

The Constitution in the Digital Era: Is the 1945 Constitution Ready to Address Cyber Threats and Data Security?

Fitri Kartika Sari^{1*} , Salman Salman² , Febrian Chandra³ , Alya Lavina Arken⁴ 

¹⁻⁴ Law Study Program, Faculty of Law, Universitas Merangin, Merangin, Jambi, 37313, Indonesia

ARTICLE INFO	ABSTRACT
Received: 16 June 2026	Digital governance, electronic transactions, cloud infrastructure, and public-sector data processing have transformed constitutional law in Indonesia. Cyberattacks, ransomware, data breaches, unlawful surveillance, and insecure personal data processing are no longer merely technical problems; they challenge constitutional guarantees of privacy, legal certainty, personal security, public service continuity, and state sovereignty. This article examines whether the 1945 Constitution of the Republic of Indonesia is normatively prepared to respond to cyber threats and personal data security risks. It asks, first, how the Constitution guarantees the protection of privacy and personal data security, and second, to what extent the state is constitutionally obliged to protect cyber sovereignty and respond to digital security threats. This research uses normative legal research with statutory, conceptual, case, and limited comparative approaches. The legal materials include the 1945 Constitution, the Personal Data Protection Law, the Electronic Information and Transactions Law, cybersecurity regulations, Constitutional Court decisions, and relevant legal scholarship. The article finds that the 1945 Constitution provides an implicit but strong basis for personal data protection through Articles 28G (1), 28D (1), 28H (4), 28F, 28I (4), and 28J. However, constitutional readiness remains incomplete at the operational level because cybersecurity governance is fragmented, independent personal data supervision has not been fully consolidated, and Indonesia still lacks a comprehensive statutory framework on cyber resilience. The article concludes that Indonesia's Constitution is normatively adaptable but requires stronger statutory translation, independent supervision, risk-based cybersecurity duties, and constitutional proportionality safeguards. The originality of this study lies in integrating privacy, personal data protection, cybersecurity, and cyber sovereignty into one constitutional analysis, while prior studies generally examine these fields separately.
Accepted: 06 July 2026	
Published: 05 August 2026	
Keywords: Constitution, Personal Data Protection, Cybersecurity, Cyber Sovereignty	

Copyright © 2026 The Author(s)

Published by CV Wahana Publikasi.

This article is an open access article under the [CC BY-NC 4.0 License](https://creativecommons.org/licenses/by-nc/4.0/)

1. Introduction

Digital transformation has altered the constitutional setting in which public power is exercised and individual rights are protected. In Indonesia, digitalization is visible in electronic-based government services, population administration databases, digital taxation, online health services, financial technology, electronic transactions, public procurement systems, and the migration of public-sector data to cloud and inter-agency platforms. These developments have expanded efficiency and administrative reach, yet they also create new legal risks: personal data breaches, identity theft, ransomware, unlawful surveillance, manipulation of electronic information, disruption of public services, and attacks against vital information infrastructure. From a constitutional perspective, those risks are not merely technological disturbances. They affect the legal relationship between the state, citizens, and private actors that process data on behalf of or in connection with public authority.^{1,2}

The constitutional problem becomes more complex because the digital environment simultaneously strengthens and threatens constitutional rights. Digital technologies can improve access to information, accelerate public services, and support democratic participation. At the same time, they can expose citizens to intrusive profiling, insecure databases, automated exclusion, and cross-border exploitation of personal information. In a constitutional democracy, the question is therefore not whether the state may use digital technology, but whether the use of digital technology remains controlled by law, human dignity, accountability, and proportionality. When a citizen's personal data is collected without a lawful basis, retained without security, or disclosed without consent or legitimate justification, the legal issue concerns the substance of constitutional protection, not only administrative compliance.³

The 1945 Constitution does not expressly use the terms "personal data," "data security," "cybersecurity," or "cyber sovereignty." This textual silence often raises doubts about whether the Constitution is sufficiently ready for digital-era threats. Nevertheless, constitutional readiness should not be measured only by the presence of technological terminology. Constitutions generally provide principles rather than technical codes. The Indonesian Constitution contains several provisions that can be interpreted as a normative foundation for the protection of privacy and data security, including the right to personal protection, family, honor, dignity, property, security, fair legal certainty, communication, information, and state responsibility for human rights protection.^{4,5}

The Preamble to the 1945 Constitution strengthens this interpretation by requiring the state to protect the whole people of Indonesia and the entire homeland of Indonesia. In the digital era, the mandate to protect the people cannot be limited to physical security and territorial integrity. It must also include the protection of digital identity, public-sector databases, electronic public services, and national cyber resilience. If public services become unavailable because critical systems are compromised, or if citizens lose control over their personal information because public data systems are insecure, the constitutional mandate of

¹ Dizon, "Socio-Legal Study of Technology: A Norms and Values Approach to Hacking and Encryption Law and Policy."

² Rosadi, "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia."

³ Yuniarti, "Perlindungan Hukum Data Pribadi di Indonesia."

⁴ The 1945 Constitution of the Republic of Indonesia, arts. 28D (1), 28F, 28G (1), 28H (4), 28I (4), and 28J.

⁵ Fauzy and Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi."

protection is substantively implicated.^{6,7}

Legislative developments confirm that personal data protection is increasingly understood as a constitutional matter. Law No. 27 of 2022 on Personal Data Protection defines personal data protection as all efforts to protect personal data in a series of personal data processing activities in order to guarantee the constitutional rights of personal data subjects. The explicit reference to constitutional rights is important because it prevents personal data from being reduced to a mere administrative asset or contractual object. Personal data becomes a legal interest attached to human dignity, autonomy, and equality before the law.⁸

However, statutory recognition does not automatically solve the constitutional problem. Indonesia has enacted or issued several legal instruments relevant to the digital sphere: the Personal Data Protection Law, the Electronic Information and Transactions Law as most recently amended by Law No. 1 of 2024, Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation, Presidential Regulation No. 95 of 2018 on Electronic-Based Government System, Presidential Regulation No. 28 of 2021 on the National Cyber and Crypto Agency, Presidential Regulation No. 82 of 2022 on Vital Information Infrastructure Protection, and Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy and Cyber Crisis Management. These instruments are significant, but they do not yet form a fully integrated constitutional regime of data security and cyber resilience.^{9,10}

Prior scholarship has addressed related issues from several angles. Studies on privacy and data protection generally emphasize that personal data protection is a modern expression of privacy, autonomy, and human dignity. Studies on cybersecurity tend to emphasize institutional coordination, risk management, national security, and critical infrastructure protection. Meanwhile, digital constitutionalism scholarship argues that constitutional values must be translated into the digital ecosystem, including through limits on public and private power, protection of rights, and accountability of digital intermediaries. This article joins those debates but focuses specifically on the dogmatic constitutional question: how the 1945 Constitution can be read as a normative basis for data security and cyber sovereignty in Indonesia.^{11,12}

Although these works are important, they leave three gaps that this article addresses. First, privacy scholarship tends to focus on individual consent, data subject rights, or the institutional design of data-protection authorities, while paying less attention to how weak cybersecurity can make those rights ineffective. Second, cybersecurity literature often discusses national resilience, cyber incidents, or critical infrastructure as questions of

⁶ Preamble to the 1945 Constitution of the Republic of Indonesia.

⁷ Aqilah, Waryenti, and Susanti, "Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi."

⁸ Law No. 27 of 2022 on Personal Data Protection, art. 1(2).

⁹ Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions; Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation; Presidential Regulation No. 95 of 2018 on Electronic-Based Government System; Presidential Regulation No. 28 of 2021 on the National Cyber and Crypto Agency; Presidential Regulation No. 82 of 2022 on Vital Information Infrastructure Protection; Presidential Regulation No. 47 of 2023 on National Cybersecurity Strategy and Cyber Crisis Management.

¹⁰ Disemadi, "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia"; Sabadina, "Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi oleh Korporasi Berbasis Online."

¹¹ Celeste, "Digital Constitutionalism: A New Systematic Theorisation"; De Gregorio and Radu, "Digital Constitutionalism in the New Era of Internet Governance."

¹² Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia"; Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara."

administrative capacity and national security, but does not sufficiently test them against constitutional limitations on public power. Third, digital constitutionalism literature offers a broad theory of constitutional values in digital space, yet it has rarely been applied to the specific structure of the 1945 Constitution, particularly Articles 28G(1), 28D(1), 28F, 28I(4), and 28J. The novelty of this article is therefore its integrated constitutional reading: it treats personal data protection, cybersecurity duties, and cyber sovereignty as mutually dependent elements of one constitutional regime rather than as three separate legal fields.¹³

The research questions are formulated as follows. First, how does the 1945 Constitution provide constitutional protection for privacy and personal data security amid cyber threats? Second, to what extent is the state prepared and constitutionally obliged to protect cyber sovereignty and respond to digital security threats in Indonesia? The contribution of this article lies in connecting two issues that are often discussed separately: personal data protection as a constitutional right and cybersecurity as a constitutional obligation of the state. The article argues that the two cannot be separated because data rights are ineffective without cybersecurity duties, while cybersecurity policy is constitutionally legitimate only when it respects rights, legality, accountability, and proportionality.

1.1 Concept and Theory

This article uses three main conceptual frameworks. The first is the constitutional right to privacy and personal data protection. Privacy in the digital environment is not limited to the traditional idea of being left alone. It includes the ability of individuals to understand, control, contest, and obtain remedies for the processing of information that identifies or can identify them. Personal data protection therefore operates as a bridge between human dignity, autonomy, legal certainty, and security. The right is especially important when the state or powerful private actors collect data at scale and use it for decisions affecting public services, mobility, finance, education, health, employment, and political participation.^{14,15}

The relationship among the three frameworks can be described as a layered analytical model. Privacy and personal data protection identify the protected constitutional interest at the individual level. Digital constitutionalism supplies the interpretive method by ensuring that technological governance remains subject to legality, accountability, and proportionality. Cyber sovereignty then explains the institutional capacity and obligation of the state to secure national digital systems. The three concepts meet in the notion of data security. A data breach weakens privacy because it removes effective control over personal information; weak cyber resilience undermines the state's protective duty because public services and vital infrastructure become vulnerable; and overbroad security measures may violate constitutional rights if they are not limited by law. Accordingly, this article evaluates constitutional readiness through three connected questions: whether the right exists, whether the state has enforceable security obligations, and whether security measures remain

¹³ Rendi, Tamza, and Fardiansyah, "Perlindungan Data Pribadi dalam Era Digitalisasi dan Tantangan Keamanan Siber di Indonesia"; Syahrial et al., "Pertanggungjawaban Hukum Pemerintah Terhadap Insiden Siber Kebocoran Data Pribadi."

¹⁴ Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning"; Quinn and Malgieri, "The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework."

¹⁵ Rosadi, "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia"; Fauzy and Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi."

constitutionally limited.

The second framework is digital constitutionalism. Digital constitutionalism does not require every digital issue to be constitutionalized in a formal amendment. Rather, it emphasizes that constitutional principles must remain effective when power is exercised through code, platforms, databases, algorithms, cyber operations, and digital infrastructure. In this sense, digital constitutionalism is an interpretive approach that connects the rule of law, rights protection, separation of powers, public accountability, and proportional limitation of rights to technological governance. It is particularly relevant to Indonesia because many cyber and data-security policies are issued through statutes, government regulations, presidential regulations, and sectoral rules that need a coherent constitutional orientation.¹⁶

The third framework is cyber sovereignty. Cyber sovereignty in this article is not understood as an absolute state monopoly over the internet or as a justification for unrestricted state surveillance. It is better understood as the constitutional capacity of the state to protect the integrity, availability, confidentiality, and resilience of national digital systems while respecting human rights. Cyber sovereignty therefore has both institutional and rights-based dimensions. Institutionally, it requires a capable state architecture for prevention, detection, response, recovery, and accountability. Rights-based, it requires that security measures be grounded in law and limited by necessity, proportionality, transparency, and effective remedies.¹⁷

Cybersecurity itself can also be approached as a rights-enabling condition. Without cybersecurity, the right to privacy and personal data protection becomes fragile because legal consent, purpose limitation, and access rights are meaningless if systems are technically vulnerable. Conversely, without constitutional rights, cybersecurity can become over-securitized and may legitimize excessive monitoring, data retention, or opaque intelligence practices. The relationship between cybersecurity and rights must therefore be structured as mutual reinforcement. The state must protect citizens from cyber harm, but it must do so through legal mechanisms that are accountable and proportionate.^{18,19}

2. Method and Legal Material

This research is normative legal research. It examines positive law, constitutional principles, legal doctrines, and the coherence of legal norms governing privacy, personal data protection, cybersecurity, and state obligations. Following Irwansyah and Ahsan Yunus, legal research is not limited to describing rules; it also involves interpreting, systematizing, evaluating, and formulating legal arguments concerning what the law is and how the law ought to be developed. The method is appropriate because the research questions concern the constitutional status of personal data security and the legal formulation of state duties in the

¹⁶ Celeste, "Digital Constitutionalism: A New Systematic Theorisation"; De Gregorio, "The Rise of Digital Constitutionalism in the European Union."

¹⁷ Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara"; Kristalia and Wibisono, "Ancaman Siber dan Penguatan Kedaulatan Digital Indonesia dari Perspektif Geopolitik Digital."

¹⁸ Papakonstantinou, "Cybersecurity as Praxis and as a State: The EU Law Path Towards Acknowledgement of a New Right to Cybersecurity?"; Chiara, "Towards a Right to Cybersecurity in EU Law? The Challenges Ahead."

¹⁹ Rendi, Tamza, and Fardiansyah, "Perlindungan Data Pribadi dalam Era Digitalisasi dan Tantangan Keamanan Siber di Indonesia."

cyber domain.²⁰

The approaches used are statutory, conceptual, case, and limited comparative approaches. The statutory approach examines the 1945 Constitution, the Personal Data Protection Law, the Electronic Information and Transactions Law, government regulations on electronic systems, presidential regulations on electronic-based government, cybersecurity institutions, vital information infrastructure, and national cybersecurity strategy. The conceptual approach clarifies the meaning of constitutional privacy, personal data protection, digital constitutionalism, and cyber sovereignty. The case approach analyzes Constitutional Court decisions concerning privacy, surveillance, electronic evidence, and the legal requirements for limiting constitutional rights. The limited comparative approach is used only to sharpen the Indonesian analysis, particularly by considering the broader development of privacy, data protection, and cybersecurity as rights-related governance fields.

The primary legal materials consist of the 1945 Constitution, Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 on Electronic Information and Transactions as amended, Law No. 1 of 2024, Government Regulation No. 71 of 2019, Presidential Regulation No. 95 of 2018, Presidential Regulation No. 28 of 2021, Presidential Regulation No. 82 of 2022, Presidential Regulation No. 47 of 2023, and relevant regulations of the National Cyber and Crypto Agency. The secondary legal materials include books, journal articles, and doctrinal literature on constitutional law, data protection, cybersecurity, and digital constitutionalism. The tertiary materials include legal dictionaries and official legal information portals where necessary.

The analysis is qualitative and prescriptive. First, the constitutional norms are interpreted grammatically, systematically, teleologically, and contextually to identify whether privacy and personal data security can be protected under existing constitutional provisions. Second, the statutory framework is evaluated to determine whether it translates constitutional guarantees into enforceable rights and institutional duties. Third, the cybersecurity framework is assessed in relation to the constitutional obligations of the state, especially the duty to protect citizens, ensure legal certainty, and safeguard rights. Finally, the article formulates normative recommendations for strengthening the integration of personal data protection and cybersecurity in Indonesia's constitutional order.

3. Results and Discussion

3.1 *Constitutional Protection of Privacy and Personal Data Security under the 1945 Constitution*

The 1945 Constitution does not explicitly mention personal data, but several provisions provide a solid interpretive basis for constitutional protection. Article 28G (1) is the central provision because it guarantees every person the right to protection of self, family, honor, dignity, and property, and the right to security from fear. Personal data is closely connected to all of these interests. It identifies a person, reveals aspects of private life, may expose family relations, can affect reputation and dignity, and may be used to access property or public services. A breach of personal data can therefore threaten not only informational interests, but also personal security and human dignity.^{21,22}

²⁰ Irwansyah and Yunus, *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*.

²¹ The 1945 Constitution of the Republic of Indonesia, art. 28G (1).

²² Rosadi, "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia."

Article 28D (1) strengthens this protection by guaranteeing recognition, security, protection, and fair legal certainty before the law. In the context of data processing, legal certainty requires that citizens know who collects their data, for what purpose, on what legal basis, for how long, with what security standards, and through what mechanism they may exercise their rights. When data processing is vague, hidden, or uncontrolled, the citizen is placed in an unequal position against both the state and data controllers. Therefore, constitutional legal certainty demands clear statutory rules, enforceable obligations, accessible remedies, and accountable supervisory institutions.^{23,24}

Article 28H (4) is also relevant because the constitutional guarantee of property should be read in a modern context. Digital identity and personal data are not property in the narrow classical sense, but they create legal and economic interests that may be exploited, transferred, profiled, or abused. Personal data can be used for authentication, financial transactions, credit scoring, targeted advertising, and access to government benefits. The constitutional protection of property therefore supports the argument that citizens have a legally protected interest in preventing unauthorized exploitation or deprivation of control over their informational assets.²⁵

Article 28F requires a more balanced interpretation. It protects the right to communicate and obtain information, as well as the right to seek, possess, store, process, and convey information through available channels. This provision supports digital freedom, access to information, and communication rights. However, it cannot be read as a license for unlimited collection or disclosure of personal data. The right to information must be harmonized with Article 28G (1), Article 28D (1), Article 28I (4), and Article 28J. In other words, digital openness must be reconciled with privacy, security, and legal limits.²⁶

Article 28I (4) provides the state-duty dimension. It states that the protection, advancement, enforcement, and fulfillment of human rights are the responsibility of the state, especially the government. This provision is crucial because privacy and personal data protection cannot be guaranteed only by private consent or individual vigilance. Citizens usually lack bargaining power against government databases, digital platforms, employers, financial institutions, and essential service providers. The Constitution therefore requires the state to create a legal and institutional environment in which data rights can be meaningfully exercised.^{27,28}

Law No. 27 of 2022 translates this constitutional foundation into a statutory rights framework. It defines personal data, personal data subjects, controllers, processors, and personal data protection. It also recognizes the rights of personal data subjects and imposes obligations on controllers and processors. The statutory model indicates that personal data protection is not merely a matter of consent. It is a structure of lawful basis, purpose limitation, data minimization, accuracy, security, accountability, rights of access and correction, objection, deletion, and notification in cases of failure of personal data protection.²⁹

The constitutional significance of cybersecurity appears at this point. A right to personal

²³ The 1945 Constitution of the Republic of Indonesia, art. 28D (1).

²⁴ Fauzy and Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi."

²⁵ The 1945 Constitution of the Republic of Indonesia, art. 28H (4).

²⁶ The 1945 Constitution of the Republic of Indonesia, arts. 28F and 28J.

²⁷ The 1945 Constitution of the Republic of Indonesia, art. 28I (4).

²⁸ Aqilah, Waryenti, and Susanti, "Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi."

²⁹ Law No. 27 of 2022 on Personal Data Protection, arts. 1, 5–15, 20, 27–32, and 46.

data protection cannot be effective unless data controllers and processors are under a duty to ensure security. The Personal Data Protection Law requires controllers to protect and ensure the security of personal data from unauthorized processing, unauthorized access, unauthorized disclosure, alteration, misuse, destruction, or loss. This duty reflects the inseparability of privacy and security: the legal recognition of data rights must be supported by technical, organizational, and procedural safeguards.^{30,31}

Constitutional Court jurisprudence supports a rights-based understanding of digital and electronic intrusions. In decisions concerning wiretapping and electronic evidence, the Court has emphasized that intrusions into private life must be based on law and must respect constitutional safeguards. The doctrinal lesson is that the state may restrict privacy for legitimate purposes, including law enforcement and security, but the restriction must not be arbitrary. It requires a legal basis, clear procedure, institutional accountability, and proportionality. This reasoning is directly relevant to cybersecurity policy because cyber monitoring, incident response, and digital forensics may involve access to personal or sensitive information.³²

These decisions are important not because they already establish a detailed constitutional doctrine on personal data, but because they supply the minimum test for digital intrusions. Decision No. 5/PUU-VIII/2010 shows that interception cannot be treated as an ordinary administrative technique; it must be governed by clear statutory authorization and procedural safeguards. Decision No. 20/PUU-XIV/2016 similarly indicates that electronic information obtained through intrusive measures cannot be constitutionally legitimate if the acquisition bypasses the requirements of legality and due process. Applied to data security, this jurisprudence means that a cyber policy cannot be evaluated only by its technical effectiveness. A monitoring system, digital forensic operation, or information-sharing mechanism may be useful for preventing attacks, but it becomes constitutionally vulnerable when it lacks a clear legal basis, independent control, limits on data retention, and remedies for affected citizens.³³

Practical examples also reveal the weakness of a purely administrative approach. If a public service database is compromised, citizens may face identity theft, denial of services, financial fraud, or reputational harm even though they never consented to the risky processing. If a ransomware attack disables electronic public services, the constitutional harm is not limited to system downtime; it affects legal certainty and the ability of citizens to access state services. These examples show why the state's positive obligation under Articles 28G (1), 28D (1), and 28I (4) requires preventive cybersecurity standards, rapid incident notification, recovery duties, and accessible remedies. The critical point is that constitutional rights should operate before, during, and after a cyber incident: before through security-by-design duties, during through accountable incident response, and after through remedies and institutional learning.³⁴

The constitutional mapping can be summarized as follows. Personal data security derives

³⁰ Law No. 27 of 2022 on Personal Data Protection, arts. 35–39 and 46.

³¹ Disemadi, "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia".

³² Constitutional Court of the Republic of Indonesia, Decision No. 5/PUU-VIII/2010; Constitutional Court of the Republic of Indonesia, Decision No. 20/PUU-XIV/2016.

³³ Adhari, Sitabuana, and Srihandayani, "Kebijakan Pembatasan Internet di Indonesia: Perspektif Negara Hukum, Hak Asasi Manusia, dan Kajian Perbandingan."

³⁴ Syahrial et al., "Pertanggungjawaban Hukum Pemerintah Terhadap Insiden Siber Kebocoran Data Pribadi."

primarily from Article 28G (1), is operationalized by Article 28D (1), complemented by Article 28H (4), balanced with Article 28F, imposed as a state duty through Article 28I (4), and limited through Article 28J. The combined reading produces a constitutional doctrine: personal data protection is a constitutional right, data security is a constitutional condition for the enjoyment of that right, and state cybersecurity policy must be rights-respecting and legally accountable.

Table 1. Constitutional Mapping of Privacy and Personal Data Protection in the 1945 Constitution

Constitutional provision	Digital-era implication	Legal consequence
Article 28G (1)	Protection of self, dignity, property, and security from fear includes protection against misuse of personal data.	Privacy and personal data security should be treated as constitutional interests.
Article 28D (1)	Digital governance must be based on fair legal certainty, clarity, remedies, and accountability.	Data processing requires clear rules, lawful basis, and enforceable rights.
Article 28H (4)	Digital identity and information assets may affect property and economic interests.	Unauthorized exploitation of personal data can be linked to constitutional harm.
Article 28F	Access to information and communication rights must be balanced with privacy and security.	Freedom of information does not justify unlawful disclosure of personal data.
Article 28I (4)	The state must protect, advance, enforce, and fulfill human rights in digital spaces.	The state must build institutions, supervision, and remedies for data protection.
Article 28J	Rights may be limited only by law and for legitimate constitutional purposes.	Cybersecurity measures must satisfy legality, necessity, and proportionality.

Source: Author's analysis, 2026.³⁵

Table 1 clarifies that the constitutional basis for personal data protection does not depend on a single provision. Its significance lies in showing the cumulative nature of protection: Article 28G (1) provides the core privacy and security interest, Article 28D (1) supplies legal certainty, Article 28F requires balance with information rights, Article 28I (4) transforms protection into a state duty, and Article 28J limits any security intervention. This mapping contributes to the discussion by converting broad constitutional clauses into concrete evaluation standards for data processing and cybersecurity policy.³⁶

3.2 State Readiness and Constitutional Obligations in Protecting Cyber Sovereignty

State readiness in the cyber domain must be assessed in two layers: normative readiness and operational readiness. At the normative level, the 1945 Constitution provides a broad basis for state responsibility. The Preamble requires the state to protect the people, Article 1(3) establishes Indonesia as a state based on law, Article 28I(4) imposes state responsibility for

³⁵ The table is constructed by synthesizing Indonesian constitutional privacy scholarship, particularly Rosadi, "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia"; Fauzy and Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi."

³⁶ Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia."

human rights, and Article 30 concerns national defense and security. These provisions can support a constitutional obligation to protect cyber sovereignty, provided that the concept is understood consistently with the rule of law and rights protection.^{37,38}

At the statutory and regulatory level, Indonesia has taken important steps. Presidential Regulation No. 28 of 2021 places the National Cyber and Crypto Agency as the governmental institution responsible for carrying out government duties in cybersecurity and cryptography. This institutional arrangement is important because cyber threats do not fit neatly within conventional administrative sectors. They involve defense, intelligence, law enforcement, public administration, finance, telecommunications, energy, transportation, health, education, and private digital services. A national cyber institution is therefore necessary to coordinate policy and operational response.³⁹

Presidential Regulation No. 47 of 2023 further develops the national cybersecurity framework by establishing the National Cybersecurity Strategy and Cyber Crisis Management. Its significance lies in shifting cybersecurity from isolated technical protection toward a more strategic model that includes prevention, preparedness, response, recovery, coordination, and crisis management. In constitutional terms, such a strategy is an instrument for fulfilling the state's protective function. However, because it is located at the level of presidential regulation, its capacity to impose comprehensive rights-affecting obligations, liabilities, sanctions, and independent oversight remains limited compared with a statute.⁴⁰

Presidential Regulation No. 82 of 2022 on Vital Information Infrastructure Protection is also constitutionally relevant. Vital information infrastructure includes systems whose disruption may affect public interest, public services, defense, security, economy, finance, health, energy, transportation, and other strategic sectors. Protecting this infrastructure is not merely a technical matter of network management. It is part of the constitutional duty to maintain continuity of essential services and to prevent systemic harm to citizens. A cyberattack against vital infrastructure may threaten the enjoyment of rights even when it does not directly target individual data.⁴¹

Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation provides additional obligations for electronic system operators, including reliability, security, and responsibility in operating electronic systems. Its relevance is that cybersecurity duties are not limited to state institutions. Private electronic system operators that process personal data or provide essential digital services also affect constitutional interests. The state must therefore regulate private actors whose activities can threaten privacy, access to services, economic rights, and public order.⁴²

Despite these developments, operational readiness remains incomplete. The first issue is legal fragmentation. Personal data protection, electronic information and transactions, electronic systems, public-sector digitalization, vital information infrastructure, cyber crisis management, and sectoral cybersecurity are regulated across different legal instruments. Fragmentation does not necessarily mean absence of law, but it can create uncertainty about

³⁷ The 1945 Constitution of the Republic of Indonesia, Preamble, arts. 1(3), 28I(4), and 30.

³⁸ Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara."

³⁹ Presidential Regulation No. 28 of 2021 on the National Cyber and Crypto Agency.

⁴⁰ Presidential Regulation No. 47 of 2023 on National Cybersecurity Strategy and Cyber Crisis Management.

⁴¹ Presidential Regulation No. 82 of 2022 on Vital Information Infrastructure Protection; Regulation of the National Cyber and Crypto Agency No. 7 of 2023 on Vital Information Infrastructure Identification.

⁴² Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation.

duties, coordination, reporting, sanctions, institutional authority, and remedies. For citizens, fragmented law may make it difficult to know where to complain, which authority is responsible, and what remedy is available when cyber incidents affect personal data or public services.⁴³

The second issue is institutional fragmentation. Cybersecurity involves the National Cyber and Crypto Agency, ministries, sectoral regulators, law enforcement institutions, electronic system operators, and potentially data protection supervisory authorities. Without a clear coordination model, institutional overlap can create gaps in prevention and response. Cyber incidents require speed, but constitutional accountability requires legal clarity. A cyber governance model that relies too heavily on ad hoc coordination risks weakening both effectiveness and accountability.

The third issue is the incomplete consolidation of independent personal data supervision. Law No. 27 of 2022 provides for an institution responsible for personal data protection, with functions that include policy formulation, supervision, enforcement, dispute facilitation, and cooperation. This institution is central to constitutional readiness because rights without supervision may become declaratory rather than enforceable. The more personal data is processed by both public and private actors, the more important independent and credible supervision becomes.^{44,45}

The fourth issue is the tension between security and rights. Cybersecurity may require monitoring, traffic analysis, forensic investigation, threat intelligence, vulnerability disclosure, and information sharing. These measures can be legitimate, but they may also affect privacy and freedom of expression if they are conducted without legal limits. Article 28J of the 1945 Constitution requires that limitations of rights be established by law and be consistent with morality, religious values, security, and public order in a democratic society. Therefore, cybersecurity policy should not be framed as an exception to constitutional rights; it should be designed as a constitutionally limited exercise of public power.⁴⁶

The fifth issue is the absence of a comprehensive cybersecurity and cyber resilience statute. Existing presidential regulations and agency regulations are useful, but they do not fully substitute for statutory regulation when the policy affects rights, imposes duties on private actors, creates liability, mandates incident reporting, or authorizes intrusive measures. A statute is needed to integrate cyber risk management, incident notification, protection of vital infrastructure, coordination of authorities, public-private obligations, evidence handling, sanctions, remedies, and oversight. Such a statute should also clarify the relationship between cybersecurity duties and personal data protection duties.⁴⁷

Table 2. Cyber Sovereignty Risks and Constitutional Obligations of the State

Risk area	Constitutional concern	Required legal response
Personal data breach	Threat to privacy, dignity, legal certainty, and personal security.	Strong data security duties, breach notification, supervisory enforcement, and remedies.
Cyberattack against public	Threat to the state duty to protect	Cyber resilience obligations,

⁴³ Syahrial et al., "Pertanggungjawaban Hukum Pemerintah Terhadap Insiden Siber Kebocoran Data Pribadi."

⁴⁴ Law No. 27 of 2022 on Personal Data Protection, arts. 58–60.

⁴⁵ Aqilah, Waryenti, and Susanti, "Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi."

⁴⁶ The 1945 Constitution of the Republic of Indonesia, art. 28J.

⁴⁷ Rendi, Tamza, and Fardiansyah, "Perlindungan Data Pribadi dalam Era Digitalisasi dan Tantangan Keamanan Siber di Indonesia"

services	citizens and ensure continuity of essential services.	crisis management, backup systems, and accountability.
Vital information infrastructure disruption	Threat to public order, economy, health, transportation, energy, and national security.	Risk-based designation, minimum security standards, audits, and incident coordination.
Excessive surveillance or monitoring	Threat to privacy, freedom of expression, and rule of law.	Legal basis, necessity, proportionality, judicial or independent oversight, and remedies.
Institutional overlap	Threat to legal certainty and effective state protection.	Clear allocation of authority, coordination protocols, and transparent reporting lines.
Cross-border data and cyber operations	Threat to jurisdiction, accountability, and protection of citizens abroad.	International cooperation, data transfer safeguards, mutual assistance, and cyber diplomacy.

Source: Author's analysis, 2026.⁴⁸

Table 2 shows that cyber sovereignty is constitutionally relevant only when specific risks are linked to rights, public services, and institutional accountability. The table contributes to the analysis by distinguishing between different types of cyber risk and the corresponding legal response. It also confirms that cyber sovereignty should not be understood merely as control over digital infrastructure, but as the state's capacity to prevent harm, coordinate response, impose duties, and provide remedies while respecting constitutional limitations.⁴⁹

3.3 Reconstructing Constitutional Readiness in the Digital Era

The readiness of the 1945 Constitution should be understood dynamically. A constitution does not become obsolete merely because it lacks technical vocabulary. Its function is to provide basic principles that can guide legal development across changing social and technological conditions. In this sense, the 1945 Constitution is normatively adaptable because it contains rights, state duties, the rule of law, and limitation clauses that can be applied to digital problems. The main weakness is not the absence of constitutional principles, but the incomplete translation of those principles into coherent statutory duties, institutions, and remedies.⁵⁰

The first reconstruction needed is doctrinal affirmation that personal data protection is a constitutional right. This affirmation can be developed through Constitutional Court jurisprudence, legislative interpretation, academic doctrine, and administrative practice. The doctrine should clarify that personal data protection is not an isolated statutory benefit but part of the constitutional protection of self, dignity, property, security, and fair legal certainty. This would provide a stronger basis for reviewing laws or policies that enable excessive data collection, weak security, or disproportionate surveillance.

The second reconstruction is the strengthening of independent personal data supervision.

⁴⁸ For Indonesian cybersecurity governance and incident accountability, see Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara"; Syahrial et al., "Pertanggungjawaban Hukum Pemerintah Terhadap Insiden Siber Kebocoran Data Pribadi."

⁴⁹ Kristalia and Wibisono, "Ancaman Siber dan Penguatan Kedaulatan Digital Indonesia dari Perspektif Geopolitik Digital."

⁵⁰ Adhari, Sitabuana, and Srihandayani, "Kebijakan Pembatasan Internet di Indonesia: Perspektif Negara Hukum, Hak Asasi Manusia, dan Kajian Perbandingan."

Comparative data protection theory emphasizes that rights over data require institutional enforcement because individual data subjects cannot realistically monitor complex processing ecosystems alone. An effective supervisory authority should have adequate independence, budget, expertise, investigative powers, corrective powers, administrative sanctioning power, coordination capacity, and public complaint mechanisms. Without these features, constitutional rights may be formally recognized but practically unenforced.^{51,52}

The third reconstruction is the adoption of a comprehensive cybersecurity and cyber resilience law. The law should not merely criminalize cyber conduct or institutionalize a security agency. It should create a full governance cycle: prevention, risk assessment, minimum security standards, secure-by-design duties, supply-chain security, protection of vital information infrastructure, incident notification, crisis management, evidence preservation, vulnerability reporting, public communication, recovery, sanctions, and remedies. It should also determine which obligations apply to state institutions, public service providers, private operators, and critical-sector entities.⁵³

The fourth reconstruction is the integration of personal data protection and cybersecurity. At present, the two fields are often treated separately: data protection as a privacy issue, cybersecurity as a security issue. This separation is doctrinally and practically weak. A personal data breach is frequently a cybersecurity failure, while cyber incident handling often involves personal data. Legal integration should require controllers, processors, and electronic system operators to implement risk-based technical and organizational measures, conduct audits, notify relevant authorities and affected individuals, and document accountability. The same incident should not produce conflicting reporting duties or gaps in remedies.⁵⁴

The fifth reconstruction is the constitutionalization of proportionality in digital security measures. Every interference with privacy or communications in the name of cybersecurity should pass a proportionality test. First, it must have a clear legal basis. Second, it must pursue a legitimate constitutional aim. Third, it must be suitable to achieve that aim. Fourth, it must be necessary in the sense that less intrusive alternatives are inadequate. Fifth, it must be balanced, meaning the benefit to security must not be disproportionate to the harm to rights. This model gives practical meaning to Article 28J in digital governance.⁵⁵

The sixth reconstruction is a more precise understanding of cyber sovereignty. Cyber sovereignty should not be reduced to data localization or state control over digital space. Data localization may be relevant in specific contexts, but it does not automatically produce cybersecurity or rights protection. Cyber sovereignty should instead be defined as the capacity to protect citizens, institutions, and vital digital systems through lawful, accountable, resilient, and rights-respecting governance. This definition avoids both technological dependency and authoritarian overreach.⁵⁶

⁵¹ Bastos and Pałka, "Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?"; Mantelero et al., "The Common EU Approach to Personal Data and Cybersecurity Regulation."

⁵² Disemadi, "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia"

⁵³ Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara."

⁵⁴ Rendi, Tamza, and Fardiansyah, "Perlindungan Data Pribadi dalam Era Digitalisasi dan Tantangan Keamanan Siber di Indonesia"

⁵⁵ The 1945 Constitution of the Republic of Indonesia, art. 28J; Mujaddidi, "Konstitusionalitas Pembatasan Hak Asasi Manusia dalam Putusan Mahkamah Konstitusi."

⁵⁶ Kristalia and Wibisono, "Ancaman Siber dan Penguatan Kedaulatan Digital Indonesia dari Perspektif Geopolitik"

The seventh reconstruction concerns artificial intelligence and automated governance. Future cyber and data threats will not only involve database leaks or ransomware. They will also involve automated profiling, synthetic identity fraud, deepfakes, algorithmic discrimination, manipulation of public opinion, and exploitation of large-scale datasets. The constitutional framework should therefore anticipate the convergence of personal data protection, cybersecurity, and AI governance. The state's duty to protect must extend to the risks created by automated systems, while maintaining transparency, contestability, and human oversight.^{57,58}

Based on these reconstructions, the question whether the 1945 Constitution is ready for cyber threats and data security must be answered in layers. It is ready at the level of principles because it protects dignity, personal security, property, legal certainty, information rights, human rights duties, and lawful limitation of rights. It is partly ready at the level of statutory translation because the Personal Data Protection Law and several cybersecurity regulations already exist. It is not yet fully ready at the level of institutional and operational enforcement because supervision, coordination, comprehensive cyber resilience duties, and remedies remain insufficiently integrated.⁵⁹

4. Conclusion

This article concludes that the 1945 Constitution is normatively capable of addressing cyber threats and personal data security even though it does not expressly mention personal data, cybersecurity, data security, or cyber sovereignty. Constitutional protection can be derived from Article 28G (1) on protection of self, dignity, property, and security; Article 28D (1) on fair legal certainty; Article 28H (4) on property; Article 28F on communication and information; Article 28I (4) on state responsibility for human rights; and Article 28J on lawful and proportionate limitation of rights. Read systematically, these provisions support a constitutional doctrine that personal data protection is a constitutional right and that data security is a necessary condition for the enjoyment of that right.

The state also has a constitutional obligation to protect cyber sovereignty. This obligation derives from the Preamble, the principle of the rule of law, state responsibility for human rights, and the constitutional function of defense and security. Indonesia has developed important legal instruments, including the Personal Data Protection Law, the Electronic Information and Transactions Law, regulations on electronic systems and electronic-based government, the institutional framework of the National Cyber and Crypto Agency, protection of vital information infrastructure, and the National Cybersecurity Strategy and Cyber Crisis Management. These instruments indicate normative progress, but they do not yet amount to a fully coherent constitutional regime of data security and cyber resilience.

The ideal formulation is to strengthen the connection between constitutional rights and cybersecurity obligations. Indonesia needs clearer doctrinal recognition of personal data protection as a constitutional right, an effective and independent supervisory authority for personal data protection, a comprehensive cybersecurity and cyber resilience statute, integrated incident notification and remedy mechanisms, risk-based duties for public and

Digital."

⁵⁷ Qian, Siau, and Nah, "Societal Impacts of Artificial Intelligence: Ethical, Legal, and Governance Issues."

⁵⁸ Disemadi, "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia"

⁵⁹ Rendi, Tamza, and Fardiansyah, "Perlindungan Data Pribadi dalam Era Digitalisasi dan Tantangan Keamanan Siber di Indonesia"

private operators, and proportionality safeguards for all digital security measures that affect privacy and freedom of communication. Cyber sovereignty should be understood not as unlimited state control over digital space, but as lawful, accountable, resilient, and rights-respecting capacity to protect citizens and national digital infrastructure.

The contribution of this article is to connect two fields that are often separated: personal data protection as a constitutional rights issue and cybersecurity as a state obligation. The analysis shows that neither field can function properly without the other. Data rights need cybersecurity to be effective, while cybersecurity needs constitutional rights to remain legitimate. The limitation of this research is its normative character; it does not empirically measure institutional performance or technical readiness. Future research may examine the effectiveness of incident response, the design of the personal data protection authority, sectoral compliance with cybersecurity duties, and the role of courts in developing digital constitutionalism in Indonesia.

Acknowledgments

The authors would like to thank Faculty of Law, Universitas Merangin for academic support during the preparation of this manuscript. Any remaining errors are the responsibility of the authors.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this article. The authors have no financial, professional, or personal relationships that could inappropriately influence the research, analysis, or conclusions presented in this manuscript.

Authors' contribution

Fitri Kartika Sari: Conceptualization, Data curation, Formal analysis, Writing – original draft, Writing – review & editing

Salman: Formal analysis, Investigation, Methodology, Project administration, Resources, Software

Febrian Chandra & Alya Lavina Arken: Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing

Statement of the use of AI

The authors declare that generative AI or AI-assisted tools were used only as an auxiliary tool to improve language quality, grammar, structure, and readability during manuscript preparation. All legal arguments, citations, references, analysis, and conclusions were independently reviewed, corrected, and verified by the authors. The authors remain fully responsible for the accuracy, originality, and integrity of the manuscript.

References

Adhari, Ade, Tundjung Herning Sitabuana, and Luisa Srihandayani. "Kebijakan Pembatasan Internet di Indonesia: Perspektif Negara Hukum, Hak Asasi Manusia, dan Kajian

- Perbandingan." *Jurnal Konstitusi* 18, no. 2 (2021): 262–293. <https://doi.org/10.31078/jk1821>.
- Aqilah, Rosa, Deli Waryenti, and Pipi Susanti. "Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Ilmiah Kutei* 23, no. 2 (2024): 158–172. <https://doi.org/10.33369/jik.v23i2.34476>.
- Bastos, Filipe Brito, and Przemysław Pałka. "Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?" *European Constitutional Law Review* 19, no. 3 (2023): 487–517. <https://doi.org/10.1017/S1574019623000202>.
- Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning." *German Law Journal* 20, no. 6 (2019): 864–883. <https://doi.org/10.1017/glj.2019.66>.
- Celeste, Edoardo. "Digital Constitutionalism: A New Systematic Theorisation." *International Review of Law, Computers & Technology* 33, no. 1 (2019): 76–99. <https://doi.org/10.1080/13600869.2019.1562604>.
- Chiara, Pier Giorgio. "Towards a Right to Cybersecurity in EU Law? The Challenges Ahead." *Computer Law & Security Review* 53 (2024): 105961. <https://doi.org/10.1016/j.clsr.2024.105961>.
- Chotimah, Hidayat Chusnul. "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara." *Politica* 10, no. 2 (2019): 113–128. <https://doi.org/10.22212/jp.v10i2.1447>.
- Constitutional Court of the Republic of Indonesia. *Decision No. 5/PUU-VIII/2010*.
- Constitutional Court of the Republic of Indonesia. *Decision No. 20/PUU-XIV/2016*.
- De Gregorio, Giovanni. "The Rise of Digital Constitutionalism in the European Union." *International Journal of Constitutional Law* 19, no. 1 (2021): 41–70. <https://doi.org/10.1093/icon/moab001>.
- De Gregorio, Giovanni, and Roxana Radu. "Digital Constitutionalism in the New Era of Internet Governance." *International Journal of Law and Information Technology* 30, no. 1 (2022): 68–87. <https://doi.org/10.1093/ijlit/eaac004>.
- Disemadi, Hari Sutra. "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–199. <https://doi.org/10.25072/jwy.v5i2.460>.
- Dizon, Michael Anthony C. "Socio-Legal Study of Technology: A Norms and Values Approach to Hacking and Encryption Law and Policy." *Computer Law & Security Review* 52 (2024): 105958. <https://doi.org/10.1016/j.clsr.2024.105958>.
- Fauzy, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissance* 7, no. 3 (2022): 445–461. <https://doi.org/10.20885/JLR.vol7.iss3.art1>.
- Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation.
- Irwansyah, and Ahsan Yunus. *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Yogyakarta: Mirra Buana Media, 2020.
- Kristalia, BRM. Yehizkia Y., and Indra Wisnu Wibisono. "Ancaman Siber dan Penguatan Kedaulatan Digital Indonesia dari Perspektif Geopolitik Digital." *Jurnal Ilmiah Multidisiplin* 3, no. 2 (2024): 83–93. <https://doi.org/10.56127/jukim.v3i02.1584>.
- Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.
- Law No. 27 of 2022 on Personal Data Protection.
- Mantelero, Alessandro, Giuseppe Vaciago, Maria Samantha Esposito, and Nicole Monte. "The

- Common EU Approach to Personal Data and Cybersecurity Regulation." *International Journal of Law and Information Technology* 28, no. 4 (2020): 297–328. <https://doi.org/10.1093/ijlit/aaaa021>.
- Mujaddidi, Sipghotulloh. "Konstitusionalitas Pembatasan Hak Asasi Manusia dalam Putusan Mahkamah Konstitusi." *Jurnal Konstitusi* 18, no. 3 (2021): 539–561. <https://doi.org/10.31078/jk1833>.
- Papakonstantinou, Vagelis. "Cybersecurity as Praxis and as a State: The EU Law Path Towards Acknowledgement of a New Right to Cybersecurity?" *Computer Law & Security Review* 44 (2022): 105653. <https://doi.org/10.1016/j.clsr.2022.105653>.
- Presidential Regulation No. 28 of 2021 on the National Cyber and Crypto Agency.
- Presidential Regulation No. 47 of 2023 on National Cybersecurity Strategy and Cyber Crisis Management.
- Presidential Regulation No. 82 of 2022 on Vital Information Infrastructure Protection.
- Presidential Regulation No. 95 of 2018 on Electronic-Based Government System.
- Qian, Yuzhou, Keng L. Siau, and Fiona F. Nah. "Societal Impacts of Artificial Intelligence: Ethical, Legal, and Governance Issues." *Societal Impacts* 3 (2024): 100040. <https://doi.org/10.1016/j.socimp.2024.100040>.
- Quinn, Paul, and Gianclaudio Malgieri. "The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework." *German Law Journal* 22, no. 8 (2021): 1583–1612. <https://doi.org/10.1017/glj.2021.79>.
- Regulation of the National Cyber and Crypto Agency No. 5 of 2024 on National Cybersecurity Action Plan 2024–2028.
- Regulation of the National Cyber and Crypto Agency No. 7 of 2023 on Vital Information Infrastructure Identification.
- Rendi, Muhammad, Fristia Berdian Tamza, and Ahmad Irzal Fardiansyah. "Perlindungan Data Pribadi dalam Era Digitalisasi dan Tantangan Keamanan Siber di Indonesia." *Jurnal Hukum Lex Generalis* 6, no. 12 (2025). <https://doi.org/10.56370/jhlg.v6i12.2452>.
- Rosadi, Sinta Dewi. "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016): 35–53. <https://doi.org/10.20961/yustisia.v5i1.8712>.
- Sabadina, Uni. "Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi oleh Korporasi Berbasis Online." *Lex Renaissance* 6, no. 4 (2021): 799–814. <https://doi.org/10.20885/JLR.vol6.iss4.art11>.
- Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018): 369–384. <https://doi.org/10.24815/kanun.v20i2.11159>.
- Syahrial, Shafira Meutia, Edmon Makarim, Zahrashafa Putri Mahardika, and Ayu Galuh Anggraini. "Pertanggungjawaban Hukum Pemerintah Terhadap Insiden Siber Kebocoran Data Pribadi." *Technology and Economics Law Journal* 5, no. 1 (2026): Article 5. <https://doi.org/10.21143/TELJ.vol5.no1.1075>.
- The 1945 Constitution of the Republic of Indonesia.*
- Yuniarti, Siti. "Perlindungan Hukum Data Pribadi di Indonesia." *Business Economic, Communication, and Social Sciences Journal* 1, no. 1 (2019): 147–154. <https://doi.org/10.21512/becossjournal.v1i1.6030>.