DOMAIN .go.id AS A VITAL DIGITAL OBJECT: ANALYSIS OF THE ENHANCEMENT OF CRIMINAL SANCTIONS IN THE ITE LAW

Abdurrahman

Fakultas Hukum, Universitas Sriwijaya, Indonesia

Email: abdurrahman@fh.unsri.ac.id

Info Artikel

Masuk: 09-11-2025
Diterima: 24-12-2025
Terbit: 25-12-2025

Keywords:
.go.id Domain, Digital Vital Object, UU ITE, Criminal Sanctions, Digital Governance.

Abstract

This study aims to analyze the position of the .go.id domain as a Vital Digital Object from a national legal perspective and examine the provisions of enhanced criminal sanctions for cybercrimes that attack the .go.id domain based on the Electronic Information and Transactions Law (UU ITE). The .go.id domain not only functions as the technical identity of government websites, but also has a strategic role in government administration, public services, and the realization of the country's digital sovereignty. This study uses a normative legal research method with a statute approach and a conceptual approach. The analysis was carried out on relevant laws and regulations, legal doctrines, and the concept of national vital objects and digital infrastructure protection in the Indonesian legal system. The results of the study indicate that as the country's dependence on digital systems increases, the concept of national vital objects has expanded to include non-physical assets in the form of electronic systems and strategic digital infrastructure. The .go.id domain can be qualified as a Vital Digital Object because of its direct relationship with the government administration sector and information and communication technology, as regulated in Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure. The provisions on increased criminal sanctions for cyber attacks on the .go.id domain in the ITE Law serve as a preventive and repressive legal instrument that strengthens the protection of government electronic systems while safeguarding the country's digital sovereignty.

Kata kunci:
domain .go.id, Objek Vital Digital, UU ITE, Sanksi Pidana, Pemerintahan Digital

Corresponding Author:
Abdurrahman, E-mail: abdurrahman@fh.unsri.ac.id

Intisari

Penelitian ini bertujuan untuk menganalisis kedudukan domain .go.id sebagai Objek Vital Digital dalam perspektif hukum nasional serta mengkaji pengaturan sanksi pidana yang diperberat terhadap tindak pidana siber yang menyerang domain .go.id berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Domain .go.id tidak hanya berfungsi sebagai identitas teknis situs web pemerintah, tetapi juga memiliki peran strategis dalam administrasi pemerintahan, pelayanan publik, dan perwujudan kedaulatan digital negara.Penelitian ini menggunakan metode penelitian hukum normatif dengan

pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Analisis dilakukan terhadap peraturan perundang-undangan yang relevan, doktrin hukum, serta konsep objek vital nasional dan perlindungan infrastruktur digital dalam sistem hukum Indonesia.Hasil penelitian menunjukkan bahwa seiring meningkatnya ketergantungan negara terhadap sistem digital, konsep objek vital nasional mengalami perluasan yang mencakup aset nonfisik berupa sistem elektronik dan infrastruktur digital strategis. Domain .go.id dapat dikualifikasikan sebagai Objek Vital Digital karena keterkaitannya yang langsung dengan sektor administrasi pemerintahan serta teknologi informasi dan komunikasi, sebagaimana diatur dalam Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital. Pengaturan sanksi pidana yang diperberat terhadap serangan siber atas domain .go.id dalam UU ITE berfungsi sebagai instrumen hukum preventif dan represif yang memperkuat perlindungan sistem elektronik pemerintah sekaligus menjaga kedaulatan digital negara.

.

1. Introduction

The development of information and communication technology has driven a significant transformation in government governance towards a digital-based system (Hibatullah, 2024; Kamil et al., 2024; Supriadi et al., 2024; Yuliana & Natalia, 2025). The Indonesian government has adopted the use of the internet as a means of increasing transparency, efficiency, and the quality of public services, one of which is realized through the use of official government domain names with the suffix .go.id (Rizky et al., 2025). This domain not only functions as the technical identity of a government agency website, but also becomes the main medium for implementing e-government and a symbol of state legitimacy in the digital space (Rusmini et al., 2025; H. Tan et al., 2022). According to Regulation of the Minister of Communication and Digital of the Republic of Indonesia Number 5 of 2025, a domain name is a unique address that reflects the authority and legitimacy of an institution in communicating on the internet. Therefore, the existence of the.go.id domain has strategic value closely related to government administration, public services, and the country's digital sovereignty.

Various previous studies on national vital objects generally still focus on physical assets such as energy facilities, transportation, and strategic state installations as regulated in Presidential Decree Number 63 of 2004 concerning the Security of National Vital

Objects (Daryono et al., 2023; Eng et al., 2024). As reliance on digital systems increases, a number of studies are beginning to highlight the importance of protecting digital infrastructure, particularly electronic government systems (Maisarah et al., 2025; Salam et al., 2024; Tommy & Nasution, 2025). However, the study still places electronic systems in general without specifically discussing the position of government agency domains, such as .go.id, as part of national vital objects (Ariprawira et al., 2023; Israyudin et al., 2025; Kartasasmita et al., 2024; Suhendra & Santiko, 2022). To date, explicit recognition of government domains as vital digital objects remains fragmentary and has not been comprehensively integrated into the national legal framework.

Based on these conditions, this study aims to analyze the position of the.go.id domain as a vital digital object from a national legal perspective and examine the criminal sanctions for cybercrimes specifically targeting the.go.id domain, based on Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments. This study seeks to provide conceptual and normative clarity regarding the position of the.go.id domain within the national digital infrastructure protection system, given its crucial role in governance.

This study is based on the argument that the.go.id domain meets the characteristics of a vital digital object because its existence concerns state interests, the livelihoods of the public, and has the potential to cause widespread impacts if disrupted. Cyberattacks against the.go.id domain, such as hacking, domain forgery, or system disruptions, not only result in technical damage but also threaten public trust and the stability of digital governance. Meanwhile, the norms in the ITE Law are still general and do not provide special treatment for state-owned electronic systems of high strategic value. Therefore, a legal construction is needed that places the.go.id domain as a vital digital object that receives stronger legal protection, including through the regulation of increased criminal sanctions as a form of preventive and repressive protection for the country's digital sovereignty.

2. Method

This research uses a normative legal research method. (doctrinal legal research) (Negara, 2023). This research focuses on the analysis of positive legal norms, legal

principles, and legal doctrines to address the legal issues under study. This approach was chosen because the research aims to examine legal construction, normative classification, and the consistency of regulations related to the protection of government domains as part of the country's digital infrastructure. This research does not examine empirical behavior, but rather emphasizes legal reasoning regarding relevant laws and legal concepts..

The approaches used include a statutory approach, by systematically and hierarchically analyzing the laws and regulations governing electronic systems, vital infrastructure protection, and cybercrime, as well as a conceptual approach, by examining the concepts, principles, and legal doctrines related to national vital objects, digital sovereignty, and the protection of the country's digital infrastructure (Wicaksono & Yasin, 2024). These two approaches are used in a complementary manner to build a coherent normative argument.

The legal materials used consist of primary legal materials, including Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure. Secondary legal materials were obtained from academic literature in the form of legal textbooks, reputable national and international journal articles, and opinions of legal scholars relevant to the research issues. Tertiary legal materials include legal dictionaries and other non-legal sources that support terminological understanding.

The technique for collecting legal materials is carried out through library-based research with a process of inventory, classification and systematization of legal materials (Poltak & Widjaja, 2024). All collected legal materials were analyzed using normative qualitative analysis through systematic, conceptual, and teleological legal interpretation. The results of the analysis were presented descriptively and analytically to provide structured and academically justifiable legal arguments.

3. Analysis and Discussion

The research results show that conceptually, a domain is a unique digital identity that serves as the primary address for a website on the internet. Domains replace difficult-to-remember numeric IP addresses, facilitating public access to digital services and information. In the context of government, the use of the .go.id domain allows the public

to access official government websites easily, quickly, and reliably, directly supporting the effectiveness of electronic-based communication and public services.

The legal definition of domain names, as stipulated in Article 1, number 20 of the ITE Law, strengthens the position of domains as internet addresses with unique characteristics and function as location indicators in cyberspace. This norm emphasizes that ownership and use of domain names are not limited to private individuals but also include state administrators. Thus, the .go.id domain is part of the government's electronic system, legally subject to state management and protection. Global developments in internet governance, particularly through ICANN's New Generic Top-Level Domain (New gTLD) program, demonstrate that domains are no longer simply geographic markers but also represent specific functions, sectors, and identities. In this context, the.go.id domain specifically represents the authority of the Indonesian government, so it has a broader symbolic and legal meaning than other generic domains.

The research also shows that in the Indonesian domain system, go.id holds a special status compared to other domains such as.co.id, ac.id, or.mil.id. Use of the .go.id domain is exclusively restricted to central and regional government agencies. This restriction emphasizes that the go.id domain is not merely an administrative identity, but rather an instrument of state legitimacy in carrying out government functions and public services in the digital space.

The implementation of electronic government (e-government) since Presidential Instruction Number 6 of 2001 and Presidential Instruction Number 3 of 2003 demonstrates that the .go.id domain is the initial foundation for an integrated government information system. This domain serves as the public's primary gateway to policy information, administrative services, and a channel for public participation, thus determining transparency, accountability, and public trust in the government. The analysis shows that although the concept of National Vital Objects in Presidential Decree Number 63 of 2004 still focuses on physical assets, digital developments have expanded the scope of vital objects to include non-physical assets. Government electronic systems, including the.go.id domain, have strategic value and, if disrupted, could have widespread impacts on government stability, public services, and national security. Therefore, the.go.id domain functionally fulfills the characteristics of a national vital object.

The digital transformation of state administration has also shifted the national

security paradigm from physical protection to information and digital infrastructure protection. The high reliance on electronic systems makes official government domains an integral part of the country's strategic infrastructure. Cyberattacks against the.go.id domain have the potential to disrupt state administrative functions and undermine the legitimacy of public information, placing it on par with vital physical objects.

From a criminal law perspective, the ITE Law stipulates heightened criminal sanctions for disruptions to government electronic systems through Article 52 paragraphs (2) and (3). Research shows that the element of "government electronic systems" normatively includes the .go.id domain, given that the rights to manage and use it are granted exclusively to state-run agencies. Therefore, cyberattacks against the .go.id domain are legally subject to heightened criminal sanctions.

Technical regulations regarding the .go.id domain, both through Regulation of the Minister of Communication and Information Technology Number 28 of 2006 and Regulation of the Minister of Communication and Information Technology Number 5 of 2025, further emphasize that the .go.id domain is the official electronic address of state-run agencies used for government administration and national public services. This provision strengthens the argument that the .go.id domain is a strategic electronic system legally owned by the state.

Based on these findings, this study concludes that the .go.id domain is normatively and functionally worthy of being classified as a Vital Digital Object within the context of national law. The ITE Law's provisions for heightened criminal sanctions against cyberattacks targeting the.go.id domain are an important legal instrument for protecting the public interest, maintaining public trust, and strengthening the country's digital sovereignty. Consistent implementation of these norms by law enforcement officials is key to ensuring effective protection of government digital infrastructure.

Table 1 Finding Research

No.	Main Aspect	Core Findings	Legal Implications
1	Domain Status	The *.go.id* domain constitutes an official digital identity and a government-owned electronic system	Possesses strategic value and legal legitimacy as a state asset
2	Strategic Function	*.go.id* plays a central role in public service delivery and the implementation of e-government	Domain disruptions directly affect administrative operations and public trust
3	Digital Vital Object	The concept of national vital objects has expanded to include non-physical, digital-based assets	*.go.id* is eligible to be classified as a Digital Vital Object
4	Protection Regulation	Presidential Regulation No. 82 of 2022 covers strategic electronic systems in the government and ICT sectors	*.go.id* meets the criteria of Vital Information Infrastructure
5	Criminal Sanctions	Article 52 of the ITE Law provides aggravated penalties for attacks on government electronic systems	Cyberattacks targeting *.go.id* may be subject to enhanced criminal sanctions

Discussion

This research is based on the theory of state interest protection (state interest protection theory) as a grand theory (Block, 1984). This theory positions the state as a legal subject that has a constitutional obligation to protect its strategic interests, including the continuity of government functions, public services, and national stability. (Alimova & Рифатевна, 2024). In the context of the digital era, state interests are no longer limited to protecting physical assets, but extend to non-physical assets in the form of electronic systems and digital infrastructure that support government administration (Riabchenko et al., 2025; Wibowo, 2023). Domain.go.id as the official identity of the government in cyberspace is a concrete representation of state interests whose protection must be guaranteed by law.

This theory is strengthened by the progressive legal theory put forward (Siregar, 2024). Progressive law views law as a means to achieve substantive justice and social welfare, not merely a collection of static norms (Kurniawan & Suyatno, 2025; Suherman,

2025). In the context of this research, progressive law allows for a dynamic interpretation of the concept of national vital objects, thus not being confined to a purely physical approach (Cakal, 2023; Jaeger et al., 2024; Jubaidi & Khoirunnisa, 2023). Although legislation does not explicitly mention the.go.id domain as a national vital object, progressive law provides room for the development of legal meaning to align with the realities of digital transformation and the need to protect the public interest.

As a supporting theory, this research also uses the theory of digital sovereignty (K. L. Tan et al., 2023). This theory emphasizes that the state has the right and authority to regulate, protect, and control digital infrastructure within its jurisdiction. State sovereignty in the digital era is not only manifested through control of physical territory, but also through control of data, electronic systems, and the state's digital identity. Within this framework, the .go.id domain is seen as a symbol of Indonesia's digital sovereignty, reflecting the state's authority in cyberspace.

The use of digital sovereignty theory strengthens the argument that cyberattacks against the .go.id domain constitute a direct threat to state sovereignty, not simply a common cybercrime. Therefore, the legitimacy of enforcing special legal protection, including recognizing the .go.id domain as a vital digital object and imposing enhanced criminal sanctions under the ITE Law, becomes theoretically stronger. By integrating the theories of protecting state interests, progressive law, and digital sovereignty, this study builds a comprehensive analytical framework for assessing the urgency of legal protection for the .go.id domain within the national legal system.

The first finding regarding the position of the .go.id domain as an official digital identity and government-owned electronic system indicates a shift in the meaning of state assets from physical to non-physical, digital-based ones. The .go.id domain serves not only as a technical address but also as a symbol of state authority and legitimacy in cyberspace. This confirms that government domains have legal and strategic value equivalent to other state assets. The legal legitimacy of the .go.id domain as a state asset is reflected in the restrictions on its ownership and use, which are granted only to state-run institutions. This restriction places the .go.id domain within a public, not a private, legal regime. Therefore, any disruption to the .go.id domain must be viewed as a disruption to state interests, not simply a technical violation of the electronic system.

The second finding regarding the strategic function of the .go.id domain

demonstrates its central role in the provision of public services and the implementation of e-government. This domain serves as the primary gateway for interaction between the state and citizens, both in the delivery of policy information and administrative services. Therefore, the stability and security of the .go.id domain have direct implications for the quality of governance and public trust. Disruptions to the .go.id domain, such as hacking or domain forgery, not only cause technical losses but also have the potential to create disinformation, hinder public services, and undermine government legitimacy. This multidimensional impact strengthens the argument that protecting government domains must be prioritized in national security policy in the digital age.

The third finding shows that the concept of national vital objects has undergone significant expansion along with the digital transformation. Vital objects are no longer limited to physical installations but also encompass digital assets that support government functions. In this context, domain.go.id fulfills the characteristics of a vital object because it concerns state interests, public services, and the stability of digital governance. Recognition of domain.go.id as a digital vital object requires a paradigm shift in legal protection. Protection no longer focuses solely on the technical aspects of cybersecurity, but also on legal and institutional aspects. The state needs to ensure that strategic electronic systems receive special treatment, both in security policies and in criminal law enforcement.

The fourth finding, related to Presidential Regulation Number 82 of 2022, shows that the national legal framework has begun to accommodate the protection of vital information infrastructure. By including the government administration and information and communication technology sectors as strategic sectors, this Presidential Regulation implicitly places domain.go.id within the category of Vital Information Infrastructure, which requires special protection. However, the lack of explicit mention of domain.go.id as a digital vital object presents challenges in implementation. This opens up room for differing interpretations among law enforcement officials and policymakers. Therefore, consistency in interpretation and strengthening of derivative regulations are needed so that protection for the .go.id domain can be implemented effectively and uniformly.

The fifth finding regarding the increased criminal sanctions in Article 52 of the ITE Law demonstrates that the Indonesian criminal law system has provided instruments to protect government electronic systems. The increased criminal penalties reflect the state's

recognition of the high strategic value of government electronic systems, including the .go.id domain, which, if attacked, can have widespread impacts on the public interest. However, the effectiveness of these regulations depends heavily on consistent law enforcement. Differences in the application of increased criminal sanctions in judicial practice demonstrate the need to improve the capacity of law enforcement officials to understand the characteristics of cybercrime and the strategic value of government domains. With consistent law enforcement based on an understanding of vital digital objects, protection of the .go.id domain can function optimally in safeguarding the nation's digital sovereignty.The main novelty of this research lies in the conceptual reconstruction of the .go.id domain as a vital digital state object with strategic value equivalent to conventional national vital objects. Unlike previous research, which generally positioned government domains as merely technical instruments in e-government governance or cybersecurity, this study systematically places.go.id within the regime of protecting state interests, integrating theories of state interest protection, progressive law, and digital sovereignty as a unified analytical framework.

Further novelty lies in the progressive interpretation of the concept of national vital objects by extending it to the realm of digital-based non-physical assets. This research demonstrates that digital transformation has shifted the paradigm of legal protection from a physical-territorial approach to a functional-strategic approach. Within this framework, the .go.id domain is no longer understood as a mere technical address, but rather as a symbol of state authority, legitimacy, and sovereignty in cyberspace, the disruption of which has direct implications for government stability and public trust.

Furthermore, this research offers novelty in the normative synchronization between the ITE Law and Presidential Regulation No. 82 of 2022 by placing the .go.id domain as an inherent part of Vital Information Infrastructure, even though it has not been explicitly mentioned in the regulation. This approach produces a new contribution in the form of a legal argument that the increased criminal sanctions in Article 52 of the ITE Law have a strong theoretical and normative basis when applied to cyberattacks on government domains. Thus, the novelty of this research is not only descriptive, but also conceptual and normative, as it offers a new paradigm for legal protection of government domains as vital digital objects while strengthening the theoretical foundation for policy development and law enforcement in the field of national digital sovereignty.

4. Conclusion

This research confirms that the.go.id domain holds a strategic position as the official digital identity and state-owned electronic system that supports government administration and public services. Key findings indicate that digital transformation has expanded the meaning of state assets from physical to digital-based non-physical assets, thus qualifying the.go.id domain as a vital digital asset. Furthermore, this research finds that the national legal framework, specifically Presidential Regulation Number 82 of 2022 and Article 52 of the Electronic Information and Transactions Law, implicitly provides a basis for legal protection for government domains, including through a mechanism for increasing criminal sanctions for cyberattacks that threaten state electronic systems.

This research's contribution is both conceptual and normative. Conceptually, this research enriches legal discourse by reconstructing the.go.id domain as a vital digital asset from the perspective of protecting state interests and digital sovereignty. The integration of theories of state interest protection, progressive law, and digital sovereignty yields a comprehensive analytical framework for understanding the urgency of protecting government domains in the digital era. Normatively, this research contributes legal arguments that strengthen the legitimacy of implementing increased criminal sanctions in the ITE Law for cyberattacks on.go.id domains, while simultaneously encouraging synchronization and strengthening of regulations protecting vital information infrastructure.

However, this research has limitations. It is normative in nature and has not empirically examined law enforcement practices against cybercrimes targeting .go.id domains, including court rulings and implementation obstacles in the field. Furthermore, the analysis has not made an in-depth comparison with government domain protection regimes in other countries. Therefore, further research is recommended that combines empirical and comparative approaches to assess the effectiveness of government domain legal protection and formulate more adaptive policy models to safeguard the nation's digital sovereignty.

5. Reference

Alimova, D. R., & Рифатевна, А. Д. (2024). Legal regulation of national interests in Russia: Theory and practice. *RUDN Journal of Law*, *28*(4), 730–742. https://doi.org/10.22363/2313-2337-2024-28-4-730-742

Ariprawira, G., Aji, L. S., Wahyudin, A., & Hikmaturokhman, A. (2023). Policy Mechanism for Security of National Vital Objects in the Telecommunications Sector in Indonesia. *Buletin Pos Dan Telekomunikasi*, *21*(2), 57–73. https://doi.org/10.17933/bpostel.v21i2.379

Block, F. (1984). The Ruling Class Does Not Rule: Notes on the Marxist Theory of the State. In *The Political Economy: Readings in the Politics and Economics of American Public Policy*. Routledge.

Cakal, E. (2023). Torture and progress, past and promised: Problematising torture's evolving interpretation. *International Journal of Law in Context*, *19*(2), 236–254. https://doi.org/10.1017/S1744552323000010

Daryono, B. S., Sarosa, W., Ubaidillah, R., Widyatmoko, D., Purnomo, D. W., Djohan, T. S., Hadisusanto, S., Aipassa, M. I., & Setyawati, T. (2023). *Pembangunan Berkelanjutan di Ibu Kota Negara Nusantara Perspektif Biologi*. UGM PRESS.

Eng, D. I. A. S., S. T. ,. M. AP ,. IPU ,. ACPE ,. CIQaR ,. ASEAN, MA, E. P. D., S. Sos ,. MIS, MPPM, D. D. H. T., CIT, D. I. A. P. S., S. A. P. ,. M. M. ,. CIPA, M.Psi, D. D. S., Ph.D, P. A. A. B. P., PSC, D. S., S. E. ,. M. M. ,. M. Sc, M.M, D. I. E. S., M.Pd, D. D. M. M., MDA, D. U. H., CIQaR, D. S., M. Sc, Eng, D. I. S. A. P., S. E. ,. M. Eng ,. Sc ,. IPU ,. CIPA ,. ASEAN, Eng, D. I. E. S., S. T. ,. M. Si ,. CIPA ,. ASEAN, & M.Han, D. D. G. R. D. (2024). *Transformasi Manajemen Pertahanan Indonesia di Era Modernisasi Militer*. Indonesia Emas Group.

Hibatullah, M. N. R. (2024). Transformasi Administrasi Publik di Era Digital: Menuju Tata Kelola Pemerintahan yang Inovatif dan Transparan. *Distingsi: Journal of Digital Society*, *2*(4), 11–21.

Israyudin, R., Arrofi, F. M., & Dwiardi, A. R. (2025). Digital Transformation through Electronic-Based Government System Policy in Indonesia: A Policy Narrative Analysis. *Journal La Sociale*, *6*(2), 281–292. https://doi.org/10.37899/journal-la-sociale.v6i2.1825

Jaeger, J., Riedl, A., Djedovic, A., Vervaeke, J., & Walsh, D. (2024). Naturalizing relevance realization: Why agency and cognition are fundamentally not computational. *Frontiers in Psychology*, *15*. https://doi.org/10.3389/fpsyg.2024.1362658

Jubaidi, D., & Khoirunnisa, K. (2023). *The Significance Of The Living Law Concept In The New Criminal Code: A Perspective Of Progressive Law* (SSRN Scholarly Paper No. 5068325). Social Science Research Network. https://doi.org/10.2139/ssrn.5068325

Kamil, M., Mas'udi, S. Y. F., & Kristiani, N. N. (2024). Strengthening urban governance: Digital transformation through the development of electronic-based government systems to create smart cities in Malang City. *BIS Information Technology and Computer Science*, *1*, V124024–V124024. https://doi.org/10.31603/bistycs.198

Kartasasmita, D. G., Cempaka Timur, F. G., & Reksoprodjo, A. H. S. (2024). The Internet Exchange and .ID Domain Name Service as a National Critical Information Infrastructure. *2024 IEEE 24th International Conference on Communication Technology (ICCT)*, 700–707. https://doi.org/10.1109/ICCT62411.2024.10946489

Kurniawan, I. D., & Suyatno. (2025). Realizing Substantive Justice Enforcement Through the Implementation of Progressive Law. *International Journal: Interdisciplinary Journal of Education, Humanities, Law, and Social Entrepreneurship*, *1*(1), 8–15.

Maisarah, P. A., Fonna, F., & Firdaus, R. (2025). Peran Kritis Sistem Informasi Manajemen Dalam Mewujudkan E-Government Yang Responsif, Transparan, Dan Berkelanjutan Di Indonesia. *Jurnal Keuangan dan Manajemen Terapan*, *6*(3). https://ejurnals.com/ojs/index.php/jkmt/article/view/2901

Negara, T. A. S. (2023). Normative Legal Research in Indonesia: Its Originis and Approaches. *Audito Comparative Law Journal (ACLJ)*, *4*(1), 1–9. https://doi.org/10.22219/aclj.v4i1.24855

Poltak, H., & Widjaja, R. R. (2024). Pendekatan Metode Studi Kasus dalam Riset Kualitatif. *Local Engineering*, *2*(1), 31–34. https://doi.org/10.59810/lejlace.v2i1.89

Riabchenko, Y., Onyshchenko, A., Kudin, V., Kononets, O., & Holdskyi, V. (2025). Digital assets and property rights: Regulation and legal implications within the EU and globally. *Statute Law Review*, *46*(3). https://doi.org/10.1093/slr/hmaf029

Rizky, A. M., Pratiwi, M. P., Chairunnisa, A., Aiko, I. A., & Ariesmansyah, A. (2025). E-Goverment: Meningkatkan Efisiensi dan Efektivitas Pelayanan Publik di Indonesia. *Innovative: Journal Of Social Science Research*, *5*(1), 2070–2089. https://doi.org/10.31004/innovative.v5i1.17827

Rusmini, R., Alamsah Deliarnoor, N., Yuningsih, N. Y., & Sagita, N. I. (2025). Rethinking e-government failure: A readiness-based assessment of Indonesia's digitalization efforts. *Cogent Social Sciences*, *11*(1), 2559867. https://doi.org/10.1080/23311886.2025.2559867

Salam, R., Bahasruddin, A., Wijaya, I. D., & Faisal, M. (2024). Strategi Meningkatkan Resiliensi Dalam Tata Kelola Pemerintahan Pada Era Digital. *Jurnal Administrasi Publik*, *20*(2), 309–326. https://doi.org/10.52316/jap.v20i2.437

Siregar, M. (2024). Teori Hukum Progresif dalam Konsep Negara Hukum Indonesia. *Muhammadiyah Law Review*, *8*(2). https://doi.org/10.24127/mlr.v8i2.3567

Suhendra, A., & Santiko, A. (2022). Governance Through Electronic-based Information System by Papua Provincial Government. *International Journal of Regional Innovation*, *2*(4), 43–50. https://doi.org/10.52000/ijori.v2i3.65

Suherman, H. A. (2025). Relevansi Teori Hukum Pembangunan Dan Teori Hukum Progresif Dalam Pembentukan Teori Hukum Pancasila. *HUNILA : Jurnal Ilmu Hukum Dan Integrasi Peradilan*, *4*(1), 1–13. https://doi.org/10.53491/hunila.v4i1.1703

Supriadi, E., Zulkarnaen, A. H., Paminto, S. R., & Mulyadi, D. (2024). Digital Transformation of Electronic-Based Government System (EBS) in Sukabumi District: Implementation of Central Government Policy to Realise Good Governance. *Intellectual Law Review (ILRE)*, *2*(2), 85–94. https://doi.org/10.59108/ilre.v2i2.70

Tan, H., Zhao, X., & Zhang, N. (2022). Technology symbolization: Political mechanism of local e-government adoption and implementation1. *International Review of Administrative Sciences*, *88*(2), 511–532. https://doi.org/10.1177/0020852320915637

Tan, K. L., Chi, C.-H., & Lam, K.-Y. (2023). Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. *ACM Comput. Surv.*, *56*(3), 61:1-61:36. https://doi.org/10.1145/3616400

Tommy, S., & Nasution, M. I. P. (2025). Evaluasi Manajemen Risiko Keamanan Siber Pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN). *Jurnal Manajemen Ekonomi dan Bisnis*, *4*(1), 1–26. https://doi.org/10.61715/jmeb.v4i1.104

Wibowo, A. (2023). Hukum di Era Globalisasi Digital. *Penerbit Yayasan Prima Agus Teknik*, 1–185.

Wicaksono, A. T., & Yasin, I. F. (2024). Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection. *Al-Jinayah : Jurnal Hukum Pidana Islam*, *10*(2), 237–261. https://doi.org/10.15642/aj.2024.10.2.237-261

yuliana, r. a., & natalia, n. (2025). transformasi digital desa ponggok: tantangan dan potensi menuju desa pintar yang berkelanjutan. *ACADEMIA: Jurnal Inovasi Riset Akademik*, *5*(2), 90–97. https://doi.org/10.51878/academia.v5i2.4977