JSH
Jurnal Smart Hukum
https://ejournal.ipinternasional.com/index.php/jsh
Open Access Journal
by Inovasi Pratama Internasional. Ltd
Member of Crossref
ISSN. 2961-841X

Cross-Border Data Flows and State Sovereignty: Balancing Globalization and National Security in the Digital Age

Ica Karina[1], Yosef Serano Korbaffo [2] Ronaldus Nurak [2], Fridus Bria[2], Yosef Kristoforus Taekab[2], Irsyad Sudirman[3]

[1] Universitas Katolik Santo Thomas, Indonesia
[2] Universitas Timor, Indonesia
[3] Universitas Kaltara, Indonesia
Correspondance Authors: ichakarina14@gmail.com

DOI: https://doi.org/10.55299/jsh.v4i1.1467
***Article history:** Received June 21, 2025: Revised July 10, 2025: Accepted July 20, 2025*

Abstract

The rise of cross-border data flows has transformed global connectivity and economic integration, but it also challenges traditional notions of state sovereignty and national security. This article employs a qualitative research approach to analyze the legal, political, and technological dimensions of cross-border data governance. Focusing on the tension between global digital integration and the imperative to safeguard national interests, the study explores regulatory trends, state responses, and the evolving landscape of digital sovereignty. The findings highlight the need for balanced approaches that protect national security without stifling innovation and international cooperation.

***Keywords:** national, security, cross-border*

INTRODUCTION

The digital revolution has fundamentally transformed the global landscape, ushering in an era where data is not only a critical economic asset but also a strategic resource that underpins national security, governance, and societal development. At the heart of this transformation lies the phenomenon of cross-border data flows, which refer to the movement of digital information across national boundaries. These flows are integral to the functioning of the global digital economy, enabling seamless communication, international trade, cloud computing, and the proliferation of digital services that transcend geographical limitations. Yet, as data increasingly traverses borders, it challenges the traditional Westphalian notion of state sovereignty, which has historically been defined by clear territorial boundaries and exclusive jurisdictional authority (Cui, 2025).

The tension between the borderless nature of cyberspace and the territorial logic of sovereignty has become one of the defining legal and policy dilemmas of the digital age. States are confronted with the dual imperatives of harnessing the benefits of globalization—such as economic growth, technological innovation, and international cooperation—while simultaneously safeguarding their national interests, protecting citizens' privacy, and ensuring the security of critical information infrastructures. This dynamic interplay has given rise to the concept of data sovereignty, which asserts that states have the right and authority to regulate, control, and protect data generated within their territories, regardless of where that data is stored or processed.

The Rise of Data Sovereignty

Data sovereignty has emerged as a central pillar in contemporary debates over digital governance. It represents the extension of state sovereignty into the digital domain, encompassing both the internal dimension—where states exercise supreme authority over data within their borders—and the external dimension, which involves asserting influence over data that may be stored or processed abroad but is deemed relevant to national interests. This extension is not merely theoretical; it is reflected in a growing body of national legislation, regulatory frameworks, and international agreements that seek to define and enforce the boundaries of data jurisdiction (Kaya & Shahid, 2025).

The evolution of data sovereignty is closely linked to concerns over national security, economic competitiveness, and the protection of fundamental rights such as privacy. For example, the United States, leveraging its technological dominance and the global reach of its digital corporations, has enacted laws like the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which asserts extraterritorial jurisdiction over data held by U.S. companies, regardless of the physical location of the data. The European Union, through the General Data Protection Regulation (GDPR), has established stringent rules for the transfer of personal data outside its borders, requiring recipient countries to provide an "adequate" level of protection. China, meanwhile, has adopted a robust data localization regime and enacted the Data Security Law to reinforce state control over critical data and mitigate perceived security risks associated with cross-border data transfers.

Competing Models and Global Fragmentation

These divergent approaches reflect broader geopolitical and ideological differences regarding the governance of digital spaces. The United States traditionally champions the free flow of data as essential to innovation and economic growth, yet it also employs long-arm jurisdiction to protect its interests and maintain strategic advantage. The European Union prioritizes data protection and privacy, seeking to project its regulatory standards globally through mechanisms such as adequacy decisions and the promotion of "technological sovereignty". China and Russia, on the other hand, emphasize cyber sovereignty and national security, implementing strict data localization requirements and asserting comprehensive state control over digital infrastructures (Zinovieva, 2024).

This multiplicity of models has led to what scholars describe as the "balkanization" or "fragmentation" of the global digital environment. Instead of a unified, interoperable cyberspace, the world is witnessing the emergence of competing regulatory spheres, each with its own rules, standards, and enforcement mechanisms. This fragmentation poses significant challenges for multinational corporations, which must navigate a complex web of legal obligations, and for smaller states, which risk being caught between competing regulatory blocs.

Legal and Policy Dilemmas

The legal dilemmas arising from cross-border data flows are multifaceted. On one hand, the free flow of data is indispensable for digital trade, cloud computing, artificial intelligence, and the functioning of global supply chains. Restrictions on data transfers—such as data localization mandates or excessive regulatory barriers—can stifle innovation, increase costs, and undermine the competitiveness of domestic industries. On the other hand, the absence of effective controls may expose states to significant risks, including cyber espionage, unauthorized surveillance, and the erosion of privacy protections for citizens.

The challenge, therefore, is to strike a balance between openness and control—between the imperatives of globalization and the demands of national security. This balancing act is further complicated by the technical characteristics of data, which is inherently mobile, easily replicable, and often controlled by private actors with transnational reach. The traditional tools of territorial jurisdiction are often ill-suited to the realities of the digital world, where data may be stored simultaneously in multiple jurisdictions, subject to overlapping and sometimes conflicting legal claims (Choi & Ji, 2024).

The Indonesian Perspective and the Global South

For countries like Indonesia and other members of the Global South, the stakes are particularly high. These states are major consumers of digital technologies developed and controlled by foreign entities, raising concerns about digital dependency, loss of regulatory autonomy, and the potential for foreign surveillance or economic exploitation. At the same time, the need to participate in the global digital economy compels them to adopt policies that facilitate cross-border data flows and attract foreign investment. The development of robust, context-sensitive legal frameworks that protect national interests while fostering innovation is thus a pressing priority (Fauzi et al., 2024).

Toward Harmonization and Cooperative Governance

Recognizing the risks of excessive fragmentation, international organizations such as the OECD and the G20 have initiated efforts to promote trust-based frameworks for cross-border data governance, emphasizing principles such as transparency, accountability, and mutual recognition of standards. While these initiatives offer a pathway toward harmonization, they face significant obstacles, including divergent national interests, varying levels of technological development, and the reluctance of major powers to cede regulatory authority.

METHOD

This study employs a qualitative research approach to comprehensively analyze the multifaceted dynamics of cross-border data flows and state sovereignty. Qualitative research is particularly well-suited to exploring complex phenomena within their natural settings, providing rich insights into the perspectives, experiences, and contextual factors that shape legal and policy outcomes. This approach allows for an in-depth examination of the legal instruments, policy documents, and case studies relevant to cross-border data governance, uncovering nuanced understandings and identifying emergent patterns (Bantugan, 2025).

Research Design

The research design is structured around a multi-method qualitative approach, incorporating doctrinal legal analysis, policy document review, and comparative case studies. This triangulation of methods enhances the validity and reliability of the findings, providing a holistic view of the interplay between cross-border data flows and state sovereignty.

Doctrinal Legal Analysis: This involves a systematic examination of primary legal sources, including national laws, international treaties, and regulatory frameworks governing cross-border data flows. The doctrinal analysis focuses on identifying the legal principles, rules, and standards that define the scope of state authority over data and regulate its movement across borders. Key legal instruments examined include the European Union’s General Data Protection Regulation (GDPR), the United States’ Clarifying Lawful Overseas Use of Data (CLOUD) Act, China’s Cybersecurity Law and Data Security Law, and relevant provisions of the World Trade Organization (WTO) agreements. The analysis seeks to elucidate how these legal instruments reflect and reinforce competing conceptions of sovereignty, privacy, and national security.

Policy Document Review: This aspect of the research involves an in-depth review of policy documents issued by governments, international organizations, and civil society groups. These documents include white papers, policy statements, regulatory guidelines, and reports that articulate the strategic objectives, policy positions, and practical measures adopted by various actors in response to the challenges posed by cross-border data flows. The policy document review aims to understand the rationales behind different policy choices, identify common themes and points of contention, and assess the effectiveness of various policy interventions.

Comparative Case Studies: The study incorporates comparative case studies of selected jurisdictions to illustrate the diverse approaches to cross-border data governance and their implications for state sovereignty. Case studies are chosen to represent different legal systems, economic models, and geopolitical contexts, allowing for a comparative analysis of the factors that shape regulatory outcomes. Key case studies include:

The European Union: The EU is examined as a regional leader in data protection, with the GDPR serving as a global standard for privacy regulation. The case study analyzes the EU's approach to balancing data protection with the promotion of digital trade, focusing on the mechanisms for cross-border data transfers, such as adequacy decisions and standard contractual clauses.

The United States: The US is analyzed as a proponent of free data flows and minimal regulatory intervention, with a focus on the role of market forces and self-regulation in governing cross-border data transfers. The case study examines the implications of the CLOUD Act for the extraterritorial reach of US law enforcement and the potential conflicts with other jurisdictions.

China: China is examined as a proponent of cyber sovereignty and data localization, with a focus on the Cybersecurity Law and Data Security Law. The case study analyzes the implications of these laws for cross-border data flows and the ability of foreign companies to operate in the Chinese market.

Indonesia: Indonesia is analyzed as a developing country seeking to balance the benefits of participating in the global digital economy with the need to protect national sovereignty and promote domestic innovation. The case study examines the regulatory challenges faced by Indonesia in governing cross-border data flows and the strategies adopted to promote data localization and build domestic digital capabilities.

Data Collection

Data collection for this study involves the following methods:

Legal and Policy Document Collection: Primary legal sources, policy documents, and regulatory guidelines are collected from official government websites, international organization databases, and legal research repositories. The collection process is systematic and comprehensive, ensuring that all relevant materials are included in the analysis.

Literature Review: A comprehensive literature review is conducted to identify scholarly articles, books, and reports that address the legal, economic, and political dimensions of cross-border data flows. The literature review serves to contextualize the research, identify key debates and theoretical frameworks, and inform the development of research questions.

Data Analysis

The data collected through doctrinal legal analysis, policy document review, and comparative case studies are analyzed using qualitative content analysis techniques. Qualitative content analysis involves a systematic process of coding, categorizing, and interpreting textual data to identify patterns, themes, and relationships.

Coding: The coding process involves assigning codes to segments of text based on their content and meaning. Codes are developed both deductively, based on the research questions and theoretical framework, and inductively, based on emergent themes identified in the data. Codes are organized into a codebook, which provides definitions and examples for each code to ensure consistency and reliability in the coding process.

Categorization: The coded data are then categorized into broader themes and categories based on their common characteristics and relationships. This process involves identifying patterns and connections across different codes and grouping them into higher-level categories that represent key aspects of the research topic.

Interpretation: The final stage of data analysis involves interpreting the categorized data to draw conclusions and answer the research questions. This process involves examining the relationships between different categories, identifying trends and patterns, and providing explanations for the observed phenomena. The interpretation is grounded in the data and supported by evidence from the legal and policy documents and case studies.

Validity and Reliability

To ensure the validity and reliability of the research findings, several measures are implemented:

- Triangulation: The use of multiple methods of data collection and analysis (doctrinal legal analysis, policy document review, and comparative case studies) enhances the validity of the findings by providing multiple sources of evidence to support the conclusions.
- Peer Review: The research design, data analysis, and findings are reviewed by experts in the field to ensure the rigor and credibility of the study.
- Transparency: The research process is documented in detail, including the methods of data collection, coding, and analysis, to ensure transparency and replicability.
- Reflexivity: The researcher acknowledges and reflects on their own biases and assumptions, recognizing the potential impact on the research process and findings.

RESULT & DISCUSSION

This section presents the findings of the qualitative analysis of cross-border data flows and state sovereignty, drawing from doctrinal legal analysis, policy document review, and comparative case studies. The results are organized around key themes that emerged from the data, supported by qualitative data presented in tables.

The analysis reveals a significant divergence in approaches to data governance across jurisdictions, reflecting differing priorities and values. This divergence is evident in the legal and policy frameworks adopted by the European Union, the United States, China, and Indonesia, as summarized in Table 1.

Table 1. Comparative Analysis of Data Governance Approaches

Jurisdiction	Approach to Data Governance	Key Legal Instruments	Priorities
European Union	Comprehensive data protection and privacy; emphasis on individual rights and consent; restrictions on cross-border data transfers to countries without "adequate" protection.	General Data Protection Regulation (GDPR)	Protecting individual privacy; promoting trust in the digital economy; asserting regulatory leadership; ensuring fair competition.
United States	Emphasis on free flow of information; minimal regulatory intervention;	Clarifying Lawful Overseas Use of Data (CLOUD) Act, California Consumer	Promoting innovation and economic growth; protecting national

Jurisdiction	Approach to Data Governance	Key Legal Instruments	Priorities
	sectoral approach to privacy; reliance on market forces and self-regulation; extraterritorial application of U.S. law.	Privacy Act (CCPA)	security; facilitating law enforcement access to data; maintaining technological leadership.
China	Cyber sovereignty and data localization; strict control over data and digital infrastructure; emphasis on national security and social stability; restrictions on cross-border data transfers without government approval.	Cybersecurity Law, Data Security Law, Personal Information Protection Law (PIPL)	Ensuring national security and social stability; maintaining state control over information; promoting domestic innovation; reducing reliance on foreign technology.
Indonesia	Balancing economic development with data protection; promoting data localization; developing a comprehensive data protection law; addressing digital sovereignty concerns; aligning with international standards.	Government Regulation No. 71/2019 on Electronic Systems and Transactions, draft Personal Data Protection Bill	Fostering economic growth and digital transformation; protecting personal data; promoting digital sovereignty; ensuring regulatory clarity and certainty; attracting foreign investment.

The EU's GDPR sets a high standard for data protection, emphasizing individual rights and imposing strict requirements for cross-border data transfers. The US CLOUD Act, in contrast, asserts extraterritorial jurisdiction over data held by US companies, potentially conflicting with other jurisdictions' laws. China's Cybersecurity Law and Data Security Law reflect a strong emphasis on cyber sovereignty and data localization, requiring certain data to be stored and processed within China. Indonesia is in the process of developing a comprehensive data protection law to balance economic development with data protection and digital sovereignty.

Data localization policies, which require data to be stored and processed within a country's borders, are a prominent feature of the cross-border data governance landscape. The analysis reveals that data localization policies have both benefits and drawbacks, as summarized in Table 2.

Table 2. Advantages and Disadvantages of Data Localization Policies

Advantages	Disadvantages
Enhanced national security and law enforcement access to data	Increased costs for businesses and consumers
Greater regulatory control and enforcement	Reduced innovation and competitiveness
Promotion of domestic data centers and digital infrastructure	Fragmentation of the global digital economy

Advantages	Disadvantages
Protection of personal data and privacy	Potential for protectionism and trade barriers
Promotion of local job creation and economic development	Hindrance to cross-border data flows and digital trade

Data localization policies can enhance national security by ensuring that sensitive data is stored within the country, making it more accessible to law enforcement and intelligence agencies. However, they can also increase costs for businesses, reduce innovation, and fragment the global digital economy.

International cooperation is essential for addressing the challenges posed by cross-border data flows and state sovereignty. The analysis reveals that international organizations, such as the G20, play a key role in promoting dialogue, developing common principles, and facilitating the harmonization of data governance frameworks.

Table 3. International Cooperation Initiatives

Initiative	Objectives	Key Participants
G20 Digital Economy Working Group (DEWG)	Promote international cooperation on digital economy issues; facilitate cross-border data flows with trust; develop common principles for data governance.	G20 member states
OECD initiatives on data governance	Promote trust-based frameworks for cross-border data flows; develop guidelines for data protection and privacy; facilitate international cooperation on cybersecurity.	OECD member states
APEC Cross-Border Privacy Rules (CBPR) System	Establish a framework for facilitating cross-border data flows while protecting personal data; promote interoperability of privacy frameworks across APEC economies.	APEC member economies

The G20 DEWG has focused on promoting cross-border data flows with trust, emphasizing principles such as transparency, lawfulness, and fairness. The OECD has developed guidelines for data protection and privacy and promoted trust-based frameworks for cross-border data flows. The APEC CBPR System provides a framework for facilitating cross-border data flows while protecting personal data.

Indonesia faces the challenge of balancing economic development with data protection and digital sovereignty. The analysis reveals that Indonesia is seeking to develop a comprehensive data protection law that aligns with international standards while addressing specific national interests.

Table 4. Indonesia's Approach to Data Governance

Policy Objectives	Key Challenges	Strategies
Promoting economic growth and digital	Ensuring regulatory clarity and certainty to attract foreign	Developing a comprehensive data protection law; promoting data localization; investing in

Policy Objectives	Key Challenges	Strategies
transformation	investment	digital infrastructure; fostering digital literacy.
Protecting personal data and privacy	Addressing the lack of a comprehensive data protection law	Enacting a personal data protection law; strengthening enforcement mechanisms; raising awareness of data protection rights.
Promoting digital sovereignty	Reducing reliance on foreign technology and digital platforms	Promoting domestic innovation; supporting local businesses; developing national digital infrastructure; encouraging data localization.

Indonesia's approach to data governance involves developing a comprehensive data protection law, promoting data localization, and investing in digital infrastructure. The aim is to foster economic growth and digital transformation while protecting personal data and promoting digital sovereignty

DISCUSSION

The research findings underscore the multifaceted challenges and opportunities presented by cross-border data flows in the context of state sovereignty. The analysis reveals a complex interplay of economic, legal, political, and technological factors that shape the governance of data in the digital age. This discussion delves into the key themes that emerged from the research, providing a nuanced understanding of the issues at stake and proposing potential pathways for navigating the intricate landscape (Wang, 2025).

Divergent Approaches to Data Governance: A Reflection of National Priorities

The research highlights a significant divergence in approaches to data governance across jurisdictions, reflecting differing priorities and values. The European Union, with its GDPR, emphasizes individual rights and imposes strict requirements for cross-border data transfers. This reflects a commitment to protecting personal data and promoting trust in the digital economy. The United States, while also valuing data protection, prioritizes the free flow of information and minimal regulatory intervention, reflecting a belief in the power of market forces and innovation. China, on the other hand, prioritizes cyber sovereignty and data localization, reflecting concerns about national security and social stability. Indonesia, as a developing country, seeks to balance economic development with data protection and digital sovereignty.

This divergence in approaches poses significant challenges for multinational businesses, which must navigate a complex web of overlapping and sometimes conflicting legal obligations. It also raises questions about the potential for regulatory arbitrage, where companies may seek to locate their data processing activities in jurisdictions with less stringent regulations (Maharani et al., 2025).

The Double-Edged Sword of Data Localization Policies

Data localization policies, which require data to be stored and processed within a country's borders, are a prominent feature of the cross-border data governance landscape. While such policies may enhance national security and regulatory control, they can also increase costs for businesses, reduce innovation, and fragment the global digital economy. Blindly pursuing cyber sovereignty through policies like data localization may create excessive barriers to cross-border data flow that, in the end, could negatively impact growth.

The decision to implement data localization policies involves a trade-off between competing interests. On the one hand, data localization can enhance national security by ensuring that sensitive data is stored within the country, making it more accessible to law enforcement and intelligence agencies. It can also promote the development of domestic data centers and digital infrastructure. On the other hand, data localization can increase costs for businesses, particularly small and medium-sized enterprises (SMEs), which may lack the resources to establish data centers in multiple countries. It can also reduce innovation by limiting access to global data sets and hindering the development of cross-border digital services.

The Imperative of International Cooperation

Given the inherently transnational nature of data flows, international cooperation is essential for addressing the challenges posed by cross-border data flows and state sovereignty. International organizations, such as the G20 and the OECD, play a key role in promoting dialogue, developing common principles, and facilitating the harmonization of data governance frameworks. However, progress in this area is often hindered by divergent national interests and geopolitical tensions. The free flow of data promoted by Western countries such as the United States emphasizes market dominance and technology drive, while countries such as China emphasize data sovereignty and advocate strict regulation of data flow by the state (Chang, 2024).

Despite these challenges, there is a growing recognition of the need for greater international cooperation in the area of data governance. One promising approach is the development of "trust-based" frameworks for cross-border data flows, which emphasize principles such as transparency, accountability, and the protection of fundamental rights. These frameworks seek to strike a balance between facilitating data flows and safeguarding legitimate public policy objectives.

Indonesia's Balancing Act: Economic Development, Data Protection, and Digital Sovereignty

Indonesia, as a developing country, faces the challenge of balancing economic development with data protection and digital sovereignty. On the one hand, Indonesia seeks to attract foreign investment and participate in the global digital economy. This requires a regulatory environment that is conducive to cross-border data flows. On the other hand, Indonesia also seeks to protect the personal data of its citizens and promote digital sovereignty. This may require stricter regulations on data flows and the development of domestic digital infrastructure.

The dilemma between liberalization and protection of resources has been going on for a long time, especially in developing economies like Indonesia. As a highly valuable resource, governments have an incentive to maintain sovereignty over its data through policies that may appear as barriers to cross-border data flow (Belli et al., 2024).

Indonesia's approach to data governance involves developing a comprehensive data protection law, promoting data localization, and investing in digital infrastructure. The aim is to foster economic growth and digital transformation while protecting personal data and promoting digital sovereignty. However, Indonesia must also be mindful of the potential costs of data localization policies and the need to maintain an open and competitive digital economy.

The Broader Implications for Global Governance

The challenges posed by cross-border data flows and state sovereignty have broader implications for global governance. The rise of digital technologies is transforming the nature of power and authority, challenging traditional notions of sovereignty and creating new forms of interdependence. As data becomes an increasingly important economic and strategic resource, states are seeking to assert greater control over its flow and use. However, the inherently transnational nature of data flows makes it difficult for any one state to exercise effective control.

This has led to a proliferation of competing regulatory frameworks and a fragmentation of the global digital space. The challenge for global governance is to find ways to manage these tensions and promote a more cooperative and inclusive approach to data governance. This will require a willingness to compromise and a recognition that the benefits of global digital interdependence can only be realized through collective action.

CONCLUSION

The discussion highlights the complex and multifaceted nature of the challenges and opportunities presented by cross-border data flows and state sovereignty. The research findings suggest that there is no one-size-fits-all solution to governing data in the digital age. Instead, states must adopt adaptive, collaborative, and rights-based approaches that take into account their specific national contexts and priorities. International cooperation is essential for promoting common principles and facilitating the harmonization of data governance frameworks. Indonesia, in particular, faces the challenge of balancing economic development with data protection and digital sovereignty, requiring a nuanced and context-sensitive approach to data governance. The current regulatory approach risks hindering reciprocity from other nations and weakening India's credibility in the global data economy. However, it must not only address concerns of arbitrariness and uncertainty but also critically examine its own role in undermining citizens' privacy rights. The effective governance of cross-border data flows will require a concerted effort by governments, businesses, civil society organizations, and international organizations to develop innovative legal and institutional frameworks that can accommodate diverse national interests while preserving the benefits of global digital interdependence.

Acknowledgment

We would like to express our deepest gratitude to all those who contributed to the completion of this research to the journal editorial team and reviewers for their constructive feedback and guidance, which greatly enhanced the quality of this work. This study would not have been possible without the collective efforts or support of all those involved.

REFERENCES

Bantugan, B. (2025). Qualitative Mindset behind Phenomenology: Implications to Qualitative Research Training. *International Journal of Research and Innovation in Social Science*, *IX*(IV), 4627–4641. https://doi.org/10.47772/IJRISS.2025.90400331

Belli, L., Gaspar, W. B., & Singh Jaswant, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, *54*, 106017. https://doi.org/10.1016/j.clsr.2024.106017

Chang, Q. (2024). The Legal and Regulatory Issues of AI Technology in Cross-Border Data Flow in International Trade. *Transactions on Economics, Business and Management Research*, *8*, 111–117. https://doi.org/10.62051/cyw9y102

Choi, K. M., & Ji, S. W. (2024). A Comparative Study on the Regulatory Philosophy and Methods for Online Platforms : Focusing on the EU Digital Services Act and the EU Audiovisual Media Services Directive. *Korean Constitutional Law Association*, *30*(4), 259–299. https://doi.org/10.35901/kjcl.2024.30.4.259

Cui, Y. (2025). Competition in the Digital Economy from the Perspective of Technonationalism: A Power Structure Model. *Journal of Research in Social Science and Humanities*, *4*(3), 64–79. https://doi.org/10.56397/JRSSH.2025.03.09

Fauzi, E., Citra, H., Marwenny, E., & Alfitrianti, N. (2024). Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty. *Jurnal Ilmiah Ekotrans & Erudisi*, *4*(1), 149–157. https://doi.org/10.69989/5f8ff494

Kaya, M., & Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. *Interdisciplinary Studies in Society, Law, and Politics*, *4*(2), 219–233. https://doi.org/10.61838/kman.isslp.4.2.20

Maharani, D. P., Kusumadara, A., Widhiyanti, H. N., & Dewantara, R. (2025). Revisiting personal data : Ownership theories and comparative legal perspectives from Europe, Indonesia and the United States. *Journal of Data Protection & Privacy*, *7*(3), 274. https://doi.org/10.69554/ZMLG9061

Wang, J. (2025). Challenges and Countermeasures in Cross-Border Data Collection. *Lecture Notes in Education Psychology and Public Media*, *79*(1), 25–31. https://doi.org/10.54254/2753-7048/2025.LC19166

Zinovieva, E. (2024). *Evolution of the Concept "Territorial Sovereignty" in the Digital Age* (pp. 187–195). https://doi.org/10.1007/978-3-031-50407-5_15