VOL. 04, NO. 01, 2024 (149-157)
JIEE:
Jurnal Ilmiah Ekotrans & Erudisi
EISSN: 2777-0184
PISSN: 2797-2259

Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty

Engrina Fauzi[1*], Helfira Citra[2], Elwidarifa Marwenny[3], Nia Alfitrianti[4]
[1,2,3,4]Faculty of Law, Universitas Dharma Andalas, Indonesia
** Corresponding author: engrina.f@unidha.ac.id*

ARTICLE INFO

Article history:
Received 01 April 2024
Received in revised form 27 May 2024
Accepted 29 May 2024

Keyword:
Global platform, Surveillance Capitalism, Global Platform.

ABSTRACT

The dominance of foreign digital platforms in the application ecosystem within Indonesia poses significant implications for the sovereignty of the Indonesian state; the utilization of such foreign digital technologies results in the inadvertent surrender and delegation of citizen data to foreign entities for monitoring and processing purposes. This phenomenon has elicited concern among legal scholars, as the usage of foreign applications signifies the applicability of the legal frameworks from the countries of origin of these applications. This raises critical questions regarding the sovereignty of the Indonesian state, particularly concerning its ability to exert control over data and cyberspace in the context of global platforms. The methodological approach employed in this investigation is grounded in normative legal research, utilizing a conceptual framework that examines relevant legal statutes. The aggregation and distribution of personal data constitutes an infringement upon individual privacy rights, as the right to privacy inherently encompasses the prerogative to determine the provision of personal information. The strategic policies and initiatives undertaken by the Indonesian government to bolster national digital sovereignty can be realized through several measures: the implementation of comprehensive personal data protection standards to enhance national digital sovereignty, the establishment of an independent authority for personal data protection, the fortification of cybersecurity measures to mitigate data security risks, and the jurisdictional enforcement of cyberspace law towards achieving digital economic sovereignty. There exists a pressing need for extensive regulatory frameworks to safeguard personal data as an integral component of human rights. A balance must be struck in the management of personal data processing, ensuring the protection of rights and fostering awareness among data subjects, thereby facilitating the development of a secure digital economic ecosystem that offers legal certainty for enterprises and enhances consumer confidence. Furthermore, the establishment of equitable international personal data protection regulations is essential to support the advancement of the digital economy through arrangements governing cross-border data flow.

INTRODUCTION

The incidence of cyber assaults targeting Indonesia has exhibited a year-on-year escalation. The BSSN National Cybersecurity Operations Centre has duly observed this phenomenon. In the context of attempted data breaches occurring

[1]*engrina.f@unidha.ac.id*

between January and August of 2020, a staggering 190 million cyber-attacks were documented, alongside 36,771 compromised data accounts across various sectors, notably including the financial domain. The recorded incidents of cyber-attacks have manifested a fivefold increase in comparison to the year 2019. In the landscape of contemporary digital technology, cybercrime is capable of not only infringing upon the safety of personal data and information but also disrupting economic and commercial endeavors, compromising infrastructure, and potentially posing threats to the stability of national security. The trend of escalation continued into the year 2021. Kaspersky, an established cybersecurity organization, indicates that 40% of consumers in the Asia Pacific region have dealt with situations involving personal data breaches initiated by unapproved parties. As delineated in Presidential Regulation 28/2021, Articles (2) and (3), BSSN is designated as the agency responsible for assisting the President (Government) in matters pertaining to cybersecurity. This agency is entrusted with the formulation of standards and oversight, as the digital activities of citizens are invariably linked to the management of personal data. The utilization of individual data necessitates robust and accountable governance frameworks. Comprehensive, stringent, and unequivocal regulations are imperative. Concurrently, there exists a critical need for the preparedness of intelligent, resilient, and adaptive human resources.

Reports from We Are Social predict that the worldwide internet user population will grow to 5 billion by 2023. Within the context of Indonesia, this figure stands at 212.9 million. These individuals are referred to as netizens. A significant concern arises from the boundless nature of the cyber realm. The digital platforms predominantly utilized by Indonesian netizens are primarily of foreign origin. Indonesia, as a nation, is characterized by its vastness. The enforcement of territorial control and physical sovereignty from Sabang to Merauke, as well as from Miangas Island to Rote Island, poses considerable challenges. This archipelago comprises more than 17,000 islands surrounded by extensive oceans. The unification, preservation, and establishment of physical sovereignty across Indonesia's land, waters, and airspaces necessitate substantial endeavors from the nation's founders to the present day. Furthermore, the matter of sovereignty within the digital domain, which is accessible from any location, presents an equally formidable challenge.

The constitution, as delineated in Article 33 of the 1945 Constitution, posits that "The earth, water, and the natural resources contained therein are controlled by the state and shall be utilized for the maximum benefit of the populace." Nevertheless, the preservation of these resources necessitates not merely regulatory frameworks and physical oversight but also diligent state supervision, a task that has been demonstrated to be intricate and formidable. Despite having attained 78 years of sovereignty, the objectives delineated in Article 33 have yet to be fully actualized in an exemplary manner. The advent of the digital era has presented novel challenges, particularly concerning the security of personal data, where incidents of breaches and cyber-attacks have surged in frequency owing to the unbounded character of the digital landscape (Hafid et al., 2023).

The interrelatedness engendered by digital infrastructure has established a global network wherein computers, and by extension, individuals, are interconnected socially, economically, and politically. This transformation has facilitated the migration of numerous activities from the

tangible realm to the digital domain, resulting in an augmentation of time allocated to cyberspace, which has now become an essential component of actual existence. Within this framework, a novel form of power termed instrumentarianism functions asymmetrically via global platforms. The digital behaviors of individuals are converted into significant data by technology corporations, which subsequently commodify this data as a valuable economic asset. This epoch of surveillance capitalism has positioned individuals in a vulnerable state, as their private digital information is governed and processed by multinational corporations for capitalist objectives, with Google serving as a salient illustration, as elucidated by Zuboff (2023).

Surveillance capitalism epitomizes a contemporary manifestation of capitalism's intrinsic avarice, wherein the emphasis has transitioned from the domination of financial resources and land to the hegemony over data and cyberspace (Mayer-Schönberger & Ramge, 2018). The overarching objective remains unchanged: to proficiently exert control over the lives of individuals. This transition has rendered the enforcement of cybercrime legislation increasingly intricate, as the requisite data for legal substantiation is frequently dispersed and governed by corporations that operate under divergent national legal frameworks, thereby impeding law enforcement access. Furthermore, the utilization of digital technology is irrevocably connected to political and legal dilemmas, which further muddies attempts to attain digital sovereignty and to implement laws effectively in the context of these emergent challenges.

Using a foreign digital technology platform means handing over and entrusting the data of citizens who use the technology to be monitored and processed by the foreign company while also being subject to the laws of the country where the company originates. Therefore, technological independence is essential for a large country like Indonesia. Without it, digital sovereignty related to state interests is difficult to achieve.

The impact of weak digital sovereignty and law enforcement in cyberspace can be sterile. Content and actions that are clearly cybercrimes cannot be punished because of the difficulty of accessing the perpetrator's data or because the perpetrator is in another country. It is time to strengthen digital sovereignty. The method, in addition to re-evaluating regulations, must also foster a lot of cooperation with other countries that have the same problems. The goal is for law enforcement to access data controlled by global companies easily. In addition, it is also necessary to develop independent digital technology so that data is genuinely processed and placed domestically.

RESEARCH METHODS

This study uses a normative legal method, which is a process to find legal rules, legal principles, or legal doctrines to answer the legal issues faced. In order to get answers and resolve legal issues from this study, the problem-solving approach used the statutory approach and the conceptual approach (Soekanto, 2007).

RESULTS AND DISCUSSION

The Concept of Digital Economic Sovereignty

The concept of "digital sovereignty" has arisen concomitantly with the advancement of information and communication technologies, most notably the Internet. The Indonesian Dictionary characterizes the Internet as an electronic communication framework that interlinks computer networks and systematically organizes computer infrastructures globally through satellite or telephonic means. The American Supreme Court categorizes the Internet as "a distinctive

and entirely novel medium of global communication." Collectively, these instruments (email, mailing list servers, newsgroups, chat rooms, World Wide Web) form an exceptional new medium—referred to by its users as cyberspace, which is not situated in any specific geographical locale but is accessible to any individual, anywhere in the world possessing internet connectivity (Schweighofer & Proksch, 2001).

The digital economy encompasses all economic endeavors that leverage the internet and artificial intelligence (AI). This paradigm shift has revolutionized economic practices and enterprises, transitioning from manual operations to entirely automated frameworks. The digitization of the economy has demonstrated its capacity to effectuate substantial alterations, providing advantages such as enhanced efficiency, improved effectiveness, diminished production expenses, augmented collaboration, and increased interconnectedness among diverse entities (Pramono et al., 2024). Consequently, the transformation of the digital economy ought to be regarded as a viable alternative and a novel catalyst for economic advancement.

The notion of the digital economy was initially articulated by Don Tapscott, who delineated it as a sociopolitical and economic framework defined by an intelligent environment that incorporates information, diverse access modalities, capabilities, and the organization of information (Zahara et al., 2023). The digital economy is predicated upon four fundamental dimensions: the non-importance of physical location, the prominence of particular platforms as pivotal components, the evolution of interconnected networks, and the application of extensive data analytics. As the digital economy has progressively advanced, it has emerged as a novel phenomenon assuming an increasingly strategic position in the trajectory of global economic progress. This assertion is corroborated by the report published by Huawei and Oxford Economics, entitled "Digital Spillover" (2016), which asserts that the global digital economy has attained a valuation of $11.5 trillion, representing approximately 15.5 percent of the worldwide GDP.

The significant contribution of the digital economy can be observed through online trade, which has reshaped the global economic landscape as the "new face" of the worldwide economy. According to a McKinsey report (2018), online trade impacts at least four key areas. First, it brings substantial financial benefits to the economies of nations such as Indonesia, which is the largest e-commerce market in Southeast Asia. Its value is currently around $2.5 billion and is projected to reach $20 billion by 2022.

The implementation of Law No. 1 of 2024 concerning Information and Electronic Transactions, alongside Law No. 27 of 2022, provides a comprehensive framework governing all issues associated with electronic data utilization in the context of public welfare and the safeguarding of personal data. At the outset, these legislative measures encountered considerable dissent, as they were viewed as potentially inhibiting the exercise of freedom of expression within the digital realm.

State Protection Against the Use of Citizens' Personal Data in Terms of Human Rights and Justice for Global Platforms of Digital Technology Rulers

Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia articulates that every individual possesses the fundamental right to personal protection, familial integrity, honor, dignity, and property within their dominion, in addition to the right to security and protection against the

apprehensions arising from threats that may compel or inhibit actions constituting a human right. In relation to personal rights as integral components of human rights, Danrivanto Budhijanto elucidates that "The safeguarding of personal or private rights enhances human values, fortifies the bond between individuals and their communities, augments independence or autonomy in exercising control and procuring equity, and fosters tolerance while inhibiting discrimination and constraining governmental authority" (Budhijanto, 2010).

In light of the preceding elucidation, personal protection, as articulated in Article 28G, paragraph (1) of the 1945 Constitution, is intrinsically linked to the safeguarding of individual or private rights. From a historical perspective, the notion of privacy constitutes a universal principle acknowledged across various nations, whether enshrined in statutory law or articulated through ethical norms. This right is intertwined with the spiritual requisites of humanity, precisely the imperative for individuals to have their emotions and thoughts and the entitlement to relish their existence honored, commonly referred to as "the right to be let alone." The notion of data protection is frequently encompassed within the broader framework of privacy protection. Data protection is fundamentally associated with privacy, as defined by Allan Westin, who posited that privacy includes the prerogative of individuals, collectives, or organizations to ascertain whether information pertaining to them will be disseminated to external parties. This particular definition, recognized as information privacy, pertains explicitly to personal data. Furthermore, data protection is recognized as a fundamental human right, with numerous nations acknowledging data protection either as a constitutional right or in the form of "habeas data," which empowers individuals to safeguard their data and pursue rectification in instances of inaccuracies. Nations such as Albania, Armenia, the Philippines, Timor Leste, Colombia, and Argentina, despite their distinct historical and cultural contexts, have recognized the significance of data protection in promoting democratic processes and have enshrined its preservation within their constitutional frameworks (Greenleaf, 2014).

The accumulation and circulation of personal details infringe upon an individual's right to privacy, as this right fundamentally includes the power to decide about sharing personal information. Personal data is recognized as a valuable resource or commodity possessing considerable economic significance. The discourse surrounding the criticality of personal data protection has ascended to prominence alongside the burgeoning population of mobile phone and internet users. Numerous prominent incidents, especially those relating to personal data breaches that culminate in fraudulent or illicit behaviors such as sexual exploitation, have bolstered the argument for the necessity of legal frameworks aimed at safeguarding personal data (Djafar & Komarudin, 2014).

Indonesian State Policy and Strategy in Strengthening Digital Sovereignty Nationally

Implementation of Digital Sovereignty in Indonesia

The swift advancement of technology has yielded both advantages and potential hazards to operations conducted in cyberspace. To optimize the utilization of cyberspace, it is imperative to maintain national sovereignty within this domain through governmental instruments instituted by the state. A pivotal strategy for safeguarding digital sovereignty is the establishment of legal frameworks. In Indonesia, the notion of sovereignty in cyberspace is manifested in a variety of regulations promulgated by the

government. Presently, Indonesia has enacted several regulations aimed at attaining digital sovereignty, including Law No. 1 of 2024 concerning Information and Electronic Transactions and Law No. 27 of 2022 pertaining to Personal Data Protection (PDP Law). The PDP Law delineates classifications of data into personal data and specific data. Data related to individuals covers any information linked to a person that can be distinguished or is distinguishable, including their complete name, gender, nationality, faith, and various personal details that might be aggregated to identify an individual (Djafar & Komarudin, 2014). Focused data incorporates sensitive information such as health logs, biometric traits, genetic specifics, sexual orientation, political beliefs, criminal histories, information about minors, personal finance data, and other private information as indicated by legal statutes. In the framework of specific data under the General Data Protection Regulation (GDPR), Ardhanti elucidates the imperative of obtaining explicit consent.

Consequently, any agreement involving the procurement of personal data that lacks explicit consent from the data subject is deemed legally invalid. The commercial sector must also comprehend personal data protection within the context of technological innovations, such as the application of artificial intelligence (AI) in diverse industries, which presents a risk of infringing on privacy rights. Ardhanti accentuates the criticality of enforcing the PDP Law in the evolution of AI technology, which includes the necessity for enterprises to grasp personal data protection principles applicable in other jurisdictions and the requirement for binding agreements between data controllers and processors.

Optimal Implementation of Personal Data Protection to Strengthen National Digital Sovereignty

A legal framework designed to safeguard privacy and personal data in the contemporary digital economy must satisfy a minimum of three essential criteria: (1) it should possess an international dimension; (2) it ought to function as a unifying component for both individuals and the economic community. The initial criterion stipulates those transnational regulations must underpin the protection of privacy and personal data. Such regulations encompass stipulations that the transfer of privacy and personal data beyond national borders necessitates explicit consent and may only occur in jurisdictions that provide commensurate levels of privacy and data protection. The subsequent criterion asserts that, within the framework of the Digital Economy Era, the safeguarding of privacy and personal data must additionally encompass the protection of individual rights. In essence, these rights should not solely be characterized as negative rights demanding that the state abstain from specific actions but must also be construed as positive rights that can only be realized through proactive engagement by the state. The swift evolution and distinctive attributes of the digital economy compel the state to adopt more assertive measures. The third criterion posits that the protection of privacy and personal data can bolster individuals' confidence in their participation in the Digital Economy Era. On the matter of appropriate regulations for personal data safeguarding, Indonesia may look towards adopting models from other locales, especially the European Union's General Data Protection Regulation (EU GDPR) and the 1995 Personal Data Privacy Ordinance (PDPO) of Hong Kong, which defines six essential principles: (1) Confined collection of personal data solely for legitimate purposes

tied to the collector's functions; (2) Restricting the use and sharing of personal data strictly to the original purposes for which it was gathered, absent the consent of the data subject; (3) Ensuring data accuracy and taking feedback from third parties; (4) Obliging the deletion and disposal of data once it is deemed unnecessary for its intended purposes; (5) Enforcing security measures to protect personal data from unauthorized access or misuse; (6) Ensuring clarity in data management practices. The principles enshrined in the EU GDPR, which advocate for lawful, fair, and transparent data processing alongside secure data storage, also function as critical guidelines. Moreover, the establishment of an autonomous authority dedicated to personal data protection and the enhancement of cybersecurity protocols are imperative measures for mitigating data security vulnerabilities (Murray, 2007).

Jurisdiction in Cyber Space Law Towards Digital Economic Sovereignty

The advent of computer technology, subsequently succeeded by the internet, has catalyzed the development of novel communities or social collectives. As advancements in computer technology and the internet continue to progress at an accelerated pace, the proliferation of these communities escalates on a daily basis. Thus, activities occurring within cyberspace that involve individuals commonly designated as Netizens have also escalated in frequency, incorporating both constructive and detrimental behaviors. In light of this phenomenon, numerous scholars contend that it is imperative to impose regulations on cyberspace and the activities transpiring therein. The underlying rationale is that legal structures, by their inherent nature, are requisite in cyberspace to guarantee that activities are conducted in an orderly manner and are subject to oversight, thereby mitigating the emergence of radicalism within this domain. These apprehensions are substantiated, especially considering the prevailing notion of unrestricted access inherent in cyberspace. A significant obstacle that arises from cybercrime revolves around jurisdiction—specifically, how much a country can claim its legal authority or, on the flip side, the ability of a state to handle international legal matters. The discourse surrounding jurisdiction in cases of cybercrime has incited a bifurcation of perspectives among two distinct factions. The first faction, identified as Cyber-paternalists, asserts that cyberspace ought to be governed by extant laws and principles analogous to those employed in the tangible world.

Conversely, the second faction, termed Cyber-libertarians, posits that cyberspace constitutes a singular domain necessitating its distinct legal frameworks and principles, separate from those of the physical realm. Amidst this vigorous discourse, David R. Johnson posits four models as prospective resolutions: (a) exercising authority through current judicial systems; (b) instituting international accords on the regulation of cyberspace; (c) the establishment of an international entity tasked explicitly with overseeing cyberspace. These models seek to address the intricate challenges of jurisdiction and law enforcement within the digital sphere as nations confront the complexities of attaining digital economic sovereignty.

CONCLUSION

The Indonesian State Policy and Strategy for Enhancing Digital Sovereignty on a National Level can be achieved through the implementation of optimal personal data protection measures to fortify digital sovereignty at the national level, the establishment of an Independent Authority tasked with Personal Data

Protection, the reinforcement of Cybersecurity measures aimed at mitigating Data Security Risks, and the jurisdictional application of Cyber Space Law in relation to Digital Economic Sovereignty. Consequently, it is imperative to develop comprehensive regulations that safeguard personal data as an integral component of human rights. A balance must be struck in the governance of personal data processing alongside the assurance of rights protection and the awareness of data subjects. Furthermore, it is essential to construct a secure digital economic ecosystem by providing legal certainty for enterprises and enhancing consumer trust. Finally, uniformity in Personal Data Protection regulations at the international level is necessary to promote the advancement of the digital economy.

LIMITATION

This investigation fundamentally employs normative legal research, which is intrinsically concentrated on legal statutes, principles, and doctrines. Although this methodology is instrumental in comprehending and scrutinizing legal frameworks, it restricts the capacity to encompass the dynamic and swiftly transforming characteristics of digital technology and cyber threats. The study's dependence on pre-existing legal doctrines may inadequately reflect the practical challenges and instantaneous developments transpiring within the cyberspace ecosystem. Also, the analysis is constrained by the geographical and legal environment of Indonesia, which may affect the relevance of the insights to other nations with diverse legal arrangements and technological systems. The research also does not extensively incorporate empirical data or case studies, which could furnish a more holistic understanding of how digital sovereignty is being contested and enforced in practical scenarios.

IMPLICATION

The outcomes of this investigation possess profound ramifications for policymakers, legal professionals, and technology stakeholders within Indonesia and in the broader international context. Primarily, the research emphasizes the imperative for Indonesia to formulate and implement comprehensive legal structures that ensure the protection of national digital sovereignty, especially in relation to the pervasive global digital platforms that dominate the online sphere. The introduction of extensive personal data protection legislation, alongside the establishment of an autonomous regulatory body for data protection, constitutes vital measures for the preservation of Indonesia's digital environment. Furthermore, the research accentuates the necessity for international cooperation and the harmonization of data protection standards to guarantee that Indonesia's digital sovereignty is acknowledged and upheld on a worldwide level. For the commercial sector, the implications are unmistakable. There exists an immediate requirement to recalibrate operations in response to these regulatory transformations by ensuring adherence to data protection statutes, particularly concerning the deployment of emerging technologies such as artificial intelligence. In summary, the study advocates for a reasonable approach that not only safeguards individual privacy rights but also promotes innovation and economic development within a secure and sovereign digital landscape.

REFERENCES

Budhijanto, D. (2010). *Hukum telekomunikasi, penyiaran, dan teknologi informasi: Regulasi dan konvergensi*. Refika Aditama.

Djafar, W., & Komarudin, A. (2014). Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci.

Elsam, Jakarta.

Greenleaf, G. (2014). *Asian data privacy laws: trade & human rights perspectives*. OUP Oxford.

Hafid, M., Firjatullah, F. Z., & Pamungkaz, B. W. (2023). Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara. *Jurnal Pendidikan Tambusai*, *7*(2), 9548–9556.

Mayer-Schönberger, V., & Ramge, T. (2018). *Reinventing capitalism in the age of big data*. Hachette UK.

Murray, A. (2007). *The regulation of cyberspace: control in the online environment*. Routledge-Cavendish.

Pramono, W., Hariadi, B., Mulia, R. A., Putri, R. P., Meilina, S., & Suryaningsih, S. (2024). A Literature Review on the Impact of Legal Reforms on Administrative Efficiency in Local Governments. *Jurnal Ilmiah Ekotrans & Erudisi*, *4*(1), 123–133.

Schweighofer, E., & Proksch, W. (2001). *Internet Governance and Territoriality, Nationalisation of Cyberspace*.

Soekanto, S. (2007). *Penelitian hukum normatif: Suatu tinjauan singkat*.

Zahara, A., Kabullah, M. I., & Putera, R. E. (2023). Effectiveness of the OSSRBA (Online Single Submission Risk Based Approach) System in Business Licensing Services in Payakumbuh City DPMPTSP. *Jurnal Ilmiah Ekotrans & Erudisi*, *3*(2), 22–40.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203–213). Routledge.