

The Urgency of Regulating Cyber Sovereignty Within the Constitutional Law System to Ensure Digital Sovereignty

Lailatul Kusuma Jatri¹, Fifiana Wisnaeni²

¹Master of Law, Faculty of Law, Diponegoro University

²Faculty of Law, Diponegoro University

ABSTRACT: Global digital transformation has significantly altered the classical paradigm of state sovereignty, including within the constitutional legal system of Indonesia. The state is now required not only to ensure physical security but also to safeguard its sovereignty in the digital domain. The absence of constitutional provisions concerning cyber sovereignty has created a legal vacuum that poses threats to state legitimacy and resilience. This study employs a normative juridical method with a qualitative approach to analyze the urgency and direction of the development of Indonesia's constitutional legal system in accommodating digital sovereignty. The analysis reveals the necessity of constitutional recognition of cyberspace as part of the sovereign territory, the establishment of specialized institutions, and the strengthening of regulations related to data protection and cybersecurity. The regulation of cyber sovereignty is not merely a reactive measure against digital threats, but a manifestation of a rule-of-law-based state that adapts to the digital era. With appropriate constitutional arrangements, Indonesia can enhance its legal standing both nationally and internationally in protecting the integrity of its digital space.

KEYWORDS: Cyber Sovereignty; Constitutional Law; Digital Sovereignty

I. INTRODUCTION

The development of information and communication technology has brought great transformations in various aspects of state life. The state is not only required to be able to guarantee the physical security of its territorial territory, but also to uphold sovereignty in digital or cyber space.¹ Departing from the condition *of a quo*, then there is the urgency of regulating cyber sovereignty as an integral part of the modern Constitutional Law (HTN) system.²

Normatively, Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia states that Indonesia is a state of law. The implication of this norm is that all state activities, including in the digital realm, must be based on the law. However, until now, there has been no explicit or systematic constitutional regulation regarding cyber sovereignty in Indonesia's HTN system.³ The absence of this regulation creates a legal *vacuum* that risks weakening the country's position in the face of cross-border cyber threats and digital attacks that can have a serious impact on national stability.⁴

Cyber sovereignty basically refers to the exclusive authority of a country in regulating and protecting its digital space, including internet networks, data, digital infrastructure, and cyber activities that occur within its jurisdiction.⁵ The state has the right and obligation to ensure that digital spaces are used for national interests, not infiltrated by foreign actors that can harm the

¹ Muhammad Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]," *Jurnal Politika Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13, no. 2 (2023): 222–38, <https://doi.org/10.22212/jp.v13i2.3299>.

² Wahyu Beny Mukti Setiawan dkk., *Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia*, t.t.

³ Dery Ardianto dkk., "Pengaturan Keamanan Jaringan dan Kejahatan Siber dalam Hukum IT," *POSTULAT* 2, no. 1 (2024): 7–11, <https://doi.org/10.37010/postulat.v2i1.1454>.

⁴ Alief Tanding Pamungkas dkk., "Tracing Legal Regulations in Dealing with Cybercrime in Indonesia: Examining Obstacles and Solutions," *DELICTUM: Jurnal Hukum Pidana Islam* 2, no. 2 (2024): 71–83, <https://doi.org/10.35905/delictum.v2i2.10613>.

⁵ Arief Bakhtiar Darmawan dkk., "Kedaulatan Negara dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook dan Google," *Jurnal Hubungan Internasional* 16, no. 1 (2023): 211–28, <https://doi.org/10.20473/jhi.v16i1.38971>.

The Urgency of Regulating Cyber Sovereignty Within the Constitutional Law System to Ensure Digital Sovereignty

public interest, and are able to guarantee the protection of citizens' personal data as a form of respect for constitutional rights.⁶

The phenomenon of data breaches, the spread of hoaxes, algorithm manipulation by irresponsible entities, and cyberattacks on vital infrastructure owned by the state, such as financial systems, transportation, and public services are real threats that require a quick and structured legal response.⁷ Based on data from the State Cyber and Cryptography Agency (BSSN), Indonesia has experienced more than 3.6 billion cyberattacks over the past five years until mid-2025.⁸ This number shows the high vulnerability of Indonesia's digital space to disturbances that have the potential to damage the country's social, economic, and even political order. However, until now there is no HTN framework that explicitly regulates who has the constitutional authority to protect digital sovereignty.⁹

In the HTN system, the principle of division of power and constitutional supremacy is the main foundation in determining the authority and responsibility of state institutions.¹⁰ Therefore, it is important to review the extent to which Indonesia's current constitutional structure is able to accommodate and accommodate the issue of digital sovereignty constitutionally.

Although Law No. 27 of 2022 on Personal Data Protection (PDP Law) and a number of other technical regulations have been born, it is not enough to guarantee the country's constitutional position in maintaining its cyber sovereignty.¹¹ The PDP Law focuses more on individual protection, not on the constitutional structure of the state in managing and maintaining the national digital space.¹² Thus, there is an urgency to encourage a more comprehensive and constitutional regulation in HTN regarding digital sovereignty.¹³

The regulation of digital sovereignty in HTN will also strengthen Indonesia's position in the global arena regarding the right to data and digital sovereignty.¹⁴ In an era of data globalization and cross-border digital system interconnection, countries that do not have strong legal legitimacy at the constitutional level will find it difficult to fight for their sovereignty at the international level.¹⁵ Therefore, an HTN design is needed that ensures the existence of the principle of digital sovereignty as a derivative of the principle of people's sovereignty and constitutional supremacy.¹⁶

II. RESEARCH METHODS

This study uses a normative juridical method with a qualitative approach to analyze the urgency of regulating cyber sovereignty in the Indonesian HTN system. The study was conducted through the examination of legal documents such as laws and regulations, court decisions, and legal literature related to digital sovereignty and HTN. In addition, secondary data from official reports such as the State Cyber and Cryptography Agency (BSSN) is used to strengthen analysis of cyber threats. This method aims to produce an in-depth legal understanding and constitutional recommendations to strengthen the regulation of digital sovereignty in order to maintain the legitimacy and security of the state in the digital era.

III. RESULT AND DISCUSSION

The Urgency of Regulating Cyber Sovereignty in Indonesia's Constitutional Law System (HTN) in the Era of Digital Transformation

The advancement of information technology has driven major changes in the social, economic, and government structure of

⁶ Kadek Rima Anggen Suari dan I Made Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–42, <https://doi.org/10.38043/jah.v6i1.4484>.

⁷ Muhammad Izzar Damargara dkk., *Urgensi Realisasi Pengaturan Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi*, 10 (2022).

⁸ Defara Dhanya, "BSSN Catat 3,64 Miliar Serangan Siber di Indonesia Setengah Tahun Ini," Article, TEMPO, Agustus 2025, <https://www.tempo.co/digital/bssn-catat-3-64-miliar-serangan-siber-di-indonesia-setengah-tahun-ini-2056396>.

⁹ Febri Jaya Dan Wilton Goh, "Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia," *SUPREMASI HUKUM* 17, no. 02 (2021): 01–11, <https://doi.org/10.33592/jsh.v17i2.1287>.

¹⁰ Febra Anjar Kusuma dkk., "Analisis Peran Konstitusi Dalam Sistem Hukum Tata Negara," *Indonesian Journal of Law and Justice* 2, no. 2 (2024), <https://doi.org/10.47134/ijlj.v2i2.3400>.

¹¹ Juan Matheus dan Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU," *JUSTISI* 10, no. 1 (2023): 20–35, <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.

¹² Cindy Gladys Pratiwi Sianturi dkk., *Peran Hukum Dalam Melindungi Data Pribadi*, t.t.

¹³ Febri Jaya dan Wilton Goh, "Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia," *SUPREMASI HUKUM* 17, no. 02 (2021): 01–11, <https://doi.org/10.33592/jsh.v17i2.1287>.

¹⁴ Siti Yuniarti, "Analisis Hukum Kedaulatan Digital Indonesia," . . *Number* 15, no. 2 (2020).

¹⁵ Lazarus, *Pengaruh Teknologi dan Globalisasi Terhadap Sistem Hukum dan Identitas Sosial Masyarakat*, Zenodo, 16 Juni 2024, <https://doi.org/10.5281/ZENODO.11782822>.

¹⁶ Wahyu Beny Mukti Setiawan dkk., *Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia*, t.t.

The Urgency of Regulating Cyber Sovereignty Within the Constitutional Law System to Ensure Digital Sovereignty

the country.¹⁷ The advancement of information technology has driven major changes in the social, economic, and government structure of the country.¹⁸ This creates a new challenge to the classic concept of state sovereignty that has been based on physical territoriality. In the context of HTN, this requires an adjustment of the sovereignty paradigm to accommodate the dynamics of cyberspace as a new public space that must also be guaranteed by the state of law.

In practice, the state is not only required to defend its geographical boundaries from external threats, but must also be able to protect its citizens and state systems from digital attacks, data theft, disinformation, sabotage of public information systems, and other forms of cyber threats.¹⁹ Therefore, there is an urgent need to reinterpret the principle of sovereignty in the context of the digital era, as well as construct its regulation systematically within the framework of HTN Indonesia.

Reality shows that cyber threats to the state are no longer theoretical. These types of attacks include *malware*, *phishing*, *ransomware*, and exploitation of security loopholes that can disrupt the stability of the country and threaten national interests.²⁰ The State Cyber and Cryptography Agency (BSSN) reported that in 2024 there will be 2,487,041 *Advanced Persistent Threat* (APT) activities, 514,508 *Ransomware* activities and 26,771,610 *phishing activities*.²¹ Based on *the a quo conditions*, it can be seen that the intensity and complexity of cyberattacks have reached a level that demands a much stronger legal and institutional response. These attacks not only cause economic losses, but also have the potential to weaken government functions that are vital to the country's sustainability. Thus, strengthening the constitutional legal framework in dealing with cyber threats is an urgent need that cannot be delayed. Countries must have clear constitutional legitimacy to act quickly, measurably, and legitimately in protecting strategic digital infrastructure. Without a solid constitutional foundation, the state's response to cyber threats risks being ineffective and may even lead to new legal issues that disrupt the stability of national governance.

Cyber threats are not only technical, but also have an impact on the legitimacy of the state in the eyes of the people.²² When a state is unable to protect the personal data of its citizens, ensure the security of the government's digital systems, or fight disinformation that divides society, then the principle of the rule of law becomes questionable. In this context, HTN is required not only to be normative, but also responsive to the times. For example, in 2021, there was a data leak incident that affected around 279 million Indonesians²³, where the leaked information includes data from BPJS Kesehatan. The Ministry of Communication and Information Technology (Kominfo) corroborates the allegation that the source of the leak came from BPJS Kesehatan. The information that is disseminated includes names, phone numbers, residential addresses, salary amounts, and other population data. This hack not only harms citizens' constitutional right to privacy, but also exposes the weak state regulation and institutions in ensuring cyber protection. Within the framework of HTN, this shows that the structure and function of the state in the digital space still does not have sufficient legitimacy and legal framework.

Although Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) and Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) have provided a legal basis related to digital activities and data protection, both have not touched on aspects of state sovereignty systematically.²⁴ The absence of constitutional norms or even HTN that explicitly regulates who is authoritative, how the control mechanism, and the principles of digital space protection as part of national sovereignty are gaps that need to be filled immediately. Regulatory vacuums have the potential to create uncertainty in the implementation of state functions, especially when faced with cyber emergency situations that require a quick and coordinated response. Without constitutional clarity on the authority structure, efforts to address digital threats can lead to overlapping jurisdictions between state agencies and undermine policy effectiveness. Therefore, the formulation of digital sovereignty norms in HTN is a must to ensure that there is a legal and accountable mechanism in line with the principles of the rule of law.

Indonesia's HTN system currently does not clearly define the boundaries of digital sovereignty jurisdiction. There is no provision in the 1945 Constitution of the Republic of Indonesia (1945 Constitution of the Republic of Indonesia) that stipulates cyberspace as part of the object of state protection. Similarly, no state institution has been constitutionally mandated to carry out the function of supervision and protection of digital sovereignty. This creates institutional ambiguity and is prone to overlapping authority.

¹⁷ Heru Sulistiyo dkk., "Government Performance Pada Kebijakan Transformasi Digital: Bagaimana Transformation Capability Mempengaruhinya? (Studi Empiris Di Provinsi Maluku Utara)," *Jurnal Kebijakan Pemerintahan*, 28 Desember 2023, 95–113, <https://doi.org/10.33701/jkp.v6i2.3679>.

¹⁸ Tri Andika, "Kedaulatan Di Bidang Informasi Dalam Era Digital: Tinjauan Teori Dan Hukum Internasional," *Jurnal Bina Mulia Hukum* 1 (2016).

¹⁹ Wahyu Yudhayana, dkk, *Yudhagama (Media Informasi dan Komunikasi TNI-AD)*, Maret 2025.

²⁰ Sandi Jaelani, *Peran Klasifikasi Serangan Sistem Informasidalam Memperkuat Keamanan Nasional Danmemerangi Cyberwarfare*, no. 3 (2024).

²¹ Letjen Tni dan Hinsia Siburian, *LANSKAP KEAMANAN SIBER 2024*, no. 70 (2024).

²² Faiz Emery Muhammad dan Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web," *JURNAL USM LAW REVIEW* 6, no. 1 (2023): 226–41, <https://doi.org/10.26623/julr.v6i1.6649>.

²³ BBC News Indonesia, "BPJS Kesehatan: Data ratusan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat', kata pakar," News, BBC News, Mei 2021, <https://www.bbc.com/indonesia/indonesia-57196905>.

²⁴ Muhammad Taufik Rusydi, *Perbandingan Hukum Siber Indonesia dengan Negara ASEAN: Suatu Kajian Normatif*, t.t.

The Urgency of Regulating Cyber Sovereignty Within the Constitutional Law System to Ensure Digital Sovereignty

In addition, the separation between aspects of digital security and the protection of constitutional rights has not yet been explicitly formulated in the framework of national regulations. The unclear boundaries have the potential to cause overlapping authorities and open up space for state actions that go beyond the principle of limiting power. On the other hand, the increasingly complex development of cyber threats requires countries to comprehensively strengthen digital security instruments. However, such strengthening measures should not be carried out by ignoring the state's obligation to maintain freedom of expression, the right to information, and the right to privacy of citizens. From HTN's perspective, the state is obliged to ensure that every cybersecurity policy remains within the constitutional corridor and the principles of the state of law. Therefore, the concept of digital sovereignty regulated in the national legal system must be structured by affirming the balance between the state's protective function and respect for constitutional human rights. This balance is needed so that digital security policies do not become a tool of justification for the practice of disproportionate restriction of rights. Thus, the formulation of digital sovereignty based on the principles of prudence and human rights protection is an important prerequisite for the realization of legitimate and accountable cyber governance.

The paradigm change in state sovereignty in the digital era requires a reformulation of HTN norms.²⁵ In this case, basic principles such as constitutional supremacy, power-sharing, and protection of constitutional rights must be integrated with emerging issues such as digital rights, cyber jurisdiction, and national data policy. The state needs to design an HTN system that includes: 1) constitutional recognition of digital space as a state sovereign territory; 2) the establishment of constitutionally valid institutions to manage, protect, and supervise digital activities; 3) guarantee the protection of citizens' digital rights as part of constitutional rights that must not be violated; 4) limiting state power in the digital space so as not to cause abuse of power or human rights violations.

Without this reformulation, the state will always lag behind in responding to cyber threats and have difficulty carrying out its function as a protector of the people in the digital realm. Furthermore, the state's absence in cyberspace has the potential to cause public distrust and weaken the legitimacy of constitutional power.²⁶

Some countries have begun drafting HTN policies that explicitly recognize and regulate digital sovereignty. The People's Republic of China, for example, in the 2017 Cybersecurity Law establishes the state as the primary holder of control over digital infrastructure and data flows within its territory.²⁷ Meanwhile, the European Union emphasizes the principle of digital *constitutionalism*, which is the placement of digital rights as an integral part of human rights.²⁸ These models provide important lessons for Indonesia to form its own approach that is contextual with the presidential system and constitutional structure based on the 1945 Constitution. Indonesia's approach should be rooted in the principles of people's sovereignty, social justice, and protection of human dignity, which are tailored to national digital challenges.

The regulation of cyber sovereignty in the HTN system is not just a response to increasing cyberattacks, but is part of the realization of a modern legal state that is adaptive to the changing times. With constitutional recognition and systematic regulation, states can: 1) strengthen their legal position in international relations on digital cross-border issues; 2) protect citizens from violations of digital rights by foreign and domestic actors; 3) ensuring the accountability of state institutions in the management of the digital space; 4) provide legal certainty in data governance, algorithms, and artificial intelligence.

Thus, the urgency of regulating cyber sovereignty in the HTN system cannot be ignored. This is the demand of the times as well as a constitutional need to maintain the sustainability and legitimacy of the Indonesian state in entering the era of a digital society.

Development of a Constitutional Law System (HTN) to Accommodate the Needs of Digital Sovereignty Regulations in the Era of Global Cyber Transformation

Global digital transformation has changed the traditional paradigm of state sovereignty. Digital sovereignty is now a strategic issue that includes control over data, digital infrastructure, and information technology regulation.²⁹ In this context, Indonesia's HTN system needs to be developed to accommodate the increasingly complex needs of digital sovereignty regulation.

Digital sovereignty is defined as the ability of a state to regulate and protect the data, infrastructure, and digital activities of its citizens without foreign intervention. This includes aspects such as personal data protection, cybersecurity, and regulation of digital platforms. Countries like the European Union have adopted a proactive approach through regulations such as *the General*

²⁵ Nurul Hidayah dkk., "Reformasi Hukum Tata Negara Di Indonesia: Kritik Dan Prospek Untuk Perbaikan," *Jurnal Dunia Ilmu Hukum (JURDIKUM)* 2, no. 1 (2024): 04–08, <https://doi.org/10.59435/jurdikum.v2i1.83>.

²⁶ Alief Tanding Pamungkas dkk., "The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions," *DELICTUM: Jurnal Hukum Pidana Islam* 2, no. 2 (2024): 71–83, <https://doi.org/10.35905/delictum.v2i2.10613>.

²⁷ Maud Descamps, *China's Cybersecurity Legislation*, 2020.

²⁸ Pier Giorgio Chiara, "Towards a Right to Cybersecurity in EU Law? The Challenges Ahead," *Computer Law & Security Review* 53 (Juli 2024): 105961, <https://doi.org/10.1016/j.clsr.2024.105961>.

²⁹ Nanang Subekti dan Arief Hidayat, *Konstitusionalisme Digital di Indonesia: Mengartikulasikan Hak dan Kekuasaan di Era Digital*, t.t.

The Urgency of Regulating Cyber Sovereignty Within the Constitutional Law System to Ensure Digital Sovereignty

Data Protection Regulation (GDPR) and *the Digital Services Act (DSA)* to enforce their digital sovereignty.³⁰

Indonesia faces various challenges in upholding digital sovereignty. Indonesia's dependence on foreign digital infrastructure remains a serious challenge in maintaining national data sovereignty.³¹ Many digital services and data storage centers are still located abroad, which opens up potential risks to the control and security of data belonging to citizens and strategic institutions. This dependence can limit the government's ability to ensure that the digital data of the Indonesian people is fully managed in accordance with national interests and the principles of state sovereignty.

On the other hand, even though Law No. 27 of 2022 concerning Personal Data Protection has been issued, its implementation still faces various obstacles. These obstacles include a lack of public understanding of the importance of personal data protection.³² In addition, the limited capacity of institutions to supervise and enforce regulations consistently is also an undeniable challenge. Without increasing awareness and strengthening institutions, the effectiveness of legal protection of personal data has not been optimally achieved.

Threats to cybersecurity are also increasing, marked by the rise of hacks, data theft, and ransomware attacks. This situation demands a more integrated and comprehensive response, both in terms of regulation and technical readiness. In the midst of this dynamic, coordination between government agencies, the private sector, and civil society is critical to building a resilient and sovereign digital ecosystem. Cross-sectoral collaboration is needed so that the management of digital sovereignty issues can be carried out effectively and sustainably.

The lack of synergy between institutions in managing digital sovereignty issues creates a gap that can be exploited by various threats, both from within and outside the country. To build a secure and sovereign digital ecosystem, a structured and inclusive coordination mechanism is needed, involving not only the government as a regulator, but also the private sector as a service provider and civil society as users as well as supervisors. This cross-sector collaboration is not only about sharing roles, but also about forming a common vision in maintaining the integrity and independence of the national digital space.

Several countries have succeeded in developing a comprehensive legal framework in regulating data and digital space, which can be used as a reference for Indonesia in building its digital sovereignty. For example, the European Union sets high standards through policies such as GDPR and DSA that emphasize transparency, accountability, and the protection of user rights in the digital ecosystem. Meanwhile, China is taking a stricter approach with dominant state oversight of data and digital infrastructure through various regulations, which shows how strong controls can be a strategic tool in maintaining cyber sovereignty.³³

To realize sustainable digital sovereignty, Indonesia needs to carry out fundamental reforms in its legal system. One strategic step is to incorporate the principles of digital sovereignty into the constitution or constitution. With a strong legal foundation, the state will have a clear foothold in setting policies and taking action against various challenges in the digital realm, both in terms of security, data protection, and supervision of cross-border digital activities.

In addition to constitutional reform, strengthening regulations is also crucial. The government needs to design and improve regulations that regulate personal data protection, cybersecurity, and the comprehensive management of *digital platforms*. In this process, it is important to adopt best practices from countries that have already successfully built effective digital regulatory systems. Harmonization with global standards can also open up opportunities for international cooperation in terms of data protection and use in a fair and safe manner.

The next step is to increase institutional capacity, especially for institutions that have a strategic role in the digital field, such as the State Cyber and Cryptography Agency (BSSN). These institutions need to be supported through continuous training, adequate budget allocation, and expanded authority to ensure the effectiveness of their work in addressing national digital issues. Without strengthening institutions, existing policies and regulations will be difficult to implement optimally.

On the other hand, the involvement of various parties should be strengthened through a collaborative approach that systematically involves the private sector, academia, and civil society. This collaborative approach is important because digital issues are multidimensional and cannot be solved through state intervention alone. Multistakeholder collaboration is needed so that the digital policies formulated are not only on the side of one interest, but are able to reflect the needs and aspirations of all elements of society. The involvement of various actors also serves as a mechanism of public oversight that can prevent the dominance of certain groups in the policy formulation process. In addition, an open dialogue between the government and stakeholders will enrich perspectives in understanding the social, economic, and legal impacts of a digital regulation. The active

³⁰ Yohanes Hermanto Sirait, "General Data Protection Regulation (Gdpr) Dan Kedaulatan Negara Non-Uni Eropa," *Gorontalo Law Review* 2, no. 2 (2019): 60, <https://doi.org/10.32662/golrev.v2i2.704>.

³¹ Tri Bagus Prabowo dan Rezya Agnesica Sihalo, "Analisis Ketergantungan Indonesia Pada Teknologi Asing Dalam Sektor Energi dan Dampaknya Pada Keamanan Nasional," *Jurnal Lemhannas RI* 11, no. 1 (2023): 72–82, <https://doi.org/10.55960/jlri.v11i1.426>.

³² Trias Palupi Kurnianingrum, *Urgensi Pelindungan Data Pribadi Konsumen Di Era Ekonomi Digital*, 25, No. 3 (2020).

³³ Faqih Albiruni Yahya dan R.Tuty Nur Mutia, "The Great Firewall of China: Praktik Kebijakan Sensor Internet Pada Era Xi Jinping," *Historia: Jurnal Pendidik dan Peneliti Sejarah* 6, no. 1 (2023): 13–24, <https://doi.org/10.17509/historia.v6i1.50007>.

The Urgency of Regulating Cyber Sovereignty Within the Constitutional Law System to Ensure Digital Sovereignty

participation of civil society can encourage transparency and increase the legitimacy of the resulting policies. With a comprehensive range of inputs, digital policies can be structured in a more inclusive, proportionate, and sensitive manner to changing times. Thus, strengthening multistakeholder collaboration is an important prerequisite for the realization of democratic and accountable digital governance.

Finally, efforts to strengthen digital sovereignty will not achieve effective results without the support of a community that has a high level of awareness about the importance of digital rights, privacy, and cybersecurity. This awareness is the main foundation for the creation of a digital ecosystem that is safe, ethical, and in line with the principles of the rule of law. Therefore, digital education and literacy must be placed as an integral part of the national strategy in building sustainable cyber resilience. Adequate digital literacy not only increases the capacity of individuals to understand digital risks, but also strengthens people's ability to participate critically in the digital public space. Through formal education programs, relevant curricula can be developed to instill an understanding of personal data protection and the ethics of using technology from an early age. In addition, intensive public campaigns are needed to reach out to community groups that are not accommodated in the formal education system. The public must be given practical knowledge on how to protect personal data, recognize various forms of cyber threats, and use technology responsibly and safely. Thus, increasing people's digital literacy is one of the important pillars in ensuring the success of strengthening digital sovereignty at the national level.

Digital sovereignty is a crucial aspect in the era of cyber transformation which requires countries to be able to control their digital space independently. In this context, Indonesia is faced with an urgent need to build an HTN system that is adaptive and responsive to the dynamics of information technology that is developing very quickly. The adaptive legal system must be designed by integrating the principle of personal data protection as the main foundation for the protection of citizens' digital rights. In addition, strengthening the cybersecurity regime is also an essential element to ensure that every digital activity takes place within a safe framework and free from external threats. Protection of digital rights, including access to information, privacy, and freedom of expression, must be guaranteed through clear and accountable legal mechanisms. These efforts can only be achieved through comprehensive legal reform and strengthening of institutions that have adequate technical capacity and authority. In addition, multistakeholder collaboration involving the government, the private sector, academia, and civil society is a prerequisite for the creation of inclusive and legitimate digital governance. Thus, Indonesia can enforce digital sovereignty effectively, sustainably, and in accordance with the principles of the modern state of law.

IV. CONCLUSIONS

Cyber sovereignty is an expansion of state sovereignty that is urgent to be regulated in the Indonesian Constitutional Law system to face threats and challenges in the digital era. Currently, there is no explicit recognition in the constitution of digital space as part of the state's jurisdiction, thus creating a legal vacuum. Constitutional reform and institutional strengthening are needed so that the state is able to protect data, digital infrastructure, and citizens' digital rights. With clear arrangements, Indonesia can maintain national integrity while realizing a sovereign and secure digital democracy.

REFERENCES

- 1) Aji, Muhammad Prakoso. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]." *Jurnal Politika Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13, no. 2 (2023): 222–38. <https://doi.org/10.22212/jp.v13i2.3299>.
- 2) Alief Tanding Pamungkas, Andi Mulyono, dan Nurjana Lahangatubun. "The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions." *DELICTUM : Jurnal Hukum Pidana Islam* 2, no. 2 (2024): 71–83. <https://doi.org/10.35905/delictum.v2i2.10613>.
- 3) Alief Tanding Pamungkas, Andi Mulyono, dan Nurjana Lahangatubun. "Tracing Legal Regulations in Dealing with Cybercrime in Indonesia: Examining Obstacles and Solutions." *DELICTUM : Jurnal Hukum Pidana Islam* 2, no. 2 (2024): 71–83. <https://doi.org/10.35905/delictum.v2i2.10613>.
- 4) Andika, Tri. "Kedaulatan Di Bidang Informasi Dalam Era Digital: Tinjauan Teori Dan Hukum Internasional." *Jurnal Bina Mulia Hukum* 1 (2016).
- 5) Anggen Suari, Kadek Rima, dan I Made Sarjana. "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–42. <https://doi.org/10.38043/jah.v6i1.4484>.
- 6) Ardianto, Dery, Mas Agus Priyambodo, dan Fikrotul Jadidah. "Pengaturan Keamanan Jaringan dan Kejahatan Siber dalam Hukum IT." *POSTULAT* 2, no. 1 (2024): 7–11. <https://doi.org/10.37010/postulat.v2i1.1454>.
- 7) Chiara, Pier Giorgio. "Towards a Right to Cybersecurity in EU Law? The Challenges Ahead." *Computer Law & Security Review* 53 (Juli 2024): 105961. <https://doi.org/10.1016/j.clsr.2024.105961>.
- 8) Creemers, Rogier. "The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy." *Journal of Contemporary China* 33, no. 146 (2024): 173–88. <https://doi.org/10.1080/10670564.2023.2196508>.

- 9) Damargara, Muhammad Izzar, Muhammad Alhidayah, dan Muhammad Raihan Faiqy. *Urgensi Realisasi Pengaturan Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi*. 10 (2022).
- 10) Darmawan, Arief Bakhtiar, Kholifatut Saadah, dan I Putu Arya Aditia Utama. “Kedaulatan Negara dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook dan Google.” *Jurnal Hubungan Internasional* 16, no. 1 (2023): 211–28. <https://doi.org/10.20473/jhi.v16i1.38971>.
- 11) De Gregorio, Giovanni, dan 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>.
- 12) Descamps, Maud. *China’s Cybersecurity Legislation*: 2020.
- 13) Dhanya, Defara. “BSSN Catat 3,64 Miliar Serangan Siber di Indonesia Setengah Tahun Ini.” Article. TEMPO, Agustus 2025. <https://www.tempo.co/digital/bssn-catat-3-64-miliar-serangan-siber-di-indonesia-setengah-tahun-ini-2056396>.
- 14) Febra Anjar Kusuma, Dini Apriliani, Rezky Tania, Susan Febriyanti, dan Rozalia. “Analisis Peran Konstitusi Dalam Sistem Hukum Tata Negara.” *Indonesian Journal of Law and Justice* 2, no. 2 (2024). <https://doi.org/10.47134/ijlj.v2i2.3400>.
- 15) Indonesia, BBC News. “BPJS Kesehatan: Data ratusan juta peserta diduga bocor - ‘Otomatis yang dirugikan masyarakat’, kata pakar.” News. BBC News, Mei 2021. <https://www.bbc.com/indonesia/indonesia-57196905>.
- 16) Jaelani, Sandi. *Peran Klasifikasi Serangan Sistem Informasidalam Memperkuat Keamanan Nasional Danmemerangi Cyberwarfare*. no. 3 (2024).
- 17) Jaya, Febri, dan Wilton Goh. “Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia.” *SUPREMASI HUKUM* 17, no. 02 (2021): 01–11. <https://doi.org/10.33592/jsh.v17i2.1287>.
- 18) Jaya, Febri, dan Wilton Goh. “Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia.” *SUPREMASI HUKUM* 17, no. 02 (2021): 01–11. <https://doi.org/10.33592/jsh.v17i2.1287>.
- 19) Kurnianingrum, Trias Palupi. *Urgensi Pelindungan Data Pribadi Konsumen Di Era Ekonomi Digital*. 25, no. 3 (2020).
- 20) Lazarus. *Pengaruh Teknologi dan Globalisasi Terhadap Sistem Hukum dan Identitas Sosial Masyarakat*. Zenodo, 16 Juni 2024. <https://doi.org/10.5281/ZENODO.11782822>.
- 21) Matheus, Juan, dan Ariawan Gunadi. “Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU.” *JUSTISI* 10, no. 1 (2023): 20–35. <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.
- 22) Muhammad, Faiz Emery, dan Beniharmoni Harefa. “Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web.” *JURNAL USM LAW REVIEW* 6, no. 1 (2023): 226–41. <https://doi.org/10.26623/julr.v6i1.6649>.
- 23) Nurul Hidayah, Syabrina Az-Jahra, Aprillia Amanda, dan Karina Yunitasari. “Reformasi Hukum Tata Negara Di Indonesia: Kritik Dan Prospek Untuk Perbaikan.” *Jurnal Dunia Ilmu Hukum (JURDIKUM)* 2, no. 1 (2024): 04–08. <https://doi.org/10.59435/jurdikum.v2i1.83>.
- 24) Rusydi, Muhammad Taufik. *Perbandingan Hukum Siber Indonesia dengan Negara ASEAN: Suatu Kajian Normatif*. t.t.
- 25) Setiawan, Wahyu Beny Mukti, Erifendi Churniawan, dan Femmy Silaswaty Faried. *Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia*. t.t.
- 26) Sianturi, Cindy Gladys Pratiwi, Roida Nababan, dan Ria Juliana Siregar. *Peran Hukum Dalam Melindungi Data Pribadi*. t.t.
- 27) Sirait, Yohanes Hermanto. “General Data Protection Regulation (Gdpr) Dan Kedaulatan Negara Non-Uni Eropa.” *Gorontalo Law Review* 2, no. 2 (2019): 60. <https://doi.org/10.32662/golrev.v2i2.704>.
- 28) Subekti, Nanang, dan Arief Hidayat. *Konstitusionalisme Digital di Indonesia: Mengartikulasikan Hak dan Kekuasaan di Era Digital*. t.t.
- 29) Sulistiyo, Heru, Aleknaek Martua, Sayuti Sayuti, Mulyana Mulyana, dan Irka Tia Ginting. “Government Performance Pada Kebijakan Transformasi Digital: Bagaimana Transformation Capability Mempengaruhinya? (Studi Empiris Di Provinsi Maluku Utara).” *Jurnal Kebijakan Pemerintahan*, 28 Desember 2023, 95–113. <https://doi.org/10.33701/jkp.v6i2.3679>.
- 30) Tni, Letjen, dan Hinsa Siburian. *LANSKAP KEAMANAN SIBER 2024*. no. 70 (2024).
- 31) Tri Bagus Prabowo dan Rezya Agnesica Sihalo. “Analisis Ketergantungan Indonesia Pada Teknologi Asing Dalam Sektor Energi dan Dampaknya Pada Keamanan Nasional.” *Jurnal Lemhannas RI* 11, no. 1 (2023): 72–82. <https://doi.org/10.55960/jlri.v11i1.426>.
- 32) Yahya, Faqih Albiruni, dan R.Tuty Nur Mutia. “The Great Firewall of China: Praktik Kebijakan Sensor Internet Pada Era Xi Jinping.” *Historia: Jurnal Pendidik dan Peneliti Sejarah* 6, no. 1 (2023): 13–24. <https://doi.org/10.17509/historia.v6i1.50007>.
- 33) Yudhayana, dkk, Wahyu. *Yudhagama (Media Informasi dan Komunikasi TNI-AD)*. Maret 2025.
- 34) Yuniarti, Siti. “Analisis Hukum Kedaulatan Digital Indonesia.” . . *Number* 15, no. 2 (2020).