Journal of Law & Social Politics
Volume 3, Issue 2, 84-96
e_ISSN: 2807-6311
https://jolastic.id/index.php/jlsp/index
DOI: doi.org/10.59261/jlsp.vx3i2.71

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

***Rahayudin**
Universitas Sehati, Indonesia

Muchammad Naseer
Universitas Teknologi Bandung, Indonesia

Nova Agustina
Universitas Teknologi Bandung, Indonesia

Antonio Guterres
Universidade Oreintal Timor Lorosa'e, Timor Leste

***Corresponding author:**
Rahayudin, Universitas Sehati, Indonesia.
✉ ayudrahayudin90@gmail.com

Article Info :

Article history:
Received: July 18, 2025
Revised: August 19, 2025
Accepted: November 24, 2025

Keywords:
digital sovereignty; personal data protection; comparative law; cross-border data governance; national data policy

Abstract

Background: The rapid expansion of the global digital economy has intensified the importance of regulating data governance, particularly in relation to digital sovereignty and the protection of personal data. However, significant differences persist among national legal frameworks, creating regulatory gaps in cross-border data governance and oversight mechanisms. This condition raises critical legal and policy challenges, especially for developing countries such as Indonesia.
Objective: 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, as well as to assess their legal implications for national policy formulation in each jurisdiction.
Methods: This research employs a descriptive qualitative approach using a comparative juridical method. A statutory approach is applied to examine relevant laws and regulations, a comparative approach is used to analyze differences in data governance frameworks across jurisdictions, and a conceptual approach is employed to explore theoretical perspectives on digital sovereignty and data rights.
Results: The findings indicate that Indonesia emphasizes state control over data and the obligations of electronic system operators, the European Union prioritizes comprehensive protection of data subjects' rights through the General Data Protection Regulation, while the United States adopts flexible, sectoral regulations oriented toward private sector innovation. These differing paradigms result in variations in oversight effectiveness, levels of data protection, and cross-border data transfer mechanisms.
Conclusion: This study highlights the urgency for Indonesia to strengthen regulatory harmonization, enhance institutional oversight capacity, and develop equitable cross-border data transfer mechanisms in order to reinforce digital sovereignty while aligning with international data protection standards.

To cite this article: Rahayudin, R., Naseer, M., Agustina, N., & Guterres, A. (2025). Digital Sovereignty and The Right to Data: A Comparative Study Between Indonesia, The European Union, and The United States. *Journal of Law and Social Politics*, 3(2), 84-96. https://doi.org/10.59261/jlsp.v3i2.71

INTRODUCTION

Nearly every aspect of contemporary human life relies on the use and processing of data, driven by the rapid development of information and communication technology (ICT). Activities ranging from social communication and economic transactions to access to public services and participation in digital platforms generate vast data footprints. This development presents opportunities for governments to enhance service efficiency and stimulate the growth of the

digital economy, while simultaneously posing serious challenges related to the management, security, and protection of sensitive personal data that may be vulnerable to misuse. In this context, the concept of digital sovereignty becomes increasingly relevant as it reflects a state's capacity to regulate, control, and safeguard data and digital infrastructure within its jurisdiction, including cybersecurity regulation and oversight of cross-border data storage and transfers. Consequently, digital sovereignty requires a legal and policy framework capable of balancing the protection of personal data rights with the utilization of digital technologies for public service delivery and economic development (Hummel et al., 2021).

The European Union has established itself 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 mandates strict compliance by businesses in the collection, processing, storage, and cross-border transfer of data. This regulation sets high protection standards by recognizing rights such as access, rectification, and erasure of personal data, as well as imposing mandatory data breach notification requirements. In contrast, the United States has adopted a more sectoral and adaptive regulatory approach through frameworks such as the California Consumer Privacy Act (CCPA), resulting in varied levels of protection across states and a fragmented data protection landscape. Meanwhile, Indonesia, as a developing country with a rapidly expanding digital ecosystem, is constructing its legal framework through the enactment of the Personal Data Protection Law (PDP Law) and regulations governing electronic systems. Nevertheless, Indonesia continues to face challenges related to consistent implementation, supervisory capacity, and harmonization with international standards. Accordingly, a balanced policy strategy is required to protect personal data rights while fostering innovation and development within the national digital sector (Houtan et al., 2020).

As technological advancement accelerates and the volume of personal data increases, countries are confronted with the challenge of safeguarding individual data rights without constraining digital economic growth. Differences in regulatory priorities and institutional capacity have led Indonesia, the European Union, and the United States to adopt diverse approaches to digital sovereignty and data protection. The European Union emphasizes strict compliance and comprehensive protection through the GDPR, while the United States favors more flexible, sector-based regulations. Indonesia, through the PDP Law and electronic system regulations, continues to refine its evolving legal framework. These differing models generate complex legal challenges, particularly concerning cross-border data transfers, regulatory harmonization, and effective law enforcement. Consequently, a comprehensive comparative analysis is necessary to identify best practices and regulatory gaps, providing a foundation for contextual policy recommendations aimed at strengthening digital sovereignty and personal data protection in Indonesia (Bühler et al., 2023).

Key issues addressed in this research include the effectiveness of regulatory frameworks in protecting individual personal data rights, the digital sovereignty mechanisms implemented across jurisdictions, and the degree of harmonization between national regulations and international standards—particularly in relation to interoperability, data security, and the obligations of cross-border electronic system operators (Calzada, 2021).

Recent studies indicate a global increase in personal data breaches, highlighting that the implementation of privacy-by-design principles and early-stage data protection measures remains insufficient. Despite the enactment of various regulatory frameworks, data management practices across many sectors frequently fall short of adequate protection standards, maintaining a high risk of data breaches. In Indonesia, (Fajri, 2023) identified inconsistent regulatory enforcement and weak oversight of electronic system providers as major contributors to rising data breaches in both public and private sectors, particularly as digital services increasingly process sensitive citizen data. In contrast, international research demonstrates that the European Union, through the GDPR, has significantly strengthened data subject rights, including rights to access, rectification, and erasure, while requiring organizations to adopt stringent data protection standards. However, GDPR implementation also presents challenges for international businesses, especially regarding cross-border compliance, information technology system adaptation, and international data transfer mechanisms (Bradford, 2020).

The literature on digital sovereignty underscores the importance of regulating cross-border data transfers, protecting national digital infrastructure, and maintaining control over domestically stored and processed data to preserve national security in an era of digital globalization. This concept encompasses legal and policy mechanisms enabling states to regulate, monitor, and enforce data rights, as well as technical dimensions such as network security and data center governance. The European Union has developed a comprehensive framework through the GDPR to ensure uniform data control and protection of data subjects' rights, while the United States continues to favor a sectoral, market-oriented regulatory model that offers flexibility but limits state control over data governance. In Indonesia, digital sovereignty initiatives are pursued through the PDP Law and electronic system regulations; however, implementation challenges persist, including limited oversight capacity, low stakeholder awareness, and discrepancies between legal norms and operational practices. Consequently, a more integrated, capacity-based national policy approach is necessary to enhance data protection effectiveness and reinforce Indonesia's digital sovereignty (Fabbrini & Celeste, 2020).

Research by (Putri, 2022) indicates that Indonesia is not yet fully prepared to implement comprehensive data protection standards, particularly in the management of sensitive and cross-sectoral data that require strong regulatory coordination and supervisory capacity. This condition reflects a gap between legal norms—such as those embodied in the PDP Law—and their practical implementation across public and private sectors. Furthermore, (Fajri, 2023) emphasizes that weak implementation of privacy-by-design principles, which integrate data protection at the system design stage, significantly contributes to the high risk of data breaches in Indonesia. As a result, data governance practices remain largely reactive and administrative, increasing vulnerability to data leaks, misuse, and unauthorized access. These findings underscore the urgency of strengthening institutional oversight, enhancing data management competencies, and consistently applying privacy-by-design principles to align Indonesia's data protection regime with global standards and to build public trust.

International studies by (Bradford, 2020) and (Kuner, 2021) reveal fundamental differences between European Union and United States data protection regimes. The GDPR is widely regarded as more effective in strengthening data subject rights, oversight mechanisms, and cross-border regulatory harmonization, whereas U.S. regulations remain fragmented, sectoral, and state-dependent. While the U.S. approach promotes market freedom and private sector innovation, it often results in uneven data protection, whereas the EU ensures consistency through uniform legal standards. Nonetheless, most existing studies focus on single jurisdictions and lack comprehensive analysis of digital sovereignty principles and their cross-national policy implications. This gap is particularly relevant for developing countries such as Indonesia, which are actively shaping digital regulatory frameworks amid limited institutional capacity. Therefore, a comparative study involving Indonesia, the European Union, and the United States is essential to provide an empirical foundation for contextual policy formulation and to support alignment with international standards without undermining digital sovereignty or citizens' personal data rights.

This study adopts a descriptive qualitative approach using a comparative juridical method to analyze legal principles and regulatory frameworks related to digital sovereignty and data rights in Indonesia, the European Union, and the United States. Through a statutory approach, the study examines relevant laws and regulations, including Indonesia's PDP Law and ITE Law, the GDPR and associated EU regulations, and the CCPA alongside sectoral privacy regulations in the United States. A comparative approach is employed to assess the implementation of data sovereignty principles, national policy orientations, domestic data control mechanisms, and cross-border data transfer regulations across the three jurisdictions. Additionally, a conceptual approach is applied to analyze theoretical perspectives on digital sovereignty, cybersecurity, and personal data rights, thereby constructing an integrated analytical framework that links legal, policy, and practical dimensions. This approach facilitates the identification of best practices and regulatory shortcomings and supports the formulation of context-sensitive policy recommendations for strengthening digital sovereignty in Indonesia (Zichichi et al., 2022).

The study aims to analyze and evaluate the impact of data sovereignty principles on the development and implementation of national policies in Indonesia, the European Union, and the United States, while comparing regulatory approaches to personal data protection across these jurisdictions. Through comparative analysis, the study seeks to identify best practices and regulatory gaps as a basis for developing policy recommendations to support Indonesia in establishing an effective, equitable, and adaptive data protection framework that responds to technological developments, safeguards digital sovereignty, protects personal data rights, and remains aligned with international norms and standards.

METHOD

Types of Research

This study employs a descriptive qualitative approach combined with a comparative legal method. Given that the research focuses on the legal analysis of laws and principles governing digital sovereignty (data sovereignty) and personal data rights across different jurisdictions, as well as their implications for national policy formulation, the comparative juridical method is considered the most appropriate. Through this approach, legal phenomena, regulatory frameworks, and implementation practices in Indonesia, the European Union, and the United States are systematically described, explained, and analyzed in depth using qualitative legal reasoning (Gravett, 2023).

Research Approach

This study is conducted using three main analytical approaches. First, the Statute Approach examines and evaluates relevant legislation in each jurisdiction, including the Personal Data Protection Law (PDP Law), the Electronic Information and Transactions Law (ITE Law), and implementing regulations governing electronic systems in Indonesia; the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the e-Privacy Directive in the European Union; as well as the California Consumer Privacy Act (CCPA), the Privacy Act, and federal regulations related to data governance and cybersecurity in the United States. This approach aims to identify the legal foundations of data regulation, control mechanisms, and the obligations imposed on electronic system providers.

Second, the Comparative Approach is applied to analyze similarities and differences in the implementation of digital sovereignty (data sovereignty) and personal data rights across the three jurisdictions, with particular attention to domestic data control regimes, cross-border data transfer regulations, and their influence on public, private, and national policymaking.

Third, the Conceptual Approach is used to construct an analytical framework by examining theories and concepts related to digital sovereignty, the right to personal data, privacy, and cybersecurity. This framework serves as the basis for linking legal principles with national policies and practices, as well as for formulating contextual and applicable legal recommendations for Indonesia (Adler-Nissen & Eggeling, 2024).

Sources and Types of Legal Materials

This research relies primarily on secondary data obtained from several categories of legal and academic sources. The first category consists of primary legal materials, including statutory laws and regulations such as the Personal Data Protection Law (PDP Law), the Electronic Information and Transactions Law (ITE Law), the GDPR, the Digital Services Act (DSA), the ePrivacy Directive, the California Consumer Privacy Act (CCPA), the Privacy Act, and other supporting regulations related to digital sovereignty and personal data protection.

The second category comprises secondary legal materials in the form of academic literature, including books, peer-reviewed journals, scientific articles, and research reports that discuss data sovereignty, personal data rights, and digital governance frameworks across jurisdictions.

The third category includes international policy reports and official documents issued by organizations such as the European Commission, UNCTAD, and the OECD, which provide additional insights into regulatory implementation, institutional capacity, and the broader impact of data protection policies on national governance. All these sources are examined

comprehensively to ensure an in-depth understanding of the concepts, practices, and legal implications of digital sovereignty and data rights at both national and international levels (Pins et al., 2022).

Data Collection

Data collection in this study is conducted in several stages. The first stage involves library research, focusing on the collection of relevant academic literature, statutory laws, and regulatory documents. The second stage includes systematic searches of official government websites, international organizations, and legal databases to obtain the most recent regulations, guidelines, and policy reports related to digital sovereignty and personal data protection.

The third stage consists of secondary document analysis, in which selected materials are reviewed and evaluated based on their relevance to the research objectives, including data sovereignty principles, regulatory impacts on national policies, and legal implications that inform policy recommendations. These stages are carried out in a structured and methodical manner to ensure that the collected data are current, relevant, and sufficiently robust to support the objectives of the study (Yun, 2025).

Data Analysis and Interpretation

Data analysis in this research is conducted through several qualitative, descriptive, and comparative stages. The first stage involves data classification, in which laws, legal doctrines, and academic literature are organized according to jurisdiction and thematic focus. The second stage applies regulatory content analysis to identify legal principles, individual rights, the obligations of electronic system operators, and oversight mechanisms embedded within the regulations.

The third stage consists of cross-jurisdictional comparison, assessing the strengths, weaknesses, and similarities of each legal framework concerning digital sovereignty and personal data protection. The fourth stage evaluates policy implications by examining how regulatory frameworks influence the formulation, implementation, and supervision of data governance in both public and private sectors. Finally, conclusions are drawn and policy recommendations are formulated by identifying best practices relevant to the Indonesian context and proposing feasible regulatory improvements (Obendiek, 2022).

Data Validity

To ensure the credibility, accuracy, and consistency of the analysis, several data validity techniques are applied. First, data source triangulation is conducted by comparing information derived from statutory regulations, academic publications, and official institutional reports. Second, regulatory cross-checking is performed to assess consistency between legal texts, implementation guidelines, and independent evaluations published by oversight bodies or academic sources.

Third, the validity of the analysis is reinforced through academic referencing and peer-reviewed literature, ensuring that conclusions are grounded in previously verified and reputable scholarly work. These combined strategies strengthen the reliability of the findings and support conclusions drawn from credible and authoritative sources (Kukutai, 2023).

RESULTS AND DISCUSSION

Result

To systematically examine differences in the application of data sovereignty principles across jurisdictions, a comparative overview of Indonesia, the European Union, and the United States is required. Each jurisdiction adopts a distinct regulatory orientation in governing data management, protecting data subject rights, and regulating cross-border data transfers. Table 1 presents a comparative analysis of data sovereignty principles and their practical implementation in the three jurisdictions, providing a foundational basis for the subsequent legal and policy 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.
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.

source: processed data

Based on table 1, 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. These variations reflect differing policy trade-offs between state control, individual rights protection, and digital innovation.

Beyond regulatory frameworks, data sovereignty principles significantly shape national policy directions in areas such as electronic system governance, digital public services, and data-driven economic development. To assess these policy-level impacts, Table 2 compares how data sovereignty principles influence national policy formulation and implementation across Indonesia, the European Union, and the United States.

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.

source: processed data

Table 2 illustrates that national policy trajectories are closely linked to the underlying data sovereignty models adopted by each jurisdiction. Indonesia utilizes data regulation as a tool to strengthen national digital governance, although further harmonization with international standards remains necessary. The European Union demonstrates high policy coherence through the uniform application of the GDPR, ensuring legal certainty and regulatory consistency. Conversely, the United States maintains fragmented yet flexible policies that support sectoral innovation but result in uneven data protection standards.

In addition to shaping regulatory and policy frameworks, data sovereignty principles generate distinct legal implications and necessitate tailored policy responses. To capture these dimensions, Table 3 presents a comparative overview of the legal implications and corresponding policy recommendations in Indonesia, the European Union, and the United States.

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.

source: processed data

As summarized in Table 3, each jurisdiction faces distinct legal consequences arising from its approach to data sovereignty. 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.

Discussion

Comparison of Data Sovereignty Principles Between Countries

The research findings indicate that the principle of data sovereignty is implemented differently in Indonesia, the European Union, and the United States, reflecting each jurisdiction's policy orientation and digital governance model (Holfelder et al., 2022). In Indonesia, the strengthening of state control over digital data is reflected in the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), both of which emphasize obligations related to domestic data processing and storage. This regulatory orientation aims to safeguard national security and protect citizens' sensitive data from the risks associated with cross-border data leakage (Mackinnon, 2022). These findings are consistent with (Putri, 2022), who argues that reinforcing digital sovereignty constitutes a strategic necessity for Indonesia amid the intensification of global digital activities (Janardhanan & Mas-Machuca, 2022).

However, the effective implementation of data sovereignty principles in Indonesia continues

to face substantial challenges. Although the Personal Data Protection Law mandates lawful, secure, and consent-based data processing, empirical practices demonstrate weak oversight and limited compliance among electronic system operators. Fajri (2023) highlights that insufficient supervisory capacity, low levels of business awareness, and the suboptimal application of security standards contribute significantly to the persistent occurrence of data breaches (Lee et al., 2020). This condition suggests that data sovereignty in Indonesia remains largely normative and has yet to be fully realized in substantive practice, thereby necessitating stronger audit mechanisms, clearer sanctions, and enhanced institutional capacity (Twigt, 2024).

In contrast to Indonesia, the European Union implements data sovereignty through an integrated and highly stringent legal framework centered on the General Data Protection Regulation (GDPR), which positions the protection of data subjects' rights as a fundamental pillar. The GDPR not only governs data collection and processing activities but also grants individuals extensive control through rights of access, rectification, restriction, and erasure. Moreover, the regulation of cross-border data transfers through adequacy decisions and standard contractual clauses ensures that the personal data of EU citizens remains subject to uniformly high protection standards. These findings align with (Bradford, 2020)**,** who characterizes the GDPR as the most comprehensive global model for enforcing digital sovereignty and facilitating cross-jurisdictional compliance (Celeste & Fabbrini, 2021).

The robustness of the European Union's approach is further reinforced by the application of the principles of privacy by design and privacy by default, which require the integration of data protection considerations from the earliest stages of system development. This regulatory requirement significantly enhances internal privacy governance and reduces the risk of data misuse (Kuner, 2021). By comparison, the United States adopts a sectoral regulatory framework through instruments such as the California Consumer Privacy Act (CCPA) and industry-specific regulations, offering considerable flexibility for private-sector innovation. While this model promotes digital economic growth, the absence of a unified federal data protection standard results in regulatory fragmentation, uneven levels of protection, and legal uncertainty for organizations operating across state boundaries, as noted by (Bradford, 2020)**.**

Comparative analysis of these three jurisdictions demonstrates that each model of data sovereignty reflects a distinct policy choice balancing state control, individual rights protection, and innovation flexibility (Cordes et al., 2024). Indonesia emphasizes domestic data control, the European Union prioritizes harmonization and strong data subject rights, and the United States favors market-driven flexibility (Calzada, 2023). These findings underscore the importance for Indonesia of strengthening its digital sovereignty framework while aligning with global standards—particularly those embodied in the GDPR—without undermining national interests (Kuenzler, 2021). This conclusion is consistent with the recommendations of Putri (2022) and Fajri (2023), both of whom emphasize the urgency of legal reform, enhanced oversight mechanisms, and strengthened institutional capacity to ensure effective data protection within an increasingly interconnected global digital ecosystem.

Impact on National Policy

The implementation of the principle of data sovereignty in Indonesia has had a significant influence on 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 citizens' data must be managed within national jurisdiction has encouraged the government to develop strategic digital infrastructure, including the establishment of a national data center and the enhancement of cybersecurity standards (Adelson & Mickelson, 2022). This policy direction is also closely aligned with the government's digital transformation agenda, encompassing e-government initiatives and the digitization of public services. Consistent with the findings of Fajri (2023), the reinforcement of data sovereignty is viewed as a prerequisite for building a secure, independent, and accountable digital ecosystem, while simultaneously strengthening the state's capacity to manage digital risks and deliver reliable technology-based public services.

The Personal Data Protection Law (PDP Law) was formulated as a key instrument for harmonizing national policies by establishing uniform principles, procedures, and standards for

data processing that must be observed by all electronic system operators in both the public and private sectors (Meireles, 2024). Nevertheless, various studies indicate that the implementation of this policy continues to face structural challenges, particularly in relation to limited technical guidelines, inadequate supporting infrastructure, and insufficient institutional capacity at both the central and regional levels. Divergent standards and operational practices across institutions have resulted in inconsistent application of data protection measures, thereby preventing the objective of harmonization from being fully realized (J. Gstrein, 2023). This condition highlights the urgent need to strengthen cross-institutional coordination and enhance institutional capacity to ensure the effective implementation of data sovereignty policies.

In contrast, the European Union demonstrates a higher degree of policy consistency through the implementation of the General Data Protection Regulation (GDPR), which obliges all member states to align their national legislation with uniform regional standards (Egbert & Ulbricht, 2024). This harmonized framework provides legal certainty in data protection, particularly with respect to cross-border data transfers and the fulfillment of data subjects' rights. According to (Bradford, 2020), the existence of a single regulatory standard enhances business compliance and facilitates effective oversight by data protection authorities. Moreover, the establishment of independent supervisory authorities in each member state, supported by clear sanctions mechanisms and accessible complaint procedures, strengthens law enforcement effectiveness and ensures equal protection of individual rights across the European Union (Gao, 2023).

The United States adopts a markedly different approach through sectoral and state-based regulations, such as the California Consumer Privacy Act (CCPA), which affords substantial flexibility for industry sectors to innovate (Islam et al., 2024). However, this regulatory model also results in fragmented data protection policies and non-uniform standards at the national level. (Kuner, 2021) emphasizes that regulatory disparities across sectors and states complicate compliance efforts and undermine consistency in data protection practices. Consequently, while the U.S. model supports digital economic growth and technological innovation, the level of data protection remains more varied and relatively less stringent compared to the European Union's integrated framework (Makanadar, 2024).

These differences in policy approaches demonstrate that the principle of data sovereignty directly affects the effectiveness of data protection regimes, cross-border interoperability, and the overall competitiveness of national digital ecosystems (Wenzelburger & König, 2025). Indonesia occupies a strategic position in balancing the reinforcement of digital sovereignty with the need for global regulatory 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 must strengthen the capacity of oversight institutions, improve cross-sectoral coordination, and selectively adopt relevant international best practices without relinquishing state control over citizens' data. Such an approach would enable Indonesia to develop a data sovereignty policy that is adaptive, competitive, and firmly committed to the protection of individual rights amid the evolving 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 generated significant legal implications by strengthening the national framework for personal data protection (Der Sylvestre Sidibe & Dhouib, 2024). The PDP Law establishes a more structured legal foundation for digital data governance, encompassing data collection, processing, storage, and destruction. However, as noted by Putri (2022), this regulatory advancement has not yet been fully matched by implementation readiness, particularly with regard to supervisory capacity, inter-institutional coordination, and the technical capabilities of the PDP Authority. In addition, limited public awareness of personal data rights constrains effective law enforcement, rendering the success of digital sovereignty highly dependent on institutional strengthening and sustained public education initiatives (Sun et al., 2024).

From the European Union's perspective, the implementation of the General Data Protection Regulation (GDPR) demonstrates that the principle of data sovereignty can function effectively when supported by comprehensive protection standards, robust oversight mechanisms, and cross-

jurisdictional regulatory harmonization (Graessler et al., 2024). The GDPR not only reinforces the position of individuals as data subjects through the recognition of fundamental rights, but also compels all entities including multinational corporations to adapt their internal policies and technological systems. According to Bradford (2020), the effectiveness of the GDPR is largely determined by the presence of independent supervisory authorities capable of coordinating across jurisdictions and consistently enforcing sanctions. This regulatory model illustrates how data sovereignty can be upheld without obstructing international data flows through legal 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 results in distinct legal consequences (Toki, 2024). The absence of a uniform federal data protection standard allows significant space for private sector innovation, but simultaneously leads to fragmented protection of individual rights. Kuner (2021) emphasizes that regulatory disparities across sectors and states generate legal uncertainty and create gaps in data protection. Consequently, while the U.S. model supports a dynamic and innovation-driven digital economy, the overall level of data protection remains uneven and comparatively weaker than the European Union's integrated regulatory framework (Catanzariti, 2024).

The comparative findings indicate that each jurisdiction must navigate a balance among three core interests: state control over data flows, the protection of individual rights, and the facilitation of private sector innovation (Wylde, 2023). For Indonesia, which is undergoing rapid digital transformation, the establishment of legal certainty and an adaptive regulatory ecosystem is particularly critical. Accordingly, Indonesia should strengthen oversight mechanisms under the PDP Law, enhance the institutional capacity of the Data Protection Authority, and develop clear technical guidelines governing data security, cross-border data transfers, and cloud computing services (Sharma & Aggarwal, 2024). These measures are consistent with the findings of Fajri (2023), who highlights the importance of public education and improved digital legal literacy as essential prerequisites for effective data protection.

As a policy recommendation, Indonesia should adopt a hybrid regulatory approach that integrates the stringent protection standards of the European Union with the innovation-oriented flexibility characteristic of the United States. Harmonization with international norms such as the GDPR is essential to enhance global interoperability, yet it must be pursued without undermining national digital sovereignty or the strategic interests of data-driven economic development (Haq et al., 2023). Strengthening independent supervisory authorities, formulating comprehensive technical standards, and actively involving the private sector in policy development can contribute to balanced and sustainable data governance. By selectively adopting best practices from both regulatory models, Indonesia has the opportunity to establish a responsive and competitive data sovereignty framework that effectively safeguards individual rights amid the evolving dynamics of the global digital ecosystem.

CONCLUSION

The application of the principles of digital sovereignty and the right to personal data reveals significant differences among Indonesia, the European Union, and the United States. Indonesia prioritizes domestic control over data and emphasizes the obligations of electronic system providers, the European Union places data subject rights at the core of regulation through the strict and harmonized cross-border implementation of the General Data Protection Regulation (GDPR), while the United States adopts a flexible, sectoral regulatory approach that strongly supports private sector innovation. These differing regulatory orientations directly shape national policy outcomes: the European Union has been relatively successful in establishing uniform and consistent data protection standards, the United States offers regulatory flexibility with varying levels of protection across sectors and states, and Indonesia continues to face challenges related to effective implementation and alignment with international standards.

The legal implications of these findings highlight the importance of strengthening oversight capacity, enhancing regulatory harmonization, and developing secure and reliable cross-border data transfer mechanisms. Within this context, Indonesia may draw on best practices from the European Union in reinforcing data subject rights, supervisory authority

independence, and enforcement mechanisms, while simultaneously adopting aspects of the United States' regulatory flexibility to foster digital innovation and economic growth. Such a balanced approach would allow Indonesia to strengthen its digital sovereignty without constraining the development of its national digital economy.

This research is distinguished by its integrated comparative analysis of regulatory frameworks, implementation practices, and the conceptual foundations of digital sovereignty. Nevertheless, the study is limited by its normative orientation and reliance on secondary data sources. Despite these limitations, the findings remain highly relevant as a foundation for the formulation of national data governance policies, the development of operational guidelines for both public and private sectors, and the enrichment of academic discourse for future research on digital sovereignty and personal data protection.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to all institutions and individuals who supported the completion of this research. Appreciation is extended to the academic community and legal scholars who provided valuable insights and constructive feedback during the research process. The authors also acknowledge the contribution of public institutions and open-access legal databases that facilitated access to regulatory documents and comparative legal materials essential for this study. Any remaining errors or interpretations presented in this article remain the sole responsibility of the authors.

AUTHOR CONTRIBUTION STATEMENT

Rahayudin contributed to the conceptualization of the study, research design, comparative legal analysis, and the drafting of the original manuscript. Muchammad Naseer was responsible for the literature review, theoretical framework development, and comparative analysis of international data protection regimes. Nova Agustina contributed to data collection, regulatory mapping, and analysis of national policy implications. Antonio Guterres provided critical review, methodological refinement, and editorial revisions to enhance the academic rigor of the manuscript. All authors reviewed, revised, and approved the final version of the manuscript.

REFERENCES

Adelson, N., & Mickelson, S. (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, R., & Eggeling, K. A. (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*. Oxford University Press.

Bühler, M. M., Calzada, I., Cane, I., Jelinek, T., Kapoor, A., Mannan, M., Mehta, S., Mookerje, V., Nübel, K., Pentland, A., Scholz, T., Siddarth, D., Tait, J., Vaitla, B., & Zhu, J. (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, I. (2021). Data Co-Operatives through Data Sovereignty. *Smart Cities*, *4*(3), 1158–1172. https://doi.org/10.3390/smartcities4030062

Calzada, I. (2023). *Postpandemic Technopolitical Democracy: Algorithmic Nations, Data Sovereignty, Digital Rights, and Data Cooperatives* (pp. 97–117). https://doi.org/10.1007/978-3-031-08608-3_6

Catanzariti, M. (2024). *Disconnecting Sovereignty* (Vol. 65). Springer International Publishing. https://doi.org/10.1007/978-3-031-60734-9

Celeste, E., & Fabbrini, F. (2021). *Competing Jurisdictions: Data Privacy Across the Borders* (pp. 43–58). https://doi.org/10.1007/978-3-030-54660-1_3

Cordes, A., Bak, M., Lyndon, M., Hudson, M., Fiske, A., Celi, L. A., & McLennan, S. (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, G., & Dhouib, S. (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, S., & Ulbricht, L. (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, F., & Celeste, E. (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, R. Y. (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, I., Pottebaum, J., Holland, M., Wiechel, D., Dickopf, T., & Stjepandić, J. (2024). *Leveraging Data Ecosystems in Model-Based Systems Engineering for Ecological, Circular Added Value*. https://doi.org/10.3233/ATDE240858

Gravett, W. (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, M. Y. M., Abhishta, A., Sommese, R., Jonker, M., & Nieuwenhuis, L. 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, W., Mayer, A., & Baumgart, T. (2022). Sovereign Cloud Technologies for Scalable Data Spaces. In *Designing Data Spaces* (pp. 419–436). Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_25

Houtan, B., Hafid, A. S., & Makrakis, D. (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, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1). https://doi.org/10.1177/2053951720982012

Islam, M., Valiani, A. A., Datta, R., Chowdhury, M., & Turin, T. 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, O. (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, S., & Mas-Machuca, C. (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, A. (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, T. (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 University Press.

Lee, A. R., Kim, M. G., Won, K. J., Kim, I. K., & Lee, E. (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, R., Mayr, S., Syrmoudis, E., Grossklags, J., Kübler-Wachendorff, S., & Kranz, J. (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, K. (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, A. (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, A. V. (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, N., & Jenkins, P. (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, A. S. (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, D., Jakobi, T., Stevens, G., Alizadeh, F., & Krüger, J. (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, I., & Aggarwal, A. (2024). *Digital Footprints and the Battle for Data Sovereignty* (pp. 74–83). https://doi.org/10.4018/979-8-3693-3253-5.ch005

Sun, N., Zhu, C., & Liu, Y. (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, V. (2024). *Indigenous Rights, Climate Change and Governance*. Edward Elgar Publishing. https://doi.org/10.4337/9781803924984

Twigt, M. (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, G., & König, P. 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, A. (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, H. (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, M., Ferretti, S., D'Angelo, G., & Rodríguez-Doncel, V. (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