Advances in Public Law and Policy (AiPLaP)
Vol 1, No 1, 2026, 39-49 https://doi.org/10.35912/aiplap.v1i1.3918.

Data-Driven Analysis of Cyber Threats and Public Policy Responses in Indonesia

Eka Septi Nur Jannah[1*], Dini Eka Prasasti[2], Nada Alfaiza Fisabilazkia[3]
Universitas Gadjah Mada, Yogyakarta, Indonesia[1-3]
ekaseptinurjannah@mail.ugm.ac.id[1*], diniekaprasasti@mail.ugm.ac.id[2],,
nadaalfaizafisabilazkia@mail.ugm.ac.id[3]

Article History
Received on 19 December 2025
1st Revision on 20 January 2026
2nd Revision on 26 January 2026
Accepted on 6 February 2026

Abstract
Purpose: This study aims to examine cybersecurity vulnerabilities in Indonesia's digital public service transformation using a data-driven public policy perspective and to generate evidence-based policy recommendations.
Research Methodology: This study applies a qualitative data science approach by combining systematic policy review with social media analytics. Public discourse on cybersecurity incidents was collected from Platform X through data scraping and analyzed using Orange software for sentiment analysis, keyword mapping, and temporal visualization to assess public perception and governance-related risks.
Results: The analysis reveals a dominance of negative sentiment associated with public distrust, institutional dissatisfaction, and concerns over recurring data leaks. Data patterns indicate three systemic drivers of cybersecurity vulnerability: delayed implementation of derivative regulations under the Personal Data Protection Law, technical fragility and centralized risk exposure within the National Data Center, and uneven digital literacy across the population. The findings demonstrate that cybersecurity failures are not isolated technical incidents but reflect broader governance and policy implementation gaps.
Conclusions: This study concludes that Indonesia's digital transformation agenda is constrained by insufficient data-driven cybersecurity governance. The absence of integrated regulatory, technical, and social interventions weakens the state's capacity to manage digital risks effectively.
Limitations: This study is limited to publicly available social media data and does not include direct institutional or field-level validation.
Contributions: This research contributes to data science for public policy by demonstrating how social media analytics can support policy diagnosis, risk assessment, and evidence-based cybersecurity reform in digital government systems.

Keywords: *Cyber Security, Data Science, Digital Transformation, Personal Data Protection, Public Policy*

How to Cite: Prasasti, D. E Jannah, E. S. N., & Fisabilazkia, N. A. (2026). Data-Driven Analysis of Cyber Threats and Public Policy Responses in Indonesia. *Advances in Public Law and Policy (AiPLaP)*. 1(1), 39-49.

1. Introduction

Digital transformation has become a widely adopted strategy for public organizations to respond to rapid technological advancements. Through digital innovation, public institutions develop applications and digital platforms that aim to improve the accessibility, efficiency, and quality of public services (Vial, 2021). In theory, digital transformation represents a positive and progressive change in public

sector governance. However, in practice, digital transformation in Indonesia has not been fully successful because of persistent digital security challenges. Indonesia has experienced multiple high-profile cases that highlight the government's limited capacity to ensure robust cybersecurity (Sahatatua, Setiady, Astawa, & Ansari, 2024; Widyastuti & Tarumingkeng, 2025)

These digital security issues stem from several, interrelated factors. First, weak cybersecurity capacity is largely driven by insufficient human resource competencies and inadequate governance mechanisms for managing data breach incidents in public institutions. Many civil servants and information system administrators lack advanced cybersecurity skills, and low public service motivation further reduces institutional responsiveness to cyberattacks and public complaints. This condition weakens the overall resilience of digital public-service systems (Yulita, 2025).

Second, Indonesia faces a regulatory gap, particularly the absence of detailed guidelines and enforceable sanctions for data breach incidents involving public institutions. Consequently, there is limited institutional accountability and weak enforcement mechanisms to ensure compliance with cybersecurity standards. A notable example occurred during the 2024 Jakarta local election, when citizens' national identity numbers were misused to support independent candidates without the owners' consent (Albaldan & Lisasih, 2025). Despite the severity of the incident, the lack of effective regulatory enforcement resulted in minimal government accountability and systematic evaluation (Nisa & Ali, 2025).

Third, low digital literacy among the public exacerbates cybersecurity vulnerability. Many citizens have limited awareness of personal data protection, digital risk, and cybersecurity ethics. This condition further constrains public institutions that lack clear and structured policies for managing digital risks. The rapid growth of online gambling in Indonesia illustrates how limited digital awareness exposes citizens to legal, ethical, and cybersecurity threats. According to an OJK survey (2022), Indonesia's digital and financial literacy rates remain at 41.48% and 49.6%, respectively, indicating a substantial gap between digital access and digital competence (Ahludzikri, Hasibuan, Aziz, & Triloka, 2025).

Considering these factors, it can be concluded that the Indonesian government urgently needs to strengthen its national cybersecurity framework. The primary concern is the vulnerability of the data security infrastructure managed by public institutions. Personal data breaches can be exploited for disinformation campaigns, voter intimidation, and identity-based crimes, thereby undermining the democratic processes and public trust. Therefore, comprehensive improvements in data protection systems are necessary (Nisa & Ali, 2025).

Several arguments support this urgency. First, as digitalization accelerates across public service sectors, the potential impact of cyberattacks on citizens' personal data and national security will increase significantly (Singer & Friedman, 2013). Poorly protected systems create opportunities for cybercrimes, including fraud and identity theft, which ultimately erode public confidence in government-led digital initiatives. Second, strong cybersecurity governance is essential to safeguard Indonesia's economic growth and development (Balaji, 2025). A country's cybersecurity capacity reflects its commitment to protecting citizen and investor data, and a secure digital environment enhances investor confidence while ensuring the stability of critical infrastructure (Leahovcenco, 2021). Finally, with a rapidly expanding Internet user population, Indonesia requires proactive cybersecurity governance that enforces privacy rights, prevents cybercrime, and fosters a resilient digital society supported by data-driven policy formulation and evidence-based decision-making (Janssen & Helbig, 2018).

2. Literature Review and Hypothesis/es Development

2.1 Cybersecurity Governance and Institutional Capacity

Cybersecurity has emerged as a critical pillar of public sector digital transformation, particularly as governments increasingly depend on digital infrastructure to deliver essential public services, manage population data, and support economic activities. The expansion of e-government systems, digital identity platforms, and integrated public service portals has significantly increased the volume,

sensitivity, and interconnectivity of the data managed by public institutions. Consequently, cybersecurity governance is no longer merely a technical issue but has evolved into a strategic public policy concern that directly affects national security, public trust and institutional legitimacy.

The existing literature consistently emphasizes that weak institutional frameworks and fragmented governance structures substantially undermine national cybersecurity resilience (Bada & Nurse, 2019; von Solms & van Niekerk, 2013). Cybersecurity governance requires clearly defined roles, responsibilities, and accountability mechanisms across government agencies, as well as alignment between legal frameworks, organizational capacity, and technological infrastructure. Without coherent governance arrangements, cybersecurity policies tend to be reactive, sectoral, and ineffective in addressing systemic risks. This condition is particularly problematic in the public sector, where cybersecurity failures can disrupt essential services and compromise citizens' personal data on a large scale.

At the global level, cybersecurity governance faces persistent coordination challenges. Differences in legal traditions, data protection regimes, incident reporting standards, and institutional capacities across countries hinder the development of a unified global cybersecurity architecture (Karaman & Aybar, 2016). While international frameworks and norms have been promoted through multilateral institutions, their implementation remains uneven, especially in developing countries with limited technical and financial resources. Consequently, global cybersecurity governance is characterized by asymmetrical capabilities and fragmented enforcement, which further complicate cross-border data protection and cyber-incident responses.

In the Indonesian context, cybersecurity governance is marked by regulatory fragmentation and limited institutional coordination. Multiple public institutions are involved in managing cybersecurity-related functions, including data protection, digital infrastructure management, and cyber-incident response; however, their mandates often overlap or remain insufficiently integrated. Studies on information security governance in Indonesia indicate that the absence of harmonized national standards and weak inter-agency collaboration significantly reduce the government's capacity to prevent, detect, and respond to cyber threats effectively (Kang & Hovav, 2020) .This fragmentation not only delays policy implementation but also creates regulatory gaps that can be exploited by malicious actors.

Institutional capacity constraints remain a major challenge in strengthening cybersecurity governance. The limited availability of skilled human resources, uneven digital competencies across public institutions, and inadequate investment in cybersecurity infrastructure reduce the effectiveness of existing policies. Therefore, institutional strengthening requires more than regulatory reform; it necessitates sustained capacity building, including professional training, organizational learning, and the development of specialized cybersecurity units within government agencies. In addition, effective cybersecurity governance demands cross-sectoral coordination involving public institutions, private technology providers, and civil society actors, as cyber risks increasingly transcend organizational and sectoral boundaries.

Ultimately, strengthening cybersecurity governance in the public sector requires an integrated institutional approach that combines regulatory coherence, organizational capacity, and collaborative governance. By enhancing institutional coordination and capacity, governments can move beyond reactive cybersecurity measures toward a more proactive, resilient, and trust-based digital governance system capable of supporting sustainable public-sector digital transformation.

2.2 Data Leakage, Accountability, and Legal Enforcement

Data leakage incidents in public institutions raise critical questions regarding accountability and the effectiveness of legal enforcement mechanisms. Studies focusing on data breaches in government agencies show that insider threats, weak internal controls, and inadequate legal sanctions contribute significantly to recurring data leak cases (D'Arcy, Herath, & Shoss, 2014; Hadlington, 2017). In Indonesia, empirical analyses have revealed that data breaches involving public officials often fail to

result in meaningful legal consequences, thereby undermining deterrence and public trust in digital governance (Sahatatua et al., 2024).

The enactment of the Personal Data Protection Law represents a normative milestone; however, scholars argue that without derivative regulations, enforcement mechanisms, and institutional oversight, legal frameworks remain largely symbolic (Bennett & Raab, 2017; Greenleaf, 2017). Thus, effective cybersecurity governance depends on integrating legal enforcement with institutional accountability and operational capacity.

Digital public services have expanded access and efficiency but have simultaneously increased exposure to data protection risks. Research on digital document management systems and public digital libraries demonstrates that inadequate access control, insufficient encryption, and weak data classification mechanisms significantly heighten vulnerability to data breaches (Tschider, 2018; Martín, De Fuentes, & González-Manzano, 2016). These risks are exacerbated by organizational negligence and limited cybersecurity awareness among employees in the public sector. Scholars have highlighted that robust data governance frameworks, supported by automated monitoring systems and security-by-design principles, are essential to mitigate the risks associated with digital public service delivery (Janssen, Weerakkody, Ismagilova, Sivarajah, & Irani, 2020; Vial, 2021). Without such safeguards, digital transformation may paradoxically erode public trust rather than strengthening it.

2.3 Digital Literacy and Cybersecurity Awareness

Cybersecurity is increasingly recognized not merely as a technical or infrastructural concern, but as a socio-behavioral challenge shaped by human knowledge, attitudes, and digital practices. Although advanced security technologies and regulatory frameworks are essential, their effectiveness is fundamentally constrained by the level of digital literacy and cybersecurity awareness among users. A growing body of literature highlights that low levels of digital literacy significantly increase individuals' exposure to cybercrime, data misuse, misinformation, and identity theft (Van Deursen & Van Dijk, 2019). Human error, rather than technological failure, remains one of the most persistent vulnerabilities in cybersecurity systems. From a policy perspective, digital literacy encompasses not only the ability to access and use digital technologies but also the capacity to understand digital risks, protect personal data, and make informed decisions in online environments. Studies have emphasized that insufficient awareness of privacy rights, weak password practices, and limited understanding of digital security mechanisms undermine the effectiveness of national cybersecurity strategies (Alshammari & Simpson, 2017). In many cases, users unknowingly become entry points for cyberattacks through practices such as phishing, unsafe data sharing, and poor authentication behavior.

These challenges are particularly pronounced in developing countries, where rapid digitalization often outpaces investment in digital education and awareness. Limited access to cybersecurity training, uneven educational infrastructure, and socioeconomic disparities contribute to persistent gaps in digital competence. Consequently, cybersecurity governance in such contexts cannot rely solely on technical solutions or legal enforcement; it must also address the human dimension of cyber risk through systematic public education and capacity-building initiatives.

In the Indonesian context, existing studies indicate that disparities in digital literacy and cybersecurity awareness remain substantial, especially in rural areas and among marginalized communities. Research suggests that a limited understanding of personal data protection reduces public responsiveness to cybersecurity policies and weakens compliance with data protection regulations (Bendovschi, 2015). These gaps are further exacerbated by uneven Internet access, limited exposure to formal digital education, and the rapid adoption of digital platforms without adequate user guidance. Consequently, despite the expansion of digital public services, many citizens remain vulnerable to online fraud, data exploitation, and misinformation (Van Deursen & Van Dijk, 2019).

Moreover, challenges in digital literacy are not confined to the general public. Public sector employees and local government officials often exhibit varying levels of cybersecurity awareness, which can create institutional vulnerabilities in sensitive data management. This highlights the importance of extending

cybersecurity education beyond citizens to include public officials, educators, and service providers who play a critical role in implementing and enforcing data protection policies. Taken together, these findings underscore the necessity of integrating digital literacy and cybersecurity awareness into broader cybersecurity governance. An effective cybersecurity policy must combine regulatory instruments and technological safeguards with sustained educational interventions aimed at shaping safer digital behavior. By strengthening public awareness and digital competencies, governments can enhance compliance, reduce human-related cyber risks, and build a more resilient and inclusive digital ecosystems.

2.4 Data Governance and Strategic Cybersecurity Reform

Cybersecurity is increasingly recognized not merely as a technical or infrastructural concern but as a socio-behavioral challenge shaped by human knowledge, attitudes, and digital practices. Although advanced security technologies and regulatory frameworks are essential, their effectiveness is fundamentally constrained by the level of digital literacy and cybersecurity awareness among users. A growing body of literature highlights that low levels of digital literacy significantly increase individuals' exposure to cybercrime, data misuse, misinformation, and identity theft (Van Deursen & Van Dijk, 2019). Human error, rather than technological failure, remains one of the most persistent vulnerabilities in cybersecurity systems. From a policy perspective, digital literacy extends beyond basic technical skills to include awareness of privacy rights, risk assessment, and responsible digital behavior (Hadlington, 2017). Studies have consistently shown that insufficient understanding of data protection obligations, weak authentication practices, and limited familiarity with cybersecurity mechanisms undermine the effectiveness of national cybersecurity strategies (Alshammari & Simpson, 2017). In this context, citizens are not merely passive beneficiaries of digital services, but active actors whose behavior directly affects the resilience of digital governance systems.

These challenges are particularly evident in developing countries, where the rapid expansion of digital public services is often not matched by adequate investment in digital education and cybersecurity awareness. Socioeconomic disparities, uneven access to digital infrastructure, and limited institutional capacity contribute to persistent gaps in digital competence. Consequently, cybersecurity governance cannot rely solely on legal compliance or technical safeguards but must incorporate sustained public education and behavioral interventions as integral components of policy design. In Indonesia, empirical studies have indicated that gaps in digital literacy and cybersecurity awareness remain substantial, particularly in rural areas and among marginalized communities. A limited understanding of personal data protection reduces public responsiveness to cybersecurity policies and weakens compliance with regulatory frameworks. These vulnerabilities are further exacerbated by the increasing use of digital platforms without sufficient guidance on data security practices, increasing citizens' exposure to online fraud, identity misuse and misinformation.

Recent literature emphasizes that effective cybersecurity policy requires a holistic data governance approach that integrates legal, technical, and institutional dimensions (De Hert & Papakonstantinou, 2016). Strategic reviews of data protection governance in Indonesia suggest that cybersecurity reform should prioritize regulatory coherence, institutional leadership, and public participation to ensure a sustainable digital transformation (Novitasari, Dewi, & Oktavia, 2022). Without meaningful public engagement and adequate digital literacy, even well-designed regulatory frameworks risk weak implementation and have limited societal impact.

Comparative policy studies further demonstrate that countries with centralized cybersecurity authorities, clear enforcement mechanisms, and strong public–private collaboration achieve higher levels of digital trust and economic stability (Baldwin, Cave, & Lodge, 2011; Leahovcenco, 2021). These findings reinforce the argument that cybersecurity capacity building, digital literacy enhancement, and integrated governance structures are essential pillars of resilient digital public services. Therefore, strengthening cybersecurity awareness among citizens and public officials is not a supplementary policy objective but a foundational requirement for safeguarding digital transformation and maintaining public trust in government-led digital initiatives.

2.5 Research Gap

While existing studies provide valuable insights into cybersecurity governance, data protection, and digital literacy, limited research integrates institutional analysis, legal enforcement, and public perception using data-driven methods in Indonesia. Most studies focus on regulatory frameworks or technical vulnerabilities, leaving a gap in understanding how public discourse and societal trust interact with policy implementation. Addressing this gap requires a data science–informed public policy approach that combines qualitative policy analysis with empirical digital trace data to support evidence-based cybersecurity reform.

3. Methodology

This study adopts a qualitative research approach, as it is particularly suitable for developing an in-depth understanding of complex and multifaceted issues, such as data breaches, within the digital transformation of public services. Qualitative methods allow researchers to capture contextual nuances, social dynamics, institutional responses, and public perceptions that are often overlooked by purely quantitative approaches (Creswell & Poth, 2016). This approach is especially relevant for cybersecurity and public policy studies, where governance structures, regulatory gaps, and societal trust play a central role.

Methodologically, this study integrates two complementary techniques: a systematic literature review and social media data scraping. The literature review establishes a robust theoretical foundation and informs policy-oriented analysis. The reviewed literature encompasses global studies on data governance, privacy regulations, public sector digital transformation, and cybersecurity policies, enabling comparative insights across institutional and national contexts (Snyder, 2019). In addition, this study draws upon established cybersecurity theories that emphasize the strategic importance of data governance and privacy protection in fostering public trust and sustaining digital economic growth (Silic & Back, 2014).

The second method involved data scraping from the social media platform X (formerly Twitter) to collect real-time empirical data reflecting public discourse on cybersecurity issues in Indonesia. Social media scraping enables the identification of emerging trends, dominant narratives, and public sentiments that may not yet be documented in formal policy reports or academic publications. The resulting unstructured data were subsequently analyzed using text mining techniques, including keyword frequency analysis, word cloud visualization, sentiment analysis, and temporal heat map mapping. These analytical tools allow for a systematic examination of public concerns, trust dynamics, and perceived institutional performance in cybersecurity governance. Within this research design, the literature review provides a conceptual framework and analytical indicators for policy assessment, while data scraping offers contextualized empirical insights into public perceptions and real-world cybersecurity challenges. By combining these two methods, the study aims to identify critical gaps between formal cybersecurity policies and their practical implementation, and to formulate evidence-based strategic recommendations to support a secure, inclusive, and sustainable digital transformation in Indonesia (Snyder, 2019).

4. Results and Discussions

4.1 Keyword Distribution and Public Discourse on Data Breaches

Figure 1 shows that public discourse surrounding cybersecurity in Indonesia is strongly dominated by concerns over data breaches and personal data protection. The analysis is grounded in data scraped from the social media platform X using the keywords “kebocoran data”, “data Indonesia”, and “kebocoran data Indonesia” over the period January 2020 to May 2025. A total of 860 textual data points were collected and processed using the Orange data-mining application. The analytical techniques employed included word cloud visualization, sentiment analysis, and hierarchical heatmap clustering. Word cloud analysis provides an initial descriptive overview of the dominant themes in public discourse related to data breaches in Indonesia. Word clouds visualize the most frequently occurring terms within textual

datasets, where the font size corresponds to relative frequency. The visualization reveals that the terms “kebocoran”, “data”, and “bahaya” dominate the discourse, indicating that data leakage is primarily framed as a threat or risk by the public.

In addition to these core terms, several institutional and political keywords frequently appear, including “pemerintah”, “negara”, “keamanan”, and the hashtag “#sahkanruupdp”. The presence of these terms suggests that public concern extends beyond technical incidents to state responsibility, governance, and regulatory accountability. The hashtag “#sahkanruupdp” reflects public pressure for the enactment and enforcement of personal data protection legislation. From a policy analysis perspective, the word cloud indicates that cybersecurity is perceived not merely as an IT issue but as governance failure with political and legal implications. This finding aligns with prior research emphasizing that digital security crises often evolve into legitimacy crises when state institutions are perceived to be incapable of protecting citizens’ personal data.

Figure 1. Word cloud analysis

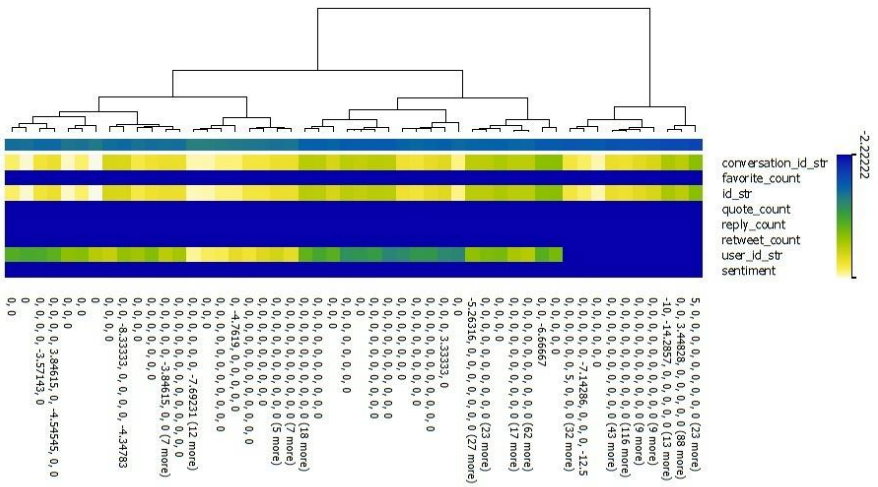

Figure 2. Sentiment heatmap of data

While word clouds highlight thematic salience, they do not capture the evaluative or emotional orientations of public discourse. Figure 2 illustrates the results of the hierarchical clustering and sentiment analysis of public interactions on the social media platform X related to cybersecurity issues in Indonesia. The heatmap visualizes variations in sentiment scores alongside engagement attributes,

such as replies, retweets, quotes, and favorites. Therefore, sentiment analysis was conducted to identify whether public reactions to cybersecurity issues tended toward positive, neutral, or negative sentiments.

The results indicate that although neutral sentiment constitutes the largest single category, negative sentiment significantly exceeds positive sentiment. This imbalance becomes more pronounced when examining the extreme sentiment values. Several data points exhibit highly negative sentiment scores, such as −10, −12.4, and −7.6, which reflect expressions of anger, fear, distrust, and frustration, which are commonly associated with recurring data breach incidents, perceived government negligence, weak law enforcement, and failures in national digital infrastructure. Conversely, positive sentiment appears in a much smaller subset of data and is typically linked to informational posts, legal advocacy, and references to proposed policy solutions.

The hierarchical heatmap visualization further supports these findings. In the heatmap, dark blue hues dominate the sentiment column, representing strongly negative sentiment. Neutral sentiment appears in lighter colors, whereas positive sentiment is sparse and localized. This pattern demonstrates that negative emotional responses are not isolated incidents but form structurally dominant discourse patterns.

4.2 Public Trust, Institutional Capacity, and Data-Driven Cybersecurity Governance

The dominance of negative sentiment in digital discourse signals a broader crisis of trust in Indonesia's digital governance system. Public trust is a critical intangible asset in digital transformation initiatives, particularly in public service delivery systems that rely on centralized data storage and citizen participation.

Repeated cybersecurity incidents undermine confidence in state institutions, reduce the willingness to adopt digital public services, and increase resistance to data sharing. From a data science for public policy perspective, sentiment analysis functions as an early diagnostic tool that reveals public dissatisfaction before it manifests as political backlash or policy rejection. The findings suggest that Indonesia's cybersecurity challenges are not solely technical but also deeply institutional and communicative. Therefore, effective cybersecurity governance must address both infrastructural resilience and public perception through transparent, participatory, and accountable policy mechanisms.

Although Indonesia enacted Law No. 27 of 2022 on Personal Data Protection (UU PDP), the absence of derivative regulations significantly limits its enforceability in the digital realm. Without detailed implementing regulations, public institutions lack clear technical standards, reporting obligations and sanction mechanisms. This regulatory gap increases the risk of data misuse, weakens compliance incentives, and hampers law enforcement. Derivative regulations are essential for operationalizing the key principles of the law, including consent management, breach notification procedures, data transfer protocols, and enforcement mechanisms.

International experience demonstrates the importance of derivative regulation. Singapore's Personal Data Protection Act is supported by sector-specific guidelines and certification schemes, such as the Data Protection Trustmark, which incentivizes compliance and strengthens organizational accountability. The National Data Center (PDN) is a cornerstone of Indonesia's digital governance. However, recent cyber incidents have revealed serious weaknesses in its technical infrastructure, operational capacity, and governance arrangements (Budiman, 2026).

Strengthening the PDN requires a holistic approach that includes upgrading physical infrastructure, enhancing cybersecurity architecture, and investing in human resource capacity. Continuous security audits, adaptive threat monitoring, and cross-sector coordination are essential to prevent systemic failures. The comparative experience from South Korea's Government Integrated Data Center illustrates how a centralized data infrastructure, when combined with institutional independence and technical authority, can significantly improve system reliability and efficiency.

Digital literacy is a critical, but often underestimated, component of cybersecurity governance. Low public awareness of data protection rights and cybersecurity risks increases vulnerability to fraud, identity theft and misinformation. In Indonesia, digital literacy gaps persist among citizens and within public institutions. Uneven technical capacity among civil servants creates weak points that can be exploited by cyber-attackers.

Therefore, policy interventions must include nationwide digital literacy programs targeting citizens, civil servants, educators, and small businesses. These programs should be complemented by investments in cybersecurity infrastructure, including encryption systems, updated firewalls, and automated intrusion detection technologies. Findings confirm that cybersecurity governance must be treated as a data-driven public policy domain. Social media analytics provide valuable insights into public trust, institutional performance and emerging risks.

Integrating these analytical tools into policymaking enables governments to move from reactive responses to anticipatory and adaptive governance models. Indonesia's digital transformation will remain fragile unless its cybersecurity policy evolves into a coherent system that harmonizes law, technology, institutions, and public participation. Overall, this chapter demonstrates that the cybersecurity challenges in Indonesia are systemic and multidimensional. Effective solutions require not only technical upgrades but also regulatory clarity, institutional reform, and sustained engagement with the public sentiment. By grounding policy reform in empirical data and international best practices, Indonesia can strengthen its digital governance framework and restore public trust in its digital public services.

5. Conclusions

5.1. Conclusion

Digital transformation is a strategic instrument for improving public service quality through technology. However, recurring data breach incidents indicate that this transformation has not been supported by adequate cybersecurity infrastructure. Consequently, strengthening cybersecurity systems has become an urgent policy priority. This study argues that effective personal data protection in Indonesia requires evidence-based policy interventions, including the formulation of implementing regulations for the Personal Data Protection Law, strengthening the National Data Center, and improving digital literacy and digital security infrastructure. From a data-driven public policy perspective, the integration of a national Single Sign-On (SSO) system with a digital public complaint portal can enhance cybersecurity governance by improving data integration, accountability, and incident traceability. These measures must be implemented sequentially and coherently to ensure that digital transformation is secure, efficient, and capable of safeguarding national data sovereignty.

5.2. Research Limitations

This study is limited to publicly available social media data and does not incorporate direct institutional interviews or field-level validations. Consequently, the findings primarily reflect public discourse and perceptions rather than the internal operational practices of government institutions or the lived experiences of the affected stakeholders. While this approach is effective for capturing large-scale sentiment and policy-related narratives, it may not fully represent the implementation dynamics or decision-making processes within public organizations.

5.3 Suggestions and Directions for Future Research

Future research should address this study's limitations by incorporating institutional and field-level validation through interviews with policymakers, cybersecurity authorities, and public service operators to complement social media–based findings. Expanding data sources to include official government complaint systems, administrative records, and news databases will improve data reliability and reduce platform bias. From a data science for public policy perspective, subsequent studies could employ advanced methods, such as machine learning–based topic modeling, network analysis, and predictive analytics, to detect emerging cybersecurity risks and assess policy effectiveness. Longitudinal and comparative cross-country analyses, particularly within ASEAN, are also recommended to deepen the

understanding of how governance structures and digital infrastructure shape cybersecurity resilience in public sector digital transformation.

Acknowledgement

The author gratefully acknowledges the use of open-access data, academic literature, and analytical tools that supported this research. This research received no external funding. All interpretations and conclusions presented are solely the authors' responsibility.

References

Ahludzikri, F., Hasibuan, M. S., Aziz, R. Z. A., & Triloka, J. (2025). Blibiometric analysis of detection lung cancer. *Advances in Artificial Intelligent and Machine Learning, 1*(1), 61-71. doi:https://doi.org/10.35912/aaiml.v1i1.3776

Albaldan, K. A., & Lisasih, N. Y. (2025). Personal Data Security Violations in East Jakarta Regional Elections: Legal Analysis Through Personal Data Protection Legislation. *Journal of Law and Economics, 4*(2), 145-152. doi:https://doi.org/10.56347/jle.v4i2.330

Alshammari, M., & Simpson, A. (2017). *Towards a principled approach for engineering privacy by design.* Paper presented at the Annual Privacy Forum.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393-410. doi:https://doi.org/10.1093/cybsec/tyz006

Balaji, K. (2025). E-Government and E-Governance: Driving Digital Transformation in Public Administration. *Public Governance Practices in the Age of AI*, 23-44. doi:https://doi.org//0.4018/979-8-3693-9286-7.ch002

Baldwin, R., Cave, M., & Lodge, M. (2011). *Understanding regulation: theory, strategy, and practice*: Oxford university press.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance, 28*, 24-31. doi:https://doi.org/10.1016/S2212-5671(15)01077-1

Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*: Routledge.

Budiman, E. M. (2026). Philosophical Critique of Capital Market Regulation: A Case Study between Public Interest and Privacy. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia, 5*(2), 1-13. doi:https://doi.org/10.35912/jihham.v5i2.4728

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*: Sage publications.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of management information systems, 31*(2), 285-318. doi:https://doi.org/10.1111/isj.12012

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review, 32*(2), 179-194. doi:https://doi.org/10.1016/j.clsr.2016.03.012

Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Including Indonesia and Turkey (January 30, 2017), 145*(12), 10-13.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7). doi:https://doi.org/10.1016/j.heliyon.2017.e00346

Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle: Policy-makers be prepared! *Government Information Quarterly, 35*(4), S99-S105. doi:https://doi.org/10.1016/j.giq.2015.11.009

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management, 50*, 302-309. doi:https://doi.org/10.1016/j.giq.2020.101512

Kang, M., & Hovav, A. (2020). Benchmarking methodology for information security policy (BMISP): Artifact development and evaluation. *Information Systems Frontiers, 22*(1), 221-242. doi:https://doi.org/10.1007/s10796-018-9855-6
Karaman, M., & Aybar, C. (2016). Institutional cybersecurity from military perspective. *International journal of information security science, 5*(1), 1-7.
Leahovcenco, A. (2021). Cybersecurity as a fundamental element of the digital economy. *MEST Journal, 9*(1). doi:https://doi.org/10.1108/JES-01-2020-0032
Nisa, S. R., & Ali, R. (2025). Application of Fuzzy Matching in chatbot development to improve user experience on e-commerce sites (Case study: Cutiw Fashion Store). *Advances in Artificial Intelligent and Machine Learning, 1*(1), 51-60. doi:https://doi.org/10.35912/aaiml.v1i1.3775
Novitasari, E., Dewi, F. G., & Oktavia, R. (2022). Determinants of e-government implementation in Indonesia. *Asian Journal of Economics, Business, and Accounting, 22*(19), 25-33.
Sahatatua, R., Setiady, T., Astawa, I., & Ansari, T. (2024). role of Investment Law in Indonesia's Economic Recovery Efforts. *Journal of Multidisciplinary Academic and Practice Studies, 2*, 257-259. doi:https://doi.org/10.35912/jomaps.v2i3.2218
Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security, 22*(3), 279-308. doi:https://doi.org/10.1108/IMCS-05-2013-0041
Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know®*: Oxford University Press.
Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research, 104*, 333-339. doi:https://doi.org/10.1016/j.jbusres.2019.07.039
Van Deursen, A. J., & Van Dijk, J. A. (2019). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *New media & society, 21*(2), 354-375. doi:https://doi.org/10.1177/1461444818797082
Vial, G. (2021). Understanding digital transformation: A review and a research agenda. *Managing digital transformation*, 13-66. doi:https://doi.org/10.1016/j.jsis.2021.101695
von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:https://doi.org/10.1016/j.cose.2013.04.004
Widyastuti, L. A., & Tarumingkeng, R. C. (2025). The effect of Artificial Intelligence (AI) and Customer Experience (CX) use in telemedicine on customer satisfaction moderated by service duration. *Advances in Artificial Intelligent and Machine Learning, 1*(1), 1-20. doi:https://doi.org/10.35912/aaiml.v1i1.3763
Yulita, Y. (2025). Expert system for early detection of autism in children using forward chaining method based on android. *Advances in Artificial Intelligent and Machine Learning, 1*(1), 21-39. doi:https://doi.org/10.35912/aaiml.v1i1.3773