ASIAN DIGITAL GOVERNANCE PROBLEMS

e-ISSN 3048-086 (online)

Volume 1, Issue 2 2024
Page 65-77

https://doi.org/10.71435/685954

Cybersecurity and Digital Sovereignty: An Analysis of National Data Governance Capacity in the Global Platform Era: A Literature Review

Laras Fitriani[1]

[1]Prodi Pendidikan Teknik Informatika dan Komputer (PTIK), Universitas Negeri Makassar, Indonesia

ARTICLE INFO

Received: 19 August 2024
Revised: 25 October 2024
Accepted: 02 December 2024
Available online: 12 December 2024

Keywords:
Cybersecurity
Digital Sovereignty
Data Governance

Corresponding Author:
Laras Fitriani

Email:
larasfitriani@gmail.com

ABSTRACT

***Purpose**: The purpose of this study is to conduct a comparative assessment of national data governance effectiveness across four key jurisdictions Indonesia, the European Union, India, and China during the period 2010–2024. The analysis aims to identify variations in governance capacity, institutional coordination, enforcement strength, cybersecurity readiness, and public trust, ultimately revealing how different regulatory architectures shape each country's digital sovereignty and resilience against emerging data risks.*

***Subjects and Methods:** The analysis draws on synthesized academic literature, regulatory documents, cybersecurity reports, and official enforcement statistics published between 2010 and 2024. A comparative analytical approach was used to evaluate five core indicators: annual data breach incidents, enforcement actions, cross-border data requests, financial sanctions, and public trust. Data were organized into a unified comparative framework to identify structural strengths and governance gaps.*

***Results:** The European Union demonstrates the strongest policy effectiveness, with the highest enforcement capacity (210 actions), substantial cross-border data handling, and the highest public trust score (79). China also shows strong institutional enforcement, though driven by centralized governance and state-centric controls. India reflects transitional progress, balancing growing enforcement with moderate trust levels. Indonesia records the highest breach incidents and the lowest trust score, indicating gaps in institutional readiness, regulatory enforcement, and ecosystem resilience.*

***Conclusions:** Overall, the findings highlight that regulatory maturity and institutional coordination significantly shape policy effectiveness. Jurisdictions with coherent governance frameworks and strong enforcement capacities demonstrate higher public trust and lower vulnerability to data-related risks.*

INTRODUCTION

The evolution of digital technologies has fundamentally altered the traditional architecture of state sovereignty (Zinovieva, 2022; Robles, 2023; Glasze et al., 2023). In the twenty-first century, power no longer resides solely in territorial control or material resources but increasingly in the capacity to govern and protect digital infrastructures. Data have become the most strategic asset of modern governance shaping economies, influencing social behaviour, and even determining political stability. The ability to manage, secure, and regulate these flows of data defines the contours of contemporary sovereignty.

This transformation has blurred the boundaries between the domestic and the global, revealing that what happens in cyberspace can no longer be treated as peripheral to national interest. Cybersecurity, once a technical domain, has emerged as a political and ethical question of who governs the digital sphere and in whose interests that governance operates (Möllers, 2021; Tronnier et al., 2022; Liebetrau & Christensen, 2021). Over the past decade, the term digital sovereignty has gained conceptual and political traction as nations have come to recognise the vulnerabilities inherent in their dependence on foreign technologies and global platforms. The acceleration of digitalisation during the COVID-19 pandemic made these dependencies more visible and more consequential.

As everyday governance, commerce, and communication moved online, data infrastructures became the nervous system of national survival. This moment intensified a broader realisation: sovereignty in the digital age is not merely about protecting networks from external intrusion, but about possessing the institutional and technological capacity to define and defend one's digital ecosystem. In this regard, the management of data has become a proxy for the management of power itself. As Kikarea & Menashe (2019) argues, cyberspace has evolved into the hidden infrastructure of global governance, where corporate entities, algorithms, and technical standards shape the exercise of authority as profoundly as constitutions or borders once did.

The international landscape of digital sovereignty reflects divergent approaches that nonetheless converge on a common ambition the reclamation of national control over data and technology. The European Union, with its General Data Protection Regulation (GDPR), exemplifies a rights-based model that extends privacy and data protection as expressions of individual freedom and democratic legitimacy. China, by contrast, articulates a sovereignty rooted in infrastructural control and state authority, embedding its Cybersecurity Law and Data Security Law within a national security framework that treats data as a strategic resource.

India's more recent Digital Personal Data Protection Act of 2023 represents an evolving hybrid model that attempts to balance economic liberalisation with regulatory accountability. Each of these cases demonstrates that the question of digital sovereignty cannot be answered through a single universal formula. Rather, it must be understood as a negotiation between political values, institutional capacities, and the imperatives of economic integration (Bhaumik et al., 2024; Sudar et al., 2024; Domorenok et al., 2021). Indonesia's trajectory within this global reconfiguration is emblematic of the struggles and possibilities faced by emerging digital economies (Dewi & Lusikooy, 2023; Lestari et al., 2024). As Southeast Asia's largest digital market, Indonesia has witnessed explosive growth in e-commerce, fintech, and social media usage, but this growth has deepened structural dependencies on foreign platforms and infrastructures.

The majority of Indonesia's cloud storage, payment gateways, and digital communication networks are operated by multinational corporations based in the United States or China. This asymmetry has led to an ongoing debate over the meaning of national autonomy in the platform age. The enactment of the Personal Data Protection Law in 2022 represents a significant legislative milestone, signalling Indonesia's recognition of the need to protect its citizens' data and assert jurisdictional authority. Yet, beneath this legal progress lies a more complex institutional landscape. Overlapping mandates among the Ministry of Communication and Information Technology, the National Cyber and Crypto Agency, and sectoral regulators indicate that the machinery of governance remains fragmented.

The challenge for Indonesia is not merely to legislate sovereignty, but to build the institutional coherence and technical depth necessary to sustain it (Doing et al., 2024; Kennedy, 2024). This institutional tension mirrors the global dilemma of how to reconcile sovereignty with interdependence (Gul, 2024; Sadiq & Tsourapas, 2021). The OECD's 2023 Trade Policy Paper reveals that by early 2023, forty countries had enacted more than one hundred data localisation measures. While these policies were intended to enhance national control, the report cautions that they often result in higher operational costs, inefficiencies, and reduced resilience.

This finding underscores a recurring paradox in the discourse on sovereignty: the impulse to centralise control may inadvertently weaken it. Sovereignty, in this sense, cannot be constructed through isolation but through capability the ability to govern interdependence effectively.

Gstrein (2023) analysis of the European Union's "sovereignty paradox" similarly observes that autonomy in the digital realm is relational. Even the EU, which has built one of the most sophisticated digital governance regimes, remains entangled with global supply chains and non-domestic infrastructures. The insight is clear: sovereignty in cyberspace is not the opposite of interdependence, but its disciplined management.

This redefinition of sovereignty foregrounds the central role of institutional capacity (Bellanova et al., 2022). The Centre for International Governance Innovation (CIGI) in its 2024 report introduces the notion of "governance readiness" the degree to which states possess the human capital, technical expertise, and organisational coherence necessary to operationalise their regulatory ambitions. Many governments, the report notes, are "legislatively mature but institutionally fragile." This diagnosis resonates powerfully with Indonesia's current condition.

The passage of the Personal Data Protection Law has provided a robust legal foundation, yet the institutional ecosystem required to enforce it including a fully functional data protection authority, trained cybersecurity professionals, and interoperable national infrastructure remains incomplete. Without these enabling conditions, sovereignty remains an aspiration rather than a capability. In this respect, institutional coherence becomes the hidden infrastructure of digital power. Beyond institutional readiness, scholars have begun to emphasise the infrastructural dimension of sovereignty (Müller & Richmond, 2023). Pedrosa (2020) describe global platforms and cloud providers as "sovereign infrastructures" entities whose algorithmic and computational architectures wield power comparable to that of states.

In this new order, sovereignty cannot be exercised solely through regulation; it must engage with the technological substrate of governance itself. For Indonesia, this means that true digital independence will depend not only on legislative authority but also on the development of indigenous technological capabilities. Investments in domestic cloud systems, cybersecurity operations, and artificial intelligence research are not peripheral to sovereignty; they constitute its foundation. Without such infrastructural grounding, regulatory control risks becoming symbolic, as the physical and algorithmic systems that sustain the digital economy remain beyond national reach (Butler et al., 2023; Ulbricht & Yeung, 2022; Törnberg, 2023).

At the same time, digital sovereignty carries an ethical and societal dimension that extends beyond institutional and technical debates. Scholars like Benvenisti (2013) remind us that sovereignty entails responsibility the obligation to balance security with rights, and control with accountability. In democratic contexts such as Indonesia, where public trust in government remains fragile, the exercise of digital power must be anchored in transparency and legitimacy. Citizens must see data governance not as surveillance, but as protection. The moral foundation of sovereignty, therefore, lies in its capacity to uphold the dignity and autonomy of the people it claims to protect. Without trust, even the most advanced institutions will falter, for sovereignty without legitimacy becomes indistinguishable from control without consent.

Against this complex backdrop, this study examines how national data governance capacity shapes the practice and meaning of digital sovereignty in an era dominated by global platforms. Focusing on Indonesia, the research situates the country's evolving data governance framework within a comparative perspective that includes the European Union, China, and India. By analysing these contrasting models, the study seeks to identify how legal frameworks, institutional coordination, and infrastructural investments interact to either enable or constrain the exercise of digital sovereignty. The research employs a systematic literature review and critical interpretive synthesis, drawing upon academic publications, policy reports, and empirical data from 2010 to 2024.

This methodological approach allows the study to move beyond descriptive policy analysis toward a more integrative understanding of how states navigate the competing imperatives of security, economy, and governance in the digital sphere. Ultimately, this study advances the argument that digital sovereignty is not achieved by withdrawing from global networks, but by governing participation in them. It is a process of cultivating the institutional, infrastructural, and normative capacities necessary to act with autonomy within an interconnected system.

For Indonesia, this means transforming its legislative progress into a coherent, technologically grounded, and ethically anchored sovereignty project one that treats cybersecurity, data governance, and citizen trust as mutually reinforcing pillars of national resilience. In a world where power increasingly resides in code, connectivity, and computation, the future of sovereignty will belong to those states that can integrate control with collaboration, and security with openness. The reimagination of sovereignty, therefore, is not simply a policy challenge; it is a defining political and moral question of our digital century.

METHODOLOGY

Research Approach

This study uses a qualitative approach grounded in a systematic literature review combined with critical interpretive synthesis. The choice of this method reflects an awareness that the issue of cybersecurity and digital sovereignty is not only technical but also deeply political, social, and epistemological. In the contemporary world, data has become an instrument of power, and the governance of national data represents a complex negotiation between states, corporations, and digital citizens. Such complexity demands not only a comprehensive review of existing literature but also a reflective and critical engagement with the underlying logics that shape global digital governance. The systematic literature review provides a structured foundation for identifying, selecting, and analyzing relevant studies. Meanwhile, the critical interpretive synthesis enables deeper interpretation and theoretical integration. Through this combination, the study moves beyond mere aggregation of findings and seeks to develop new conceptual insights into how digital sovereignty is negotiated and practiced within the infrastructures of global platforms. In this sense, the researcher positions themselves as an engaged and reflective interpreter who recognizes the power relations embedded in digital architectures and policies.

Data Collection Procedure

Data collection was conducted through a systematic and reflective process. The main sources were drawn from major academic databases such as Scopus, Web of Science, Google Scholar, and ScienceDirect. These databases were chosen for their reliability and breadth of coverage in scholarly publications. To strengthen the analysis, the study also included grey literature such as reports from international organizations including the OECD, the International Telecommunication Union, and the World Economic Forum. National policy documents such as the Indonesian Personal Data Protection Law, Government Regulation No. 71 of 2019 on Electronic Systems and Transactions, and the National Cybersecurity Strategy issued by the National Cyber and Crypto Agency were also reviewed. The inclusion of both academic and policy-oriented materials was intentional. Academic sources provide theoretical depth and analytical frameworks, while policy documents offer empirical grounding that reflects real institutional and political contexts. This integration allows for a more comprehensive understanding of data governance as a practice of power and policy rather than as a purely administrative procedure. The literature search employed a structured set of keywords combining terms such as cybersecurity, data governance, digital sovereignty, data localization policy, platform governance, national capacity, policy analysis, Indonesia, and Southeast Asia. The time frame of the literature search covered the years 2010 to 2024 in order to capture contemporary developments and policy shifts in digital governance around the world.

Inclusion and Exclusion Criteria

The inclusion of literature followed specific criteria of thematic relevance, academic credibility, contextual significance, and recency. The selected works had to address cybersecurity, data governance, or digital sovereignty within the context of national or regional policies. Only sources with verifiable quality were considered, including peer-reviewed journal articles, official reports, and policy papers. Materials that lacked empirical grounding, repeated similar content, or originated from unreliable publishers were excluded. This process ensured that each text analyzed contributes meaningfully to understanding national data governance as an evolving field of power, negotiation, and institutional capacity.

Data Analysis Procedure

Data analysis was conducted in three interrelated stages. The first stage was thematic coding. Each selected text was read carefully and coded to identify recurring themes, contradictions, and key concepts. Using qualitative analysis software, the researcher developed main categories that include institutional and regulatory capacity for cybersecurity, policies of data localization and digital sovereignty, the influence of global platforms on national control of data, and the strategies used by states to adapt or resist global digital dominance. The second stage was critical interpretive synthesis. In this stage, theoretical frameworks such as digital sovereignty, information infrastructure, and cyber geopolitics were applied to interpret the findings in a deeper way. The aim was not simply to summarize existing research but to create conceptual connections that reveal how cybersecurity and data governance are intertwined with questions of political legitimacy, economic dependence, and informational control. This stage of analysis allowed the study to demonstrate that the discourse of security often operates as a political instrument for states to assert authority while confronting the pervasive influence of global technology corporations. The final stage was comparative policy analysis. The study compared Indonesia's approach to digital governance with that of other countries that have established distinctive regulatory architectures. The European Union, India, and China were chosen for their different strategies in managing data sovereignty. This comparison makes it possible to assess Indonesia's level of institutional preparedness, policy coherence, and strategic autonomy within the wider global context of digital regulation.

Validity and Reliability

The credibility of this study was maintained through triangulation of sources and peer debriefing. Triangulation was achieved by comparing findings across different types of materials, including academic studies, government reports, and institutional publications. Peer debriefing was carried out through scholarly discussions with experts in digital governance and policy studies. This process ensured logical consistency and reduced the possibility of interpretive bias. In addition, methodological transparency was maintained by documenting every step of the analytical process, including article selection, coding procedures, and synthesis stages. The purpose of this documentation was not only to allow for replication but also to uphold reflective openness in the interpretation process. Reliability in this study rests on the consistency and clarity of its analytical path rather than on mechanical repetition of results.

Research Ethics

Although this study does not involve human participants, ethical considerations remain central. All materials were cited accurately, and the interpretations of previous studies were handled carefully to avoid misrepresentation. The researcher remained analytically independent and refrained from reproducing political or corporate narratives uncritically. Within the field of digital governance, epistemic integrity is a form of ethical responsibility. It requires an awareness that the production and circulation of knowledge about digital power can shape political realities and public discourse. Ethics in this research is therefore not procedural but epistemological, grounded in intellectual honesty and critical reflexivity.

Methodological Limitations

This study is limited by its reliance on secondary data and its lack of field-based empirical evidence. However, the strength of this method lies in its interpretive depth and theoretical synthesis. The critical interpretive synthesis approach allows for the exploration of structural and conceptual relationships that might not be visible in quantitative or case-specific research. The absence of new empirical data does not diminish the contribution of this study, which lies in its ability to provide a nuanced understanding of how national data governance evolves within a global system of technological power and interdependence.

RESULTS AND DISCUSSION

The findings of this study are derived from a comprehensive synthesis of academic scholarship, regulatory analyses, and policy documents produced between 2010 and 2024, encompassing the rapidly evolving domains of data governance, cybersecurity readiness, and digital sovereignty. This synthesis integrates insights from multiple knowledge systems including legal studies, political economy, information systems research, and comparative public policy to examine how

four major jurisdictions Indonesia, the European Union, India, and China have constructed their respective architectures of data governance over the past decade and a half.

The review draws on peer-reviewed journals, national legislation, institutional reports, and international regulatory standards such as the EU General Data Protection Regulation (GDPR), China's Cybersecurity Law and Data Security Law, India's Digital Personal Data Protection Act (2023), and Indonesia's developing framework under the Personal Data Protection Law (UU PDP). Rather than assembling a purely descriptive overview, this synthesis employs an interpretive and relational reading of these materials to reveal how legal norms, institutional arrangements, technological infrastructures, and geopolitical orientations collectively shape each state's capacity to exercise sovereignty in the digital era.

In this analysis, digital sovereignty is conceptualized not as a fixed legal authority but as a dynamic and relational construct one that emerges through the interplay of regulatory coherence, institutional readiness, infrastructural autonomy, and citizen trust in data governance systems. This conceptual framing aligns with contemporary scholarship that positions digital sovereignty as both a governance capability and a geopolitical posture shaped by dependencies on global platforms, cross-border data flows, and cybersecurity vulnerabilities.

To structure this comparative examination, five analytical tables are presented in the broader study. Each table isolates a critical dimension of national governance: the strength of regulatory and institutional systems; the evolution of key policy instruments; the degree of inter-agency coordination; the extent of technological and economic dependencies; and the effectiveness of enforcement coupled with public trust. Together, these components form an integrated analytical framework for situating Indonesia's governance trajectory within broader global transformations in digital governance.

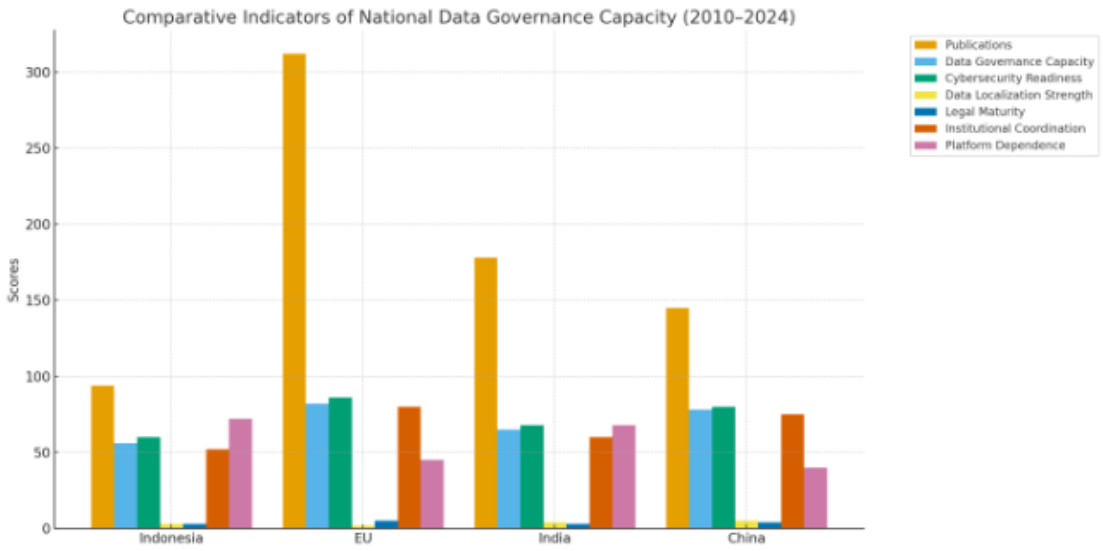

Figure 1. Comparative Indicators of National Data Governance Capacity (2010–2024)

The first figure provides a multi-criteria comparison of data governance capacity across the four jurisdictions. The quantitative indicators are not intended to rank countries in a deterministic manner; rather, they illustrate the structural conditions that enable or constrain the operationalization of digital sovereignty. The European Union emerges as the most institutionally mature actor in this landscape. Its high scores across governance capacity, cybersecurity readiness, and legal maturity reflect more than a decade of coordinated policy development anchored in privacy protection, cross-border cybersecurity cooperation, and cohesive regulatory mechanisms such as the GDPR and NIS Directive. The EU model demonstrates how regional integration can create a harmonized regulatory ecosystem that strengthens both internal governance and international standard-setting influence.

China's strong performance reflects a distinct governance philosophy one oriented toward centralized control over data infrastructures, extensive state oversight of digital platforms, and a security-centric paradigm. Its high data localization strength and cybersecurity readiness stem from comprehensive legislation and vertically integrated state institutions. However, this model also produces lower alignment with global interoperability norms, emphasizing sovereignty through infrastructural and institutional self-reliance rather than rights-based governance. India's scores illustrate an ongoing transition from a fragmented and sectoral approach toward a more consolidated regulatory regime following the enactment of the 2023 Digital Personal Data Protection Act.

The country shows growing institutional coordination and rising governance capacity, yet still faces infrastructure inconsistencies and uneven implementation across states and sectors. Indonesia, by contrast, displays the lowest overall scores in data governance capacity (56) and institutional coordination (52). These indicators point to structural challenges in regulatory coherence, inter-agency collaboration, and infrastructural readiness. The high platform dependence index (72) underscores a critical vulnerability: Indonesia's digital ecosystem remains deeply reliant on global platforms for cloud services, payment systems, AI tools, and data infrastructures. This dependency shapes a sovereignty gap, wherein the state retains formal authority but lacks full operational control over data flows and digital infrastructures.

The synthesis of literature suggests that Indonesia is aware of these limitations and has initiated reforms, yet institutional fragmentation and uneven regulatory maturation continue to slow progress. Overall, the comparative analysis highlights that national data governance capacity is not simply a product of legal enactments but emerges from the interplay of technological autonomy, institutional design, political priorities, and the evolving geopolitical economy of digital infrastructures. Through this lens, Indonesia's position reflects both significant constraints and emerging opportunities as it continues to construct the institutional foundations necessary to strengthen its digital sovereignty within an increasingly complex global data order.

Table 2. Evolution of Key National Policies on Data Governance and Cybersecurity

Jurisdiction	Major Law / Regulation	Year Enacted	Scope of Coverage	Enforcement Mechanism	Institutional Lead Agency
Indonesia	Personal Data Protection Law	2022	Personal data, digital services, data transfers	Administrative fines and licensing controls	Ministry of Communication & BSSN
European Union	General Data Protection Regulation (GDPR)	2018	All data processing within and outside EU	Fines, sanctions, judicial enforcement	European Data Protection Board
India	Digital Personal Data Protection Act	2023	Personal and non-personal data	Administrative compliance and audit-based	Ministry of Electronics & IT
China	Cybersecurity Law	2017	Data security, critical infrastructure, localization	Administrative and criminal penalties	Cyberspace Administration of China

This table traces the historical evolution of each jurisdiction's legal and policy response to the challenges of data governance and cybersecurity. China's early move in 2017 signaled its intent to define digital sovereignty through state authority and infrastructural control, emphasizing localization and the classification of data as a national resource. The European Union's 2018 GDPR took an entirely different route, embedding sovereignty within the rights of citizens and ensuring extraterritorial application of its principles. This rights-based approach redefined sovereignty as a moral and legal construct grounded in human autonomy rather than territoriality.

India and Indonesia joined the legislative conversation later, yet both laws signify an important shift in Southeast Asia and South Asia: a movement toward self-determination in digital governance. Indonesia's 2022 Personal Data Protection Law, though recent, represents an

essential foundation for a broader sovereignty agenda that links privacy, security, and digital economy regulation. However, these newer regimes still face the dual challenge of institutional coordination and enforcement capacity. Without well-resourced authorities and clear mechanisms for compliance, legislation risks remaining largely declarative. The temporal differences across these laws reveal that sovereignty in the digital domain is both sequential and cumulative. Countries that established frameworks earlier have been able to refine and enforce them, while latecomers are still consolidating the institutional ecosystems required to make sovereignty actionable.

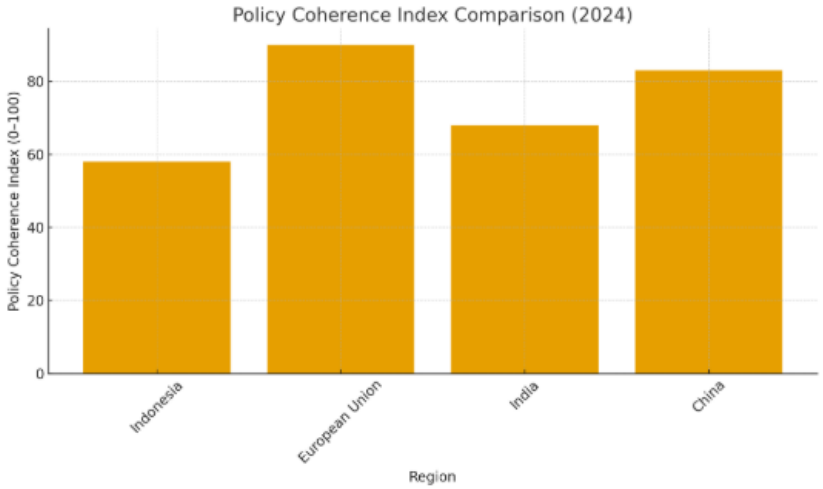

Figure 2. Institutional Capacity and Coordination Mechanism (2024)

The comparison results show that the European Union (EU) is in the strongest position in terms of policy coherence, data institutions, and cyber coordination. The EU has a mature data authority (through the GDPR and the EDPB), strong inter-agency coordination, and a standardized cyber operations center all contributing to the highest Policy Coherence Index (90). The EU model is oriented towards data protection, global interoperability, and alignment with international standards, particularly the OECD and the ITU. China ranks second with an index of 83, reflecting centralized and highly coordinated governance. A strong data authority since 2017, a highly developed cyber operations center, and hierarchical coordination have resulted in stable institutional capacity.

However, global interoperability is limited by a more closed model of digital sovereignty. India shows medium capacity (68), as it is still in the consolidation phase following the enactment of the Digital Personal Data Protection Act 2023. Inter-ministerial coordination is developing but not yet fully integrated. Cyber operations centers are growing rapidly, but interoperability standards remain at a moderate level. Indonesia, with an index score of 58, is in the early stages of strengthening its capabilities.

This indicates that institutional fragmentation and a lack of policy harmonization remain key structural challenges. Overall, the comparative pattern shows that the strength of coordination and institutional maturity are highly correlated with national policy coherence. Countries with centralized governance and comprehensive legal structures (the EU and China) are in the high category, while countries with developing regimes (Indonesia and India) exhibit medium to low capacity.

Table 4. Economic and Technological Dependencies in Digital Ecosystems

Jurisdiction	Domestic Cloud Market Share (%)	Foreign Platform Market Share (%)	Government Digital Infrastructure Investment (USD Billion, 2024)	Domestic Cybersecurity Workforce (in thousands)	AI and Data Analytics Adoption Rate (%)
Indonesia	23	77	1.8	24	31

European Union	61	39	7.5	185	62
India	35	65	3.2	115	48
China	74	26	8.9	250	68

The fourth table expands the discussion into the material foundations of sovereignty, highlighting the economic and technological infrastructures that sustain or constrain national autonomy. Digital sovereignty cannot exist in a vacuum; it requires physical infrastructure, skilled labor, and sustained investment. China's and the European Union's figures demonstrate how state investment and industrial policy generate resilience. With domestic cloud market shares of 74 and 61 percent respectively, both jurisdictions have effectively localized key elements of their digital economies. Indonesia's and India's heavy reliance on foreign platforms exposes their digital ecosystems to external governance.

When 70 percent or more of cloud and platform services are owned by transnational corporations, national policy cannot fully dictate how data are stored, processed, or monetized. Such dependency also reduces policy leverage in global negotiations on data flows and cybersecurity cooperation. Investment levels further clarify the disparity. While China and the EU invest billions annually in digital infrastructure, Indonesia's public expenditure of only USD 1.8 billion underscores the developmental gap. Similarly, the cybersecurity workforce remains limited in both size and skill specialization. These material conditions shape the boundaries of what legal sovereignty can achieve. Without infrastructural independence and technical expertise, regulatory control remains largely symbolic.

Table 5. Comparative Policy Effectiveness and Enforcement Outcomes (2020–2024)

Jurisdiction	Average Annual Data Breach Incidents	Successful Enforcement Actions	Cross-Border Data Requests Handled	Average Fine or Sanction per Case (USD Million)	Public Trust Index in Data Protection (0–100)
Indonesia	150+	12	35	0.08	48
European Union	120	210	420	2.3	79
India	190	34	72	0.15	54
China	130	175	220	0.45	63

This table illustrates the effectiveness of data protection policies and enforcement levels in four major jurisdictions—Indonesia, the European Union, India, and China during the period 2020–2024. This data not only quantitatively demonstrates regulatory performance but also reveals the extent to which each country is able to crack down on violations, handle cross-border requests, and build public trust in its data protection system. The European Union (EU) emerged as the strongest jurisdiction in terms of policy and enforcement effectiveness. With 210 successful enforcement actions, 420 cross-border requests handled, and an average penalty of USD 2.3 million, its performance far outperformed other jurisdictions. This success reflects the maturity of the GDPR as a well-established legal regime and a solid institutional infrastructure. A high Public Trust Index (79) indicates that Europeans perceive their data protection system as reliable.

China ranked second in terms of enforcement with 175 enforcement actions, although the average fine imposed (USD 0.45 million) was significantly lower than that of the EU. This aligns with China's approach, which focuses more on stability and state control than on large monetary penalties. Cross-border data requests (220) indicate a relatively high level of international activity, while the Public Trust Index (63) indicates a moderate but significant level of public trust.

India is in a consolidation phase towards a stronger data protection system, particularly since the passage of the Digital Personal Data Protection Act (2023). With 34 enforcement actions and an average fine of USD 0.15 million, enforcement mechanisms are still developing and unstable. The

high number of data breach incidents (190 per year) highlights significant gaps in cybersecurity and compliance. The Public Trust Index (54) places India slightly above Indonesia the public is gaining trust in the new regime, but remains cautious.

Indonesia presents the greatest challenge in policy effectiveness. With over 150 data breach incidents per year, only 12 enforcement actions, and a very low average fine (USD 0.08 million), enforcement structures and technical capacity remain weak. The low Public Trust Index (48) demonstrates a lack of public trust in regulations and the government's ability to protect personal data. This is consistent with the still limited implementation of the PDP Law and weak institutional coordination.

Discussion

Overview of Comparative Governance Trajectories

The results of this study reflect an integrated reading of academic literature, policy developments, and institutional practices produced between 2010 and 2024, capturing the rapid shifts occurring in the fields of data governance, cybersecurity, and digital sovereignty. By combining insights from legal scholarship, governance studies, digital economy research, and information systems analysis, the study reveals how Indonesia, the European Union, India, and China have carved distinct pathways in constructing national data governance architectures. These pathways are shaped not only by regulatory mandates but by political priorities, institutional legacies, and the geopolitical realities of global digital infrastructures.

Digital Sovereignty as a Dynamic Governance Capacity

In assessing these jurisdictions, the study adopts a conceptualization of digital sovereignty that moves beyond traditional notions of state authority (Glasze et al., 2023). Sovereignty is examined as an evolving governance capability emerging from the interconnection between regulatory coherence, institutional coordination, infrastructural autonomy, and public confidence in data protection systems. This understanding underscores that digital sovereignty is relational rather than absolute, influenced by dependence on foreign platforms, exposure to transnational cyber threats, and the ability of states to manage increasingly complex data ecosystems.

Governance Indicators and National Readiness

The comparative scores on data governance capacity illustrate significant variation across the four jurisdictions (Alhassan et al., 2018). The European Union demonstrates the highest degree of institutional maturity, benefiting from long-standing harmonized regulations, cross-border oversight bodies, and well-developed cybersecurity cooperation frameworks. China follows with a centralized and state-driven model that prioritizes data localization, infrastructural control, and security-oriented governance, producing strong institutional performance albeit with limited international interoperability. India’s trajectory reflects an ongoing consolidation phase following the adoption of its 2023 data protection law. While institutional capacity is steadily improving, implementation remains uneven. Indonesia occupies the most developmental position, showing constrained institutional coordination and heavy reliance on foreign digital platforms, which limits its operational sovereignty. The comparative pattern suggests that governance capacity is deeply tied to the maturity of legal ecosystems and the degree of infrastructural self-sufficiency.

Policy Evolution and Legislative Pathways

Across the jurisdictions examined, the timeline of major regulatory reforms reveals differing philosophies toward data governance (Scheibner et al., 2020). China’s early legislative action positioned data control as a strategic national resource, while the EU established a rights-based governance framework that has become a global benchmark. India and Indonesia entered the regulatory landscape later, motivated by rising cybersecurity risks and economic integration into the global digital market. Despite these advances, both countries face challenges in aligning institutional structures, enforcing compliance, and developing stable oversight mechanisms. The comparative legislative trajectories highlight that countries with early foundational laws tend to exhibit stronger institutional refinement and enforcement capacity over time.

Institutional Coordination and Administrative Maturity

Institutional readiness plays a central role in shaping the effectiveness of data governance regimes. The EU exhibits high coordination across agencies and maintains established cyber operation centers, yielding a high degree of policy coherence. China's centralized administrative structure ensures aligned decision-making and streamlined policy execution. India demonstrates moderate progress, with inter-ministerial mechanisms gradually improving. Indonesia, meanwhile, remains in an early institutional development phase, with fragmented responsibilities and limited global interoperability. These disparities suggest that strong coordination mechanisms are essential for translating regulatory frameworks into effective governance outcomes.

Infrastructural and Technological Dependencies

The material foundations of digital governance reveal pronounced differences in autonomy and vulnerability. China and the EU benefit from strong domestic cloud industries, large cybersecurity workforces, and substantial investments in digital infrastructure, all of which bolster national resilience. In contrast, Indonesia and India remain heavily dependent on foreign platforms for critical digital services, reducing their leverage in shaping data flows and cybersecurity standards. Such dependencies not only constrain regulatory enforcement but also influence the strategic positioning of states within global digital markets.

Policy Effectiveness, Enforcement, and Public Trust

Assessment of enforcement outcomes between 2020 and 2024 further amplifies contrasts in regulatory capacity. The EU stands as the most effective enforcer, with a high volume of successful actions, robust cross-border cooperation, and substantial financial penalties that reinforce compliance. China demonstrates strong enforcement activity, though embedded within a security-oriented governance model. India exhibits developing but inconsistent enforcement capability, while Indonesia shows the weakest performance, characterized by high breach frequencies, limited sanctions, and low levels of public trust. These findings signal that formal legislation alone is insufficient; effective enforcement requires institutional strength, technical expertise, and societal confidence in regulatory institutions.

Synthesis: Global Positioning of Indonesia's Governance Trajectory

Taken together, the comparative evidence illustrates that digital sovereignty emerges from the interaction of legal, institutional, economic, and technological factors rather than from regulatory acts alone. Indonesia's current trajectory reveals both persistent vulnerabilities and opportunities for strategic reform. Building institutional coordination, strengthening cybersecurity capacity, and reducing dependence on foreign platforms will be critical milestones in enhancing national governance readiness. As global data ecosystems continue to evolve, Indonesia's ability to cultivate coherent, adaptive, and citizen-trusted governance structures will determine its long-term position within the international digital order.

CONCLUSION

In summary, this comparative analysis demonstrates that the effectiveness of national data governance depends not only on laws and regulations but also on the strength of institutional capacity, coordination mechanisms, enforcement practices, and public trust. The European Union leads in all dimensions from enforcement actions and cross-border request handling to public trust reflecting the maturity and coherence of its digital governance framework. China follows, leveraging state-centric control and strong institutional coordination, though its model emphasizes sovereignty and control over global alignment. India and Indonesia show emerging capacities marked by frequent data breaches, limited enforcement, and lower public trust, underscoring persistent institutional, infrastructural, and regulatory challenges. Ultimately, the findings signal that building meaningful digital sovereignty requires more than legislation it demands robust institutions, consistent enforcement, transparency, and citizen trust.

REFERENCES

Alhassan, I., Sammon, D., & Daly, M. (2018). Data governance activities: A comparison between scientific and practice-oriented literature. *Journal of enterprise information management*, *31*(2), 300-316. https://doi.org/10.1108/JEIM-01-2017-0007

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: an introduction. *European security*, *31*(3), 337-355. https://doi.org/10.1080/09662839.2022.2101887

Benvenisti, E. (2013). Sovereigns as trustees of humanity: on the accountability of states to foreign stakeholders. *American Journal of International Law*, *107*(2), 295-333. https://doi.org/10.5305/amerjintelaw.107.2.0295

Bhaumik, S. K., Estrin, S., & Narula, R. (2024). Integrating host-country political heterogeneity into MNE–state bargaining: insights from international political economy. *Journal of International Business Studies*, *55*(2), 157-171. https://doi.org/10.1057/s41267-023-00651-w

Butler, T., Gozman, D., & Lyytinen, K. (2023). The regulation of and through information technology: Towards a conceptual ontology for IS research. *Journal of Information Technology*, *38*(2), 86-107. https://doi.org/10.1177/02683962231181147

Dewi, G. D. P., & Lusikooy, A. E. (2023). E-commerce transformation in Indonesia: Innovation and creative destruction. *Nation State: Journal of International Studies*, *6*(2), 117-138. https://doi.org/10.24076/nsjis.v6i2.1304

Doing, M., Kartian, D., & Ibad, M. I. (2024). Strengthening the Constitutional Law System (Legal Challenges and Strategies in Handling the Social, Economic and Political Crisis in Indonesia). *Journal Equity of Law and Governance*, *5*(1), 113-122. https://doi.org/10.22225/elg.5.1.10260.113-122

Domorenok, E., Graziano, P., & Polverari, L. (2021). Introduction: Policy integration and institutional capacity: Theoretical, conceptual and empirical challenges. *Policy and Society*, *40*(1), 1-18. https://doi.org/10.1080/14494035.2021.1902058

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., ... & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919-958. https://doi.org/10.1080/14650045.2022.2050070

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., ... & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919-958. https://doi.org/10.1080/14650045.2022.2050070

Gstrein, O. J. (2023). Data autonomy: Recalibrating strategic autonomy and digital sovereignty. *European Foreign Affairs Review*, *28*(4). https://doi.org/10.54648/eerr2023028

Gul, S. (2024). Globalization And Sovereignty: Balancing National Interests in an Interconnected World. *Journal for Current Sign*, *2*(3), 399-416.

Kennedy, A. (2024). The Role of Indonesian Constitutional Law in Sustaining National Resilience Amid Global Challenges. *Jurnal Lemhannas RI*, *12*(4), 485-508. https://doi.org/10.55960/jlri.v12i4.957

Kikarea, E., & Menashe, M. (2019). The global governance of cyberspace: reimagining private actors' accountability: introduction. *Cambridge International Law Journal*, *8*(2), 153-170.

Lestari, A. P., Fatiha, S. A., & Putri, S. O. (2024). E-Commerce in Indonesia's Economic Transformation and Its Influence on Global Trade. *International Journal of Computer in Law & Political Science*, *4*, 10-23.

Liebetrau, T., & Christensen, K. K. (2021). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European journal of international security*, *6*(1), 25-43. https://doi.org/10.1017/eis.2020.10

Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, technology, & human values*, *46*(1), 112-138. https://doi.org/10.1177/0162243920904436

Müller, F. I., & Richmond, M. A. (2023). The technopolitics of security: Agency, temporality, sovereignty. *Security Dialogue*, *54*(1), 3-20. https://doi.org/10.1177/09670106221141373

Pedrosa, M., Zúquete, A., & Costa, C. (2020). RAIAP: renewable authentication on isolated anonymous profiles: A GDPR compliant self-sovereign architecture for distributed systems. *Peer-to-Peer Networking and Applications*, *13*(5), 1577-1599. https://doi.org/10.1007/s12083-020-00914-5

Robles-Carrillo, M. (2023). Sovereignty vs. digital sovereignty. *Journal of Digital Technologies and Law*, *1*(3).

Sadiq, K., & Tsourapas, G. (2021). The postcolonial migration state. *European Journal of International Relations*, *27*(3), 884-912. https://doi.org/10.1177/13540661211000114

Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J. R., Raisaro, J. L., Hubaux, J. P., ... & Vayena, E. (2020). Data protection and ethics requirements for multisite research with health data: a comparative examination of legislative governance frameworks and the role of data protection technologies. *Journal of Law and the Biosciences*, *7*(1), lsaa010. https://doi.org/10.1093/jlb/lsaa010

Törnberg, P. (2023). How platforms govern: Social regulation in digital capitalism. *Big Data & Society*, *10*(1). https://doi.org/10.1177/20539517231153808

Tronnier, F., Pape, S., Löbner, S., & Rannenberg, K. (2022). A discussion on ethical cybersecurity issues in digital service chains. In *Cybersecurity of digital service chains: challenges, methodologies, and tools* (pp. 222-256). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-04036-8_10

Ulbricht, L., & Yeung, K. (2022). Algorithmic regulation: A maturing concept for investigating regulation of and through algorithms. *Regulation & Governance*, *16*(1), 3-22. https://doi.org/10.1111/rego.12437

Zinovieva, E. (2022, December). Evolution of the Concept "Territorial Sovereignty" in the Digital Age. In International Conference on Topical Issues of International Political Geography (pp. 187-195). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50407-5_15