce data rights, as well as technical aspects such as network security and data center management. The European Union, through the GDPR, has established a comprehensive legal framework to guarantee uniform data control and protect data subjects' rights, while the United States tends to adopt a sectoral regulatory approach oriented toward market freedom, providing greater flexibility but relatively limited state control over data. In Indonesia, efforts to protect digital sovereignty are implemented through the Personal Data Protection Law (PDP Law) and regulations governing the implementation of electronic systems. However, their implementation still faces obstacles such as limited oversight capacity, low stakeholder awareness, and gaps between legal norms and practices. Therefore, a more integrated and nationally capacity-based policy strategy is needed to improve the effectiveness of data protection and strengthen Indonesia's digital sovereignty (Fabbrini & Celeste, 2020).

(Putri, 2022) research shows that Indonesia is not yet fully ready to implement comprehensive data protection standards, particularly in the management of sensitive and cross-sectoral data, which requires regulatory coordination and adequate oversight capacity. This situation reflects a gap between legal norms, including the Personal Data Protection Law (PDP Law), and their implementation practices in both the public and private sectors. Furthermore, (Fajri, 2023) emphasized that the weak implementation of the privacy-by-design principle—which integrates data protection from the system design stage—is a major factor in the high risk of data breaches in Indonesia. As a result, data management tends to be reactive and administrative, increasing the risk of leaks, misuse, and unauthorized access to personal data. These findings emphasize the urgency of strengthening oversight capacity, improving the competence of data managers, and

consistently implementing the privacy-by-design principle to align personal data protection in Indonesia with global standards and strengthen public trust.

International research by (Bradford, 2020) and (Kuner, 2021) reveals fundamental differences between the data protection regimes of the European Union and the United States. The GDPR is considered superior in strengthening data subject rights, oversight mechanisms, and cross-border harmonization, while US regulations are sectoral, flexible, and fragmented across states. While the US approach encourages market freedom and private sector innovation, the resulting data protection tends to be uneven, while the EU is able to ensure consistent protection through uniform legal standards. However, most previous studies have focused on a single jurisdiction and have not comprehensively analyzed the application of data sovereignty principles and their impact on national policies across countries. This gap is relevant for developing countries like Indonesia, which are developing digital regulatory frameworks due to limited understanding of the relationship between legal principles, implementation mechanisms, and policy implications. Therefore, a comparative study between Indonesia, the European Union, and the United States is crucial to provide an empirical basis for contextual policy formulation, while also supporting the alignment of national regulations with international standards without compromising digital sovereignty and citizens' rights to personal data.

This study uses a descriptive qualitative approach with a comparative juridical method to analyze the principles and legal frameworks related to digital sovereignty and data rights in Indonesia, the European Union, and the United States. Using a statute approach, this study examines relevant laws and regulations, including the Personal Data Protection Law (PDP Law) and the ITE Law in Indonesia, the GDPR and related regulations in the European Union, and the CCPA and sectoral privacy regulations in the United States. Furthermore, a comparative approach is used to compare the implementation of data sovereignty principles, national policies, domestic data control mechanisms, and cross-border data transfer regulations in the three jurisdictions. Meanwhile, a conceptual approach is applied to examine theoretical concepts regarding digital sovereignty, cybersecurity, and the right to personal data, thus forming an analytical framework that integrates legal, policy, and practical aspects. This integrated approach aims to identify best practices and regulatory weaknesses, as well as formulate contextual and applicable policy recommendations for strengthening digital sovereignty in Indonesia (Zichichi, Ferretti, D'Angelo, & Rodríguez-Doncel, 2022).

This study aims to analyze and evaluate the impact of the application of data sovereignty principles on the formation and implementation of national policies in Indonesia, the European Union, and the United States, and to compare the differences in data protection regulatory approaches across these three jurisdictions. Through comparative analysis, this study also aims to identify best practices and relevant regulatory weaknesses as a basis for formulating policy recommendations for Indonesia in developing and refining an effective, equitable, and adaptive data protection legal framework to technological developments, without neglecting digital sovereignty and the right to personal data, while remaining in line with international norms and standards.

METHODS

Types of research

This study combines a descriptive qualitative approach with a comparative legal method. Because this study focuses on legal analysis of laws and principles governing digital sovereignty (data sovereignty) and personal data rights in different jurisdictions, as well as comparing their effects on national policies, the comparative juridical method was selected. In Indonesia, the EU, and the US, legal phenomena, rules, and implementation practices are systematically and thoroughly explained, described, and analyzed using the descriptive qualitative approach (Gravett, 2023).

Research Approach

Three primary methods are used to carry out this study. The first is the Statute Approach, which looks at and evaluates pertinent laws in each jurisdiction, such as the Personal Data Protection Law (PDP Law), the Electronic Information and Transactions Law (ITE Law), and implementing regulations pertaining to the implementation of electronic systems in Indonesia; the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the ePrivacy Directive in the European Union; and the California Consumer Privacy Act (CCPA), the Privacy Act, and federal regulations pertaining to data management and cybersecurity. The goal of this analysis is to comprehend the legal underpinnings of data regulation, control mechanisms, and electronic system providers' obligations. The second method is the Comparative Approach, which contrasts the concepts of digital sovereignty (also known as data sovereignty) and data rights in the three jurisdictions. It focuses on domestic data control systems, cross-border data transfer regulations, and their influence on public, private, and national policymaking. Third, the Conceptual Approach builds an analytical framework that links legal principles with national practices and policies and serves as a foundation for creating pertinent and contextual legal recommendations for Indonesia. It does this by looking at theories and concepts pertaining to digital sovereignty, the right to personal data, privacy, and cybersecurity (Adler-Nissen & Eggeling, 2024).

Sources and Types of Legal Materials

The main source for this study is secondary data, which falls into a number of categories. The Personal Data Protection Act (PDP Act), the Electronic Information and Transactions Act (ITE Act), the GDPR, the Digital Services Act (DSA), the ePrivacy Directive, the California Consumer Privacy Act (CCPA), the Privacy Act, and other supporting regulations pertaining to digital sovereignty and personal data protection are among the first legal documents and regulations. Second, the concepts of data sovereignty, data rights, and digital sovereignty frameworks in different jurisdictions are discussed in academic literature, which includes books, journals, scientific articles, and research reports. Third, international reports and policy documents from organizations like the European Commission, UNCTAD, and the OECD, which offer more details on data protection regulations, how they are implemented, and how they affect domestic policies. In order to present a thorough and in-depth summary of the concepts, procedures, and legal ramifications of digital sovereignty and data rights at the national and international levels, all of these sources were examined (Pins, Jakobi, Stevens, Alizadeh, & Krüger, 2022).

Method of collecting data

This study's data collection methods were implemented in multiple stages. The first step was library research, which involved gathering pertinent academic literature, legal

documents, and regulations. Second, in order to find the most recent rules, guidelines, and reports pertaining to data rights and digital sovereignty, official government websites, international organizations, and legal databases were searched. Third, secondary document analysis entailed choosing and assessing information pertinent to the research topic, such as data sovereignty principles, the influence of regulations on national policies, and legal ramifications that may serve as the foundation for policy recommendations. All of these methods were used in a methodical manner to guarantee that the information gathered was current, pertinent, and fully supported the goals of the study (Yun, 2025).

Data Analysis and Interpretation

This study's data analysis was carried out in multiple stages using qualitative, descriptive, and comparative methods. The first step was data classification, which arranged laws, legal theories, and literature based on jurisdiction and the analysis's primary focus. The second method was regulatory content analysis, which concentrated on determining the legal precepts, the responsibilities of electronic system administrators, the rights of individuals, and the oversight procedures outlined in the regulations. Third, comparisons between jurisdictions are made by evaluating each legal system's strengths, weaknesses, and similarities with regard to the concepts of data sovereignty and the right to personal data. Fourth, the impact on national policy was analyzed, evaluating how regulations affected the creation, application, and oversight of data in both the public and private sectors. Lastly, by developing best practices that are pertinent to the Indonesian context and gathering policy recommendations that are applicable and feasible to implement successfully, conclusions are drawn and recommendations are compiled (Obendiek, 2022).

Data Validity

To guarantee the accuracy and consistency of the information, data validity checks were carried out using a number of techniques. In order to confirm the consistency of the data, the first step is triangulation of data sources, which entails comparing information gathered from different legal documents, scholarly publications, and official reports. The second method is regulatory cross-checking, which involves analyzing supporting documents, independent agency reports, and literature reviews to determine whether the content of regulations and their implementation procedures are consistent. Third, the validity of the analysis is strengthened and conclusions derived from trustworthy data are supported by peer review and academic referencing, wherein this research refers to previously published and academically verified studies (Kukutai, 2023).

RESULTS AND DISCUSSION

Tabel 1. Comparison of Data Sovereignty Principles Between Countries

Country	Data Sovereignty Principles	Implementation Explanation
Indonesia	Local data protection, the obligation of electronic system organizers to store and process data in the territory of Indonesia	The PDP Law stipulates that personal data must be processed in accordance with regulations, under the supervision of the PDP Authority. Cross-border data transfer policies are regulated through special permits, but implementation remains limited and oversight is suboptimal.

Country	Data Sovereignty Principles	Implementation Explanation
European Union	Data localization, data subject rights, cross-border data control	The GDPR establishes the rights of access, rectification, and erasure of data; cross-border data transfers are regulated through adequacy decisions or standard contractual clauses; and oversight is carried out through Data Protection Authorities (DPAs) in each member country.
United States	Sectoral approach, regulatory flexibility, data ownership by individuals and companies	The CCPA and the Privacy Act emphasize consumer rights and corporate responsibilities, but there is no comprehensive federal rule; regulations vary from state to state; and cross-border data transfers are relatively flexible.

Although Indonesia's data sovereignty principles place a strong emphasis on domestic data storage and cross-border transfer laws, implementation is still hampered by oversight and resource limitations. While the US places more emphasis on data ownership and private sector flexibility, which leads to laxer digital sovereignty principles, the EU places more emphasis on safeguarding data subjects' rights through stringent legal mechanisms.

Tabel 2. Impact on National Policy

Country	Impact on National Policy	Implementation
Indonesia	Data regulations influence the policies for organizing electronic systems, both in the public and private sectors.	The PDP Law impacts local cloud regulations, e-government, and data security obligations for companies; some policies still need to be harmonized with the GDPR for international integration.
European Union	Strict regulations encourage the formation of national policies in line with GDPR	Member states implement national regulations in accordance with the GDPR, establish supervisory bodies, and align cross-border data transfer mechanisms with EU standards.
United States	National policies are flexible, emphasizing sector-specific compliance.	Financial, healthcare, and consumer sectors are regulated differently; national oversight is fragmented, but provides flexibility for business innovation.

National policies are directly impacted by the data sovereignty principle. The Data and Data Protection Law in Indonesia promotes local data storage and electronic system regulation, but more harmonization is required. While the United States is more flexible, allowing national policies to differ by sector and state, the European Union has successfully implemented a uniform national policy through the GDPR.

Tabel 3. Legal Implications and Policy Recommendations

Country	Legal Implications	Policy Recommendations
Indonesia	Personal data protection is stronger, but implementation is still limited.	Enhance the PDP Authority's oversight capacity, strengthen cross-border data transfer mechanisms, and align regulations with international practices.
European Union	Strict compliance increases individual protection, poses challenges for foreign companies	Maintaining a balance between data protection and business innovation; expanding standard contractual clauses mechanisms to facilitate cross-border data trade.
United States	Flexible regulations allow for innovation, but subject data protection is less comprehensive.	Develop comprehensive federal regulations to protect personal data without hindering private sector flexibility; encourage interoperability with international regulations.

Each nation's application of data sovereignty principles has distinct legal ramifications. Although there is already legal protection in Indonesia, international oversight and harmonization must be reinforced. Strong legal protections and an efficient oversight system are provided by the European Union, but this presents compliance issues for multinational corporations. Although business innovation is encouraged by the United States' greater flexibility, individual legal protection is not as extensive. International best practices are adapted to the Indonesian context in order to create policy recommendations that strike a balance between the protection of data rights and the efficacy of regulations.

Comparison of Data Sovereignty Principles Between Countries

The research findings show that the principle of data sovereignty is applied differently in Indonesia, the European Union, and the United States, depending on each jurisdiction's policy orientation and digital governance model (Holfelder, Mayer, & Baumgart, 2022). In Indonesia, strengthening state control over digital data is reflected in the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law (PDP Law), which emphasize the obligation to process and store data domestically. This approach aims to maintain national security and protect citizens' sensitive data from the risk of cross-border leakage (Mackinnon, 2022). These findings align with (Putri, 2022), who asserted that strengthening digital sovereignty is a strategic necessity for Indonesia in facing the intensification of global digital activity (Janardhanan & Mas-Machuca, 2022).

However, the effective implementation of data sovereignty principles in Indonesia still faces significant obstacles. Although the Data and Information Technology (PDP) Law mandates legal, secure, and consent-based data processing, field practices demonstrate weak oversight and compliance among electronic system administrators. (Fajri, 2023). noted that limited capacity of supervisory agencies, low business awareness, and suboptimal implementation of security standards are contributing to the high incidence of data breaches (Lee, Kim, Won, Kim, & Lee, 2020). This situation indicates that data sovereignty in Indonesia remains normative and has not been fully realized substantively, necessitating strengthening audit mechanisms, sanctions, and institutional capacity (Twigt, 2024).

Unlike Indonesia, the European Union implements the principle of data sovereignty through an integrated and stringent legal framework based on the GDPR, placing the protection of data subjects' rights as a key foundation. The GDPR not only regulates data collection and processing but also provides individuals with extensive control through the rights to access, correct, restrict, and delete data. Furthermore, the regulation of cross-border data transfers through adequacy decision mechanisms and standard contractual clauses ensures that EU citizens' data remains subject to high standards of protection. This finding is consistent with (Bradford, 2020), who consider the GDPR to be the most comprehensive global model for ensuring digital sovereignty and cross-jurisdictional compliance (Celeste & Fabbrini, 2021).

The superiority of the European Union model is further strengthened by the implementation of the principles of privacy by design and privacy by default, which mandate the integration of data protection from the system design stage. This principle significantly improves internal privacy governance and reduces the risk of data misuse, as emphasized by (Kuner, 2021), In contrast, the United States adopts a sectoral regulatory approach through instruments such as the CCPA and industry-based regulations, which provide significant flexibility for private sector innovation. While this approach fosters the growth of the digital economy, the lack of a single federal standard leads to regulatory fragmentation, uneven data protection, and legal uncertainty for companies across jurisdictions, as noted by (Bradford, 2020).

Overall, a comparison of the three jurisdictions shows that each data sovereignty model reflects a policy choice between state control, individual rights protection, and innovation flexibility (Cordes et al., 2024). Indonesia prioritizes domestic control, the European Union emphasizes harmonization and data subject rights, while the United States prioritizes market freedom (Calzada, 2023). These findings underscore the importance for Indonesia of balancing strengthening digital sovereignty with alignment with global standards, particularly the GDPR, without sacrificing national interests (Kuenzler, 2021). This conclusion aligns with the recommendations of (Putri, 2022) and (Fajri, 2023), who emphasize the need for legal reform, strengthened oversight, and enhanced institutional capacity to ensure effective data protection in the global digital ecosystem.

Impact on National Policy

The implementation of the principle of data sovereignty in Indonesia has significantly impacted the direction of national policy, particularly in strengthening data security, regulating electronic systems, and managing domestic cloud services (Luzsa et al., 2022). The affirmation that citizen data must be managed within national jurisdiction has encouraged the government to build strategic digital infrastructure, such as a national data center and improve cybersecurity standards (Adelson & Mickelson, 2022). This policy also aligns with the government's digital transformation agenda, including e-government and the digitization of public services. In line with (Fajri, 2023) findings, strengthening data sovereignty is seen as a prerequisite for building a secure, independent, and accountable digital ecosystem, while simultaneously enhancing the state's capacity to manage digital risks and provide reliable technology-based public services.

The Personal Data Protection Law (PDP Law) was designed as an instrument for harmonizing national policies by establishing data processing principles, procedures, and standards that must be adhered to by all electronic system administrators, both in the public and private sectors (Meireles, 2024). However, various studies have shown that the implementation of this policy still faces structural challenges, particularly limited technical guidelines, supporting infrastructure, and institutional capacity at the central and regional levels. Differences in standards and practices between institutions have led to inconsistent data protection implementation, thus preventing the goal of harmonization from being fully achieved (J. Gstrein, 2023). This situation emphasizes the need for strengthened cross-institutional coordination and increased institutional capacity for effective implementation of data sovereignty policies.

In contrast, the European Union demonstrated a higher level of policy consistency through the implementation of the GDPR, which requires all member states to align their national laws with uniform regional standards (Egbert & Ulbricht, 2024). This harmonization creates legal certainty in data protection, particularly regarding cross-border data transfers and the fulfillment of data subjects' rights. According to (Bradford, 2020) the existence of a single standard increases business compliance and facilitates oversight by data protection authorities. The establishment of independent supervisory authorities in each member state, along with clear sanctions mechanisms and complaints procedures, strengthens the effectiveness of law enforcement and ensures the protection of individual rights equally across the EU (Gao, 2023).

The United States adopts a different approach through sectoral and state-based regulations, such as the CCPA in California, which provides significant flexibility for industry sectors to innovate (Islam, Valiani, Datta, Chowdhury, & Turin, 2024). However, this approach also results in fragmented data protection policies and standards that are not uniform nationally. (Kuner, 2021) emphasize that differences in regulations between sectors and between states complicate compliance efforts and reduce consistency in data protection. Thus, while the US model supports digital economic growth and technological innovation, the level of data protection is more diverse and relatively looser than the European Union's integrated model (Makanadar, 2024).

These differences in policy approaches demonstrate that the principle of data sovereignty directly impacts the effectiveness of data protection, cross-border interoperability, and the competitiveness of the national digital ecosystem (Wenzelburger & König, 2025). Indonesia is strategically positioned to balance strengthening digital sovereignty with the need for global harmonization, particularly in the context of international cooperation and cross-border data exchange. In line with the recommendations of (Putri, 2022) and (Fajri, 2023), Indonesia needs to strengthen the capacity of oversight institutions, improve cross-sectoral coordination, and adopt relevant international practices without sacrificing state control over citizens' data. This approach will enable Indonesia to develop a data sovereignty policy that is adaptive, competitive, and upholds the protection of individual rights amidst the dynamics of the global digital ecosystem.

Legal Implications and Policy Recommendations

The implementation of the principle of data sovereignty in Indonesia through the Personal Data Protection Law (PDP Law) has brought significant legal implications by strengthening the national personal data protection framework (Der Sylvestre Sidibe & Dhouib, 2024). The PDP Law provides a more structured legal basis for digital data management, encompassing data collection, processing, storage, and destruction. However, as noted by (Putri, 2022), this regulatory strengthening has not been fully matched by implementation readiness, particularly regarding oversight capacity, inter-institutional coordination, and the technical capabilities of the PDP Authority. Low public awareness of the right to personal data also limits the effectiveness of law enforcement, so the success of digital sovereignty remains highly dependent on strengthening institutional structures and public education (Sun, Zhu, & Liu, 2024).

From the European Union's perspective, the implementation of the GDPR demonstrates that the principle of data sovereignty can function optimally when supported by comprehensive protection standards, robust oversight mechanisms, and cross-jurisdictional regulatory harmonization (Graessler et al., 2024). The GDPR not only strengthens the position of individuals as data subjects through the recognition of fundamental rights, but also forces all entities—including global corporations—to adapt their internal policies and systems. According to (Bradford, 2020), the effectiveness of the GDPR is largely determined by the existence of an independent supervisory authority capable of coordinating across countries and consistently enforcing sanctions. This model demonstrates how data sovereignty can be upheld without impeding international data flows through instruments such as standard contractual clauses and adequacy decisions (Naik & Jenkins, 2022).

In contrast, the United States adopts a more flexible and sectoral regulatory approach, which has implications for different legal consequences (Toki, 2024). The absence of uniform federal data protection standards provides ample room for private sector innovation, but also results in fragmented protection of individual rights. (Kuner, 2021) emphasize that differences in regulations between sectors and between states create legal uncertainty and gaps in data protection. Thus, while the US model supports a dynamic digital economy, the level of data protection is uneven and relatively weaker than the integrated EU model (Catanzariti, 2024).

The results of this comparison indicate that each jurisdiction must balance three primary interests: state control over data flows, protection of individual rights, and space for private sector innovation (Wylde, 2023). In the context of Indonesia undergoing rapid digital transformation, the need for legal certainty and an adaptive ecosystem is crucial. Therefore, Indonesia needs to strengthen the oversight mechanism for the Data Protection and Data Protection Law, increase the capacity of the Data Protection and Data Protection Authority, and develop clear technical guidelines regarding data security, cross-border transfers, and cloud computing service governance (Sharma & Aggarwal, 2024). These efforts align with findings by (Fajri, 2023), who emphasized the importance of public education and increased digital legal literacy as prerequisites for effective data protection.

As a policy recommendation, Indonesia needs to adopt a hybrid approach by integrating the strictness of European Union regulations and the innovative flexibility of the United States. Harmonization with international norms such as the GDPR is crucial for

improving global interoperability, but it must still safeguard national digital sovereignty and the interests of data-driven economic development (Haq, Abhishta, Sommese, Jonker, & Nieuwenhuis, 2023). Strengthening independent supervisory authorities, developing comprehensive technical standards, and involving the private sector in policy development can create balanced data governance. By leveraging best practices from both models, Indonesia has the opportunity to build a responsive, competitive data sovereignty policy framework capable of protecting individual rights amidst the dynamics of the global digital ecosystem.

CONCLUSION

The application of the principles of digital sovereignty and the right to personal data demonstrates significant differences between Indonesia, the European Union, and the United States. Indonesia emphasizes local control over data and the obligations of electronic system providers, the European Union places data subject rights at the center of regulation through the strict and harmonized implementation of the GDPR across borders, while the United States adopts a flexible, sectoral regulatory approach with a strong orientation toward private sector innovation. These differences in approach have a direct impact on national policies, with the European Union relatively successful in creating uniform data protection, the United States providing flexibility with varying levels of protection, and Indonesia still facing challenges in implementation and harmonization with international standards. The legal implications of these findings emphasize the importance of strengthening oversight capacity, harmonizing regulations, and developing secure cross-border data transfer mechanisms. In this context, Indonesia can adopt the best practices of the European Union in strengthening data subject rights and law enforcement, and adopt the flexibility of United States policy to encourage digital innovation. This research excels in its integrated comparative analysis of regulations, practices, and the concept of digital sovereignty, although limited by its normative nature and secondary data-based nature. Nevertheless, the findings of this study are relevant as a basis for developing national policies, data governance guidelines for the public and private sectors, and academic references for further research in the field of digital sovereignty and personal data protection.

REFERENCES

Adelson, Naomi, & Mickelson, Samuel. (2022). The Miiyupimatisiiun Research Data Archives Project: putting OCAP ® principles into practice. *Digital Library Perspectives*, *38*(4), 508–520. https://doi.org/10.1108/DLP-11-2021-0099

Adler-Nissen, Rebecca, & Eggeling, Kristin Anabel. (2024). The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X. *JCMS: Journal of Common Market Studies*, *62*(4), 993–1011. https://doi.org/10.1111/jcms.13594

Bradford. (2020). *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press.

Bühler, Michael Max, Calzada, Igor, Cane, Isabel, Jelinek, Thorsten, Kapoor, Astha, Mannan, Morshed, Mehta, Sameer, Mookerje, Vijay, Nübel, Konrad, Pentland, Alex, Scholz, Trebor, Siddarth, Divya, Tait, Julian, Vaitla, Bapu, & Zhu, Jianguo. (2023). Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and

Equitable Digital Communities. *Digital*, *3*(3), 146–171. https://doi.org/10.3390/digital3030011

Calzada, Igor. (2021). Data Co-Operatives through Data Sovereignty. *Smart Cities*, *4*(3), 1158–1172. https://doi.org/10.3390/smartcities4030062

Calzada, Igor. (2023). *Postpandemic Technopolitical Democracy: Algorithmic Nations, Data Sovereignty, Digital Rights, and Data Cooperatives*. https://doi.org/10.1007/978-3-031-08608-3_6

Catanzariti, Mariavittoria. (2024). *Disconnecting Sovereignty*. https://doi.org/10.1007/978-3-031-60734-9

Celeste, Edoardo, & Fabbrini, Federico. (2021). *Competing Jurisdictions: Data Privacy Across the Borders*. https://doi.org/10.1007/978-3-030-54660-1_3

Cordes, Ashley, Bak, Marieke, Lyndon, Mataroria, Hudson, Maui, Fiske, Amelia, Celi, Leo Anthony, & McLennan, Stuart. (2024). Competing interests: digital health and indigenous data sovereignty. *Npj Digital Medicine*, *7*(1), 178. https://doi.org/10.1038/s41746-024-01171-z

Der Sylvestre Sidibe, Guéréguin, & Dhouib, Saadia. (2024). An Approach for Sovereign Data Exchange of AAS Digital Twins Through the International Data Space Network. *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1–4. https://doi.org/10.1109/ETFA61755.2024.10711067

Egbert, Simon, & Ulbricht, Lena. (2024). Data integration and analysis platforms as digital platforms: a conceptual proposal. *Information, Communication & Society*, 1–22. https://doi.org/10.1080/1369118X.2024.2442394

Fabbrini, Federico, & Celeste, Edoardo. (2020). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, *21*(S1), 55–65. https://doi.org/10.1017/glj.2020.14

Fajri, A. (2023). Kebocoran data di sektor publik dan swasta di Indonesia: Evaluasi implementasi prinsip privacy-by-design dan efektivitas pengawasan penyelenggara sistem elektronik. *Jurnal Keamanan Siber Dan Privasi Data*, *5(2)*, 75–92.

Gao, Raymond Yang. (2023). A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows. *Chinese Journal of International Law*, *22*(4), 707–787. https://doi.org/10.1093/chinesejil/jmad040

Graessler, Iris, Pottebaum, Jens, Holland, Martin, Wiechel, Dominik, Dickopf, Thomas, & Stjepandić, Josip. (2024). *Leveraging Data Ecosystems in Model-Based Systems Engineering for Ecological, Circular Added Value*. https://doi.org/10.3233/ATDE240858

Gravett, Willem. (2023). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, *22*(2), 1–22. https://doi.org/10.17159/1996-2096/2020/v20n1a5

Haq, Muhammad Yasir Muzayan, Abhishta, Abhishta, Sommese, Raffaele, Jonker, Mattijs, & Nieuwenhuis, Lambert J. M. (2023). Assessing Network Operator Actions to Enhance Digital Sovereignty and Strengthen Network Resilience: A Longitudinal Analysis during the Russia-Ukraine Conflict. *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 487–494. https://doi.org/10.1109/EuroSPW59978.2023.00060

Holfelder, Wieland, Mayer, Andreas, & Baumgart, Thomas. (2022). Sovereign Cloud Technologies for Scalable Data Spaces. In *Designing Data Spaces* (pp. 419–436). https://doi.org/10.1007/978-3-030-93975-5_25

Houtan, Bahar, Hafid, Abdelhakim Senhaji, & Makrakis, Dimitrios. (2020). A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. *IEEE Access*, *8*, 90478–90494. https://doi.org/10.1109/ACCESS.2020.2994090

Hummel, Patrik, Braun, Matthias, Tretter, Max, & Dabrock, Peter. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1). https://doi.org/10.1177/2053951720982012

Islam, Mozharul, Valiani, Arafaat A., Datta, Ranjan, Chowdhury, Mohammad, & Turin, Tanvir C. (2024). Ethical and Equitable Digital Health Research: Ensuring Self-Determination in Data Governance for Racialized Communities. *Cambridge Quarterly of Healthcare Ethics*, 1–11. https://doi.org/10.1017/S096318012400015X

J. Gstrein, Oskar. (2023). Data Autonomy: Recalibrating Strategic Autonomy and Digital Sovereignty. *European Foreign Affairs Review*, *28*(Issue 4), 379–396. https://doi.org/10.54648/EERR2023028

Janardhanan, Shakthivelu, & Mas-Machuca, Carmen. (2022). Modeling and Evaluation of a Data Center Sovereignty. *2022 18th International Conference on the Design of Reliable Communication Networks (DRCN)*, 1–8. https://doi.org/10.1109/DRCN53993.2022.9758037

Kuenzler, Adrian. (2021). Direct Consumer Influence—The Missing Strategy to Integrate Data Privacy Preferences into the Market. *Yearbook of European Law*, *39*, 423–458. https://doi.org/10.1093/yel/yeaa002

Kukutai, Tahu. (2023). Indigenous data sovereignty—A new take on an old theme. *Science*, *382*(6674). https://doi.org/10.1126/science.adl4664

Kuner. (2021). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press.

Lee, Ah Ra, Kim, Min Gyu, Won, Kyung Jae, Kim, Il Kon, & Lee, Eunjoo. (2020). Coded Dynamic Consent framework using blockchain for healthcare information exchange. *2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 1047–1050. https://doi.org/10.1109/BIBM49941.2020.9313330

Luzsa, Robert, Mayr, Susanne, Syrmoudis, Emmanuel, Grossklags, Jens, Kübler-Wachendorff, Sophie, & Kranz, Johann. (2022). Online Service Switching Intentions and Attitudes towards Data Portability – The Role of Technology-related Attitudes and Privacy. *Mensch Und Computer 2022*, 1–13. https://doi.org/10.1145/3543758.3543762

Mackinnon, Katie. (2022). Critical care for the early web: ethical digital methods for archived youth data. *Journal of Information, Communication and Ethics in Society*, *20*(3), 349–361. https://doi.org/10.1108/JICES-12-2021-0125

Makanadar, Ashish. (2024). Digital surveillance capitalism and cities: data, democracy and activism. *Humanities and Social Sciences Communications*, *11*(1), 1533. https://doi.org/10.1057/s41599-024-03941-2

Meireles, Adriana Veloso. (2024). Digital rights in perspective: The evolution of the debate in the Internet Governance Forum. *Politics & Policy*, *52*(1), 12–32. https://doi.org/10.1111/polp.12571

Naik, Nitin, & Jenkins, Paul. (2022). Is Self-Sovereign Identity Really Sovereign? *2022 IEEE*

International Symposium on Systems Engineering (ISSE), 1–7. https://doi.org/10.1109/ISSE54508.2022.10005404

Obendiek, Anke Sophia. (2022). What Are We Actually Talking About? Conceptualizing Data as a Governable Object in Overlapping Jurisdictions. *International Studies Quarterly*, *66*(1). https://doi.org/10.1093/isq/sqab080

Pins, Dominik, Jakobi, Timo, Stevens, Gunnar, Alizadeh, Fatemeh, & Krüger, Jana. (2022). Finding, getting and understanding: the user journey for the GDPR'S right to access. *Behaviour & Information Technology*, *41*(10), 2174–2200. https://doi.org/10.1080/0144929X.2022.2074894

Putri, N. (2022). Tantangan implementasi standar perlindungan data yang komprehensif di Indonesia: Analisis kesenjangan regulasi dan praktik pengawasan. *Jurnal Regulasi Data Dan Kebijakan Publik*, *4(3)*, 112–128.

Sharma, Ishani, & Aggarwal, Arun. (2024). *Digital Footprints and the Battle for Data Sovereignty*. https://doi.org/10.4018/979-8-3693-3253-5.ch005

Sun, Nigang, Zhu, Chenyang, & Liu, Yining. (2024). A Self-Sovereign Identity Privacy-Preserving Scheme for Logistics Transportation Based on One-Time-Use Tokens. *Electronics*, *13*(14), 2799. https://doi.org/10.3390/electronics13142799

Toki, Valmaine. (2024). *Indigenous Rights, Climate Change and Governance*. https://doi.org/10.4337/9781803924984

Twigt, Mirjam. (2024). Doing Refugee Right(s) with Technologies? Humanitarian Crises and the Multiplication of "Exceptional" Legal States. *Refugee Survey Quarterly*, *43*(1), 1–21. https://doi.org/10.1093/rsq/hdad020

Wenzelburger, Georg, & König, Pascal D. (2025). Sending Signals or Building Bridges? Digital Sovereignty in EU Communicative and Co-Ordinative Discourse. *JCMS: Journal of Common Market Studies*, *63*(2), 526–547. https://doi.org/10.1111/jcms.13638

Wylde, Allison. (2023). The UN Global Digital Compact (GDC), Achieving a trusted, free, open, and Secure Internet: Trust-building. *European Conference on Cyber Warfare and Security*, *22*(1), 544–551. https://doi.org/10.34190/eccws.22.1.1448

Yun, Heylyung. (2025). China's Data Sovereignty and Security: Implications for Global Digital Borders and Governance. *Chinese Political Science Review*, *10*(2), 178–203. https://doi.org/10.1007/s41111-024-00269-9

Zichichi, Mirko, Ferretti, Stefano, D'Angelo, Gabriele, & Rodríguez-Doncel, Víctor. (2022). Data governance through a multi-DLT architecture in view of the GDPR. *Cluster Computing*, *25*(6), 4515–4542. https://doi.org/10.1007/s10586-022-03691-3