



DOI: <https://doi.org/10.38035/sijal.v4i2>
<https://creativecommons.org/licenses/by/4.0/>

Received: 10-09-2026 | Revised: 10-10-2026 | Accepted: 20-10-2026

Reconstructing Digital Sovereignty through State Resilience Legal Policy: Citizen Protection after the Cyberattack on Indonesia's Temporary National Data Center

Dian Priheryanti Havid¹, Laksanto Utomo², R. Lina Sinaulan³

¹Universitas Bhayangkara Jakarta Raya. Jakarta, Indonesia, hdian0324@yahoo.com

²Universitas Bhayangkara Jakarta Raya. Jakarta, Indonesia, -

³Universitas Bhayangkara Jakarta Raya. Jakarta, Indonesia, -

Corresponding Author: hdian0324@yahoo.com¹

Abstract: The development of information technology and Artificial Intelligence (AI) has shifted the paradigm of state resilience away from protection oriented toward territorial areas and toward the protection of a borderless digital space. This shift presents new challenges for the state in protecting its citizens, as reflected in the cyberattack on Indonesia's Temporary National Data Center (PDNS) in 2024. Although Indonesia already has various regulations concerning information technology, cybersecurity, and personal data protection, national legal policy has not yet been fully able to build an integrated framework to respond to digital threats in the AI era. This research aims to analyze the legal policy of state resilience in protecting citizens through a case study of the cyberattack on PDNS, and to reconstruct legal policy based on Digital Sovereignty as a paradigm for strengthening state resilience. This research uses the normative legal research method with statutory, conceptual, and case approaches. The results show that the national legal framework remains sectoral in nature and has not been able to comprehensively integrate cybersecurity governance, data protection, and the use of AI. Therefore, this research offers a reconstruction of legal policy based on Digital Sovereignty, which places control over data, digital infrastructure, cybersecurity, and AI governance as a new foundation for strengthening state resilience while guaranteeing the protection of citizens' constitutional rights in the era of digital transformation. The proposed model integrates data sovereignty, infrastructure resilience, AI accountability, supply chain security, and digital human capacity through preventive, adaptive, rights based governance mechanisms for public institutions.

Keywords: Artificial Intelligence, Citizen Protection, Digital Sovereignty, Legal Policy, State Resilience.

INTRODUCTION

The development of information technology and Artificial Intelligence (AI) has fundamentally transformed the relationship among the state, society, and the space of power. Since the development of the modern state concept, sovereignty has been understood as the state's ability to control its territorial domain and exercise its legal jurisdiction exclusively. However, digital transformation has given rise to a new, non-physical, borderless space that is not entirely subject to territorial logic — namely, cyberspace. This development has produced new forms of threats to the state and its citizens, ranging from cyberattacks on critical infrastructure, theft of personal data, and manipulation of information through deepfakes and algorithm-based disinformation, to the growing dominance of global technology companies over strategic digital infrastructure. As a result, a state's capacity to protect its citizens is no longer determined solely by military strength or territorial control, but also by its ability to control data, technology, and digital infrastructure as the foundation of state administration (Krasner, 1999; Bodin, 1992) (European Union Agency for Cybersecurity [ENISA], 2024; World Economic Forum, 2025).

The development of AI has further accelerated this shift. Unlike conventional information technology, AI is capable of producing automated decision-making, conducting large-scale data analysis, influencing public opinion through algorithmic systems, and increasing the complexity of cyber threats through AI-enabled cyberattacks, including adaptive malware and ransomware capable of autonomously exploiting system vulnerabilities. This condition shows that the concept of sovereignty grounded in control over physical territory faces growing difficulty in addressing digital threats that cross jurisdictional boundaries. Legal policy — as the state's fundamental policy direction in the formation and administration of law — therefore needs to shift from a paradigm oriented toward territorial protection to one that positions control over data, cybersecurity, and digital technology governance as an integral part of state resilience (UNESCO, 2021; Organisation for Economic Co-operation and Development [OECD], 2022a).

The urgency of this issue is no longer hypothetical in Indonesia. The cyberattack on Indonesia's Temporary National Data Center (PDNS) 2 in June 2024 became one of the most significant cybersecurity incidents in the history of national digital governance. Investigations revealed that the attack began with an attempt to disable security systems (Windows Defender), followed by the installation of malware, deletion of system files, and the paralysis of various public services dependent on PDNS. The government confirmed that the incident disrupted services at 282 government institutions, including ministries/agencies and regional governments, while only a small number of institutions were able to restore their services because they still had data backups. The attack was later identified as a variant of Brain Cipher ransomware, derived from LockBit 3.0, which disrupted immigration services, increased the risk of strategic data leaks, and exposed weaknesses in national data-backup governance (Ministry of Communication and Informatics of the Republic of Indonesia, 2024b) (Ministry of Communication and Informatics of the Republic of Indonesia, 2024a; Financial and Development Supervisory Agency, 2024) (National Cyber and Crypto Agency [BSSN], 2024a; Cyber Security Agency of Singapore, 2024).

The PDNS incident demonstrated that digital vulnerability no longer merely causes technical disruption, but also has direct implications for the fulfillment of citizens' constitutional rights, including the right to public services, personal data protection, and a sense of security as guaranteed under the 1945 Constitution of the Republic of Indonesia. This impact was also reflected in the decline of Indonesia's National Cybersecurity Index (NCSI) score from 63.64 in 2023 to 47.50 in 2024, accompanied by a drop in Indonesia's ranking from 48th to 84th out of 136 countries. The National Cyber and Crypto Agency (BSSN) attributed this decline to weak cybersecurity governance exposed by the PDNS case. At the same time,

emerging allegations of corruption in the procurement of PDNS infrastructure further show that national digital vulnerability is caused not only by technological factors, but also by governance and public-policy issues (Constitution of the Republic of Indonesia, 1945) (National Cyber Security Index, 2024; BSSN, 2024b).

The PDNS incident is evidence that state resilience in the digital era depends heavily on the state's ability to manage data, digital infrastructure, cybersecurity, and technology governance in an integrated manner. This condition shows that a legal-policy approach that remains sectoral is inadequate to confront increasingly complex digital threats. In this context, the concept of digital sovereignty developed by Roberto Baldoni becomes relevant as a paradigm for reconstructing the legal policy of state resilience. According to Baldoni, state sovereignty in the twenty-first century is no longer measured solely by the ability to defend territorial boundaries, but also by the ability to control national data (data sovereignty), critical digital infrastructure, the technology supply chain, artificial intelligence capacity, and competent digital human resources. This concept extends the meaning of sovereignty from the territorial dimension to the digital dimension as a prerequisite for protecting the state and its citizens in the era of digital transformation (Baldoni, 2024).

Although issues of cybersecurity, AI governance, and personal data protection have been extensively studied, most research still treats these issues as standalone fields. Cybersecurity studies generally focus on the technical aspects of incident handling and IT risk management, while legal studies more often discuss personal data protection, AI regulation, or electronic system governance separately. As a result, a gap remains in the literature regarding how Indonesia's legal policy should be reconstructed to integrate cybersecurity, AI governance, and data protection into a single Digital Sovereignty framework as a new foundation for state resilience. Yet empirical experience from the PDNS cyberattack shows that digital threats are not only technological in nature, but also reflect issues of legal policy, institutions, and the state's capacity to protect citizens' constitutional rights.

Based on this situation, this research proceeds from the argument that state resilience in the AI era is no longer determined solely by the ability to defend territorial boundaries, but also by the state's ability to build digital sovereignty through legal policy that is adaptive, integrated, and oriented toward citizen protection. Therefore, this research aims to analyze Indonesia's legal policy on state resilience in protecting citizens through a case study of the PDNS cyberattack, while also reconstructing digital-sovereignty-based legal policy as a paradigm for strengthening state resilience in the era of digital transformation.

The concept of legal policy in Indonesia developed alongside the notion that lawmaking must be directed toward realizing the ideals of law (*rechtsidee*) as contained in the Preamble of the 1945 Constitution of the Republic of Indonesia. Mahfud MD defines legal policy as the legal policy that will be or has been implemented by the state, encompassing the direction of legal development, the formation of laws and regulations, and law-enforcement strategy in order to achieve national goals. From this perspective, law is viewed as an instrument consciously designed by the state to implement constitutional values, including protecting the entire Indonesian nation and its whole homeland as mandated in the Preamble of the 1945 Constitution. Legal policy, therefore, cannot be separated from the state's function as a protective state, which is obligated to guarantee security, order, and public welfare (Mahfud MD, 2009).

The development of Artificial Intelligence (AI) shows that the character of threats to the state has undergone significant transformation. Whereas threats in the past were mostly manifested as military aggression or violations of territorial integrity, in the AI era threats can emerge through automated cyberattacks (AI-enabled cyberattacks), algorithm-based information manipulation, misuse of personal data, and disruption of the digital infrastructure that supports public-service delivery. Such threats are borderless in nature, occur rapidly, and

often involve non-state actors who are difficult to identify or reach through national legal jurisdiction. This condition renders a legal-policy paradigm oriented solely toward the protection of physical territory no longer adequate to guarantee state protection for its citizens (National Institute of Standards and Technology [NIST], 2023; OECD, 2022a).

From this perspective, legal policy must be understood as a dynamic instrument that is responsive to changes in the strategic environment. Satjipto Rahardjo asserts that law, by its very nature, is created for human beings, so that law must be able to adapt to societal developments and must not become trapped in a purely legalistic approach. This thinking is relevant to confronting the development of AI, because technological change occurs far more rapidly than the process of forming regulations. If legal policy fails to anticipate such change, the law will lag behind social reality and lose its ability to provide effective protection (Rahardjo, 2006).

In international security studies, this expanded understanding of security aligns with the thinking of Barry Buzan. According to Buzan, security is no longer understood solely in the military dimension, but also encompasses interrelated political, economic, social, and environmental dimensions. This approach shows that a state's vulnerability can arise not only from armed invasion, but also from disruption of the economic system, weakening political stability, or damage to the information infrastructure that supports government administration. National security in the contemporary era is thus a multidimensional concept that requires the state to build protective capacity against various cross-sectoral threats (Buzan, 1991).

This transformation has become increasingly evident with the rise of cyberspace as a new strategic domain for state, societal, and economic activity. Unlike land, sea, or air territory, which have clear geographical boundaries, cyberspace is cross-jurisdictional (borderless), allowing information, data, and digital attacks to move between states within seconds. This characteristic makes the concept of sovereignty grounded solely in territorial boundaries increasingly difficult to apply in confronting digital threats. As a result, a state's ability to maintain national resilience now depends heavily on the effective management of digital infrastructure, the security of electronic systems, and the protection of data as a strategic state asset (Nye, 2011).

The development of AI has accelerated this transformation by introducing automation capabilities previously unavailable in conventional digital technology. AI enables the collection, processing, and analysis of data to be carried out rapidly at very large scale, while also producing automated decision-making capable of influencing various sectors of life. At the same time, these capabilities are also exploited to increase the complexity of cyber threats through AI-enabled cyberattacks, deepfakes, algorithm-based information manipulation, and the development of adaptive malware capable of autonomously learning system weaknesses. Unlike conventional cyberattacks, AI-based threats possess far greater speed, scalability, and adaptive capability, thereby heightening the risk to national security (OECD, 2022b) (NIST, 2023; ENISA, 2024).

The objects of state protection have likewise undergone transformation. Whereas state resilience was previously associated mainly with protecting territory, natural resources, and the population in a physical sense, in the AI era state protection must also encompass the security of data, critical digital infrastructure, electronic public-service systems, and the technology ecosystem that supports government activity and societal life. Disruptions to national data centers, digital financial systems, communication networks, and digital-based energy infrastructure are no longer regarded as merely technical matters, but as threats to the continuity of state functions and the fulfillment of citizens' constitutional rights. The concept of state resilience in the AI era therefore cannot be separated from the state's ability to maintain the reliability of the digital ecosystem as part of the national strategic interest.

This paradigm shift shows that a reactive security approach is no longer adequate. It is not enough for the state to build response mechanisms after an attack occurs; it must also develop preventive governance through strengthened regulation, cybersecurity capacity building, improved digital literacy, and control over strategic technologies. State resilience in the AI era is thus no longer measured solely by conventional defense strength, but also by the state's ability to build digital resilience capable of guaranteeing the continuity of public services, maintaining public trust, and protecting national interests from increasingly complex digital threats.

The transformation of threats in the Artificial Intelligence era shows that the concept of state sovereignty, long oriented toward control over territorial areas, is no longer fully adequate to address contemporary security challenges. Cross-border data flows, the dominance of global digital platforms, dependence on cloud computing services, and the development of artificial intelligence have created new forms of power relations that cannot always be controlled through national legal instruments based on territorial boundaries. Under these conditions, the state is required not only to defend the integrity of its territory, but also to ensure its ability to control the digital space that forms the foundation of government administration, economic activity, and societal life. This shift has given rise to the conceptual development of digital sovereignty, the state's ability to effectively control strategic digital resources in accordance with national interests and constitutional principles (Nye, 2011) (Baldoni, 2024).

One of the frameworks providing a comprehensive conceptual foundation for digital sovereignty was developed by Roberto Baldoni. According to Baldoni, sovereignty in the twenty-first century can no longer be understood merely as the state's ability to defend territorial boundaries in the classical sense, but must also encompass the ability to control the digital ecosystem that underpins state administration. Within this framework, Digital Sovereignty is built through several key elements, namely data sovereignty, digital infrastructure sovereignty, artificial intelligence sovereignty, technology supply chain sovereignty, and digital human capital. These five elements are interrelated and together form the state's capacity to maintain autonomy in decision-making amid growing dependence on global technology (Baldoni, 2024).

The first element is data sovereignty, namely the state's ability to guarantee that strategic national data is managed, stored, processed, and utilized in accordance with national law and the public interest. In the digital economy, data has developed into a strategic resource possessing economic, political, and security value. Control over data is therefore no longer merely a matter of protecting individual privacy, but also concerns the state's ability to maintain the independence of public policy, national security, and the protection of citizens' constitutional rights (Baldoni, 2024).

The second element is digital infrastructure sovereignty, namely the state's ability to control critical digital infrastructure that supports government administration and public-service delivery. Such infrastructure includes national data centers, telecommunications networks, cloud computing systems, international communication cables, and digital services that form the backbone of government administration. Excessive dependence on digital infrastructure entirely under foreign control has the potential to reduce the state's ability to guarantee the continuity of public services and to increase national-security risk in the event of disruption or geopolitical conflict (Baldoni, 2024).

Baldoni further positions artificial intelligence sovereignty as an increasingly important dimension of digital sovereignty. Control over AI relates not only to the ability to develop artificial-intelligence technology, but also to the state's ability to regulate governance, ensure algorithmic transparency, reduce system bias, and ensure that the use of AI remains consistent. In this context, AI is viewed not merely as a technological innovation, but as a strategic asset

that influences economic competitiveness, national security, and the effectiveness of government administration (Baldoni, 2024).

In addition to the technological aspect, Baldoni also emphasizes the importance of technology supply chain sovereignty. The development of digital technology shows that dependence on hardware, software, semiconductors, and global digital services can become a source of strategic vulnerability for a state. Disruptions to the technology supply chain, whether due to geopolitical conflict or restrictions on international trade, can directly affect a state's ability to carry out government functions and maintain national security. Strengthening national capacity in the development, diversification, and security of the technology supply chain is therefore an important part of the Digital Sovereignty strategy (Baldoni, 2024).

Alongside the aspects of technology and infrastructure, digital sovereignty also requires the availability of adequate digital human capital. States need human resources with competencies in cybersecurity, artificial intelligence, data analysis, software engineering, and digital governance in order to manage and sustainably develop the national digital ecosystem. Without adequate human-resource capacity, investment in digital infrastructure and regulation will not produce an optimal level of digital sovereignty (Baldoni, 2024).

For Indonesia, the concept of Digital Sovereignty became increasingly relevant following the cyberattack on the Temporary National Data Center (PDNS) in 2024. The incident showed that national digital-security issues are caused not solely by technological weaknesses, but also by legal governance, institutions, inter-agency coordination, and national digital-infrastructure management strategy. The challenges facing Indonesia therefore cannot be adequately addressed through sectoral regulation alone, but require legal policy capable of integrating data management, cybersecurity, AI governance, digital-infrastructure strengthening, and national capacity building within a single, integrated policy framework. In this context, Digital Sovereignty is understood not merely as a technological concept, but as a legal-policy paradigm that provides direction for the reconstruction of state-resilience policy in the AI era (Baldoni, 2024).

Accordingly, this study asks: first, how does Indonesia's state resilience legal policy protect citizens in the AI era when examined through the PDNS cyberattack; and second, how should a digital-sovereignty-based legal policy be reconstructed to strengthen state resilience and citizen protection? The study aims to evaluate the existing legal architecture and formulate an integrated reconstruction grounded in data sovereignty, digital infrastructure sovereignty, AI sovereignty, technology supply chain sovereignty, and digital human capital.

METHODS

This research employs the normative legal research method, examining legal norms, legal principles, doctrines, and developments in national and international law relating to state resilience in the era of digital transformation and Artificial Intelligence. The approaches used include: (1) the statute approach, analyzing the 1945 Constitution of the Republic of Indonesia, Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, Law Number 27 of 2022 on Personal Data Protection, and various national policies in the fields of cybersecurity and electronic-system governance; (2) the conceptual approach, examining the concept of Digital Sovereignty developed by Roberto Baldoni, the theory of legal policy put forward by Mahfud MD, Lawrence M. Friedman's legal-system theory, and Satjipto Rahardjo's progressive-law theory; and (3) the case approach, through an analysis of the 2024 cyberattack on Indonesia's Temporary National Data Center (PDNS) as the primary case study for identifying weaknesses in the national legal framework and cybersecurity governance.

The legal materials used consist of primary legal materials, in the form of laws and regulations, government policy documents, and international legal instruments; secondary

legal materials, in the form of books, reputable scholarly journal articles, reports of international organizations, and prior research; and tertiary legal materials, in the form of legal dictionaries, encyclopedias, and other relevant reference sources. All legal materials were analyzed qualitatively using systematic, conceptual, and comparative interpretation methods to develop legal arguments regarding the reconstruction of Digital-Sovereignty-based legal policy in strengthening state resilience while enhancing the constitutional protection of citizens in the AI era.

RESULTS AND DISCUSSION

Indonesia's State Resilience Legal Policy and the PDNS Cyberattack

The development of Artificial Intelligence (AI) and digital transformation has fundamentally changed the character of threats to the state. Whereas legal policy on state resilience was previously oriented mainly toward protection against physical and territorial threats, in the digital era the state is also required to protect cyberspace, strategic data, digital infrastructure, and electronic systems that support government administration and public services. In this context, legal policy can no longer be understood merely as policy for forming laws and regulations, but rather as the direction of state policy in building a legal system capable of guaranteeing the protection of citizens from digital threats that are cross-jurisdictional, dynamic, and rapidly evolving (Mahfud MD, 2022; Rahardjo, 2014).

Normatively, Indonesia already possesses a number of legal instruments that form the basis for digital governance. Through the Preamble of the 1945 Constitution of the Republic of Indonesia, the Constitution affirms that one purpose of establishing the state is to protect the entire Indonesian nation and its whole homeland. This mandate shows that state protection is directed not only against physical threats, but also against new forms of threats emerging in digital space. In addition, the administration of electronic systems, electronic transactions, personal data protection, and digital government governance has been regulated through various laws and regulations, including Law Number 11 of 2008 on Electronic Information and Transactions as last amended by Law Number 1 of 2024, Law Number 27 of 2022 on Personal Data Protection, Government Regulation Number 71 of 2019 on the Administration of Electronic Systems and Transactions, and the Electronic-Based Government System (SPBE) policy. Nevertheless, these various regulations have not yet fully formed a comprehensive legal policy on digital resilience. Existing regulations still tend to develop sectorally, focusing on specific aspects such as electronic transactions, personal data protection, or electronic system administration, without building a single legal framework that explicitly links data governance, cybersecurity, artificial intelligence, digital infrastructure, and national capacity building as a unified state-resilience strategy.

These limitations in legal design became clearly apparent in the 2024 ransomware attack on the Temporary National Data Center (PDNS). This incident cannot be understood merely as a cybersecurity failure, but rather as an indicator of weak legal-policy design in guaranteeing the continuity of state functions in digital space. The disruption of public services, delays in system recovery, and service disruptions at a number of government agencies show that the problem Indonesia faces is not merely technical, but also one of governance, inter-agency coordination, and the unpreparedness of legal design in confronting digital threats with direct impacts on state functions. From this perspective, PDNS stands as concrete evidence that state resilience in the digital era cannot be built solely through the provision of technological infrastructure, but also requires a legal framework that guarantees resilience, accountability, and the continuity of public services (BSSN, 2024a).

Analyzed through the perspective of digital sovereignty developed by Roberto Baldoni, this issue can be examined more sharply through several dimensions. The first dimension is data sovereignty. Under this concept, the state must have the ability to control the management,

storage, processing, and utilization of strategic data in accordance with the national interest. However, Indonesia's legal policy still tends to treat personal data protection as a matter of individual privacy rather than as an instrument of state resilience. Yet in the context of digital government, data is not merely an object of rights protection, but also a strategic asset that determines the state's ability to maintain the continuity of administrative functions, public services, and data-driven decision-making. The PDNS incident showed that when data governance is not equipped with adequate backup mechanisms, rapid recovery, and protection of strategic data, cyber disruptions can transform into disruptions of the state's own capacity. The core problem, therefore, is not merely insufficient protection of personal data, but the absence of a legal policy that regards data as part of national resilience infrastructure (Baldoni, 2024).

The second dimension is digital infrastructure sovereignty. Digital infrastructure is the primary foundation for the administration of electronic government and public services in the digital era. The state must therefore be able to guarantee the security, continuity, and reliability of such infrastructure. In the PDNS case, it became apparent that the data center, which should have served as the main pillar of national digital transformation, instead proved vulnerable as a single point of failure. This condition shows that the development of digital infrastructure has not been accompanied by adequate resilience design, such as system redundancy, disaster-recovery mechanisms, and integrated risk governance. In terms of legal policy, this shows that existing regulation still focuses on the administration of electronic systems but has not comprehensively regulated obligations relating to resilience, recovery readiness, and protection of national digital infrastructure as part of the state's strategic functions. As a result, the state still tends to view digital infrastructure as an administrative tool rather than as a resilience object requiring higher legal standards (Baldoni, 2024).

The third dimension is Artificial Intelligence sovereignty. In the Indonesian context, AI sovereignty cannot yet be understood as the state's capacity to fully control artificial intelligence technology. The challenges facing Indonesia lie not only in the absence of comprehensive AI regulation, but also in the yet-to-be-established national capacity to develop AI models, high-performance computing infrastructure, hardware, semiconductors, software, and the innovation ecosystem that underpins AI development. This condition places Indonesia predominantly in the position of a technology user, with most such technologies developed by global actors, thereby limiting the state's scope of control over these strategic technologies.

The cyberattack on Indonesia's Temporary National Data Center (PDNS) in 2024 does not directly indicate the use of Artificial Intelligence as an instrument of attack. The attack was carried out through Brain Cipher ransomware, which exploited weaknesses in cybersecurity governance and data backup mechanisms. Nevertheless, the incident revealed fundamental vulnerabilities in Indonesia's digital governance that could be further exploited as malware, ransomware, and cyber penetration techniques increasingly become weaponized with Artificial Intelligence capabilities. Accordingly, the PDNS incident illustrates a baseline vulnerability, while AI functions as a threat multiplier capable of amplifying the impact of cyber threats to the state.

In the Indonesian context, relatively concrete AI-related threats extend beyond deepfakes, disinformation, or automated decision-making, to include the use of AI to enhance malware's capacity to attack operational technology (OT). Such targets include Industrial Control Systems (ICS), Internet of Things (IoT) devices, energy systems, digital health systems, transportation systems, and sensor- and drone-based agricultural technologies. Attacks on these systems have the potential not only to cause data breaches, but also to produce physical consequences that disrupt public services, economic activity, and even public safety. Indonesia's legal policy should therefore be directed not only toward establishing regulations on AI use, but also toward building national capacity to reduce dependence on foreign

technology, strengthening domestic AI development capabilities, and constructing governance frameworks capable of anticipating the risks that AI poses to state resilience.

The development of hyperscale data centers in Indonesia does indeed reflect an increase in national digital infrastructure capacity. However, the physical presence of data centers within Indonesian territory does not automatically produce digital sovereignty. Digital sovereignty is determined not only by the location of data storage, but also by the state's capacity to control system architecture, cloud computing services, AI models, software, security mechanisms, administrative access rights, and the technology supply chains that support the operation of such data centers. A distinction must therefore be drawn between data localization, infrastructure availability, and substantive digital sovereignty, so that digital infrastructure development is not narrowly understood as the sole indicator of state sovereignty.

The fourth dimension is technology supply chain sovereignty. State resilience in the digital era is determined not only by the capacity to manage data and infrastructure, but also by the degree of independence from technology supply chains. State resilience in the digital era does not require the capacity to independently produce all hardware, software, semiconductors, or AI technologies. Given the conditions of global technological interdependence, a more realistic objective is to build strategic autonomy — that is, the state's capacity to reduce critical dependencies through supplier diversification, the adoption of interoperable standards, strengthened audit rights over technologies used by government, the development of vendor exit strategies, and enhanced technology transfer and national industrial capacity. Technology supply chain sovereignty is thus understood as the state's capacity to sustain strategic functions despite geopolitical disruptions, technology export restrictions, or service termination by foreign providers.

The fifth dimension is digital human capital sovereignty. Digital resilience depends not only on technology, but also on the quality of human resources and the institutional capacity that manages it. The development of cybersecurity, data governance, electronic-system oversight, and AI risk mitigation requires personnel with high competence and effective inter-agency coordination. However, Indonesia's legal policy has not systematically built institutional and digital human-resource capacity through integrated legal design. As a result, the strengthening of digital infrastructure is often not accompanied by strengthening of the human capacity that operates it. In the PDNS case, this problem was reflected in weak inter-agency coordination and limited rapid-response capacity when disruptions occurred. This shows that digital resilience cannot be measured merely by the existence of systems or technological devices, but also by the extent to which the state is able to prepare human resources, governance, and institutional structures that support the sustainable management of digital risk (Baldoni, 2024).

Based on these five dimensions, it is evident that Indonesia's legal policy remains oriented toward sectoral regulation of electronic systems, data protection, and cybersecurity. This legal policy has not developed into a legal framework that positions digital sovereignty as the foundation of state resilience in the Artificial Intelligence era. As a result, the various legal instruments already in place have not been able to fully build the state's capacity to protect its citizens from cross-jurisdictional digital threats. The main problem, therefore, lies not only in the absence of certain rules, but in the fact that a legal-policy paradigm regarding digital space as an integral part of state resilience has not yet been established. From this perspective, the protection of citizens can no longer be adequately understood merely as the protection of personal data or the administration of electronic systems, but must be understood as the state's effort to ensure that the basic functions of government, public services, and national security continue to operate amid the increasing complexity of digital threats.

Reconstruction of Digital Sovereignty Based Legal Policy

The analysis in the preceding subsection shows that Indonesia's legal policy remains oriented toward a sectoral approach in regulating digital transformation. Regulations on electronic systems, personal data protection, cybersecurity, and electronic-based government administration already exist, but have developed separately according to their respective regulatory sectors. As a result, positive law has not yet formed a national policy framework capable of integrating data protection, digital-infrastructure security, artificial-intelligence governance, and institutional capacity building into a unified state-resilience strategy. This condition shows that Indonesia's main challenge lies not in the absence of regulation, but in the absence of a legal-policy paradigm that makes digital sovereignty the primary orientation of national legal development (Mahfud MD, 2022).

Based on this perspective, the reconstruction of Indonesia's legal policy needs to be directed toward five main dimensions. First, strengthening data sovereignty. Legal policy must regard data — particularly the state's strategic data and citizens' personal data — as a national strategic asset. Regulation of data protection should therefore not stop merely at fulfilling the rights of data subjects as regulated under Law Number 27 of 2022 on Personal Data Protection, but must also encompass the obligation of government electronic-system operators to guarantee data redundancy, national backups, disaster recovery centers, and business-continuity standards for public services in the event of a cyber incident. In this way, data protection would be oriented not only toward privacy, but also toward the continuity of state functions (OECD, 2019).

Second, strengthening digital infrastructure sovereignty. The experience of the attack on PDNS shows that digital infrastructure is a vital state object that must receive legal protection equivalent to other strategic infrastructure. National legal policy needs to develop minimum security standards for government data centers, periodic cybersecurity audit mechanisms, mandatory security certification, and regulation of national coordination in handling cyber incidents. This strengthening also needs to be accompanied by the arrangement of inter-agency authority to prevent fragmentation in the management of national digital infrastructure (Baldoni, 2024) (NIST, 2024). Third, establishing a legal framework for Artificial Intelligence. To date, Indonesia has no comprehensive regulation governing the use of AI in the public sector or in strategic sectors. Yet AI not only presents opportunities for innovation, but also increases risks in the form of automated cyberattacks, information manipulation through deepfakes, algorithmic discrimination, and misuse of automated decision-making. Indonesia's legal policy therefore needs to move from an ethics-based approach toward binding legal regulation (hard law) by establishing security standards, mandatory algorithm audits, transparency requirements for high-risk AI systems, allocation of legal responsibility, and oversight mechanisms for the use of AI by both government and the private sector.

Fourth, strengthening technology supply chain sovereignty. High dependence on foreign hardware, software, and cloud computing services has the potential to create strategic vulnerabilities for the state. National legal policy needs to develop policies that encourage diversification of technology suppliers, strengthening of the national digital industry, and mandatory risk assessment for the use of foreign technology in strategic sectors. In this way, government procurement policy would no longer consider only economic efficiency, but also aspects of national security and the continuity of public services. Fifth, strengthening institutional capacity and digital human resources. Digital sovereignty cannot possibly be realized through regulation alone. The effectiveness of law depends heavily on the capacity of the institutions that implement it. Legal policy must therefore be directed toward strengthening inter-agency coordination, improving the competence of state personnel in cybersecurity and AI, and building accountable digital-governance mechanisms that are adaptive to technological

developments. This institutional strengthening is an essential condition for legal norms to be effectively implemented.

These five dimensions essentially show that the reconstruction of legal policy in the AI era requires a shift in orientation from a sectoral regulatory approach toward an integrative strategic approach. Legal policy can no longer function merely as the basis for forming laws and regulations, but must also become an instrument for building the state's capacity to control digital space as part of the exercise of its constitutional function to protect the entire Indonesian nation. In other words, the success of legal policy in the AI era is measured not merely by the number of regulations formed, but by the extent to which those regulations strengthen the state's resilience against digital threats while guaranteeing the protection of citizens' constitutional rights.

This reconstruction also affirms that digital sovereignty is not merely a technological concept, but a new paradigm of legal policy for state resilience. This paradigm integrates the dimensions of law, technology, security, and human rights into a single, coherent policy framework. In the Indonesian context, applying this paradigm is important to ensure that digital transformation not only produces administrative efficiency in government, but also strengthens the state's ability to carry out its function of protecting citizens as mandated by the 1945 Constitution of the Republic of Indonesia.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

Indonesia's legal policy on state resilience in protecting citizens in the Artificial Intelligence era, examined through the case study of the cyberattack on the Temporary National Data Center (PDNS), has not yet been fully capable of addressing the challenges of digital transformation. Although Indonesia already has various regulations, such as the Electronic Information and Transactions Law, the Personal Data Protection Law, and various cybersecurity policies and the Electronic-Based Government System, their regulation remains sectoral in nature and has not been integrated into a single legal-policy framework for state resilience. The 2024 cyberattack on PDNS revealed weaknesses in governance, institutional coordination, digital-infrastructure security, and the protection of citizens' constitutional rights when disruptions occur to digital public services.

The reconstruction of legal policy based on Digital Sovereignty is required as a new paradigm for strengthening state resilience in the era of Artificial Intelligence. However, the implementation of this paradigm must be adapted to Indonesia's factual conditions, which still face dependence on AI technology, computing infrastructure, and global technology supply chains. Accordingly, digital sovereignty is not to be understood as absolute technological independence, but rather as the state's capacity to build strategic autonomy, reduce critical dependencies, ensure the continuity of governmental functions, and protect citizens from increasingly complex digital threats.

Limitations

This research is doctrinal and uses the PDNS incident as a legal-policy case study. It does not conduct digital forensic verification, measure the operational maturity of individual institutions, or evaluate citizen experiences through primary empirical data. Publicly available institutional reports may also provide an incomplete account of sensitive security events. The proposed reconstruction therefore requires empirical testing, periodic regulatory review, and comparison with subsequent incidents and technological developments.

Recommendations

The government needs to formulate a more integrated legal policy - specifically, a national policy that integrates the regulation of cybersecurity, personal data protection, Artificial Intelligence governance, and digital-infrastructure development within a digital-sovereignty framework, thereby creating a more unified system of state resilience.

The government, together with legislators, needs to develop an adaptive AI legal framework while simultaneously strengthening national capacity through the development of digital talent, AI research, enhanced operational technology security, strengthened governance of national data centers, and strategies to reduce dependence on foreign strategic technologies, in order to realize sustainable digital sovereignty.

Author Contributions

All authors contributed to the conceptualization, legal analysis, case-study interpretation, development of the digital-sovereignty reconstruction, manuscript preparation, critical revision, and final approval of the article.

REFERENCES

- Asshiddiqie, J. (2010). *Konstitusi dan konstiusionalisme Indonesia*. Sinar Grafika.
- Baldoni, R. (2024). *Charting digital sovereignty: A survival playbook*. Springer Nature Switzerland.
- Bodin, J. (1992). *On sovereignty*. Cambridge University Press.
- Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-Cold War era* (2nd ed.). Lynne Rienner Publishers.
- Constitution of the Republic of Indonesia. (1945).
- Cyber Security Agency of Singapore. (2024). *Singapore cyber landscape 2024*.
- European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. Publications Office of the European Union.
- Financial and Development Supervisory Agency. (2024). *Evaluasi tata kelola Pusat Data Nasional*. BPKP.
- Government Regulation Number 71 of 2019 concerning the operation of electronic systems and transactions. (2019).
- Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.
- Kusumaatmadja, M. (2006). *Konsep-konsep hukum dalam pembangunan*. Alumni.
- Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning electronic information and transactions. (2024).
- Law Number 27 of 2022 concerning personal data protection. (2022).
- Mahfud MD. (2009). *Politik hukum di Indonesia*. Rajawali Pers.
- Mahfud MD. (2022). *Politik hukum di Indonesia*. Rajawali Pers.
- Ministry of Communication and Informatics of the Republic of Indonesia. (2024a, June). *Konferensi pers penanganan gangguan Pusat Data Nasional Sementara*.
- Ministry of Communication and Informatics of the Republic of Indonesia. (2024b, June 24). *Siaran pers Nomor 373/HM/KOMINFO/06/2024 tentang perkembangan penanganan gangguan Pusat Data Nasional Sementara*.
- National Cyber and Crypto Agency. (2024a). *Laporan evaluasi insiden Pusat Data Nasional Sementara tahun 2024*.
- National Cyber and Crypto Agency. (2024b). *Laporan tahunan BSSN 2024*.
- National Cyber Security Index. (2024). *National cyber security index 2024*. e-Governance Academy Foundation.
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. U.S. Department of Commerce.

- National Institute of Standards and Technology. (2024). Cybersecurity framework (CSF) 2.0. U.S. Department of Commerce.
- Nye, J. S., Jr. (2011). The future of power. PublicAffairs.
- Organisation for Economic Co-operation and Development. (2019). Data governance in the public sector. OECD Publishing.
- Organisation for Economic Co-operation and Development. (2022a). OECD framework for the classification of AI systems. OECD Publishing.
- Organisation for Economic Co-operation and Development. (2022b). Classifying AI systems (OECD Artificial Intelligence Papers No. 8). OECD Publishing.
- Organisation for Economic Co-operation and Development. (2022c). Data governance in the digital age. OECD Publishing.
- Rahardjo, S. (2006). Ilmu hukum. Citra Aditya Bakti.
- Rahardjo, S. (2014). Ilmu hukum. Citra Aditya Bakti.
- UNESCO. (2021). Recommendation on the ethics of artificial intelligence.
- World Economic Forum. (2025). Global cybersecurity outlook 2025.