Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. Juni 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

FAILURE TO REALIZE CONSTITUTIONAL GOALS IN CYBERSPACE: A CONSTITUTIONAL LAW REVIEW OF THE NATIONAL DATA CENTER (PDN) DATA BREACH INCIDENT

Roul Alvaro Prasetyo[1a*], Eny Kusdarini[2b], Muhammad Kamil Ridha[3c]

[13]Master of Pancasila and Civic Education, Faculty of Social Sciences and Political Sciences, Universitas Negeri Yogyakarta, Yogyakarta, Indonesia
[2]Law, Faculty of Law, Universitas Negeri Yogyakarta, Yogyakarta, Indonesia

[a]roulalvaro.2025@student.uny.ac.id
[b]eny_kusdarini@uny.ac.id
[c]muhammadkamil.2025@student.uny.ac.id

(*) Corresponding Author
[a]roulalvaro.2025@student.uny.ac.id

ARTICLE HISTORY
Received : 20-01-2026
Revised : 07-02-2026
Accepted : 25-05-2026

KEYWORDS
Digital Constitutionalism;
National Data Center;
Constitutional Supremacy;
Right to Privacy;
State Responsibility;

ABSTRACT
The digital transformation of government services through the National Data Center (PDN) aims to realize effective and responsive public administration. However, a massive ransomware attack on the PDN in mid-2024 revealed a fatal vulnerability in Indonesia's cybersecurity governance architecture, paralyzing essential services and harming millions of citizens. This study analyzes the state's negligence in managing the PDN from a Constitutional Law perspective, evaluating it through the fulfillment of the functions, objectives, and supremacy of the constitution. This research employs a normative legal method using statutory and conceptual approaches. The findings indicate that the data breach at the PDN is not merely a technical IT failure, but a representation of a fundamental constitutional failure. First, the state failed to realize the constitutional objective of protecting the Indonesian nation as mandated by the Fourth Paragraph of the 1945 Constitution, and failed to guarantee the basic right to personal data protection enshrined in Article 28G Paragraph (1). Second, overlapping authority and a lack of clear institutional accountability directly contribute to the violation of citizens' constitutional rights, demonstrating the failure of the constitution's function in limiting power. Third, the government's delay in establishing an independent Personal Data Protection Supervisory Authority, as mandated by Law No. 27 of 2022, constitutes an anomaly of constitutional supremacy, where the rule of law is defeated by bureaucratic sluggishness. This study recommends the immediate establishment of an independent supervisory agency, optimization of legislative oversight, and strict legal accountability for state institutions.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. Juni 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

INTRODUCTION

The development of information and communication technology in the second decade of the 21st century has created a fundamental disruption in various aspects of national and state life. The administration of government, which historically relied on physical bureaucracy and paper-based administration, is now rapidly transforming into an electronic government administration system or e-government (Asshiddiqie, 2005). This transformation is not merely a pragmatic choice to follow global trends, but a necessity for a modern welfare state to create good governance that is efficient, transparent, and responsive to public needs (Mahfud, 2006). In Indonesia, the realization of this digitalization commitment is accelerated thru a national-scale data integration policy facilitated by the presence of the National Data Center (Pusat Data Nasional, PDN). The presence of the National Data Center (PDN) is conceptually designed as a vital state information infrastructure aimed at consolidating, integrating, and securing thousands of data centers owned by ministries, agencies, and local governments that have so far been fragmented, inefficient, and vulnerable to hacking (Dayang et al., 2025).

However, the centralization and integration of data on such a massive scale bring a logical consequence that is no less terrifying, namely the creation of a vulnerability (single point of failure) (Rosadi & Pratama, 2018). Public expectations regarding the security of the country's digital infrastructure collapsed instantly when a ransomware cyber attack (Brain Cipher variant) struck the National Data Center (PDN) server in Surabaya in mid-2024. This incident marked a historical moment as one of the worst cybersecurity disasters in Indonesia. The paralysis of the system due to data encryption by hackers not only disabled hundreds of essential public services in 282 ministries and agencies, including the total paralysis of the immigration system at various international airports, the new student enrollment system (PPDB), and the business licensing system, but also strongly suggests the exfiltration or theft of personal data belonging to millions of Indonesian citizens stored within it (Fauzi & Shandy, 2022).

From the perspective of Constitutional Law, the failure to protect this national strategic infrastructure cannot be reduced merely to a technical problem of Information Technology (IT) or just a system failure in cyberspace. There is a much more fundamental and philosophical constitutional issue, namely the state's failure to fully carry out its constitutional mandate. The 1945 Constitution of the Republic of Indonesia, as a staatsfundamentalnorm (fundamental state norm), in the Fourth Paragraph of the Preamble, asserts that the main purpose of establishing the Government of the State of Indonesia is to "protect the entire Indonesian nation and all of Indonesia's bloodshed" (Takariawan & Putri, 2018). In contemporary constitutional law discourse, the phrase "protecting the entire nation" can no longer be narrowly interpreted as merely military protection against physical threats in land, sea, and air. Such protection must be extended mutatis mutandis to efforts to protect sovereignty in cyberspace (cyber sovereignty) (Mardiana & Arsanti, 2023).

Furthermore, the Indonesian constitution provides a very explicit guaranty of human rights protection thru Article 28G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states: "Everyone has the right to personal protection, family, honor, dignity, and property under their control..."(Undang-Undang Dasar Negara Republik Indonesia Tahun 1945., n.d.). In the current digital era, electronic identities, medical records, biometric data, and tax history managed by the state thru PDN fall under the "personal self" mentioned in that article (Christine & Kansil, 2022). Therefore, the state's failure to protect data in the PDN is essentially a failure to fulfilll the constitutional rights of its citizens.

The significant gap between what is idealized and mandated by the constitution and the empirical reality of the state's cybersecurity system's powerlessness creates an urgency to examine this phenomenon thru the study of Digital Constitutionalism (Ridwan, 2014). Celeste (2019) explains that digital constitutionalism is a theoretical and practical effort to ensure that the core values of classical constitutionalism, such as the limitation of power, the guaranty of human rights, and the supremacy of law that have been upheld in the real world, can be translated and enforced absolutely in the governance of the digital space. In the PDN incident, the principles of constitutionalism were seen to have failed to be operationalized by the state organizers .

This failure became even more apparent in the dysfunction of institutional accountability that occurred post-incident. The Ministry of Communication and Information Technology (Kominfo) as the policy maker and manager

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. Juni 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

of the National Data Center (PDN), along with the National Cyber and Crypto Agency (BSSN) as the authority in the field of national cyber security, instead showcased the phenomenon of shifting the blame in the public space (Kusuma, 2024). The overlapping regulatory authorities undermine the main function of the constitution, which was originally established to clearly distribute power so that each state organ can be held legally or politically accountable in a proportional manner (Huda, 2021). This paradoxical situation becomes even more complex with the fact that Indonesia actually has a strong legal instrument, namely Law Number 27 of 2022 on Personal Data Protection (PDP Law) (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi., n.d.)

Research related to cyberspace governance in Indonesia has been extensively conducted. For example, Yuniarti (2019) focused on the legal protection of personal data in general, while Rosadi & Pratama (2018) explored privacy protection in the context of the digital economy. Furthermore, Mardiana & Arsanti (2023) analyzed the urgency of data protection thru a broader perspective of human rights. Additionally, Saleh (2021) examines the constitutionality of information and electronic transaction laws, particularly in relation to conflict resolution on social media. However, these previous studies primarily focused on the general regulatory framework, aspects of the digital economy, or social media platforms, without specifically addressing the structural failures in vital information infrastructure directly managed by the state. This research distinguishes itself by using a pure Constitutional Law approach, specifically evaluating the National Data Center (NDC) data breach incident thru the lens of function, purpose, and constitutional supremacy. By focusing on the state's failure to fulfilll the constitutional mandate to 'protect the entire nation' in the digital realm, this research fills a significant gap in the existing literature on institutional accountability in cyberspace.

METHOD

The approach applied in this study is normative legal research (doctrinal research). This type of research emphasizes the process of tracing and systematically examining the rules, basic principles, and relevant legal doctrines. This step is taken as an essential analytical foundation to formulate answers while simultaneously resolving the legal issues that are the focus of this study (Marzuki, 2017). The use of normative legal methods is based on the ontological characteristics of this research, which does not aim to test statistical hypotheses or social phenomena in the field, but rather to evaluate the consistency of the state's cyber infrastructure governance with the fundamental norms of the constitution (the 1945 Constitution of the Republic of Indonesia) and the sectoral laws beneath it. To comprehensively analyze the constitutional issues surrounding the National Data Center (Pusat Data Nasional, PDN) leak incident, this research employs two main approaches. First, the legislative approach, which is carried out by reviewing all laws and regulations related to the legal issues being addressed. This approach is used to map the hierarchy of regulations and the authority of state institutions in cybersecurity governance. Second, the conceptual approach, which is based on the evolving views and doctrines within legal science (Marzuki, 2017). This conceptual approach is specifically used to explore the philosophical meaning of the doctrine of "Digital Constitutionalism" (Celeste, 2019), the expanded meaning of "personal self" as the right to privacy (Christine & Kansil, 2022), and the limitations of state responsibility according to Constitutional Law literature.

To bridge the abstract constitutional norms with the concrete facts of the National Data Center (PDC) data breach case, this research applies teleological (sociological) and systematic interpretation techniques. Teleological interpretation is used to understand the fundamental purpose of the mandate 'to protect the entire nation' in the Preamble of the 1945 Constitution so that it remains relevant in the context of current digital sovereignty threats. Meanwhile, a systematic interpretation is used to connect Article 28G paragraph (1) regarding the protection of personal data with the state's obligation in Article 1 paragraph (3) about the principle of a state of law.

The legal materials explored and examined in this research are classified into three types. Primary legal materials, which include the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 on Personal Data Protection (PDP Law), and Presidential Regulation Number 82 of 2022 on the Protection of Vital Information Infrastructure (Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 Tentang Perlindungan Infrastruktur Informasi Vital, n.d.). Secondary legal materials, which provide explanations regarding primary legal materials, are obtained from reference books on Constitutional Law as well as articles in reputable national and international

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. Juni 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

scientific journals related to cybersecurity law and privacy protection. Next, tertiary legal materials in the form of legal dictionaries are used to provide guidance and explanations for various legal and technical terms that are not yet understood.

The technique for collecting legal materials is carried out thru library research or document studies by inventorying and classifying regulations, literature, and official government documents related to the PDN incident. After all legal materials have been collected, the analysis technique used is descriptive analysis. The reasoning process applied is deductive reasoning thru the syllogism method. Specifically, this syllogism is constructed by placing the constitutional obligation of the state to protect citizens' personal data as part of human rights based on Article 28G paragraph (1) of the 1945 Constitution and the fundamental mandate of the state as the major premise. Then, the empirical fact of a massive failure in the National Data Center (PDN) that resulted in the leakage of personal data of millions of citizens due to the negligence of state authorities in managing cyber infrastructure is positioned as the minor premise. From the connection of these two premises, a legal conclusion is drawn that the state has committed constitutional negligence because it failed to fulfilll its mandate to protect citizens' rights in cyberspace.

RESULT AND DISCUSSION

Data Protection as an Extension of Constitutional Rights: An Evaluation of State Objectives

The construction of the rule of law in Indonesia is not designed as a "night watchman state" (nachtwakersstaat) that only serves to maintain public order. On the contrary, Indonesia adheres to the concept of a welfare state, where the state is burdened with the active obligation to take affirmative actions to achieve social welfare and protection for all its citizens (Takariawan & Putri, 2018). This fundamental goal is stated in the Fourth Paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia, which declares that the formation of the Indonesian State Government aims to "protect the entire Indonesian nation and all Indonesian bloodshed, promote the general welfare, educate the nation's life, and participate in the establishment of world order."

In reading constitutional doctrine, the interpretation of the text of the basic law must not be carried out rigidly and statically. Modern constitutional law is required to possess flexibility and adaptability in responding to technological disruptions thru a progressive interpretative approach. According to Asshiddiqie (2021), advancements in information technology have given rise to a new spatial entity, namely cyberspace, which now holds an equal status to a country's physical territory. Therefore, the constitutional phrase "to protect the entire nation and all of Indonesia's blood and soil" absolutely has an expanded meaning. The state is no longer only obligated to deploy security forces to guard the territorial boundaries of land, sea, and air, but also has an imperative mandate to build a robust immunity and defense system to protect data sovereignty in cyberspace (cyber sovereignty).

More than just a national security discourse, data protection in cyberspace is directly related to the fulfillment of human rights. The Indonesian Constitution provides an explicit guaranty of protection for its citizens' privacy rights thru Article 28G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states: "Everyone shall have the right to personal protection, family, honor, dignity, and property under their control...". Digital identities that include the Population Identification Number (NIK), medical records, banking records, biometric data, and academic history, all of which are forced by the system to be integrated into the National Data Center (PDN), are not merely a series of algorithms or binary numbers. These data are a concrete manifestation and an extension of the "personal self" guarantyd by the constitution (Christine & Kansil, 2022). When someone's personal data is exposed, their honor, dignity, and even the safety of their property and life are in real danger.

Based on that theoretical foundation, the hacking incident that crippled PDN in mid-2024 became a dark precedent that proved the state's absence when its citizens needed protection the most. The ransomware attack that successfully encrypted PDN's main server, unfortunately lacking a reliable disaster recovery plan and backup server, proves that the government's digital infrastructure is very fragile (Saleh, 2021). From the perspective of constitutional law, the paralysis of the immigration system, the stagnation of healthcare services, and the leakage of population data are not merely technical administrative malfunctions. This is a form of betrayal of the social contract that has been agreed upon between the state and the people.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. Juni 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

In public law, when citizens comply with the law's mandate to submit their personal data to the state, such as in the process of obtaining an electronic ID card, passport, or national health insurance registration, a reciprocal obligation arises for the state to maintain the confidentiality, integrity, and availability of that data (Mardiana & Arsanti, 2023). The concept of state responsibility in Constitutional Law and international human rights instruments requires that the state must not act passively when violations of its citizens' rights occur. Negligence in providing multi-factor defense security standards at vital facilities such as PDN is a form of human rights violation committed by the state thru negligence.

Mahfud (2006) emphasized that the government's legal politics must be consistent with the goals of its constitution. The construction of the National Data Center, which was initially claimed to be the government's legal policy to improve public welfare thru e-government efficiency, has instead turned into a double-edged sword that threatens citizen security due to bureaucratic negligence in risk mitigation. The failure of the managing agency to implement standard cyber risk mitigation cannot be justified by the sophistication of hackers. The state's obligation in human rights is the obligation of conduct (the duty to strive to the utmost with the highest standards) and the obligation of result (the duty to ensure the outcome of safety for the community) (Saleh, 2021). Thus, it can be firmly concluded that the breach of the National Data Center represents a failure of the state in realizing its constitutional objectives. The state is deemed flawed in translating the mandate of independence to protect "the entire nation" into its digital security. As long as the cybersecurity ecosystem is not rectified using human rights standards, the government's digital transformation initiatives will only become new spaces for exploitation that continuously violate the dignity and data sovereignty of Indonesian citizens (Surbakti, 2024).

Institutional Accountability and the Illusion of Power Limitation: Measuring the Function of the Constitution

The existence of a constitution in a democratic rule of law state is not only intended as a founding document of the state but also has a very vital instrumental function. The essential function of the constitution is to limit state power (limitations of power) so that rulers do not act arbitrarily (absolutism), and to distribute that power into state organs thru checks and balances mechanisms (Huda, 2021). The fundamental philosophy of this limitation of power is that each state institution has a specific scope of work, clear authority, and most importantly, can be held fully accountable (accountability) in case of abuse of power or negligence in carrying out its duties. In the tradition of Constitutional Law and Administrative Law, there is a universal principle known as geen bevoegdheid zonder verantwoordelijkheid, which means "no authority without accountability". Every delegation of power from the constitution to the executive organ must always be followed by a proportional accountability mechanism. However, in the governance of cyberspace and digital information in Indonesia, this constitutional function has experienced severe distortions and anomalies due to overlapping regulations and unclear institutional designs.

The institutional dynamics following the incident, as previously outlined, demonstrate a dysfunction in Indonesia's cyber power architecture. The phenomenon of shifting the blame is not merely a coordination issue, but a manifestation of unclear distribution of authority in the relevant regulations. From the perspective of Constitutional Law, this ambiguity violates the principle of 'geen bevoegdheid zonder verantwoordelijkheid' (no authority without accountability). This structural chaos proves that the division of power in Indonesia's cyber realm is not designed to create accountability, but rather to create a "grey area" that allows state organizers to evade legal traps and moral sanctions (Alhakim & Tantimin, 2024). The Constitution demands measurable accountability for every failure that harms the people (Saleh, 2021). When a massive systemic failure occurs that leaks the data of millions of citizens, the public has a constitutional right to demand institutional accountability as well as individual accountability from the relevant public officials. Unfortunately, due to the absence of a rigid division of responsibilities, the state bureaucracy actually exploits this regulatory loophole to evade state responsibility from one another.

Furthermore, this dysfunction also reveals the weakness of the hierarchical oversight function within the executive power itself. Based on Article 4 Paragraph (1) of the 1945 Constitution of the Republic of Indonesia, the President holds executive power and bears the highest responsibility for the administration of the state (Huda, 2021). The central government's inability to orchestrate its ministries and non-ministerial institutions to collectively take joint

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. Juni 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

responsibility for the PDN incident in a gallant manner shows that the control instruments within the government have not yet adapted to the complexities of the crisis in the digital era. Thus, from the perspective of Constitutional Law, the PDN case represents a moment of state failure in fulfilling its constitutional functions. The division of authority between the data management ministry and the cyber agency does not result in a mutually reinforcing oversight system; instead, it creates gaps for evading responsibility. Without improvements to the national cyber institution that requires a single point of accountability, the constitution's function as a tool for controlling state power in the digital space will continue to be reduced to merely an administrative illusion.

Delay in the Establishment of the Supervisory Authority: Anomaly of Constitutional Supremacy

The main pillar that supports the establishment of a rule of law state (rechtsstaat) is the principle of the supremacy of law. In the context of Indonesian constitutional law, this principle manifests itself in the form of constitutional supremacy, which means that the Constitution and the entire hierarchy of laws beneath it must be placed as the highest authority in organizing the life of the nation and state (Asshiddiqie, 2005). The supremacy of the constitution requires an absolute principle of legality; every action of state organizers must be subject to the law, and conversely, the law must not be subordinated to the pragmatic will of the rulers, let alone be defeated by the bureaucracy's sluggishness and negligence. In response to the rampant exploitation of data and cyber threats in the digital era, the supremacy of law has been concretized by lawmakers thru the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law). The enactment of this regulation is viewed as a milestone in the implementation of digital constitutionalism in Indonesia (Suzor, 2018). One of the most crucial law enforcement instruments mandated by the PDP Law is outlined in Article 58, which requires the President to establish a government agency that serves as the Personal Data Protection Authority (Data Protection Authority/DPA). According to universal data protection principles, this institution is absolutely required to be independent in carrying out oversight, investigation, law enforcement, and imposing administrative sanctions on data controllers, whether they come from the private sector or public/government institutions (Ghafur, 2022).

The absence of an independent supervisory authority prior to the PDN incident represents an anomaly of constitutional supremacy. The PDP Law's mandate to establish a supervisory agency is an imperative legal order; however, its delay creates a situation where the government acts ambiguously as both "player and referee." In the perspective of the rule of law, this condition eliminates the checks and balances mechanism that should function to test state accountability when infrastructure failures occur. The delay in the implementation of the law's directives by the executive branch is essentially a form of covert defiance against the supremacy of the constitution. Consequently, based on the legal construction of the PDP Law, when a state institution commits a violation due to negligence in securing the system, the absence of an independent DPA creates a legal deadlock and an acute conflict of interest. Logically and juridically, the violating subject must be investigated, independently audited forensically, and subjected to compliance sanctions (Ghafur, 2022). However, the absence of an independent supervisory authority creates a legal deadlock and an acute conflict of interest.

Without an independent DPA, government agencies seem to have immunity above the law. The Ministry of Communication and Information Technology is forced to act ambiguously as both "player and referee." They are responsible for managing the compromised infrastructure, yet they also hold temporary authority to evaluate the negligence. The post-factum situation of this PDN hacking clearly violates the principle of nemo judex in causa sua (no one can be a judge in their own case), which is one of the most fundamental doctrines in upholding the rule of law (Asshiddiqie, 2005). This condition affirms that the supremacy of the constitution in Indonesia's cyberspace is currently merely a formality and has not yet transformed into a "material reality" capable of providing concrete protection for citizens. The absence of an independent institution separate from the intervention of technical ministries makes public data protection merely an illusion. The law, which should be sharp upwards to discipline negligent state officials, becomes blunt due to the absence of an oversight body with an equal or higher standing to hold the relevant ministries accountable. This anomaly confirms the hypothesis that the state has failed to place the supremacy of law as an instrument to protect the digital sovereignty of its people, and instead, has allowed the sectoral ego of the bureaucracy to prevail over the constitution.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. Juni 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

CONCLUSION

This research concludes that the National Data Center (PDC) data breach incident is not merely a technical failure, but rather a representation of the state's constitutional negligence in fulfilling the mandate to protect the entire nation and the human rights of citizens regarding personal data. The dysfunction of the cyber institutional architecture and the delay in establishing an independent supervisory authority indicate a weakening of the principles of power limitation and the rule of law mandated by the 1945 Constitution and the PDP Law. As a strategic solution, the government must promptly establish an independent data protection supervisory agency and restructure clear cyber authority to eliminate the practice of institutional accountability neglect. Although this research is limited to the normative analysis of Constitutional Law, these findings provide a crucial foundation for strengthening Indonesia's digital sovereignty, which is expected to be further developed thru empirical research on the sociological impacts of citizens' data loss in the future.

REFERENCES

Alhakim, A., & Tantimin. (2024). The legal status of cryptocurrency and its implications for money laundering in Indonesia. *Padjajaran Jurnal Ilmu Hukum*, *11*(2), 231–253. https://doi.org/10.22304/pjih.v11n2.a4

Asshiddiqie, J. (2005). *Hukum tata negara dan pilar-pilar demokrasi*. Konstitusi Press.

Asshiddiqie, J. (2021). *Konstitusi dan hak asasi manusia di era digital*. Kencana Prenada Media Group.

Celeste, E. (2019). Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*, *33*(1), 76–99. https://doi.org/10.1080/13600869.2019.1562604

Christine, B., & Kansil, C. S. . (2022). Hambatan penerapan perlindungan data pribadi di Indonesia setelah disahkannya Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi. *Syntax Literate: Jurnal Ilmiah Indonesia*, *7*(9), 16331–16339. https://doi.org/10.36418/syntax-literate.v7i9.13936

Dayang, S., Putri, S. O., & Putri, A. K. (2025). Urgensi pembentukan lembaga pengawas dalam pembaharuan hukum perlindungan data pribadi menurut Undang-Undang PDP. *Locus :Journal of Academic Literature Review*, *4*(2), 106–113. https://jurnal.locusmedia.id/index.php/jalr/article/view/433

Fauzi, E., & Shandy, N. A. R. (2022). Hak atas privasi dan politik hukum Undang-Undang nomor 27 Tahun 2022 tentang perlindungan data pribadi. *Lex Renaissance*, *3*(7), 445–461. https://doi.org/10.20885/JLR.vol7.iss3.art1

Ghafur, J. (2022). Demokratisasi internal partai politik era reformasi : Antara das sollen dan das sein. *Jurnal Hukum Ius Quai Iustum*, *30*(1), 1–25. https://doi.org/10.20885/iustum.vol30.iss1.art1

Huda, N. (2021). *Hukum tata negara Indonesia (edisi revisi)*. Rajawali Pers.

Mahfud, M. (2006). *Membangun politik hukum, menegakkan konstitusi*. Rajawali Pers.

Mardiana, N., & Arsanti, M. (2023). Urgensi perlindungan data pribadi dalam perspektif hak asasi manusia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *5*(1), 16–23. https://doi.org/10.52005/rechten.v5i1.108

Marzuki, M. (2017). *Penelitian Hukum: Edisi Revisi*. Prenada Media.

Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 Tentang Perlindungan Infrastruktur Informasi Vital.

Ridwan, H. R. (2014). *Hukum administrasi negara (edisi revisi)*. Rajawali Pers.

Rosadi, S. D., & Pratama, G. G. (2018). Perlindungan privasi dan data pribadi dalam era ekonomi digital di Indonesia. *Veritat et Justitia*, *4*(1), 88–110. https://doi.org/10.25123/vej.2916

Saleh, G. (2021). The constitutionality of the electronic information and transaction law : Towards overcoming SARA conflict on social media. *Jurnal Konstitusi*, *18*(4), 846–868. https://doi.org/10.31078/jk1846

Surbakti, F. P. S. (2024). Personal data protection in public services. *Community Empowerment*, *9*(12), 1864–1870. https://doi.org/10.31603/ce.12536

Suzor, N. (2018). Digital constitutionalism : Using the rule of law to evaluate the legitimacy of governance by platforms. *Social Media + Society*, *4*(3), 1–11. https://doi.org/10.1177/2056305118787812

Takariawan, A., & Putri, S. A. (2018). Perlindungan hukum terhadap korban human trafficking dalam perspektif hak asasi manusia. *Jurnal Hukum Ius Quai Iustum*, *25*(2), 237–255. https://doi.org/10.20885/iustum.vol25.iss2.art2

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di indonesia. *Jurnal Becoss*, *1*(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030