JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i4

An Analysis of Digital Institutional Capacity and Personal Data Protection Policy Implementation in Indonesia: A Systematic Literature Review

Abednego Briantama[1*], Muhamad Yopan[2]
[1]Universitas Indonesia, Indonesia abednego.briantama@ui.ac.id
[2]Universitas Indonesia, Indonesia muhamad.yopan@ui.ac.id

[*]Corresponding Author: abednego.briantama@ui.ac.id[1]

Abstract: This study conducts a systematic literature review to examine institutional capacity in the implementation of personal data protection policy, with particular reference to Indonesia's Ministry of Communication and Digital Affairs (Komdigi). Despite the enactment of Law Number 27 of 2022 on Personal Data Protection, persistent data breaches and institutional fragmentation raise critical questions about the readiness of public institutions to enforce such policy. Utilizing the PRISMA 2020 protocol, this review identifies and synthesizes 27 peer-reviewed articles published between 2023 and 2025 from Scopus, Cambridge, and Taylor & Francis databases. The analysis reveals four principal themes: structural and regulatory capacity, human resource and technological capacity, inter-institutional coordination, and institutional values and ethics. Findings indicate that effective data protection governance depends not merely on the existence of legal frameworks but on the adaptive, coordinative, and ethical capacities of implementing institutions. The review further highlights significant gaps in longitudinal research and calls for deeper empirical investigation into how digital institutional capacity shapes policy outcomes in developing countries.

Keywords: Institutional Capacity, Personal Data Protection, Digital Governance, Ministry Of Communication And Digital Affairs, Systematic Literature Review

INTRODUCTION

The rapid advancement of digital technologies has fundamentally reshaped the production, processing, and utilization of personal data across global digital ecosystems. Over the past decade, digital transformation has intensified the integration of personal data into economic activities, governance systems, and everyday social interactions [1]. This transformation has generated significant benefits in terms of efficiency, accessibility, and innovation; however, it has simultaneously introduced complex challenges related to data privacy, security, and governance. The increasing scale of data-driven systems highlights the urgent need for robust institutional frameworks capable of ensuring effective personal data protection in an increasingly interconnected digital environment.

In Indonesia, the scale of digital adoption reflects both rapid growth and structural vulnerability. With more than 221 million internet users and the expansion of digital transactions across sectors, personal data has become a critical resource in both public and private domains [2]. Digital platforms, including e-commerce, financial technology, and electronic-based public services, rely heavily on personal data processing to support service delivery and policy implementation. At the same time, the increasing reliance on digital infrastructure has heightened exposure to cybersecurity risks and data breaches, emphasizing the importance of strengthening governance mechanisms and institutional readiness [3].

Institutional capacity has been widely recognized as a key determinant of policy effectiveness in public administration. According to Grindle [4], institutional capacity encompasses organizational capability, coordination mechanisms, and human resource competence required to implement policies effectively. In the context of digital governance, this concept extends to the ability of institutions to manage complex data systems, ensure regulatory compliance, and adapt to rapid technological change [1]. Recent studies further highlight that institutional capacity in data governance is shaped by multiple dimensions, including regulatory structures, technological infrastructure, inter-organizational coordination, and ethical governance practices [5], [6]

Despite its theoretical importance, the implementation of institutional capacity in personal data protection policy often faces significant challenges. In Indonesia, the enactment of Law Number 27 of 2022 on Personal Data Protection represents a major regulatory milestone. However, its implementation remains constrained by institutional limitations, including the absence of comprehensive implementing regulations and the delayed establishment of an independent supervisory authority. Similar challenges have been observed in other developing countries, where fragmented institutional arrangements and weak coordination mechanisms hinder effective data governance [7], [8]. These conditions suggest that regulatory frameworks alone are insufficient without adequate institutional support.

Empirical evidence further demonstrates the gap between regulatory ambition and implementation capacity. Comparative studies indicate that countries with stronger institutional arrangements, such as Brazil and the Philippines, have developed more integrated data protection systems supported by independent supervisory bodies and coordinated governance mechanisms. In contrast, Indonesia continues to face challenges in areas such as incident response, policy coordination, and regulatory enforcement, as reflected in cybersecurity indices and reported data breach incidents. This gap highlights the need to critically examine institutional capacity as a central factor in policy implementation.

Although existing studies have explored data protection from legal, technological, and governance perspectives, limited attention has been given to the systematic relationship between institutional capacity and personal data protection policy implementation. Many studies focus on regulatory frameworks or technological solutions, while overlooking how institutional structures, coordination processes, and organizational capabilities shape policy outcomes [9], [10]. Furthermore, there is a lack of comprehensive literature synthesis that specifically addresses this issue in the Indonesian context.

This study addresses these gaps by conducting a systematic literature review on institutional capacity in personal data protection policy implementation. The study aims to synthesize existing research, identify key institutional dimensions, and analyze challenges in policy implementation within digital governance systems. Accordingly, the research seeks to answer the following questions: (1) How is institutional capacity conceptualized in the context of personal data protection governance? and (2) What institutional challenges and gaps influence the implementation of personal data protection policy, particularly in Indonesia? The findings are expected to contribute to both theoretical development and policy improvement by providing a structured understanding of institutional capacity in digital governance.

METHOD

This study employs the systematic literature review (SLR) method to address the research objectives and provide a comprehensive understanding of institutional capacity in personal data protection policy implementation. Unlike narrative reviews, which tend to focus on descriptive summaries and are susceptible to selection bias, a systematic literature review offers a structured, transparent, and replicable process for identifying, evaluating, and synthesizing relevant scholarship. This study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework [11], which enhances the reliability and credibility of findings while minimizing the risk of bias in article selection, analysis, and interpretation.

a. Searching Strategy

The study utilizes a descriptive, qualitative, and exploratory methodology grounded in the relevant literature on institutional capacity and data protection governance. Three international academic databases were selected for the search: Scopus, Cambridge, and Taylor & Francis. These databases were chosen for their comprehensive coverage of public policy, digital governance, public administration, and digital law journals. The search employed Boolean combinations of keywords focusing on three thematic clusters: “data governance” OR “personal data protection”, “digital institutional capacity” OR “institutional capacity”, and “digital governance” OR “cybersecurity policy.” The data collection was conducted between September and November 2025, covering the publication period of 2023 to 2025. This temporal scope was selected to capture the most recent wave of scholarship following the global proliferation of data protection regulations, including Indonesia’s UU PDP and the continuing influence of the European General Data Protection Regulation (GDPR).

b. Article Criterion To ensure the quality and relevance of the included studies, specific inclusion and exclusion criteria were established in accordance with a predetermined protocol

1. Inclusion Criteria
   IC1Articles published between 2023 and 2025.
   IC2: Studies in social science, public administration, digital governance, or law.
   IC3: Peer-reviewed journal articles and book chapters.
   IC4: Publications written in English.
   IC5: Studies addressing institutional capacity in data protection, digital governance, or cybersecurity policy.

2. Exclusion Criteria
   EC1: Articles published outside the 2023 to 2025 range.
   EC2: Studies from purely technical fields without governance focus.
   EC3: Non-peer-reviewed publications, including editorials and conference papers.
   EC4: Publications not written in English.
   EC5: Studies not related to institutional capacity or data governance.

c. Data Collection

In accordance with the PRISMA 2020 guidelines, this study applied a structured multi-stage screening process to ensure the relevance and quality of the selected literature. The review was conducted between September and November 2025 using major academic databases, including Scopus, Cambridge, and Taylor and Francis. The initial search, based on keywords such as data governance, personal data protection, and digital institutional

capacity, identified a total of 515 articles. The first stage involved screening titles and keywords to assess thematic relevance. The second stage evaluated abstracts and methodological alignment with the focus on institutional capacity in data protection policy. The third stage consisted of a full-text review to ensure conceptual and empirical relevance. Following the application of inclusion and exclusion criteria, the number of eligible studies was reduced to 27 articles. These articles were considered suitable for further analysis. The overall screening process is illustrated in the PRISMA flow diagram presented below.

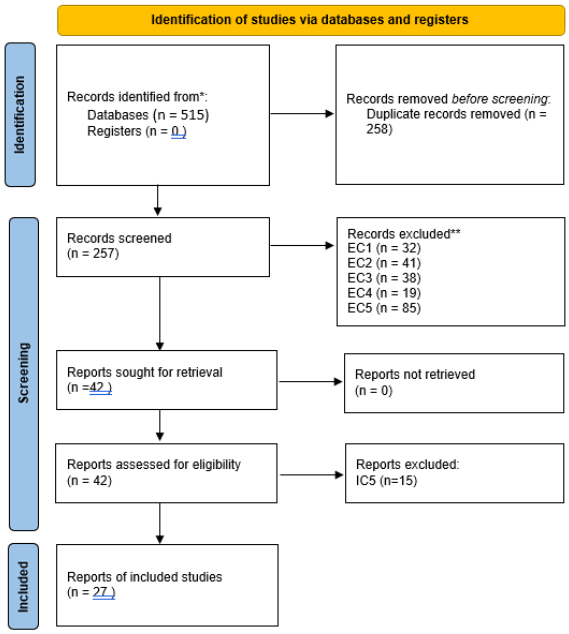

Fig. 1. PRISMA Flow Diagram

d. Data Analyses

The data analysis in this study followed a structured literature review approach. Initially, a descriptive analysis was conducted to identify key characteristics of the selected studies, including authorship, publication year, research focus, and methodological approach. Subsequently, a thematic analysis was performed to classify the findings into core dimensions of institutional capacity. These include structural and regulatory capacity, human resource and technological capacity, inter-institutional coordination, and institutional values and ethics. This analytical process enabled the identification of recurring patterns and relationships across the literature, providing a comprehensive understanding of how institutional capacity influences the implementation of personal data protection policy.

RESULTS AND DISCUSSION

Screening Result

The systematic screening process yielded 27 articles that met all predetermined inclusion criteria. The following table presents a summary of each included study, covering its title, authorship, methodology, year of publication, and key findings related to institutional capacity in personal data protection governance.

Table 1. Studies Included for Systematic Review

No	Title	Authors	Method	Year	Short Resume
1	Everyone Is Safe Now: Constructing the Meaning of Data	Huynh, T.T.	Policy & institutional analysis	2024	Centralized regulatory model strengthens state legitimacy over substantive privacy protection.

	Privacy Regulation in Vietnam				
2	Excessive Digital Surveillance and Data Privacy Invasion as a Creeping Crisis	Fossheim, K. & Lund-Tønnesen, J.	Policy & crisis management analysis	2023	Public institutions are reactive and lack inter-agency coordination for digital privacy threats.
3	Decoding the Privacy Puzzle: A Study on AI Deployment in Public Governance	Saura, J.R., Barbosa, B., & Rana, S.	Comparative policy study	2025	Effective digital governance requires cohesive data integration, digital literacy, and ethical leadership.
4	Navigating the Intersection of AI Policy, Technology, and Governance	Youssef, A. & Arslan, A.	Multi-level policy analysis	2025	Adaptive institutional capacity requires flexible structures and responsive cross-sector coordination.
5	Omani Public Governance in the Age of AI	Awashreh, R.	Descriptive policy analysis	2025	Institutional fragmentation and low digital competency impede digital policy effectiveness.
6	Navigating Public Administration 5.0: Embracing AI for Smarter Governance	Tariq, M.U.	Conceptual literature study	2025	Institutional capacity depends on innovation ability, system interoperability, and value-based governance.
7	Introduction to the Handbook on Governance and Data Science	Giest, S. et al.	Conceptual analysis	2025	Strong institutional capacity requires analytical competence, integrated infrastructure, and evidence-based decision-making.
8	Data Protection and Privacy in the Data-Driven Public Welfare in India	Noureen, N.C.K.	Public policy analysis	2025	Weak institutional coordination and limited internal oversight characterize India's data governance.
9	Agency Between Logics: Data Privacy Tactics, Ethics, and the Power of the DPO	Young, S. & Visser, F.	Institutional ethnography	2025	DPO autonomy significantly strengthens institutional transparency and ethical accountability.
10	A Paradigm: Government Contracting and Cybersecurity	Rose, R.V.	Legal & policy analysis	2025	Internal audits, transparent contracting, and standardized inter-agency procedures enhance digital security capacity.
11	Digital Transformation in Government: Lessons from GovTech Singapore	Perdana, A. & Mokhtar, I.A.	Institutional case study	2025	National data integration, agile organizational structure, and sustained digital investment drive institutional performance.
12	The Dilemma Between Digital Identity and Privacy in Modern Governance	Karmwar, M. & Kunwar, D.	Comparative analysis	2025	Institutional capacity is tested through balancing administrative efficiency with individual digital rights.
13	Ensuring Privacy in the Labour Market: Towards Full Compliance with LGPD and GDPR	Silva, H. et al.	Compliance audit analysis	2024	Tiered compliance systems and continuous training improve institutional data protection capacity.
14	Contours of Data Protection in India: The Consent Dilemma	Collaco, A.M.	Legal & public policy analysis	2024	Institutions face challenges in digital education, consent verification, and data misuse prevention.
15	Enhancing Cybersecurity and Legal Integration:	Widayanti, T.F. et al.	Normative legal analysis	2025	Institutional fragmentation and weak strategic coordination among cyber entities hinder national digital policy.

	Reforming Indonesia's Cyber Law				
16	Grand Challenges in Human-Centered Privacy	Abu-Salma, R. et al.	Cross-disciplinary conceptual analysis	2025	Human-centered institutional design fosters public trust and ethical digital governance.
17	Setting the Agenda for Research in Cybersecurity Law and Policy	Balleste, R. et al.	International legal analysis	2025	Cross-jurisdictional coordination and interoperable cyber policies strengthen national digital resilience.
18	Structural Oppression and AI: A Systematic Review of Data Policy Frameworks in India	Biju, P.R. & Gayathri, O.	Systematic review	2025	Weak ethical integration and absent algorithmic correction mechanisms perpetuate digital inequity.
19	Integrating Technology Across Sectors: Innovations in Public Administration, Engineering, and Business	Kumar, N. & Gupta, S.T.	Interdisciplinary study	2026	Cross-sector collaborative innovation and interoperable data systems significantly strengthen institutional capacity.
20	Empowering Digital Sovereignty: Balancing Privacy and Global Connectivity	Misra, S. et al.	International policy analysis	2026	Effective institutions balance digital sovereignty principles with global data integration through adaptive frameworks.
21	Digital Responsibility at the Nexus of Big Tech and Government	Haswell, C. & Whitford, A.	Transparency & policy analysis	2026	Co-governance mechanisms and data transparency partnerships with tech corporations enhance institutional legitimacy.
22	Rights in the Digital Realm: Legal and Ethical Considerations of Emerging Technologies	Al Khaldy, M. et al.	Legal & digital ethics analysis	2026	Institutional capacity functions optimally when integrating ethics, human rights, and technology governance.
23	Lost in Translation: Why Digital Twins Thrive in Research but Falter in Public Administration	Richter, F. et al.	Institutional case study	2025	Rigid organizational culture and weak coordinative structures are the main barriers to digital innovation adoption.
24	Group Closeness Effects on Co-Owned Information Sharing	Zhang, M., Turel, O., & Zöll, A.	Multilevel empirical analysis	2025	High inter-unit trust and organizational cohesion drive efficient cross-departmental data management.
25	When and How Corporate Digital Responsibility Contributes to a Firm's Reputation	Abbas, J.	Structural equation modelling	2025	Transparent and digitally responsible institutions achieve higher public legitimacy and reputational strength.
26	Defining Personal Data Sovereignty: An Ontologically-Based Framework	Baraku, V. et al.	Ontological & framework design	2025	National institutional capacity for data sovereignty requires individual-control mechanisms and rights-based authority.
27	Enhancing Cybersecurity and Legal Integration: Reforming	T. F. Widayanti, A. D. Rohman, A.	Normative legal analysis	2025	The study reveals institutional fragmentation, overlapping authority, and weak coordination in Indonesia's cybersecurity governance,

	Indonesia's Cyber Law to Foster Sustainable Growth in the Digital Economy	N. Z. Haris, E. M. Djafar, M. Z. Hakim	emphasizing the need for integrated institutional frameworks and legal harmonization.

Descriptive analyses of the paper

The 27 reviewed studies span diverse geographical contexts, including Indonesia, India, Vietnam, Oman, Singapore, South Africa, Brazil, and various European and Gulf states. The temporal distribution shows a concentration of publications in 2024-2025, reflecting the growing scholarly attention to institutional capacity in digital governance following the global wave of data protection legislation. Methodologically, the reviewed studies predominantly employ qualitative approaches, including policy analysis, institutional case studies, and comparative governance frameworks, with a smaller subset utilizing systematic reviews, structural equation modelling, and conceptual ontological analysis.

Thematic analyses

The thematic analysis of the 27 reviewed studies reveals four principal dimensions of institutional capacity that determine the effectiveness of personal data protection policy implementation. These dimensions function not as isolated variables but as interconnected pillars whose combined strength determines the resilience and responsiveness of governance systems.

a. Structural and Regulatory Capacity

The largest cluster of studies examines how organizational structures, legal frameworks, and regulatory architecture shape institutional capacity for data protection. Research by Widayanti et al. [12] demonstrates that fragmentation of institutional roles and overlapping jurisdictional authority represent critical barriers to effective cybersecurity governance in Indonesia. Balleste, Doucet, and Hanlon [13] corroborate this finding at the global level, arguing that adaptive legal institutions with cross-jurisdictional coordination mechanisms exhibit stronger digital resilience. Huynh (2024) offers a contrasting perspective from Vietnam, revealing that centralized regulatory structures may achieve administrative efficiency but risk undermining participatory governance and substantive privacy protection. The comparative study by Karmwar and Kunwa [14] on India and South Africa further illustrates how the structural design of digital identity systems directly affects the balance between administrative efficiency and individual privacy rights. Collectively, these studies affirm Grindle's [4] proposition that organizational structure constitutes a foundational element of institutional capacity, while extending it to encompass the regulatory coherence necessary for digital governance.

b. Human Resource and Technological Capacity

A second prominent theme concerns the competence of human resources and the adequacy of technological infrastructure underpinning data protection institutions. Awashreh [8] finds that institutional fragmentation in Oman is exacerbated by low digital competency among public servants, resulting in slow and unintegrated responses to technological change. Tariq [15] reinforces this conclusion by arguing that institutional effectiveness in the era of Public Administration 5.0 depends on technological readiness, organizational agility, and visionary leadership capable of driving cultural transformation toward data-driven governance. Noureen [7] reveals that India's public welfare institutions lack standardized data control mechanisms and transparent compliance audits, largely owing to limited digital literacy among bureaucratic personnel. Perdana and Mokhtar [16] provide a positive counterpoint through the GovTech Singapore case, showing that

sustained investment in digital human capital, integrated data infrastructure, and adaptive governance mechanisms enables high levels of institutional performance. These findings collectively underscore the OECD's [3] emphasis on human and organizational capacity as a critical dimension of digital institutional effectiveness.

c. Interinstitutional Coordination and Network Capacity

The third thematic cluster addresses the coordinative mechanisms that enable or constrain collaboration across institutional boundaries. Fossheim and Lund-Tønnesen [17] conceptualize excessive digital surveillance as a creeping crisis that emerges precisely because inter-agency communication and risk mitigation protocols remain weak and uncoordinated. Rose [18] extends this analysis to government contracting, arguing that multi-layered oversight of technology vendors and standardized inter-institutional security procedures are essential for maintaining state control over public data. Haswell and Whitfor [10] propose a co-governance model in which institutional capacity is enhanced through collaborative transparency mechanisms between government and technology corporations. Kumar and Gupta [19] find that cross-sector innovation mechanisms and interoperable data systems significantly strengthen institutional capacity. Zhang, Turel, and Zöll [20] add a psychosocial dimension, demonstrating that inter-unit trust and collaborative cultures are essential preconditions for effective data sharing within organizational structures. These studies collectively demonstrate that coordination capacity extends beyond formal structural arrangements to encompass relational dynamics, trust-building, and shared governance frameworks.

d. Institutional Values, Ethics, and Public Trust

The fourth and perhaps most conceptually significant theme concerns the normative and ethical dimensions of institutional capacity. Saura, Barbosa, and Rana (2025) argue that effective digital governance is determined by three factors: cohesive data governance integration, digital literacy of personnel, and ethical leadership. Young and Visser [21] demonstrate that the Data Protection Officer role, when endowed with formal autonomy, serves as a critical mechanism for embedding ethical accountability within institutional structures. Abbas [22] develops the concept of corporate digital responsibility, showing that institutions demonstrating transparent and ethically responsible data practices achieve higher public legitimacy and reputational strength. Abu-Salma et al. [23] advocate for human-centred privacy design, arguing that institutional capacity must incorporate principles of fairness, transparency, and user participation to generate meaningful public trust. Baraku et al.[24] further contend that traditional centralized institutional models are inadequate for governing personal data sovereignty, necessitating decentralized structures that empower individual data control. These studies align with Moore's [25] Public Value Theory, which posits that public institutions must generate societal value through trust, transparency, and ethical service delivery.

Synthesis and Discussion

The synthesis of findings across the four thematic dimensions reveals a consistent pattern: institutional capacity for personal data protection is a multidimensional construct that cannot be reduced to any single factor. The reviewed literature demonstrates that legal frameworks, however well-designed, remain insufficient without corresponding organizational structures capable of translating regulatory mandates into operational reality. This finding directly resonates with the Indonesian context, where Law Number 27 of 2022 has been enacted but implementing regulations remain largely absent, and the interim supervisory authority of Komdigi operates without a fully articulated operational foundation.

Grindle's [4] Institutional Capacity Framework provides a robust analytical lens for understanding these dynamics. The five nested dimensions of the framework, encompassing the action environment, the public sector institutional context, the task network, the organizational level, and the human resource level, are each reflected in the reviewed literature. The studies on structural and regulatory capacity correspond to Grindle's organizational and institutional context dimensions, while findings on human resource and technological capacity directly map onto the human resource dimension. The coordination theme reflects the task network dimension, and the values and ethics theme speaks to the action environment within which institutions operate.

The OECD's [3] Digital Institutional Capacity framework enriches this analysis by introducing dimensions that are specifically calibrated for the digital governance era. The emphasis on strategic governance capacity, data and infrastructure capacity, human and organizational capacity, and trust and accountability capacity provides a contemporary extension of Grindle's model. The reviewed literature strongly supports this extended framework, particularly in its emphasis on digital literacy, adaptive governance, and public trust as indispensable components of effective data protection institutions.

Comparative analysis across the reviewed studies further reveals that developing countries face distinctive challenges in building institutional capacity for data protection. India's experience with the Aadhaar system and its consent dilemma [7], [9], Vietnam's centralized yet symbolically oriented data governance model (Huynh, 2024), and Oman's fragmented institutional landscape [8] all demonstrate that rapid digitalization without commensurate institutional strengthening produces governance deficits that undermine policy objectives. Brazil's experience with the LGPD offers a more encouraging trajectory, where the establishment of the Autoridade Nacional de Proteção de Dados (ANPD) as an independent supervisory body has provided an institutional anchor for effective data protection governance (Bezerra). Singapore's GovTech model similarly demonstrates the benefits of integrated, strategically designed institutional capacity [16].

For Indonesia, these comparative insights carry direct implications. The continued delay in issuing implementing regulations, the absence of a permanent independent supervisory body, and the documented weaknesses in inter-agency coordination collectively indicate that Komdigi's institutional capacity requires significant strengthening across all four thematic dimensions identified in this review. The gap between Indonesia's formal legal commitment to data protection and its operational institutional capacity constitutes a critical vulnerability that demands systematic reform.

Research Gaps and Future Directions

The reviewed literature reveals several significant gaps that merit future scholarly attention. First, longitudinal studies tracking the evolution of institutional capacity over time are notably absent. Most studies provide cross-sectional analyses that capture institutional conditions at a single point, limiting understanding of how capacity develops, adapts, or deteriorates in response to policy changes and technological evolution. Second, empirical studies focusing specifically on the institutional capacity of Indonesian data protection governance remain scarce, with most comparative research drawing on cases from India, Europe, or Singapore. Third, the intersection of digital sovereignty, global data connectivity, and national institutional capacity represents an underexplored area that is increasingly relevant as cross-border data flows intensify [26]. Finally, research on the role of organizational culture, leadership quality, and institutional learning in shaping data protection capacity remains at an early stage and warrants deeper empirical investigation.

CONCLUSION

This study synthesizes 27 articles to identify four key dimensions of institutional capacity: structural and regulatory capacity, human resource and technological capacity, inter-institutional coordination, and institutional values. These dimensions determine the effectiveness of personal data protection policy implementation. The findings indicate that Indonesia, particularly the Ministry of Communication and Digital Affairs, still faces challenges in institutional fragmentation, limited capacity, and weak coordination, which hinder the implementation of Law Number 27 of 2022. Comparative insights highlight the importance of integrated and adaptive institutional frameworks. Future research should focus on empirical and longitudinal studies to better understand institutional development. Strengthening institutional capacity remains essential to ensure effective and sustainable data protection governance.

REFERENCE

J. A. Taylor and A. M. B. Lips, "The citizen in the information polity: Exposing the limits of the e-government paradigm," *Inf. Polity*, vol. 13, no. 3–4, pp. 139–152, 2008.

A. P. J. I. Indonesia, "Survei penetrasi internet Indonesia 2024," Asosiasi Penyelenggara Jasa Internet Indonesia, 2024. [Online]. Available: https://apjii.or.id.

M. Encinas-Martín and M. Cherian, *Gender, Education and Skills*. OECD. https://doi.org/10.1787/34680dd5-en, 2023.

M. S. Grindle, "Going local: Decentralization, democratization, and the promise of good governance," 2009.

S. Giest, B. Klievink, A. Ingrams, and M. M. Young, "Introduction to the Handbook on Governance and Data Science," in *Handbook on Governance and Data Science*, Edward Elgar Publishing, 2025, pp. 1–12.

J. R. Saura, B. Barbosa, and S. Rana, "Decoding the privacy puzzle: a study on AI deployment in public governance," in *Handbook on Governance and Data Science*, Edward Elgar Publishing, 2025, pp. 239–263.

N. N. CK, "Data protection and privacy in the data-driven public welfare in India," *Electron. Gov. an Int. J.*, vol. 21, no. 5, pp. 505–522, 2025.

R. Awashreh, "Omani public governance in the age of artificial intelligence," in *Public governance practices in the age of AI*, IGI Global Scientific Publishing, 2025, pp. 137–166.

P. R. Biju and O. Gayathri, "Structural oppression and AI: A systematic review of data policy frameworks in India," *Technol. Forecast. Soc. Change*, vol. 223, p. 124415, 2026.

C. Haswell and A. Whitford, "Digital Responsibility at the Nexus of Big Tech and Government: Evidence from Transparency Reports," *Surveill. Soc.*, vol. 23, no. 3, pp. 354–377, 2025.

M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *bmj*, vol. 372, 2021.

T. F. Widayanti, A. D. Rohman, A. N. Z. Haris, E. M. Djafar, and M. Z. Hakim, "ENHANCING CYBERSECURITY AND LEGAL INTEGRATION: REFORMING INDONESIA'S CYBER LAW TO FOSTER SUSTAINABLE GROWTH IN THE DIGITAL ECONOMY," *Diponegoro Law Rev.*, vol. 10, no. 1, pp. 105–119, 2017.

R. Balleste, G. Doucet, and M. L. D. Hanlon, "A Research Agenda for Cybersecurity Law and Policy," 2025.

M. Karmwar and D. Kunwar, "The Dilemma Between Digital Identity and Privacy in Modern Governance: Comparing South Africa and India," *J. Asian Afr. Stud.*, p. 00219096251352368, 2025.

A. Tariq, A. Batool, S. Liaqat, and I. H. Khan, "Institutions, Corruption and Economic

Development: PLS-SEM Analysis," *J. Polit. Stab. Arch.*, vol. 3, no. 3, pp. 1351–1374, 2025.

A. Perdana and I. A. Mokhtar, "Digital transformation in government: Lessons from GovTech Singapore," *J. Inf. Technol. Teach. Cases*, p. 20438869251362870, 2024.

J. Lund-Tønnesen and K. Fossheim, "Excessive digital surveillance and data privacy invasion as a creeping crisis," *Risk, Hazards Cris. Public Policy*, vol. 16, no. 1, p. e70005, 2025.

R. V Rose, "A paradigm: government contracting and cybersecurity," *EDPACS*, vol. 70, no. 10, pp. 33–49, 2025.

N. Kumar and S. T. Gupta, "Integrating Technology Across Sectors: Innovations in Public Administration, Engineering, and Business," in *Digital Technologies and Transformations in Public Administration, Engineering, and Sustainable Business*, IGI Global Scientific Publishing, 2026, pp. 205–234.

M. Zhang, O. Turel, and A. Zöll, "Group closeness effects on co-owned information sharing: A multilevel perspective," *Int. J. Inf. Manage.*, vol. 86, p. 102977, 2026.

S. Young and F. Visser, "Agency Between Logics: Data Privacy Tactics, Ethics, and the Power of the Data Protection Officer," *J. Tech. Writ. Commun.*, vol. 56, no. 1, pp. 79–92, 2026.

J. Abbas, "When and How Corporate Digital Responsibility Contributes to a Firm's Reputation in Society: Scale Development and Structural Analysis.," *Technol. Soc.*, p. 103067, 2025.

R. Abu-Salma *et al.*, "Grand Challenges in Human-Centered Privacy," *IEEE Secur. Priv.*, vol. 23, no. 4, pp. 103–110, 2025.

V. Baraku, I. Paraskakis, S. Veloudis, and P. Yadav, "Extending Personal Data Sovereignty by Enabling Governance of AI Training on Personal Data," in *Working Conference on Virtual Enterprises*, 2025, pp. 19–35.

A. Lindgreen, N. Koenig-Lewis, M. Kitchener, J. D. Brewer, M. H. Moore, and T. Meynhardt, "Public Value," *Public Value Deep. Enrich. Broadening Theory Pract. Routledge. https//doi. org/10.4324/9781315163437*, 2019.

H. Yun, "China's data sovereignty and security: Implications for global digital borders and governance," *Chinese Polit. Sci. Rev.*, vol. 10, no. 2, pp. 178–203, 2025.