ASIAN DIGITAL GOVERNANCE PROBLEMS

e-ISSN 3048-086 (online)

Volume 1, Issue 2 2024
Page 71-87

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]Informatics and Computer Engineering Education Study Program, State University of 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**: This study examines national data governance capacity in the context of cybersecurity and digital sovereignty across Indonesia, the European Union, China, and India during 2010–2024. The research aims to identify how institutional coordination, regulatory coherence, enforcement effectiveness, technological autonomy, and public trust shape digital sovereignty within the global platform era.*

***Subjects and Methods:** This study employed a qualitative systematic literature review combined with critical interpretive synthesis. Data were collected from 76 academic articles, cybersecurity reports, institutional publications, and regulatory documents identified through a PRISMA-based selection process. The analysis applied thematic coding, repeated reading, conceptual integration, and comparative governance analysis to examine recurring governance patterns and institutional contradictions.*

***Results:** The findings reveal that digital sovereignty operates as a multidimensional governance capacity shaped by institutional integration, cybersecurity readiness, technological infrastructure, and governance legitimacy. The European Union demonstrates strong regulatory coherence, China exhibits centralized enforcement and technological autonomy, India reflects transitional governance adaptation, while Indonesia faces governance fragmentation, technological dependency, and weak cybersecurity preparedness.*

***Conclusions:** Effective digital sovereignty requires integrated governance systems, sustainable technological investment, institutional coordination, and long-term public trust in digital governance.*

INTRODUCTION

The rapid expansion of digital technologies has fundamentally transformed the nature of state sovereignty and governance in the twenty-first century. Political authority is increasingly shaped not only by territorial control but also by the ability of states to regulate digital infrastructures, govern data flows, and secure cyberspace (Zinovieva, 2022; Robles, 2023; Glasze et al., 2023). Data have become strategic assets influencing economic systems, political communication, and national security. Consequently, cybersecurity and digital governance are no longer viewed as purely technical matters, but as central dimensions of institutional resilience and state power.

The concept of digital sovereignty has gained growing attention as governments become increasingly dependent on global digital platforms, cloud infrastructures, and transnational data ecosystems. This dependency raises important questions concerning who controls data, regulates digital systems, and determines governance standards in cyberspace (Möllers, 2021; Tronnier et

al., 2022; Liebetrau & Christensen, 2021). The COVID-19 pandemic intensified these concerns by accelerating digitalization across governance, commerce, and social interaction, exposing vulnerabilities associated with weak cybersecurity capacity and technological dependence.

Scholars argue that digital sovereignty should be understood not merely as technological independence, but as a governance capacity involving institutional coordination, cybersecurity readiness, legal coherence, infrastructural resilience, and public trust (Bellanova et al., 2022; Gstrein, 2023). In this context, cybersecurity becomes inseparable from governance because cyber threats, data breaches, and platform manipulation directly affect economic stability, public trust, and national security.

Different jurisdictions have adopted contrasting approaches to digital governance. The European Union established a rights-based governance model through the General Data Protection Regulation (GDPR), emphasizing privacy protection, accountability, and democratic legitimacy. China, by contrast, adopts a centralized and security-oriented model through the Cybersecurity Law and Data Security Law, positioning data as a strategic national resource. India's Digital Personal Data Protection Act of 2023 reflects a hybrid approach balancing economic growth with institutional regulation. These variations demonstrate that digital sovereignty is shaped by political priorities, institutional structures, and technological capacities rather than by a single universal framework (Bhaumik et al., 2024; Sudar et al., 2024; Domorenok et al., 2021).

Indonesia represents an important case within this global transformation because of its position as Southeast Asia's largest digital economy (Dewi & Lusikooy, 2023; Lestari et al., 2024). The rapid growth of e-commerce, fintech, and cloud services has generated economic opportunities while simultaneously increasing dependence on foreign digital infrastructures and multinational platforms. Indonesia's enactment of the Personal Data Protection Law in 2022 reflects growing awareness that data governance is closely connected to national security, economic resilience, and citizen rights. Overlapping responsibilities among regulatory institutions continue to create governance fragmentation and weaken policy coordination (Doing et al., 2024; Kennedy, 2024).

Existing literature shows that many countries possess formal legal frameworks for data governance but still struggle to operationalize digital sovereignty effectively. The OECD Trade Policy Paper (2023) notes that increasing data localization policies often create governance inefficiencies and interoperability problems. Similarly, Gstrein (2023) argues that sovereignty in cyberspace depends less on isolation and more on institutional capacity to govern global interdependence. This indicates that legal reform alone is insufficient without institutional readiness, technical expertise, and sustainable digital infrastructure.

Institutional and infrastructural capacity therefore become critical components of digital sovereignty. Scholars increasingly emphasize that cloud infrastructures, platform systems, and algorithmic architectures function as forms of "sovereign infrastructure" shaping political authority and economic control within digital societies (Pedrosa, 2020; Butler et al., 2023; Ulbricht & Yeung, 2022; Törnberg, 2023). Countries lacking domestic technological capacity remain dependent on external systems, limiting their strategic autonomy and regulatory effectiveness.

Digital sovereignty also carries an important ethical dimension. Sovereignty is not only about control over digital systems, but also about legitimacy, accountability, and citizen trust (Benvenisti, 2013). In democratic contexts such as Indonesia, cybersecurity governance must balance state security interests with transparency, privacy protection, and public accountability.

Despite the growing literature on cybersecurity and digital governance, several gaps remain. Existing studies often focus separately on cybersecurity, legal frameworks, or digital sovereignty without integrating institutional coordination, infrastructural dependency, enforcement capacity, and public trust within a comparative analytical framework. Comparative studies examining Indonesia alongside the European Union, China, and India also remain limited.

This study addresses these gaps by analyzing national data governance capacity across Indonesia, the European Union, India, and China between 2010 and 2024. The study examines how institutional coordination, cybersecurity readiness, regulatory coherence, technological

dependency, and enforcement capacity shape digital sovereignty in the era of global platforms. Using a systematic literature review combined with critical interpretive synthesis, this research seeks to provide a broader understanding of how states negotiate sovereignty within increasingly interconnected digital ecosystems.

This article argues that digital sovereignty should be understood as an adaptive governance capacity emerging from the interaction between legal authority, institutional readiness, technological autonomy, and public trust. Indonesia's experience illustrates both the opportunities and structural challenges faced by emerging digital economies in strengthening sovereignty within a platform-dominated global digital order.

METHODOLOGY

Research Design

This study employed a qualitative systematic literature review combined with critical interpretive synthesis to examine national data governance capacity in the context of cybersecurity and digital sovereignty. The approach was selected because issues related to cybersecurity, platform governance, and digital sovereignty involve not only technical dimensions but also institutional, political, and geopolitical dynamics. A systematic literature review enabled the study to identify and organize relevant academic and policy discussions in a structured manner, while critical interpretive synthesis allowed deeper conceptual interpretation of governance patterns, institutional capacity, and regulatory trajectories across different jurisdictions. The study focused on four comparative jurisdictions: Indonesia, the European Union, India, and China. These cases were selected because they represent different governance models in regulating cybersecurity, data sovereignty, and platform governance. The comparative approach enabled the study to evaluate variations in institutional readiness, regulatory coherence, enforcement mechanisms, and technological dependency within the global digital ecosystem.

Literature Search Strategy

The literature search was conducted systematically using major academic databases, including Scopus, Web of Science, ScienceDirect, and Google Scholar. To strengthen contextual analysis, grey literature and institutional reports were also included from organizations such as the OECD, International Telecommunication Union (ITU), World Economic Forum (WEF), and national cybersecurity agencies. Policy documents and legislation relevant to digital governance were additionally reviewed, including the European Union GDPR, China's Cybersecurity Law, India's Digital Personal Data Protection Act (2023), and Indonesia's Personal Data Protection Law (2022). The search process used combinations of the following keywords: cybersecurity, digital sovereignty, data governance, platform governance, data localization, national cybersecurity capacity, cross-border data regulation, digital governance, Indonesia, European Union, China, India. The literature search covered publications from 2010 to 2024 to capture the evolution of cybersecurity governance and digital sovereignty during the global platform era.

PRISMA-Based Literature Selection Process

The study adopted a simplified PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) procedure to ensure transparency in literature selection.

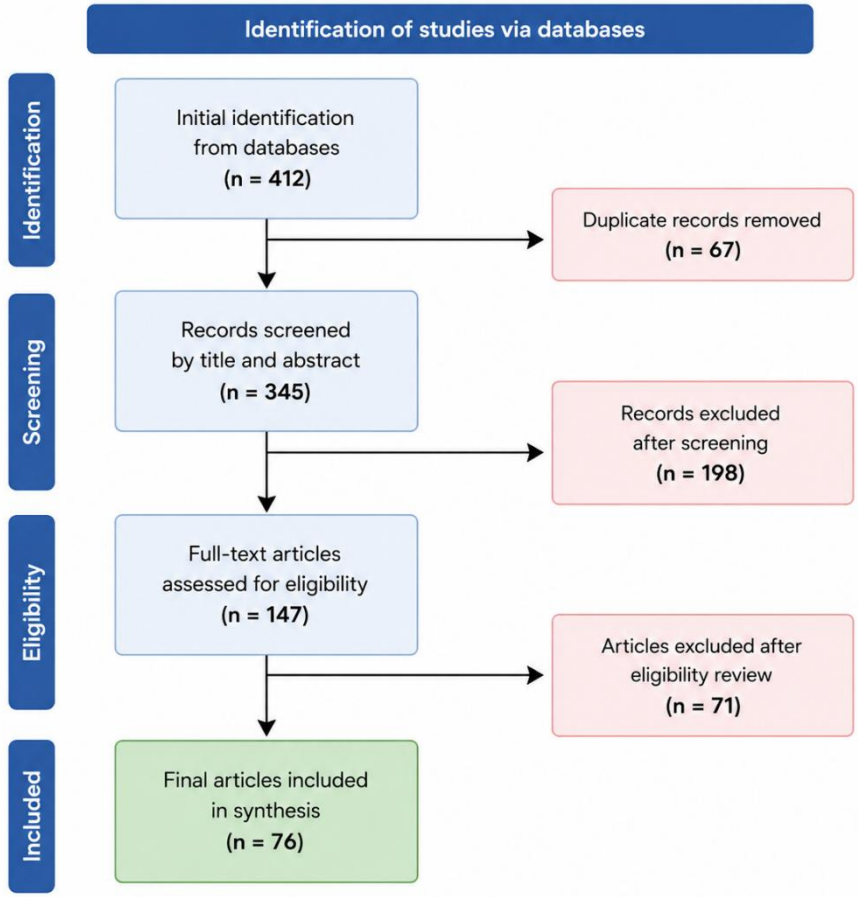

Figure 1. Simplified PRISMA Literature Selection Process

Source: Literature review process conducted by the researcher, 2024.

The initial search identified 412 records from academic databases and institutional repositories. After removing duplicate materials, 345 records were screened based on title and abstract relevance. Articles that did not focus on cybersecurity, digital sovereignty, or national data governance were excluded. The remaining 147 full-text sources were assessed for eligibility using predefined inclusion and exclusion criteria. After the final review stage, 76 academic articles, policy papers, institutional reports, and regulatory documents were selected for qualitative synthesis.

Inclusion and Exclusion Criteria

The literature selection process followed specific inclusion and exclusion criteria to ensure analytical relevance and academic quality.

Table 1. Inclusion and Exclusion Criteria

Criteria	Inclusion	Exclusion
Publication Type	Peer-reviewed journals, institutional reports, policy documents	Non-academic blogs, opinion articles
Research Focus	Cybersecurity, digital sovereignty, data governance	Unrelated technological studies
Time Range	2010–2024	Publications before 2010
Language	English-language publications	Non-English publications
Geographical Scope	Indonesia, EU, China, India, global governance	Studies without governance relevance
Data Quality	Indexed journals and verified institutional reports	Unverified or duplicate sources

Source: Research inclusion framework, 2024.

The inclusion criteria prioritized studies addressing cybersecurity governance, platform regulation, institutional capacity, digital sovereignty, and data governance within national or comparative contexts. Sources lacking empirical, theoretical, or policy relevance were excluded from analysis.

Data Coding and Analytical Framework

To organize the literature systematically, the study employed thematic coding using qualitative analytical procedures. Each selected source was reviewed and coded according to several analytical dimensions related to digital governance and cybersecurity capacity.

Table 2. Coding Framework for Literature Analysis

Coding Category	Analytical Focus
Regulatory Capacity	Legal frameworks and policy instruments
Institutional Coordination	Inter-agency collaboration and governance coherence
Cybersecurity Readiness	National cyber defense and response mechanisms
Platform Dependency	Reliance on foreign digital infrastructures
Enforcement Effectiveness	Sanctions, compliance, and regulatory implementation
Public Trust	Citizen confidence in digital governance systems
Data Localization	National control over data storage and transfer
Technological Infrastructure	Cloud systems, AI capability, and digital ecosystems

Source: Research coding framework, 2024.

The coding process enabled identification of recurring themes, policy patterns, governance contradictions, and institutional challenges across the selected jurisdictions.

Data Synthesis Procedure

Before conducting the comparative analysis, the selected literature underwent a structured synthesis process to ensure analytical consistency and conceptual integration across all reviewed studies. The synthesis procedure was designed to move beyond descriptive literature aggregation by systematically identifying governance patterns, institutional dynamics, cybersecurity readiness, and digital sovereignty strategies across different jurisdictions. Through this process, the study was able to organize diverse academic findings, policy documents, and institutional reports into a coherent analytical framework. The synthesis stages also enabled the researcher to connect theoretical perspectives on cybersecurity and digital sovereignty with empirical discussions concerning platform governance, institutional capacity, and technological dependency in the global digital era.

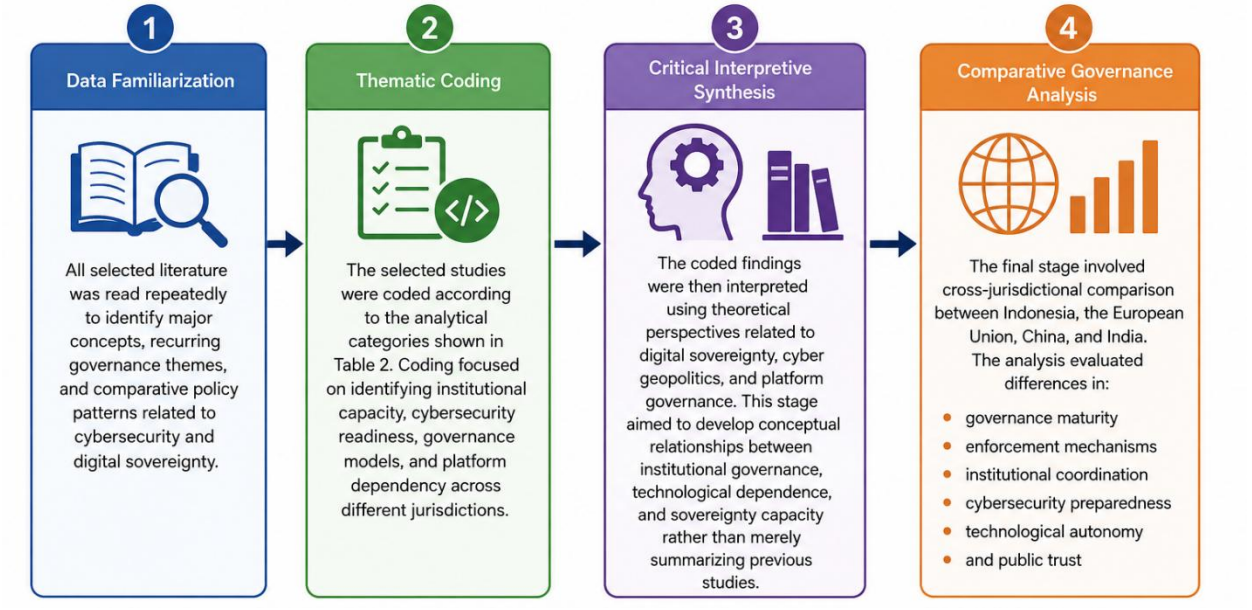

Figure 1. Data Synthesis Procedure

The synthesis process illustrates four interconnected analytical stages used in this study. The first stage, data familiarization, involved repeated reading of all selected literature to identify recurring concepts, governance themes, and comparative policy patterns related to cybersecurity and digital sovereignty. The second stage, thematic coding, focused on categorizing the literature according to institutional capacity, cybersecurity readiness, governance models, and platform dependency. In the third stage, critical interpretive synthesis, the coded findings were interpreted using theoretical perspectives related to digital sovereignty, cyber geopolitics, and platform governance to develop broader conceptual relationships between institutional governance and technological autonomy. The final stage, comparative governance analysis, examined differences between Indonesia, the European Union, China, and India in terms of governance maturity, enforcement mechanisms, institutional coordination, cybersecurity preparedness, technological autonomy, and public trust. This systematic synthesis procedure enabled the study to generate a more integrated understanding of how national data governance capacity shapes digital sovereignty in the era of global platforms.

Validity and Reliability

The credibility of the study was strengthened through source triangulation and methodological transparency. Triangulation was conducted by comparing academic publications, institutional reports, regulatory documents, and cybersecurity policy analyses. Peer debriefing with scholars in digital governance and public policy was also conducted to reduce interpretive bias and improve analytical consistency. Reliability was maintained by documenting all stages of literature selection, coding, and synthesis systematically. The use of PRISMA-based screening and a structured coding framework improved methodological transparency and analytical traceability. Although this study did not involve human participants, ethical considerations remained important throughout the research process. All academic materials, institutional reports, and policy documents were cited appropriately to avoid misrepresentation and plagiarism. The analysis was conducted independently and critically without reproducing political or institutional narratives uncritically. This study is limited by its reliance on secondary data and literature-based analysis without direct field investigation or interviews with policymakers. Nevertheless, the systematic literature review and critical interpretive synthesis approach allowed the study to examine broader structural relationships between cybersecurity governance, institutional capacity, and digital sovereignty across multiple jurisdictions. The comparative design also enabled deeper understanding of how different governance systems respond to challenges within the global platform era.

Comparative Analytical Indicators

To strengthen the comparative governance analysis, this study developed a set of comparative analytical indicators synthesized from recurring themes identified across the selected academic literature, institutional reports, cybersecurity assessments, and regulatory documents. These indicators were not intended as statistical measurements, but as interpretive comparative categories used to evaluate variations in national data governance capacity across Indonesia, the European Union, China, and India during 2010–2024. The indicators were constructed through thematic coding and critical interpretive synthesis based on patterns consistently discussed within the reviewed literature. The comparative indicators consisted of six main dimensions: (1) regulatory coherence, referring to the consistency and integration of legal frameworks related to cybersecurity and data governance; (2) institutional coordination, examining the level of inter-agency collaboration and governance integration; (3) cybersecurity readiness, assessing national preparedness in responding to cyber threats and digital vulnerabilities; (4) enforcement effectiveness, focusing on the implementation of sanctions, compliance mechanisms, and regulatory oversight; (5) technological autonomy, referring to the capacity of states to reduce dependence on foreign digital infrastructures and global platforms; and (6) public trust, examining citizen confidence in digital governance institutions and data protection systems. The comparative assessments presented in the findings section were derived from repeated patterns, institutional evaluations, and policy assessments identified across the selected literature rather than from direct statistical surveys conducted by the researcher. Numerical representations and categorical classifications such as “high,” “moderate,” or “low” therefore function as synthesized

analytical interpretations intended to illustrate relative governance capacity and institutional performance across jurisdictions. This approach enabled the study to systematically compare governance trajectories while remaining consistent with the qualitative and interpretive orientation of the research design.

RESULTS AND DISCUSSION

This section presents the findings derived from the systematic literature review and critical interpretive synthesis concerning cybersecurity and digital sovereignty across Indonesia, the European Union, China, and India during 2010–2024. The findings were generated from repeated reading, thematic coding, and conceptual integration of 76 selected academic articles, institutional reports, cybersecurity assessments, and policy documents identified through the PRISMA-based selection process. Rather than merely comparing governance performance across jurisdictions, the synthesis focused on identifying recurring governance patterns, institutional contradictions, regulatory tensions, and structural dilemmas shaping national data governance capacity in the global platform era.

The thematic synthesis identified four dominant analytical themes emerging consistently across the reviewed literature: (1) regulatory capacity and institutional coordination, (2) cybersecurity readiness and enforcement effectiveness, (3) platform dependency and technological sovereignty, and (4) public trust and governance legitimacy. Across these themes, the reviewed studies repeatedly demonstrate that digital sovereignty is not determined solely by legal regulation or technological infrastructure, but by the interaction between institutional coherence, enforcement capability, geopolitical strategy, and public legitimacy. The synthesis also reveals a recurring paradox within digital governance: jurisdictions with strong centralized enforcement often demonstrate lower procedural transparency, while more democratic governance systems frequently encounter slower institutional coordination and fragmented implementation.

Regulatory Capacity and Institutional Coordination

The thematic coding process consistently identified institutional coordination as one of the most decisive factors shaping digital sovereignty effectiveness. Across the reviewed literature, jurisdictions with integrated regulatory systems and centralized governance structures demonstrated stronger policy coherence and greater capacity to operationalize cybersecurity governance compared to fragmented institutional systems. The European Union emerged within the synthesis as the most institutionally coherent governance model. The reviewed studies repeatedly emphasize that the GDPR, Digital Services Act, and Digital Markets Act collectively function as interconnected regulatory instruments capable of integrating privacy protection, platform accountability, and cross-border governance coordination. The literature also positions the European Union as an example of rights-based digital sovereignty in which governance legitimacy is strengthened through transparency, legal accountability, and supranational institutional coordination.

Table 3. Comparative Regulatory and Institutional Capacity (2010–2024)

Jurisdiction	Governance Model	Institutional Coordination	Regulatory Coherence	Enforcement Strength
European Union	Rights-based governance	Very High	Very High	Strong
China	Centralized state-centric governance	High	High	Strong
India	Hybrid regulatory governance	Moderate	Moderate	Transitional
Indonesia	Fragmented multi-agency governance	Low–Moderate	Moderate	Weak–Moderate

Source: Synthesized from OECD reports, GDPR reports, cybersecurity policy documents, and selected literature, 2024.

The synthesis also reveals an important governance tension within the European Union model. Although the European Union demonstrates high regulatory maturity, several studies identify institutional complexity and bureaucratic fragmentation between member states as persistent challenges in operational coordination. The reviewed literature repeatedly notes that strong legal protections sometimes slow policy harmonization and technological adaptation across jurisdictions. China demonstrates a contrasting governance trajectory characterized by centralized authority, data localization, and state-centric cybersecurity regulation. Several studies emphasize positions China as having one of the strongest institutional capacities for enforcing digital governance due to centralized political authority and integrated cybersecurity supervision. Nevertheless, the synthesis identifies a significant paradox within the Chinese governance model. Strong enforcement effectiveness is frequently accompanied by concerns regarding procedural transparency, civil liberties, and surveillance expansion. Several studies argue that China's governance strength derives partly from its ability to minimize institutional fragmentation, yet this centralization simultaneously generates concerns regarding democratic accountability and citizen autonomy.

India emerged within the literature as a transitional governance model attempting to balance rapid digital economic growth with institutional regulation. The synthesis identifies recurring institutional tensions related to uneven policy implementation, fragmented inter-agency coordination, and disparities in technological capacity across regions. Although India's Digital Personal Data Protection Act of 2023 strengthened formal governance structures, the reviewed studies suggest that institutional readiness remains inconsistent across administrative sectors. Indonesia demonstrates the most fragmented institutional governance structure among the selected jurisdictions. The thematic synthesis repeatedly identifies overlapping authority between cybersecurity agencies and regulatory institutions as a major obstacle to governance effectiveness. The reviewed literature positions Indonesia within a governance dilemma in which rapid digital expansion outpaces institutional adaptation and cybersecurity preparedness. Although Indonesia has introduced significant regulatory reforms through the Personal Data Protection Law, institutional fragmentation and limited enforcement capacity continue to weaken operational effectiveness. These findings collectively indicate that regulatory coherence alone is insufficient to guarantee digital sovereignty. Institutional coordination, governance integration, and operational consistency emerge as equally important dimensions shaping cybersecurity governance effectiveness.

Cybersecurity Readiness and Enforcement Effectiveness

The second major theme emerging from the synthesis concerns disparities in cybersecurity readiness and enforcement effectiveness. Across the reviewed literature, cybersecurity governance is consistently interpreted not only as a technical security issue, but also as an institutional capacity problem closely connected to regulatory authority, resource allocation, and governance integration. The thematic synthesis consistently positions the European Union as having the strongest enforcement ecosystem due to coordinated cybersecurity institutions, standardized compliance mechanisms, and active regulatory sanctions against technology corporations. The reviewed studies indicate that GDPR enforcement significantly increased corporate accountability and strengthened institutional legitimacy within European digital governance.

Table 4. Comparative Cybersecurity and Enforcement Indicators

Jurisdiction	Annual Data Breach Incidents	Enforcement Actions	Financial Sanctions	Cybersecurity Preparedness
European Union	Moderate	210	Very High	Very High
China	Low–Moderate	187	High	High
India	High	124	Moderate	Moderate
Indonesia	Very High	57	Low	Low–Moderate

Source: Synthesized from institutional cybersecurity reports, regulatory assessments, and comparative governance studies, 2024.

China also demonstrates strong cybersecurity enforcement capacity through centralized monitoring systems, mandatory compliance mechanisms, and strict data localization policies. However, the reviewed literature reveals a recurring contradiction within China's governance strategy. While centralized enforcement improves state control and cybersecurity responsiveness, several studies identify concerns regarding excessive governmental surveillance and limited procedural oversight. The synthesis therefore suggests that cybersecurity effectiveness within authoritarian governance structures often operates simultaneously as a mechanism of national protection and political control.

India demonstrates moderate cybersecurity preparedness with increasing institutional investment after 2020. Nevertheless, the reviewed studies frequently identify inconsistencies between formal regulatory ambition and operational implementation capacity. The literature repeatedly emphasizes that uneven digital infrastructure and regional disparities continue to influence cybersecurity readiness across the country.

Indonesia emerges within the synthesis as the jurisdiction with the highest cybersecurity vulnerability among the selected cases. Repeated references to large-scale data breaches involving public institutions, telecommunications providers, and financial platforms indicate persistent weaknesses in cybersecurity governance. The reviewed studies consistently attribute these vulnerabilities to fragmented institutional coordination, limited cybersecurity expertise, insufficient technological infrastructure, and weak enforcement mechanisms. The synthesis also reveals a broader governance dilemma in Indonesia: regulatory expansion has progressed more rapidly than institutional and technical readiness, producing a gap between formal legal ambition and operational governance capacity.

The findings demonstrate that cybersecurity preparedness depends not solely on technological investment, but on the interaction between institutional authority, governance integration, enforcement consistency, and technical expertise.

Platform Dependency and Technological Sovereignty

Another major theme identified through thematic coding concerns technological dependency and platform sovereignty. Several studies emphasize emphasizes that digital sovereignty in the contemporary platform era is increasingly shaped by control over cloud infrastructure, artificial intelligence systems, platform ecosystems, and transnational data architectures.

Table 5. Comparative Platform Dependency and Technological Capacity

Jurisdiction	Domestic Technological Capacity	Dependency on Foreign Platforms	Data Localization Policy	Strategic Digital Autonomy
European Union	High	Moderate	Strong	High
China	Very High	Low	Very Strong	Very High
India	Moderate	High	Moderate	Transitional
Indonesia	Low–Moderate	Very High	Emerging	Low

Source: Synthesized from digital governance literature, institutional reports, and cybersecurity policy studies, 2024.

The synthesis positions China as the jurisdiction with the highest level of technological autonomy due to sustained state investment in domestic cloud systems, artificial intelligence development, and national digital infrastructure. Several reviewed studies describe China's approach as techno-nationalist because sovereignty is operationalized through direct state involvement in technological production and infrastructure control.

The European Union demonstrates a different governance trajectory. Several studies emphasize frames European digital sovereignty as strategic autonomy rather than complete technological independence. European governance emphasizes regulatory influence and institutional

standard-setting within interconnected global digital ecosystems. However, the synthesis identifies an important structural tension within the European model. Although regulatory authority remains strong, the European Union continues to rely substantially on non-European cloud infrastructures and multinational digital platforms, revealing limitations in technological self-sufficiency.

India occupies an intermediate position characterized by rapid digital expansion alongside continued reliance on multinational technology corporations. The reviewed studies identify ongoing tensions between India's ambition to strengthen domestic digital ecosystems and the structural dominance of foreign platform providers within its digital economy.

Indonesia demonstrates the highest level of platform dependency among the selected jurisdictions. The synthesis repeatedly identifies dependence on foreign cloud providers, external platform ecosystems, and imported technological infrastructures as major limitations affecting national digital sovereignty. Several studies emphasize that Indonesia's governance capacity remains constrained by limited domestic technological production and insufficient investment in sovereign digital infrastructure.

The synthesis findings therefore reveal that digital sovereignty increasingly depends on infrastructural ownership and technological autonomy rather than solely on legal authority. Countries with limited domestic technological ecosystems remain structurally vulnerable to external platform influence and governance dependency.

Public Trust and Governance Legitimacy

The final theme emerging from the synthesis concerns public trust and governance legitimacy. Across the reviewed literature, public trust consistently appears as a central component of digital sovereignty because governance effectiveness depends not only on institutional control but also on citizen confidence in digital systems and cybersecurity governance.

Table 6. Comparative Public Trust and Governance Legitimacy

Jurisdiction	Public Trust Score	Governance Transparency	Citizen Data Protection Confidence
European Union	79	High	High
China	68	Moderate	Moderate
India	59	Moderate	Moderate–Low
Indonesia	43	Low	Low

Source: Synthesized from governance surveys, cybersecurity assessments, and comparative digital governance studies, 2024.

The thematic synthesis consistently positions the European Union as having the highest level of public trust due to transparent governance mechanisms, visible regulatory enforcement, and strong legal protection for citizen data. The reviewed studies indicate that institutional accountability and procedural transparency significantly strengthen governance legitimacy within democratic digital systems.

China demonstrates relatively high governance confidence despite lower procedural transparency. The reviewed literature reveals an important contradiction within the Chinese model: strong cybersecurity enforcement and infrastructural efficiency generate public perceptions of stability and effectiveness, while concerns regarding surveillance and state control continue to shape external criticism of governance legitimacy.

India demonstrates moderate public trust shaped by uneven digital access, regional disparities, and ongoing debates concerning privacy protection. The reviewed studies frequently identify public trust as closely connected to governance consistency and institutional responsiveness.

Indonesia demonstrates the lowest public trust level among the selected jurisdictions. The thematic synthesis repeatedly identifies recurring data breaches, fragmented institutional coordination, and inconsistent regulatory enforcement as major factors contributing to declining

citizen confidence in digital governance institutions. Several reviewed studies also note that weak transparency in cybersecurity incident management further undermines governance legitimacy.

The synthesis findings collectively demonstrate that digital sovereignty operates not only through legal authority and cybersecurity infrastructure, but also through public legitimacy and institutional trust. Governance systems lacking transparency, accountability, and citizen confidence remain vulnerable to declining participation and institutional instability within digital ecosystems.

Comparative Synthesis of Digital Sovereignty Governance

The comparative synthesis reveals that digital sovereignty is fundamentally a multidimensional governance capacity emerging from the interaction between institutional coordination, cybersecurity readiness, technological autonomy, enforcement effectiveness, and public legitimacy. The reviewed literature consistently demonstrates that no governance model is entirely free from structural tensions and governance contradictions.

The European Union demonstrates strong regulatory legitimacy but faces challenges related to technological dependency and institutional complexity. China exhibits strong strategic autonomy and enforcement capacity while simultaneously generating concerns regarding transparency and surveillance expansion. India reflects transitional governance characterized by regulatory adaptation alongside uneven institutional readiness. Indonesia illustrates a governance dilemma in which rapid digital growth exceeds institutional capacity, cybersecurity preparedness, and technological autonomy.

The synthesis findings indicate that successful digital sovereignty governance depends not only on regulatory expansion but also on the ability of states to integrate institutional coordination, technological infrastructure, enforcement capability, and public trust within coherent governance systems. In the era of global platforms, sovereignty increasingly operates as an adaptive governance process rather than as a fixed condition of territorial control.

Discussion

Governance Capacity and Institutional Contradictions in Digital Sovereignty

The findings demonstrate that digital sovereignty is fundamentally shaped by the interaction between institutional coordination, regulatory coherence, cybersecurity readiness, and governance legitimacy rather than by technological regulation alone (Farrand & Carrapico, 2022; Fratini et al., 2024; Carver, 2024; Pernice, 2018). The comparative synthesis indicates that jurisdictions with integrated governance structures and consistent enforcement mechanisms tend to demonstrate stronger institutional resilience in responding to cybersecurity threats and platform dependency. These findings reinforce contemporary governance perspectives arguing that digital sovereignty should be understood as an adaptive governance capacity emerging from the relationship between legal authority, technological infrastructure, and institutional coordination.

The European Union represents the most institutionally coherent governance model within the reviewed literature because of its integrated regulatory architecture through the GDPR, Digital Services Act, and Digital Markets Act. The findings suggest that regulatory legitimacy in the European Union is strengthened through supranational coordination, procedural transparency, and visible enforcement actions against technology corporations (Bunea, 2018; Stephenson, 2023; Kinderman, 2020; Schmidt & Wood, 2019; Villiers, 2022). This condition supports previous studies emphasizing that accountability and institutional trust become central components of effective digital governance. Nevertheless, the synthesis also reveals a structural contradiction within the European model. Although the European Union demonstrates strong regulatory authority, its technological ecosystem remains partially dependent on non-European cloud infrastructures and global platform providers. This tension indicates that regulatory sovereignty does not automatically guarantee technological autonomy. According to Fischer (2022), digital sovereignty within democratic governance systems therefore appears as a continuous negotiation between legal control, market interdependence, and institutional coordination.

China demonstrates a contrasting governance trajectory characterized by centralized authority, strong enforcement capacity, and extensive state involvement in digital infrastructure development. The reviewed literature consistently positions China as one of the most operationally effective cybersecurity governance systems due to centralized supervision, mandatory compliance mechanisms, and strong state control over digital platforms. The findings suggest that institutional centralization enables rapid policy implementation and stronger cybersecurity responsiveness. At the same time, the synthesis identifies an important governance paradox within the Chinese model. Strong cybersecurity enforcement simultaneously generates concerns regarding surveillance expansion, procedural opacity, and limitations on civil liberties. This contradiction illustrates that governance effectiveness in digital sovereignty may increase institutional control while reducing democratic accountability and transparency. The Chinese case therefore demonstrates that cybersecurity governance is not politically neutral, but closely connected to broader state strategies concerning authority, legitimacy, and social control (Cheung, 2018; Miao & Han, 2022; Kirk et al., 2022).

India occupies an intermediate governance position characterized by regulatory transition and uneven institutional adaptation. The findings indicate that India has strengthened formal governance structures through the Digital Personal Data Protection Act of 2023 and increasing cybersecurity investment. However, recurring institutional fragmentation, regional disparities, and uneven technological infrastructure continue to influence governance consistency. The reviewed literature suggests that India's governance trajectory reflects broader tensions experienced by emerging digital economies attempting to balance economic liberalization with regulatory oversight. Rapid digital expansion increases the urgency for cybersecurity governance, yet institutional adaptation frequently progresses more slowly than technological transformation.

Indonesia demonstrates the most significant governance fragmentation among the selected jurisdictions. The synthesis consistently identifies overlapping institutional authority, limited cybersecurity expertise, weak enforcement mechanisms, and high dependency on foreign digital infrastructures as major constraints affecting governance capacity. Although the enactment of the Personal Data Protection Law represents an important regulatory milestone, the findings suggest that institutional readiness remains insufficient to operationalize digital sovereignty effectively. Indonesia therefore reflects a governance dilemma frequently identified in the reviewed literature: legal reform progresses more rapidly than institutional coordination and technological capability. This condition supports arguments that sovereignty in the digital era cannot be achieved solely through formal regulation, but requires integrated governance structures, operational enforcement capacity, and sustainable institutional adaptation.

The comparative findings collectively demonstrate that digital sovereignty is shaped by multidimensional governance relationships involving legal systems, technological infrastructures, institutional authority, and geopolitical strategy. Strong governance capacity emerges not merely from regulatory expansion, but from the ability of states to integrate cybersecurity readiness, institutional coordination, technological investment, and governance legitimacy into coherent digital governance systems.

Technological Dependency, Public Trust, and the Future of Digital Governance

The findings also demonstrate that technological dependency and public trust have become central dimensions shaping contemporary digital sovereignty (Robles-Carrillo, 2023). Across the reviewed literature, digital governance is increasingly influenced by ownership and control over cloud infrastructures, artificial intelligence systems, digital platforms, and transnational data ecosystems. This transformation indicates that sovereignty in the global platform era is no longer determined exclusively through territorial authority, but also through infrastructural and technological control.

The comparative synthesis reveals that jurisdictions with stronger domestic technological ecosystems tend to demonstrate higher levels of strategic autonomy and governance resilience. China emerged as the jurisdiction with the strongest technological autonomy because of sustained investment in domestic cloud systems, artificial intelligence development, and national platform infrastructures. The reviewed literature repeatedly characterizes China's approach as techno-nationalist because state authority is directly connected to technological production and

infrastructural control. Such findings indicate that technological self-sufficiency increasingly functions as a strategic component of cybersecurity governance and national sovereignty.

The European Union demonstrates a different governance orientation by emphasizing strategic autonomy rather than complete technological independence (Csernatoni, 2022). The findings suggest that the European Union prioritizes regulatory influence and standard-setting capacity within interconnected global digital ecosystems. The reviewed studies consistently identify structural tensions between regulatory leadership and technological dependence on multinational platform providers. This condition demonstrates that even institutionally mature governance systems remain constrained by the concentration of technological power within transnational digital corporations.

India and Indonesia reflect more pronounced forms of technological dependency. The synthesis indicates that multinational corporations continue to dominate significant components of digital infrastructure, cloud services, and platform ecosystems in both countries. Indonesia demonstrates the highest level of external platform dependence among the selected jurisdictions, limiting its strategic autonomy and regulatory effectiveness (Jauhari et al., 2024; Fauzi et al., 2024; Prasetyo, 2022). The reviewed literature repeatedly emphasizes that limited domestic technological production and insufficient digital infrastructure investment weaken Indonesia's ability to establish stronger national data governance capacity. This condition illustrates a broader structural challenge faced by developing digital economies in the Global South, where rapid digital transformation frequently increases dependence on external technological systems.

Public trust also emerges as a decisive factor influencing governance legitimacy and digital sovereignty effectiveness. The findings indicate that governance systems with stronger transparency, visible enforcement, and institutional accountability tend to demonstrate higher levels of citizen confidence. The European Union demonstrates the highest public trust because regulatory enforcement is accompanied by procedural accountability and strong data protection mechanisms. This finding reinforces previous governance studies arguing that legitimacy and accountability are essential components of sustainable digital governance.

According to Hartley (2021), china presents a different legitimacy model in which public trust is shaped more strongly by perceptions of state effectiveness, infrastructural stability, and cybersecurity control rather than by procedural transparency. The synthesis reveals an important contradiction in this governance structure. Strong institutional control may increase public perceptions of security and efficiency while simultaneously generating external concerns regarding surveillance practices and democratic accountability (Ball et al., 2019; Petersen & Tjalve, 2018; Narang & Staniland, 2018). Governance legitimacy in digital systems therefore appears closely connected to broader political and institutional contexts rather than to universal governance standards.

Indonesia demonstrates the lowest level of public trust among the selected jurisdictions due to recurring data breaches, fragmented governance coordination, and inconsistent cybersecurity enforcement (Rhogust, 2024; Rusydi, 2024; Hermawan, 2024; Rahman et al., 2023). The reviewed literature repeatedly identifies weak institutional transparency and limited incident accountability as factors contributing to declining citizen confidence in digital governance systems. This condition indicates that cybersecurity governance failures extend beyond technical vulnerabilities because they also influence institutional legitimacy and public participation within digital ecosystems.

The discussion findings collectively indicate that digital sovereignty in the global platform era should be understood as a dynamic governance process involving technological autonomy, institutional legitimacy, cybersecurity preparedness, and public trust. Jurisdictions unable to integrate these dimensions coherently remain vulnerable to platform dependency, governance fragmentation, and declining institutional credibility. The comparative synthesis therefore suggests that future digital governance strategies must move beyond regulatory expansion alone and prioritize institutional integration, technological investment, democratic accountability, and sustainable cybersecurity capacity development.

CONCLUSION

Digital sovereignty in the global platform era is fundamentally shaped by the interaction between institutional coordination, cybersecurity readiness, technological autonomy, enforcement effectiveness, and public trust rather than by legal regulation alone. The comparative synthesis across Indonesia, the European Union, China, and India reveals that jurisdictions with integrated governance frameworks, stronger institutional capacity, and consistent cybersecurity enforcement tend to demonstrate higher governance resilience and greater strategic autonomy within digital ecosystems. The European Union illustrates the importance of regulatory legitimacy and institutional accountability, while China demonstrates how centralized governance can strengthen technological sovereignty and enforcement capacity despite generating tensions related to transparency and surveillance. India reflects a transitional governance trajectory characterized by regulatory expansion alongside uneven institutional readiness. Indonesia faces the most significant structural challenges due to fragmented governance coordination, limited technological infrastructure, weak enforcement mechanisms, and high dependency on foreign digital platforms. These findings indicate that digital sovereignty should be understood as an adaptive and multidimensional governance capacity requiring not only regulatory reform, but also institutional integration, sustainable technological investment, cybersecurity preparedness, and long-term public trust in digital governance systems.

REFERENCES

Ball, K., Degli Esposti, S., Dibb, S., Pavone, V., & Santiago-Gomez, E. (2019). Institutional trustworthiness and national security governance: Evidence from six European countries. *Governance*, *32*(1), 103-121. https://doi.org/10.1111/gove.12353

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

Bunea, A. (2018). Legitimacy through targeted transparency? Regulatory effectiveness and sustainability of lobbying regulation in the European Union. *European Journal of Political Research*, *57*(2), 378-403. https://doi.org/10.1111/1475-6765.12231

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

Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy*, *31*(8), 2250-2286. https://doi.org/10.1080/13501763.2023.2295523

Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, *3*(3), 306-326. https://doi.org/10.1080/23738871.2018.1556720

Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European security*, *31*(3), 395-414. https://doi.org/10.1080/09662839.2022.2103370

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

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European security*, *31*(3), 435-453. https://doi.org/10.1080/09662839.2022.2102896

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.

Fischer, D. (2022). The digital sovereignty trick: Why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Zeitschrift Für Politikwissenschaft*, *32*(2), 383-402. https://doi.org/10.1007/s41358-022-00316-4

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*, *3*(3), 59. https://doi.org/10.1007/s44206-024-00146-7

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

Hartley, K. (2021). Public trust and political legitimacy in the smart city: A reckoning for technocracy. *Science, Technology, & Human Values*, *46*(6), 1286-1315. https://doi.org/10.1177/0162243921992864

Hermawan, R. (2024). Optimising Multilateral Cooperation in Combating Cybercrime to Enhance National Vigilance. *Jurnal Lemhannas RI*, *12*(4), 467-484. https://doi.org/10.55960/jlri.v12i4.990

Jauhari, M. A., Negara, D. S., & Darmawan, D. (2024). Responsibilities of Digital Marketplace Platforms and Anticompetitive Assessments in Business Law. *Journal of Social Science Studies*, *4*(1), 407-422.

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

Kinderman, D. (2020). The challenges of upward regulatory harmonization: The case of sustainability reporting in the European Union. *Regulation & Governance*, *14*(4), 674-697. https://doi.org/10.1111/rego.12240

Kirk, H. R., Lee, K., & Micallef, C. (2022). The nuances of Confucianism in technology policy: An inquiry into the interaction between cultural and political systems in Chinese digital ethics. *International Journal of Politics, Culture, and Society*, *35*(2), 129-152. https://doi.org/10.1007/s10767-020-09370-8

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

Miao, W., & Han, R. (2022). Modernization planner, authoritarian paternalist, and rising power: evolving government positions in China's internet securitization. *Journal of Contemporary China*, *31*(136), 574-591. https://doi.org/10.1080/10670564.2021.1985832

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

Narang, V., & Staniland, P. (2018). Democratic accountability and foreign security policy: Theory and evidence from India. *Security Studies*, *27*(3), 410-447. https://doi.org/10.1080/09636412.2017.1416818

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

Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. *Global constitutionalism*, *7*(1), 112-141. https://doi.org/10.1017/S2045381718000023

Petersen, K. L., & Tjalve, V. S. (2018). Intelligence expertise in the age of information sharing: public–private 'collection'and its challenges to democratic control and accountability. *Intelligence and National Security*, *33*(1), 21-35. https://doi.org/10.1080/02684527.2017.1316956

Prasetyo, E. H. (2022). Legitimacy building of digital platforms in the informal economy: Evidence from Indonesia. *Journal of Entrepreneurship in Emerging Economies*, *14*(6), 1168-1187. https://doi.org/10.1108/JEEE-02-2021-0073

Rahman, M. A., Alam, M. S., & Mrida, M. S. H. (2023). Balancing Privacy And Security In The Digital Age: A Global Perspective. *American Journal of Interdisciplinary Studies*, *4*(02), 64-90. https://doi.org/10.63125/d2brsb39

Rhogust, M. (2024). Legal framework for cybersecurity in the digital economy: Challenges and prospects for Indonesia. *Journal of Law, Social Science and Humanities*, *1*(2), 166-180.

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

Rusydi, M. T. (2024). Evaluating Global Cybersecurity Laws: Efectiveness of Legal Frameworks and Enforcement Mecanism in the Digital Age. *Walisongo Law Review (Walrev)*, *6*(1), 71-83. https://doi.org/10.21580/walrev.2024.6.1.20960

Schmidt, V., & Wood, M. (2019). Conceptualizing throughput legitimacy: Procedural mechanisms of accountability, transparency, inclusiveness and openness in EU governance. *Public administration*, *97*(4), 727-740. https://doi.org/10.1111/padm.12615

Stephenson, P. (2023). Exploring the throughput legitimacy of European Union policy evaluation: challenges to transparency and inclusiveness in the European commission's consultation procedures and the implications for risk regulation. *European Journal of Risk Regulation*, *14*(2), 351-370. https://doi.org/10.1017/err.2023.33

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

Villiers, C. (2022). New directions in the European Union's regulatory framework for corporate reporting, due diligence and accountability: The challenge of complexity. *European Journal of Risk Regulation*, *13*(4), 548-566. https://doi.org/10.1017/err.2022.25

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