



Juridical Problems of Ministers' Administrative Authority in the Determination of Domain Name Registrars in Indonesia

Andi Budimansyah^{1*}, Akmal Syaddad², Frida Junariah³, Indri Lestari⁴, Siti Fajri Ilaika⁵

^{1,2,3,4,5} Faculty of Law, Universitas Pamulang, Banten, Indonesia.

 : andibudimansyah@gmail.com

Corresponding Author*



Abstract

Domain name governance is no longer solely a technical issue of internet addressing, but has become part of the legal infrastructure of digital identity, cybersecurity, consumer protection, and digital sovereignty of the state. In Indonesia, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions normatively recognizes Registry and Registrar as domain name managers. However, in practice, formal designation by the Minister seems to be given to the Indonesian Internet Domain Name Manager as the ".id" State Domain Registry, while the Registrar operates mainly through an accreditation mechanism or private agreement with the Indonesian Internet Domain Name Manager. This article examines the legal gap between normative construction and administrative practice in the determination of Registrars in Indonesia. This study uses a normative juridical method with a legislative approach, a conceptual approach, and an analytical approach. The results of the study show that the absence of a direct determination by the Minister to the Registrar creates legal uncertainty, weakens administrative supervision, limits consumer protection for Registrants, and reduces the effectiveness of cybersecurity governance at the domain registration level. This article argues that the Minister's appointment of the Registrar should not be seen as a bureaucratic obstacle, but rather as a public legal instrument to strengthen accountability, legal certainty, and digital sovereignty. Therefore, a special arrangement is needed that integrates the determination of the Registrar with a proportionate, risk-based, and digitized supervision mechanism.

Keywords: Domain Name; Registrar; Registry; Digital Sovereignty; Cyber Law.

INTRODUCTION

The development of global information technology has brought fundamental changes to the way countries understand, run, and defend their sovereignty. In classical times, state sovereignty was mainly attached to the control of physical territories that can be identified geographically, whether land, sea, or air. However, in the contemporary digital landscape, the boundaries of sovereignty are no longer solely defined by conventional territorial lines. The country is now faced with a new space that is virtual, cross-border, intangible, but has very real legal, economic, political, and security consequences. The space is cyberspace, which is a digital interaction space that allows the exchange of information, electronic transactions, public communication, and economic activities to take place without always being subject to the physical boundaries of the state.¹

The existence of legal subjects in cyberspace is no longer only represented through conventional administrative identities, such as physical addresses, legal entity deeds, or citizenship. Digital identity is increasingly determined by electronic naming systems, one of which is through domain names. A domain name does not simply serve as a technical

¹ Samantha Bradshaw and Laura DeNardis, "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom," *New Media & Society* 20, no. 1 (2018): 332-350, <https://doi.org/10.1177/1461444816662932>.

address to direct internet users to a specific digital site or service. Furthermore, domain names have evolved into identity instruments, intangible assets, reputational symbols, means of public trust, as well as part of the strategic infrastructure of the digital economy. The management of domain names in the context of the state also has a sovereignty dimension because it is directly related to the control, supervision, and protection of the national digital space.

Technically, global domain name governance is in a hierarchical structure that is controlled through an international mechanism. This system involves the *Internet Assigned Numbers Authority* (IANA), whose management functions are carried out within the framework of the *Internet Corporation for Assigned Names and Numbers* (ICANN).² The governance architecture is built on the principles of stability, interoperability, and global internet connectivity. However, the internet governance model that is private, transnational, and multi-stakeholder poses its own challenges for the state. The state still has an obligation to enforce national law, maintain public order, protect citizens, and ensure the security of its digital infrastructure, while some of the technical foundations of the internet are under a global governance regime that is not fully subject to national jurisdiction.

The legal response in the Indonesian context, to the development of cyberspace began with the establishment of Law Number 11 of 2008 concerning Information and Electronic Transactions. This law is the initial foundation for the recognition of electronic activities as activities that have legal consequences. Along with technological developments and the increasing complexity of digital issues, the Electronic Information and Transaction Law has undergone several changes, including through Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transaction Law. These changes show that the state is trying to adapt national legal norms to the dynamics of cyberspace that continues to develop. However, the existence of general norms in the Electronic Information and Transaction Law still requires more operational technical arrangements, especially in terms of the implementation of electronic systems, electronic transactions, and digital infrastructure management. One of the important instruments in these technical arrangements is Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This Government Regulation not only regulates the implementation of electronic systems in general, but also contains provisions regarding domain name governance. From the perspective of state administrative law, Government Regulation 71/2019 can be understood as a concrete form of state presence in regulating the national cyberspace. The state not only acts as a norm setter, but also as an authority that has the function of supervision, granting administrative legitimacy, and control over actors who carry out strategic functions in the digital ecosystem. Normatively, domain name management in Indonesia is placed within a framework that recognizes the importance of state authorization. This is in line with the principle that digital infrastructure that impacts the public interest cannot be completely left to private mechanisms. The state must still be present through public legal instruments, especially to ensure that domain name managers meet the requirements of reliability, security, accountability, and compliance with the provisions of national law. So that domain name regulation is not only a technical issue of

² Internet Corporation for Assigned Names and Numbers. 2013 *Registrar Accreditation Agreement*. Los Angeles: ICANN, 2013.

the internet, but also a matter of administrative law, constitutional law, consumer protection, national security, and digital sovereignty.

The construction of Government Regulation 71/2019, domain name governance adopts the *Shared Registry System* (SRS) model. This model clearly distinguishes between the functions of the Registry and the Registrar. Registry is the party that manages the domain name center database, maintains system stability, ensures data integrity, and ensures the operational continuity of high-level domains of country codes. This function in the Indonesian context, is related to the management of the ".id" domain as the country code Top Level Domain.³ Meanwhile, the Registrar runs downstream functions closer to the end user. The registrar is in direct contact with the registrant, performing domain registration services, administrative verification, transaction management, and meeting the commercial and administrative needs of domain name users.

The separation of functions between *the Registry* and *the Registrar* serves an important purpose. First, the separation prevents the concentration of domain name management power in a single entity. Second, this model opens up a healthier space for competition in the national domain industry. Third, the division of functions allows for a multi-layered supervision mechanism, both by the state against the Registry, and by the Registry against the Registrar. However, the model can only work ideally if each actor acquires a clear legal position and adequate administrative legitimacy. Without clarity on the legal status, the division of roles can actually cause inequality of authority and uncertainty of responsibility.

The main problem arises when there is a gap between the legal norms regulated in Government Regulation 71/2019 and the administrative practices that occur in domain name management in Indonesia. Normatively, both the Registry and the Registrar should obtain legitimacy through the appointment of the Minister. This determination is important because it is the basis of public law for an entity to carry out certain functions in the governance of national domain names. However, in practice, the formal determination from the Minister is only given to the Indonesian Internet Domain Name Manager or the Indonesian Internet Domain Name Manager as the ".id" domain registry. Meanwhile, Registrars operating at the downstream level did not receive a letter of determination directly from the Minister.⁴

This condition raises legal problems that are not simple. The Registrar does have a legal relationship with the Indonesian Internet Domain Name Manager through an accreditation mechanism or cooperation agreement. However, the relationship is basically in the realm of private law. Accreditation by the Indonesian Internet Domain Name Manager is not entirely identical to administrative authorization from the state. As a result, the legal position of the Registrar is in a position that is not completely solid. On the one hand, the Registrar performs an important function in the national domain name ecosystem. On the other hand, its public legitimacy does not directly come from the decisions or appointments of authorized government officials.

The absence of a formal determination for the Registrar has the potential to create legal uncertainty. Every action or authority in the perspective of state administrative law related to public functions should ideally have a clear legal basis, either in the form of attributions,

³ Internet Assigned Numbers Authority. "Delegating or Transferring a Country-Code Top-Level Domain (ccTLD)." Public Technical Identifiers, 2026.

⁴ Pengelola Nama Domain Internet Indonesia. "Tentang Pengelola Nama Domain Internet Indonesia (PANDI)." PANDI, 2026.

delegations, mandates, permits, determinations, or other administrative instruments. If an entity carries out functions that have an impact on the public interest without adequate administrative legitimacy, questions arise about the basis of authority, form of accountability, supervision mechanism, and legal consequences in the event of a violation. This ambiguity can have an impact on user protection, business certainty, and the credibility of national domain governance.⁵

Furthermore, the inequality between *the Registry* and *the Registrar* can also create distortions in the structure of the national internet industry. The Registry has formal legitimacy sourced from the state, whereas the Registrar only has contractual legitimacy that comes from a private relationship with the Registry. This imbalance has the potential to put the Registrar in a weak position, both legally and economically.⁶ From a legal perspective, the Registrar may face vulnerabilities if its status is questioned by authorities, users, or third parties. From an economic point of view, the absence of formal administrative recognition can reduce the competitiveness of local registrars, especially when dealing with foreign industry players who have stronger legal recognition than their home jurisdictions.⁷

Based on this description, this study is important to examine the discrepancy between legal norms and administrative practices in the determination of domain name registrars in Indonesia. The main focus of the research is directed at three main problems. First, how is the legal construction of the Registry and Registrar regulations in Government Regulation 71/2019. Second, why the instrument of determination of the Minister has not been applied directly to the national Registrar. Third, what are the juridical and economic implications of the absence of formal determination on legal certainty, industrial structure, and strengthening Indonesia's digital sovereignty.

This research not only seeks to read the issue of domain name management as a technical issue of the internet, but also as a legal issue of state administration and digital public policy. Analysis of the incompatibility between *das sollen* and *das sein* in the governance of the Registrar is expected to make an academic contribution to the development of Indonesian cyber law. In addition, this research is also expected to provide normative recommendations for the government in formulating a more consistent, fair, and regulatory model oriented towards strengthening the national digital ecosystem.

METHODS OF THE RESEARCH

This research uses normative legal research methods or normative juridical research. The selection of this method is based on the character of the problem studied, namely the existence of ambiguity and insynchronization of norms in the regulation of domain name governance in Indonesia, especially regarding the legal position of *Registry* and *Registrar* in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This research does not focus on testing people's empirical behavior, but on the analysis of positive legal norms, the legal principles of state administration, the concept of digital sovereignty, and the construction of state authority in providing administrative legitimacy to domain name administrators. The approaches used

⁵ Goldsmith, Jack L., and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. (Oxford: Oxford University Press, 2006).

⁶ Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. (Cambridge, MA: MIT Press, 2010).

⁷ DeNardis, Laura. *The Global War for Internet Governance*. (New Haven: Yale University Press, 2014).

in this study include the statute *approach*, the conceptual *approach*, and the *analytical approach*.⁸ The statutory approach is used to examine various laws and regulations related to the implementation of electronic systems and domain name management, including Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transaction Law, and Government Regulation Number 71 of 2019 concerning the Implementation of Systems and Transactions Electronics. Conceptual approaches are used to understand relevant legal concepts, such as digital sovereignty, administrative authority, appointment of government officials, legal certainty, *Shared Registry System*, *Registry*, and *Registrar*.⁹ Meanwhile, an analytical approach is used to decipher the relationship between norms that should apply (*das sollen*) and domain name management practices that run in reality (*das sein*).¹⁰ The sources of legal materials in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations that regulate electronic information and transactions, the implementation of electronic systems, domain name management, and relevant state administrative legal provisions. Secondary legal materials are books, scientific journals, academic articles, institutional reports, policy documents, and literature on cyber law, internet governance, ICANN, IANA, *Registry*, *Registrar*, and digital sovereignty. The tertiary legal materials include legal dictionaries, legal encyclopedias, and other supporting sources used to clarify the meaning of legal terms or concepts used in this research. The technique of collecting legal materials is carried out through literature studies and document studies. Literature studies are carried out by browsing legal literature, academic books, scientific journals, and research results relevant to the issue of domain name governance and cyber law. Document studies are carried out by examining laws and regulations, official government documents, institutional documents, and technical instruments related to the domain name management system. This technique is used to obtain a complete understanding of the normative construction of *the Registry* and *Registrar regulations* as well as the legal basis for granting determination by the Minister. The analysis of legal materials was carried out qualitatively using a descriptive-analytical method. The collected legal materials are first classified based on their relevance to the research issue, then systematically interpreted to find the relationship between the norms, principles, and legal concepts used. The analysis was carried out by examining the compatibility between normative provisions in laws and regulations and the practice of domain name management in Indonesia. Furthermore, the results of the analysis were used to identify the form of ambiguity of norms, juridical implications, and administrative legal consequences of the absence of a formal determination by the Minister of the *National Registrar*. Through this method, this research is expected to be able to provide systematic legal arguments regarding the need for legal certainty in the governance of national domain names. In addition, this study also aims to formulate normative recommendations for policymakers so that *the regulation of Registry* and *Registrar* can be carried out consistently, accountably, and in line with the principles of Indonesia's digital sovereignty.

⁸ Amiruddin, and H. Zainal Asikin. *Pengantar Metode Penelitian Hukum*. (Jakarta: RajaGrafindo Persada, 2006).

⁹ Marzuki, Peter Mahmud. *Penelitian Hukum*. (Jakarta: Kencana, 2007).

¹⁰ Sanggono, Bambang. *Metodologi Penelitian Hukum: Suatu Pengantar*. (Jakarta: RajaGrafindo Persada, 2002).

RESULTS AND DISCUSSION

A. Juridical Construction of Domain Names as Legal Objects in Cyberspace

Domain names in the modern internet ecosystem can no longer be understood solely as technical instruments that function to direct users to a specific address on the internet network. Initially, the identification system in the internet relied on a string of numerical numbers known as *Internet Protocol Addresses* or IP Addresses.¹¹ However, because the structure of the numbers is difficult for users to remember, then a more recognizable naming system based on alphanumeric characters was developed, namely domain names. Domain names in their development have undergone a functional transformation from just a technical address to a digital identity that contains legal, economic, and reputational value.¹²

The definition of domain name in Indonesia's positive law has been regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions as amended several times, most recently through Law Number 1 of 2024. A domain name is understood as an internet address used by a state administrator, person, business entity, or society in communicating over the internet, which is structured in the form of a unique code or character to indicate a specific location on the internet. This definition shows that the lawmakers do not place the domain name as a neutral technical entity, but as a legal object that can have legal consequences for the holder or its use.

Domain names, in the perspective of cyber law, have a dual position. On the one hand, it is a civil object because it can be used in business activities, electronic transactions, branding, and commercial communications. On the other hand, domain names also contain a public legal dimension because they are related to cyberspace order, electronic system security, data protection, and state digital sovereignty. Therefore, the management of the domain name cannot be completely left to a private contractual mechanism. The state retains the authority and responsibility to regulate, foster, supervise, and ensure that domain name management runs in accordance with national law.

This construction is important because cyberspace has a cross-border character and is not always subject to conventional territorial boundaries. However, when a domain name is used by an Indonesian legal subject, involves the interests of the Indonesian people, or uses a national digital identity such as ".id", then the state has a legitimate basis for legal intervention. The intervention is not in the sense of hindering technological development, but to ensure legal certainty, legal protection, and administrative order in the national digital ecosystem.¹³ The implication of such a construction is that domain name management should be seen as part of the governance of the national cyberspace. The state has an interest in ensuring that domain names are not used unlawfully, do not harm others, do not create public confusion, and do not become a means of cybercrime. Therefore, the regulation of domain names is not enough to be left entirely to market mechanisms or private contractual relationships between business actors. The state still needs to be present through public legal

¹¹ Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press, 2006.

¹² Internet Corporation for Assigned Names and Numbers. "What Does ICANN Do?" ICANN. Accessed May 28, 2026.

¹³ Kohl, Uta. *Jurisdiction and the Internet: Regulatory Competence over Online Activity*. (Cambridge: Cambridge University Press, 2026).

instruments to ensure legal certainty, consumer protection, electronic system security, and digital sovereignty.¹⁴

The structure of global internet governance, each country has a high-level domain code known as the *country code Top Level Domain* (ccTLD). The ccTLD for Indonesia is ".id". The management of ccTLDs does not stand alone, but rather is in a global structure involving IANA and the Internet Corporation for Assigned Names and Numbers or ICANN. IANA performs the function of managing the internet root zone, including the recording of technical delegations for high-level domains. Meanwhile, ICANN plays a role in coordinated governance that ensures the stability, security, and interoperability of the global internet naming system.¹⁵

The Indonesian context in the Indonesian Internet Domain Name Manager or Indonesian Internet Domain Name Manager has a strategic position as the manager of the ".id" ccTLD. This position was born from a global delegation mechanism that recognizes the Indonesian Internet Domain Name Manager as the manager of the high-level domain of the Indonesian country code. In this status, the Indonesian Internet Domain Name Manager performs the function of a *national Registry* that is responsible for the management of the main database of the ".id" domain, technical arrangements for registration, system maintenance, and security of the national domain name infrastructure.¹⁶

However, the position of the Indonesian Internet Domain Name Manager as a *Registry* needs to be read in two layers of legitimacy. First, the technical-international legitimacy that comes from the IANA/ICANN delegation in the global internet governance system.¹⁷ Second, the legitimacy of national public law which comes from recognition and determination by the Indonesian government through the authorized ministries in the field of communication and digital. These two layers of legitimacy are important because the management of the ".id" ccTLD is not only related to the technical stability of the internet, but also to national interests, user protection, and the symbol of Indonesia's digital sovereignty.¹⁸ The Indonesian Internet Domain Name Manager, as a *Registry*, occupies a central position because it manages the parent database of the ".id" domain name. However, this function does not directly connect the Indonesian Internet Domain Name Manager with all end users. In the domain industry practice, there are other actors who act as a liaison between the *Registry* system and the user community, namely the *Registrar*. National domain name governance cannot only be understood from the position of the Indonesian Internet Domain Name Manager as a *Registry*, but must also pay attention to the legal position of the *Registrar* as a downstream actor who interacts directly with the public.

B. Structure of Registry, Registrar and Registrant in the Domain Name Ecosystem in Indonesia

¹⁴ Bradshaw, Samantha, and Laura DeNardis. "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom." *New Media & Society* 20, no. 1 (2018): 332–350. doi: 10.1177/1461444816662932.

¹⁵ Couzigou, Irène. "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations." *International Review of Law, Computers & Technology* 32, no. 1 (2018): 37–57. doi: 10.1080/13600869.2018.1417763.

¹⁶ Deibert, Ronald J. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32, no. 4 (2018): 411–424. doi: 10.1017/S0892679418000618.

¹⁷ Holt, Thomas J. "Regulating Cybercrime through Law Enforcement and Industry Mechanisms." *The ANNALS of the American Academy of Political and Social Science* 679, no. 1 (2018): 140–157. doi: 10.1177/0002716218783679.

¹⁸ Internet Corporation for Assigned Names and Numbers. "Information for Domain Name Registrants." ICANN. 2026.

The domain name ecosystem is essentially built on a layered structure that separates the master data management function, the commercial distribution function, and the end-use function. This structure is known in international practice as the *Shared Registry System* model. The model aims to create more efficient, competitive, and controlled governance. *Registry* in this model, is in charge of managing a central database for a high-level domain, *Registrar* is in charge of providing domain name registration services to the public, while *Registrant* is the end user who registers and uses a specific domain name.

The separation of functions has a strong rational basis. If all management, distribution, and public service functions are concentrated in one entity, there is a risk of monopoly, abuse of authority, limited innovation, and low quality of service. In contrast, by separating the functions of the *Registry* and the *Registrar*, the domain system can be developed through competition between service providers, without disturbing the stability of the main databases that remain centrally managed by the *Registry*. Therefore, the existence of a *Registrar* is not just a commercial complement, but an integral part of the domain name governance architecture. Indonesian Internet Domain Name Managers in the Indonesian context, perform functions as *Registry* for the ".id" domain, while various domain and hosting service providers perform functions as *Registrars*. These *Registrars* are the ones who deal directly with consumers or *Registrants*, perform administrative verification, accept domain registrations, process payments, assist with technical management, and handle customer service. At a more downstream level, there are also resellers who carry out the marketing or resale function of domain services based on the business relationship with the *Registrar*. However, unlike *Registrars*, *Resellers* generally do not have a direct relationship with the *Registry's* main database.

From a legal perspective, the relationship between the *Registry*, the *Registrar*, the *Reseller*, and the *Registrant* gives birth to the character of a different legal relationship. The relationship between the state and the domain name manager is in the realm of public law because it concerns authority, determination, supervision, and the public interest.¹⁹ The relationship between the *Registry* and the *Registrar* can be in the form of a contractual or accreditation relationship that is civil in nature.²⁰ Meanwhile, the relationship between the *Registrar* and the *Registrant* is a consumer legal relationship that can give rise to civil rights and obligations. This difference in the character of legal relations is important to understand why the administrative legitimacy of the state is still needed, especially for actors who carry out strategic functions in digital public services.

C. The Normative Urgency of Domain Name Regulation in the Electronic Information and Transaction Law

Normatively, domain name regulation in Indonesia has obtained a legal basis in the Electronic Information and Transaction Law. One of the main principles adopted is the first come, first served principle. This principle gives the right to state administrators, people, business entities, and the public to own a domain name based on the order of registration.²¹ This principle is commonly used in global domain governance because it provides initial certainty about who has the right to use a domain name. However, this principle is not

¹⁹ Internet Corporation for Assigned Names and Numbers. "Agreements & Policies." ICANN, 2026.

²⁰ Internet Corporation for Assigned Names and Numbers. 2013 *Registrar Accreditation Agreement*. Los Angeles: ICANN, 2013.

²¹ World Intellectual Property Organization. "Domain Name Dispute Resolution." WIPO *Arbitration and Mediation Center*, 2026.

absolute because it is still limited by provisions regarding good faith, prohibition of infringing on the rights of others, and protection of a valid trademark or identity.

The Electronic Information and Transaction Law also provides a protection mechanism for parties harmed by the unauthorized use of domain names. These arrangements are important to prevent the practice of *cybersquatting*, which is the registration of domain names that resemble brands, legal entity names, or other parties' identities for the purpose of obtaining unauthorized profits. The regulation of domain names in the Electronic Information and Transactions Act not only emphasizes the registration aspect, but also the protection of the legal rights and interests of legitimate parties.²² More technical arrangements are contained in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This PP divides domain name managers into two categories, namely Domain Name Registry and Domain Name Registrar. This division shows that Indonesia's positive law normatively recognizes two main actors in domain name management. In other words, *Registry* and *Registrar* are both placed as part of the domain name manager, although they both perform different functions. An important problem arises from the provision that states that the domain name manager is determined by the Minister. Grammatically speaking, the phrase "domain name manager" should not be interpreted only as limited to *the Registry*, as the previous provision had included *the Registrar* as part of the domain name manager. If the norm is interpreted systematically, then both *the Registry* and *the Registrar* should obtain a determination from the Minister. The determination is a form of public legal legitimacy that provides the basis for authority, compliance standards, and administrative supervision mechanisms for actors involved in the management of national domain names.

D. Discrepancy Between *Das Sollen* and *Das Sein*, Minister's Administrative Authority in Determining Domain Name Management and Implications for Digital Sovereignty

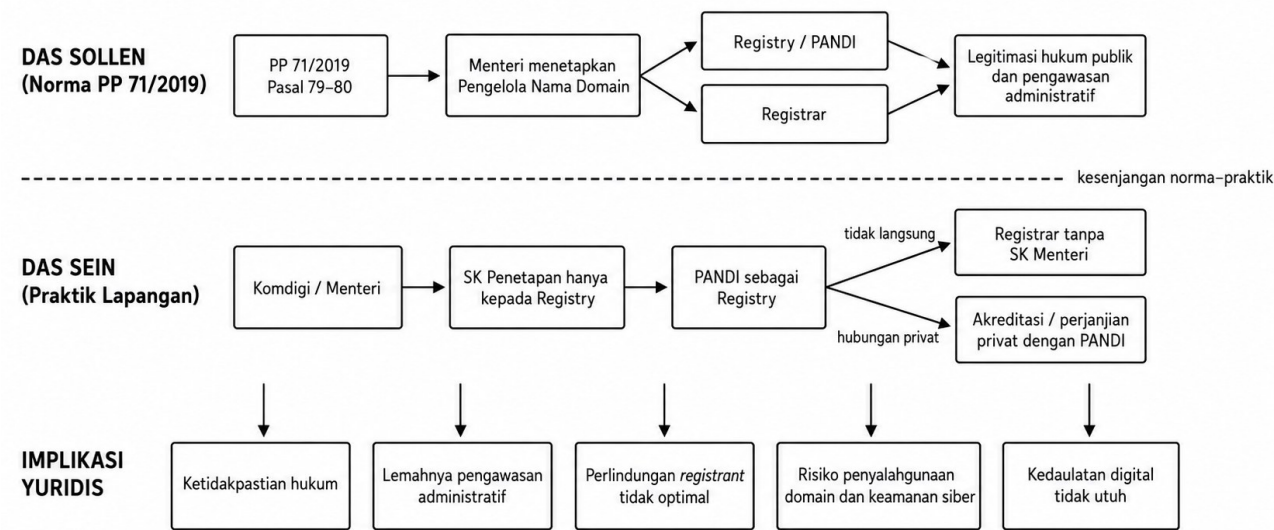
The main problem in the governance of the ".id" domain name lies in the gap between normative construction and administrative practice. *Das sollen*, Government Regulation 71/2019 provides a framework that the domain name manager, which includes *the Registry* and *Registrar*, is determined by the Minister. This norm confirms the existence of a public legal obligation for the state to ensure that entities that perform domain name management functions have clear administrative legitimacy. The absence of a Minister's appointment of a *Registrar* raises several juridical implications. First, there is legal uncertainty regarding the *Registrar*'s position as a domain name manager. Although factually *the Registrar* performs the functions of registration and services to the public, its administrative status is not explicitly strengthened by the decision or determination of the authorized government official. This may create legal vulnerabilities in the event of a dispute between *the Registrar* and *the Registry*, between *the Registrar* and *the Registrant*, or between *the Registrar* and the government. Second, the absence of a determination weakens the supervisory mechanism and administrative sanctions. Administrative sanctions in state administrative law, generally related to the existence of permissions, approvals, determinations, or initial forms of legitimacy granted by authorized officials. If *the Registrar* does not obtain a direct determination from the Minister, then the government's instrument to freeze, revoke, or provide administrative guidance will not be as strong as if the determination already exists.

²² World Intellectual Property Organization. "WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)." *WIPO Arbitration and Mediation Center*. 2026.

As a result, supervision of *the Registrar* is more dependent on the contractual mechanism between the Indonesian Internet Domain Name Manager and *the Registrar*.

Third, the absence of determination has the potential to create an imbalance in the bargaining position between *the Registry* and *the Registrar*. Since the legitimacy of *the Registrar* is derived from the accreditation relationship with *the Registry*, the *Registrar* is in a position of relative dependence on the *Registry's policies*. In the event of a termination of accreditation, a change in the terms of cooperation, or a restriction of technical access, *the Registrar* may suffer significant business losses. Legal protection in such conditions, which is available, tends to be civil in nature, even though the functions carried out by *the Registrar* also have a public dimension. Fourth, from the perspective of consumer protection, the absence of a determination can cause a gap in accountability. *The Registrant* as the end user is in direct contact with *the Registrar*. In the event of a service failure, data misuse, verification error, unauthorized domain transfer, or unilateral termination of service, consumers need an effective remedy mechanism. Without strong administrative arrangements, consumer protection risks relying solely on service contracts that are often drawn up unilaterally by service providers. The mechanism will be explained in the image:

Figure 1. Gap in Minister's Administrative Authority in Determining Domain Name Management



Sumber: Analyzed by the author

The absence of a Minister's designation of a *Registrar* also has implications for national cybersecurity. *Registrar* is the entry point in the domain registration process. It is at this stage that the identity of the registrant is collected, verified, and recorded. If this process is not adequately supervised, there is a risk of domain registration using false identities, invalid data, or information that is difficult to trace. These risks can be used by cybercriminals to build fraudulent sites, *phishing*, malware spread, online gambling, and other illegal digital activities.²³ Supervision of *the Registrar* should not be understood as a bureaucratic obstacle, but rather as part of a cyber risk mitigation system. The State needs to ensure that *the Registrar*

²³ Aleksander, Jedi, Emilda Kuspraningrum, and Febri Noor Hediati. "Asas Iktikad Baik dalam Pencegahan dan Penyelesaian Tindakan Penyerobotan Nama Domain (Cybersquatting) di Indonesia." *Yuriska: Jurnal Ilmiah Hukum* 17, no. 2 (2025): 195-209. doi: 10.24903/yrs.v17i2.3629.

applies the principles of prudence, identity verification, personal data protection, incident reporting mechanisms, and cooperation with law enforcement officials. Without clear administrative determinations and standards, these obligations could potentially become only contractual clauses, rather than public legal obligations that can be directly enforced by the state. The determination of the Indonesian Internet Domain Name Manager as a country code Top Level Domain (ccTLD) ".id" Registry has been carried out twice through official government decisions, namely through the Decree of the Minister of Communication and Information Number 806 of 2014 and the Decree of the Minister of Communication and Information Technology Number 218 of 2023. The determination is a manifestation of the state's administrative legality within the framework of national telematics law, as well as reflecting the fulfillment of the *das sollen aspect* in internet governance in Indonesia, where the state through its attributive authority gives a mandate to manage strategic digital infrastructure to national institutions that are considered to meet technical, institutional, and legal compliance requirements. From the perspective of state administrative law, the two decisions are not only declarative, but also constitutive because they give birth to formal legitimacy for the Indonesian Internet Domain Name Manager to carry out the function of the national Registry for the ".id" domain.

The first determination was made through the Decree of the Minister of Communication and Information Number 806 of 2014 which was issued on September 16, 2014 and signed by the Minister of Communication and Information Technology at that time, Tifatul Sembiring. Juridically, the decision was issued in order to carry out the mandate of articles related to domain name management as stipulated in Government Regulation Number 82 of 2012, which at that time was still the main legal regime before it was amended through Government Regulation Number 71 of 2019. Therefore, normatively, the legal basis for the determination of the Indonesian Internet Domain Name Manager in Decree Number 806 of 2014 must be directly related to the enactment of Government Regulation Number 82 of 2012, not Government Regulation Number 71 of 2019 which only came into effect five years later. The Decree also confirms the national legitimacy of the technical delegation that had previously been granted by IANA/ICANN to the Indonesian Internet Domain Name Manager in 2013 in the management of the ".id" ccTLD. Furthermore, the second determination was carried out through the Decree of the Minister of Communication and Information Number 218 of 2023 issued on May 25, 2023 under the authority of the Ministry of Communication and Information Technology which is now transformed into the Ministry of Communication and Digital. This decision is essentially a form of extension as well as an update of the mandate of national Registry management to the Indonesian Internet Domain Name Manager. The issuance is based on the results of a comprehensive review, assessment, and evaluation conducted by the government on the operational aspects, institutional governance, cybersecurity, and legal compliance of Indonesian Internet Domain Name Managers during the period August to November 2022. In its legal substance, Decree Number 218 of 2023 does not fundamentally change the institutional architecture of the national Registry, but rather affirms the continuity of the state's mandate to the Indonesian Internet Domain Name Manager as the official manager of the ".id" ccTLD based on the principle of sustainability of accountable, secure, and sovereign national internet governance.

Indonesia's digital sovereignty is also not enough to be realized through symbolic control over the ".id" domain. Digital sovereignty must be reflected in the state's ability to regulate,

supervise, and ensure the accountability of all actors in the national digital ecosystem. If *the Registry* has obtained public legal legitimacy but *the Registrar* has not, then digital sovereignty is only strong at the central level, but weak at the level of distribution and public services. In fact, it is precisely at the *Registrar level* that the interaction between the domain system and the community occurs directly. Therefore, the Minister's appointment of the *Registrar* needs to be placed as an instrument to strengthen governance, not as a form of business restriction. The designation can be designed through a risk-based approach, by distinguishing the scale of the business, the volume of domain registrations, the level of access to user data, and the security obligations that must be met. Such a model allows the state to maintain legal certainty and cybersecurity without overburdening the industry.²⁴

E. Ideal Arrangement Construction Model for the Establishment of a National Registrar

Based on the above analysis, the ideal regulatory model for *national Registrars* needs to be prepared with the principles of proportionality, legal certainty, accountability, and ease of doing business.²⁵ First, the government needs to issue derivative regulations that specifically regulate the procedures for determining *Registrars*. This regulation can be in the form of a Ministerial Regulation that contains administrative requirements, technical requirements, security standards, data protection obligations, reporting mechanisms, and administrative sanctions. Second, the determination mechanism should be integrated with the risk-based business licensing system. The determination of *the Registrar* in this way, does not become a lengthy bureaucratic process, but becomes an instrument of measurable verification and supervision. Governments can assign risk categories based on the scale of the service, the number of domains managed, the type of data processed, and the level of connectivity to *the Registry* system. The greater the risk posed, the higher the compliance standards that must be met.

Third, the relationship between the Minister, the Indonesian Internet Domain Name Manager as *a Registry*, and *the Registrar* needs to be strictly regulated. The Indonesian Internet Domain Name Manager can still carry out the technical functions of accreditation and system management, but the determination of public law on *the Registrar* needs to be placed under the authority of the state. So that accreditation by *the Registry* and determination by the Minister do not negate each other, but complement each other. Accreditation functions as a technical-operational instrument, while the appointment of the Minister functions as administrative legitimacy and the basis for public legal supervision. Fourth, ideal regulations also need to regulate protection for *Registrants*. In the event that *the Registrar* goes bankrupt, loses accreditation, commits a serious breach, or discontinues services, a secure domain migration mechanism must be available to another *Registrar*. This is important to prevent consumer losses and maintain the sustainability of digital services. In addition, the government needs to ensure that domain registration data remains protected and accessible for legal purposes in accordance with the provisions of laws and regulations. Therefore, the arrangement for the determination of *the Registrar* is not only aimed at fulfilling the normative order of Government Regulation 71/2019, but also strengthens the structure of the national domain industry. The appointment of the Minister can be the basis for the creation of more orderly, competitive, transparent, and sovereign domain governance. Legal

²⁴ Marketa Trimble, "Territorialization of the Internet Domain Name System," *Pepperdine Law Review* 45, no. 4 (2018): 623–682.

²⁵ Fratini, Samuele, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi. "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models." *Digital Society* 3 (2024): Article 59. <https://doi.org/10.1007/s44206-024-00146-7>.

certainty in the long term, for *the Registrar*, will also strengthen the competitiveness of the ".id" domain as a national digital identity that is safe, reliable, and economically valuable.

CONCLUSION

Domain names have a strategic position in cyber law because they not only serve as technical addresses on the internet, but also as digital identities that have legal, economic, reputational, and sovereign value. The ".id" domain in the Indonesian context, is part of the national digital identity whose management cannot be completely left to a private mechanism. The state still has the authority and responsibility to ensure that domain name governance runs based on the principles of legal certainty, consumer protection, cybersecurity, and digital sovereignty. Normatively, Government Regulation Number 71 of 2019 has stipulated that domain name managers consist of Registry and Registrar. The phrase "domain name manager is designated by the Minister" should be interpreted to include both actors. However, in practice, formal determination seems to be given to the Indonesian Internet Domain Name Manager as a Registry, while the Registrar carries out the function of registration and services to the public based on an accreditation relationship or private agreement with the Indonesian Internet Domain Name Manager. This condition shows that there is a discrepancy between *das sollen* and *das sein* in the governance of national domain names. The absence of a Minister's appointment of a Registrar raises several juridical implications. First, there is legal uncertainty regarding the position of the Registrar as part of the domain name manager. Second, the administrative supervision and sanction mechanism from the state becomes less strong because the legal relationship of the Registrar is more dependent on private contractual mechanisms. Third, protection for Registrants or end users is potentially suboptimal in the event of service failure, data misuse, unauthorized domain transfer, or unilateral termination of services. Fourth, the weak administrative legitimacy of the Registrar can also increase cybersecurity risks because the Registrar is the initial door for identity verification in the domain registration process. Therefore, the Minister's appointment of the Registrar needs to be placed as an instrument to strengthen governance, not as a form of business restriction. The government needs to formulate derivative regulations that specifically regulate the procedures for the determination of national registrars, including administrative requirements, technical standards, data protection, reporting obligations, supervisory mechanisms, and administrative sanctions. These arrangements should be designed proportionately and risk-based to continue to support ease of doing business, but at the same time be able to strengthen legal certainty, consumer protection, cybersecurity, and digital sovereignty in Indonesia.

REFERENCES

- Aleksander, Jedi, Emilda Kuspraningrum, and Febri Noor Hediati. "Asas Iktikad Baik dalam Pencegahan dan Penyelesaian Tindakan Penyerobotan Nama Domain (Cybersquatting) di Indonesia." *Yuriska: Jurnal Ilmiah Hukum* 17, no. 2 (2025): 195–209. doi: 10.24903/yrs.v17i2.3629.
- Amiruddin, and H. Zainal Asikin. *Pengantar Metode Penelitian Hukum*. Jakarta: RajaGrafindo Persada, 2006.
- Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press, 2006.

- Bradshaw, Samantha, and Laura DeNardis. "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom." *New Media & Society* 20, no. 1 (2018): 332–350. doi: 10.1177/1461444816662932.
- Couzigou, Irène. "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations." *International Review of Law, Computers & Technology* 32, no. 1 (2018): 37–57. doi: 10.1080/13600869.2018.1417763.
- DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014.
- Deibert, Ronald J. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32, no. 4 (2018): 411–424. doi: 10.1017/S0892679418000618.
- Fratini, Samuele, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi. "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models." *Digital Society* 3 (2024): Article 59. <https://doi.org/10.1007/s44206-024-00146-7>.
- Goldsmith, Jack L., and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press, 2006.
- Holt, Thomas J. "Regulating Cybercrime through Law Enforcement and Industry Mechanisms." *The ANNALS of the American Academy of Political and Social Science* 679, no. 1 (2018): 140–157. doi: 10.1177/0002716218783679.
- Internet Corporation for Assigned Names and Numbers. *2013 Registrar Accreditation Agreement*. Los Angeles: ICANN, 2013.
- Internet Assigned Numbers Authority. "Delegating or Transferring a Country-Code Top-Level Domain (ccTLD)." Public Technical Identifiers, 2026.
- Internet Corporation for Assigned Names and Numbers. "What Does ICANN Do?" ICANN, 2026.
- Internet Corporation for Assigned Names and Numbers. "Information for Domain Name Registrants." ICANN. 2026.
- Internet Corporation for Assigned Names and Numbers. "Agreements & Policies." ICANN, 2026.
- Internet Corporation for Assigned Names and Numbers. *2013 Registrar Accreditation Agreement*. Los Angeles: ICANN, 2013.
- Kohl, Uta. *Jurisdiction and the Internet: Regulatory Competence over Online Activity*. Cambridge: Cambridge University Press, 2026.
- Marketa Trimble, "Territorialization of the Internet Domain Name System," *Pepperdine Law Review* 45, no. 4 (2018): 623–682.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2007.
- Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.
- Pengelola Nama Domain Internet Indonesia. "Tentang Pengelola Nama Domain Internet Indonesia (PANDI)." PANDI, 2026.

- Samantha Bradshaw and Laura DeNardis, "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom," *New Media & Society* 20, no. 1 (2018): 332–350, <https://doi.org/10.1177/1461444816662932>.
- Sanggono, Bambang. *Metodologi Penelitian Hukum: Suatu Pengantar*. Jakarta: RajaGrafindo Persada, 2002.
- World Intellectual Property Organization. "Domain Name Dispute Resolution." *WIPO Arbitration and Mediation Center*, 2026.
- World Intellectual Property Organization. "WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)." *WIPO Arbitration and Mediation Center*. 2026.