Reconstruction The Principle of Legitimate Interest in Data Processing on Indonesia Data Protection Law[1]

Indra Rahmatullah[1], Pujiyono[2], Hari Purwadi[3]

{indra.rahmatullah@student.uns.ac.id[1], pujifhuns@staff.uns.ac.id[2], hpurwadie@gmail.com[3]}

Sebelas Maret University
Jl. Ir. Sutami No. 36, Jebres, Surakarta, Jawa Tengah 57126[1,2,3]

Abstract. All companies that serve commercial transactions require personal data. With the data obtained, it will be easier increase expansion. To protect the right of data subjects so that they are processed under applicable legal provisions, there are principles when data is processed. Legitimate interest is one of the principles in processing personal data, which is essential to ensure that it does not harm the data subject. However, the legitimate interest principle is not clearly regulated in Indonesian data protection law, which causes interpretation gaps and legal uncertainty and tends to abuse the power of the government. To solve the problem, the research uses normative legal research methodology, statute and conceptual approach and analyzed in normative philosophy. The legitimate interest principle in Indonesia's personal data protection law has still not adopted the balancing test mentioned in international regulation. Therefore, it is necessary to reconstruct the legitimate interest principle.

Keywords: Data Processing, Legitimate Interest; Personal Data.

1 Introduction

Data and globalization are closely related since data is a component of the globalization of technology. There are 4 different kinds of foreign service offers in the context of globalization, including: 1. Cross border supply, namely foreign services, 2. Consumption abroad, namely the movement of foreign consumers, such as tourism. 3. Commercial presence, namely the presence of foreign businesses, such as foreign banks, and 4. Presence of natural persons, specifically, the flow of professionals moving from one nation to another, including physicians, accountants, teachers, and nurses [2]. Commercial presence is dominant nowadays because technological developments with the rise of online platforms and telecommunications drive it. Online transactions accounted for 58.9% of all types of international trade in 2020.[2] In 2025, the potential for digital trade will have an economic impact of up to 2,305 trillion rupiah [3].

Data is the primary fuel for digital economy activity. Businesses can profile the customers they are targeting using the data (profiles and target people). Typically, this technique uses data to produce ads that match the profile of the intended audience. Future models can also be predicted

ICHSS 2023, December 27, Surakarta, Indonesia

DOI 10.4108/eai.27-12-2023.2349690

using data (model probabilities). A digital system (digital things), which is a system utilized by online platforms like Uber and Go-Jek for its operations, can be built using a range of data and with assistance from algorithm analysis by the company. The web platform will not function without data [4].

In other hand, data is like new engine lubricant or oil in promoting economic innovation and creativity. Amazon, Uber, Twitter, and Airbnb are examples of unicorn digital companies that think their data may help with commercial growth [5], [6]. Data can be used in various ways, including: 1. Data is sold or licensed; 2. New goods are developed, or products are licensed; 3. Increase product output, and 4. Boost manufacturing effectiveness [5].

However, instead of expanding business expansion, on the contrary, it results in losses for data subjects because there is no guarantee that the data being processed has received consent from the data subjects. Personal data that other parties have processed without the consent of the data subject is in various storage places where security is not guaranteed, the use of the data is uncontrolled, and the party who uses the data needs to be clarified. Hence, incidents of personal data leaking to the public often occur [7]–[11]. To protect data subjects, the personal data protection regime at the international level has created a rigorous concept of personal data processing. There are several principles in the processing of personal data, one of which is the principle of legitimate interests, namely processing requested by the controller or by a third party with the needs, objectives and balance of the personal data subject [5], [12].

However, the problem is that the principle of legitimate interests in Indonesia, regulated in Law No. 27 of 2022 concerning the Protection of Personal Data is still general. It needs to be clarified what is meant by legitimate interests and the criteria or indicators of the legitimate interests and balance of data controllers and personal data subjects. The lack of clarity and ambiguity in the formulation of the principle of legitimate interest has the potential to result in abuse of power from the state, which is detrimental to data owners both materially and morally.

2 Research Methods

To solve the problem, the research uses normative legal research methodology, statute and conceptual approach and analyzed in normative philosophy.

3 Result and Discussion

3.1 Personal Data Processing

Personal data is one of the rights to privacy in the concept of Human Rights (HAM), namely a right that humans have because they are solely human. This right is not granted by society and applicable law but because it is naturally human dignity [13]. According to Article 12 Universal Declaration of Human Rights (UDHR), the right of privacy: “No one may have their personal, family, domestic, or correspondence issues unilaterally interfered with, and it is forbidden to trample on their honor and good reputation.”

In Europe, the issue of privacy had spread to the issue of protecting personal data, which began with the end of the Second World War and the expansion of sophisticated communication and information tools until it culminated in the World Cold War when governments stalked their people. Since then, a legal consciousness has grown to safeguard personal data through laws.

Germany and Switzerland were the first to establish rules, followed by other European nations in 1970 and 1973.[14] In 1980, Austria, Germany, Luxembourg, and has continued to expand up to the present [15].

On a larger scale, the Organization for Economic Cooperation and Development (OECD) and the Council of Europe both introduced legislation governing the use of personal data (the Council of Europe). Both groups were established following the Second Cold War. The goal of the OECD is to advance international commerce and global economic growth. The Council of Europe is working to promote democracy, the rule of law, human rights, and social welfare in Europe. These two organizations gave rise to two laws protecting the privacy of individuals. In 1980, the OECD published The Protection of Privacy and Trans-border Flows of Personal Data Guidelines. The Convention for the Protection of Individuals concerning Automatic Processing of Personal Data (Convention 108) was signed by the Council of Europe in 1981 [15].

Convention 108 of 1981 was amended in 2018, and the Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data of 1980 were amended in 2013. Apart from that, there are also The Guidelines for regulating computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72) and the APEC Privacy Framework in 2004 and amended in 2015 [12]. Significant developments in data protection occurred when the European Union carried out legal unification through the European Union General Data Protection Regulation (EU GDPR—General Data Protection Regulation) in 2016 and came into force on 25 May 2018 in 27 countries within the European Economic Area (EEA). GDPR is called "The toughest data protection law in the world" because it has strict rules and sanctions for violators. GDPR has extra-territorial jurisdiction[16] because it applies to all parties wherever located, including those outside the European Union, as long as they carry out data processing activities for someone who lives within the European Union [17], [18].

In Europe, GDPR is a replacement for previous regulations, namely the 1995 Data Protective Directive, which is out of date in protecting personal data and data security standards in the digital era. This regulation regulates the processing, storage and management of public data in the European Union. GDPR aims to strengthen data protection in Europe due to developments in digital technology. Even though GDPR only protects the people of the European Union, the impact of GDPR affects the global order targeted by the European market [19].

Many personal data regulations above show that personal data is essential in today's digital era. According to research by economists who have proven personal data has enormous economic value [20], [21]. Even personal data has become a powerful tool for digital companies. Personal data used for specific purposes must go through a data processing stage. According to GDPR, processing personal data is the entire process of collection, recording, organisation, structuring, storage, adaptation or change, retrieval, consultation, use, disclosure by transmission, disclosure, alignment or combination, restriction, and erasure or destruction [5].

The collection of personal data must based on the data subject's consent and the legitimate interests principle. The data collected must be used for the initial purpose and signed by the right person based on information security/authentication principles (username, password, digital certificate, PIN). Data must be valid and accurate, and if it transfers to another person or country, that country must have well-established regulations. In addition, there must be a time limit for storing and deleting data if it is no longer used [22].

Any processing of personal data must be conducted based on applicable principles to protect the data owner's rights [5], [17], [23], [24] as follows:

a. *Consent*. Processing of personal data is based on consent from the data subject. This principle is the most important because it gives the data subject the right to control the data. This consent must be clear, unambiguous, specific, informative and written even in digital form.

b. *Performance of Contract/Contractual Obligation*. Processing of personal data is conducted to fulfil contractual obligations.

c. *Legal Obligation*. Processing of personal data is carried out due to the data controller's legal obligations in accordance with statutory provisions. For example, companies process their employees' data to register for the social security system and taxation.

d. *Vital Interest*. The processing of personal data aims at the vital interests of the data owner or another person. Example: The government monitors disease development during endemic status, and emergency in hospital.

e. *Public Interest*. Data processing aims to serve legitimate interests carried out by official authorities. This principle must be explained in the statutory regulations regarding its intent and scope so as not to cause an abuse of power.

f. *Legitimate Interest*. Processing is necessary for legitimate purposes and interests.

These principles are carried out by the European Convention on Human Rights (The European Convention on Human Rights/ECHR) to maintain personal data confidentiality. In Article 8, paragraph 2, public authorities should not interfere with privacy rights except based on law and in the interests of national security, public security, national economy, crime prevention, protection of health and morality, and other freedom rights [25].

3.2 Problem with Legitimate Interest in Processing Personal Data

The principles of data processing as applicable within the scope of international law have been adopted by Indonesia through Law no. 27 of 2022 concerning Personal Data Protection in Article 20 paragraph (2), namely: a. explicit valid consent from the personal data subject, b. fulfilment of contractual obligations, c. fulfilment of legal obligations, d. completion of protecting vital interests, e., public services and f. legitimate interests.

Specifically, the principle of legitimate interest is regulated in letter (f) above, namely "carrying out duties of legitimate interest". However, the principle of "legitimate interest" has unclear norms. There are no clear and measurable indicators, so they have the potential to be misinterpreted and lead to abuse of power by certain parties, whether the state or other parties, in utilizing someone's personal data.

Supposedly, Law No. 27 of 2022 concerning Personal Data Protection as the primary regulation for personal data protection in Indonesia clearly explains the principle of legitimate interest by referring to the provisions of Article 6 paragraph 1 letter f of the General Data Protection Regulation (GDPR). The principle of legitimate interest is a principle in the processing of personal data that is very flexible and situational under any conditions, so it demands to be clearly articulated. Therefore, implementing this principle must be carried out carefully by using a "balancing test" to measure the balance of interests of both the interests of the personal data subject and the data controller in the context of safeguarding fundamental rights and freedoms [26]. The interests mentioned are for commercial, personal, and, more significantly, social benefits [27].

The steps for data controllers in carrying out balance tests are as follows [28]:

1. The position of authority between the data subject, the data controller, and the third party needs to be solved. The parties must be placed in an equal position even though the data owner is in a weaker position than the data controller in some situations. For example, employees in a company are lower parties compared to company management, who process employees' data.
2. Characteristics of personal data. Unique or sensitive personal data such as beliefs, religion, race, genetics, and health must be processed carefully.
3. Processing is carried out proportionally and considers the impact on the personal data subject.
4. The processing goal must be rational regarding what happens to the data. The data controller must certify that the data processed is fit for purpose. If the data controller is not sure about this, then the data controller is obliged to carry out consultations, FGDs and market studies.
5. Additional security measures. Apart from ensuring system security, data controllers are also required to take extra security measures when processing personal data, such as carrying out anonymization, aggregation, improving data security systems, and assessment.

The steps above attempt to reconstruct the principle of legitimate interest by adopting a balancing test in every personal data processing activity. This legal reconstruction aims to create legal certainty in personal data protection law in Indonesia because good regulation does not open up opportunities for broad interpretation and ambiguity, resulting in legal chaos.

According to Utrecht, legal certainty contains two meanings: first, general rules that make someone know what actions they can or cannot do. Second, it guarantees a person's security from arbitrary government actions. With these regulations, people can know what can be done and how far the state intervenes in them [29]. Jan M. Otto explained the characteristics of legal certainty with the availability of legal rules that are clear, consistent, accessible, and issued by state authorities [30].

Legal certainty is part of three legal values. According to Gustav Radbruch, the law must have three values [31]: First, the principle of legal certainty (*rechtmatigheid*), namely certainty based on laws or regulations. The form is positive or written law from an authorized institution, has strict sanctions, and is promulgated by state institutions. Second, the principle of legal justice (*gerectigheit*), namely the equal rights of everyone before the court. This justice is the moral foundation of law and a barometer of positive law. Without justice, a rule does not deserve to become law. Third, the principle of legal utility (*zwechmatigheid*), namely that the law must provide benefits or be useful (utility) in people's lives.

Meanwhile, Mochtar Kusumaatmadja stated that to achieve order, there must be legal certainty in human interactions in society because humans cannot optimally develop the talents and abilities given to them by God without the certainty of law and order [32]. The reconstruction of the principle of legitimate interest is also a step to strengthen a person's privacy rights so that their personal data is not misused by any party, including the state. Personal data, which constitutes the right to privacy, emerged along with the development of theories of state and society.

According to Alan Westin, there is a relationship between privacy and the type of government in society. In a society with an authoritarian government, the state places public and individual affairs as the primary goal. Hence, the state refuses to protect the privacy of individuals, families, social groups and associations legally and socially as a consequence of a hedonistic and dangerous regime. An authoritarian government constantly monitors community groups. In contrast, in a society with a democratic government, the state has a solid commitment to guaranteeing individual and associational freedom. The state considers the private sector the main force of social dynamics and morality. Public affairs carried out by the state function to serve and protect the people. The power of the government or state is limited to protecting citizens' civil liberties from all kinds of interference ranging from beliefs, associations, behaviour (except in extraordinary situations), and strict procedures [33].

What Alan Westin expressed about the concept of an authoritarian state that makes a person's privacy a threat is in line with the characteristics of repressive law. According to Nonet and Selznick, repressive law is an unjust system because the law is attached to power, making power above the law. Legal institutions are close to political institutions because law is subject to state power. Every policy or decision of the government in power makes other parties subordinate by ignoring equality. The law becomes repressive because it is forced to become a tool of social order [34].

In summary, the character of repressive law is as follows: 1. Order is the primary goal of the law, 2. The legitimacy of binding law is state power, 3. The regulations are strict and detailed towards the object of the law but soft towards the ruler, 4. The reasons for making laws follow the tastes of the ruler; 5. The power above the law, 6. Community law obedience is unconditional, and disobedience to the law is a crime, 7. Community participation through submission and criticism is defined as disobedience [35].

Nonet and Selznick's repressive law above aligns with the thinking of Adam Podgorecki, who equates it with authoritarian law. According to Adam, authoritarian law has the following characteristics: 1. The law's substance contains rules binding unilaterally and changes according to the tastes of the ruler; 2. The law is created as a cover for unlimited power intervention; 3. The public accepts the law because it is forced (fake), 4. Legal sanctions cause social disintegration, and 5. The ultimate goal of law is institutional legitimacy without regard to the response from society [35], [36].

Historically, privacy is the antithesis of a situation where the King's power is so absolute that it threatens a person's freedom. Privacy gives citizens the right not to be interfered with by anyone regarding their private lives. It is a contradiction to the situation of the King's absolutism. In the Middle Ages, the church's dominance was powerful in state life. Some kings claimed that they reigned because of God's will; the King's power came from God, and the King was God's representative or shadow in the world [37]. The thoughts of state philosophers such as Machiavelli, Jean Bodin, and Thomas Hobbes regarding the theory of sovereignty have significantly contributed to the absolute power of the King, which is known in the theory of state sovereignty.

According to Machiavelli, the state's goal is to create order and tranquillity, which can only be achieved when the king has absolute power that cannot be obstructed or prevented by anyone or any institution. Even a king or country can justify any means (the end justifies the means). Jean Bodin believes that sovereignty is personified in a king so that he is not responsible to anyone other than God. Meanwhile, Hobbes states that naturally, life is disorderly, unfair and

chaotic, which is illustrated as animal life (homo homini lupus). Therefore, to survive, they agreed to hand over several rights to the king so that he had absolute power [37].

This situation brought about the French Revolution, which is considered a form of monumental change and development in law, namely the recognition of human rights and the theory of popular sovereignty. The French Revolution triggered the concept, understanding and struggle to be free from the oppression of absolutism and monarchy. The French Revolution was known as political and social revolution because it caused a cultural shift with the emergence of new norms, socio-cultural practices and religious beliefs [38]. It is also what made philosophers such as John Locke and Montesquieu introduce the idea of limiting the absolutism of state power [39].

From these figures, theories of the relationship between the people and the state in the constitutional system emerged, such as the theory of separation of powers, protection of civil and political freedoms and the independence of judicial power [39]. These concepts are the philosophical basis for protecting a person's privacy in the form of personal data.

The relevance of the reconstruction of the principle of legitimate interest is increasingly urgent not only because it symbolizes the protection of individuals from state intervention as taught in the theory of popular sovereignty. However, in the current digital era, forming a legal system must also consider the theory of digital sovereignty. This theory emerged because of various threats of attacks on state security via the internet [40]. Not only domestic, the issue of digital sovereignty has also become a severe concern internationally since the Covid-19 pandemic. Moreover, there are indications of neocolonialism through data ownership [41].

Digital sovereignty is interpreted as a concept that the state must have full authority over internet technology and protect its citizens from various challenges posed by digital transformation and internet infrastructure by making legal regulations manifesting digital sovereignty [42]–[44]. Therefore, reconstructing the principle of legitimate interest in processing personal data in Indonesia must have explicit norms, size and scope. Thus, the principle of legitimate interest in data processing fulfils the fundamental legal values, namely legal certainty, justice and legal benefits that protect the rights of citizens.

4 Conclusion

The right to privacy is one of the human rights that state and non-state actors must protect. The right to privacy has transformed into personal data, which has become the focus of attention in the current era of globalization, especially in the digital economy. The data processing stages are a core part of the concept of privacy protection, which is formed into personal data protection.

The data processing stage includes collecting, recording, organizing, structuring, storing, adapting or changing, retrieving, consulting, using, disclosing through transmission, opening, aligning or combining, restricting, deleting or destroying data with economic value. Therefore, the law provides stringent restrictions when other parties process personal data. The principle of public interest must be reconstructed with a balancing test so that legal norms are clear and specific. It aims to avoid losses to data subjects and abuse of power by the state.

References

[1] Steven Vago, *Law and Society*, 5th ed. New Jersey: Prentice Hall, Upper Saddle River, 1997.

[2] UNCTAD, *Digitalisation of Services : What Does It Imply to Trade and Development ?* Geneva: UNCTAD, 2022.

[3] H. Foundation and Alphabeta, "Komodo Digital : Cara Indonesia bisa menangkap domestik dan luar negeri," Jakarta, 2017.

[4] J. Sadowski, "When data is capital: Datafication, accumulation, and extraction," *Big Data Soc.*, vol. 6, no. 1, pp. 1–12, 2019, doi: 10.1177/2053951718820549.

[5] C. Giakoumopoulos, G. Buttarelli, and M. O'Flaherty, *Handbook on European data protection law 2018 edition*, 2018th ed. Luxembourg: European Union Agency for Fundamental (FRA), the EU Agency for Fundamental Rights Europe, the Council of Supervisor, the Registry of the European Court of Protection, Human Rights) and the European Data, 2018. doi: 10.2811/58814.

[6] D. Nguyen and M. Paczos, *Measuring the economic value of data and cross-border data flows*, 297th ed., no. 297. Paris: OECD, 2020.

[7] S. Dewi, "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya," *Sosiohumaniora*, vol. 19, no. 3, pp. 206–212, 2017.

[8] S. Dewi Rosadi and G. Gumelar Pratama, "Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia," *Verit. Justitia*, vol. 4, no. 1, pp. 88–110, 2018, doi: 10.25123/vej.2916.

[9] M. H. Rumlus and H. Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik," *J. HAM*, vol. 11, no. 2, p. 285, 2020, doi: 10.30641/ham.2020.11.285-299.

[10] Faiz Rahman, "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia," *J. Legis. Indones.*, vol. 18, no. 1, pp. 107–15, 2021.

[11] Nurhasanah and I. Rahmatullah, "Financial Technology and the Legal Protection of Personal Data: The Case of Malaysia and Indonesia," *Al-Risalah*, vol. 20, no. 2, pp. 197–214, 2020, doi: 10.30631/al-risalah.v20i2.602.

[12] W. Djafar and M. J. Santoso, "Perlindungan Data Pribadi Konsep. Instrumen dan Prinsipnya," Jakarta, 2019.

[13] Retno Kusniati, "Sejarah Perlindungan Hak Hak Asasi Manusia Dalam Kaitannya Dengan Konsepsi Negara Hukum," *Inov. J. Ilmu Huk.*, vol. 4, no. 5, pp. 79–91, 2011, [Online]. Available: https://online-journal.unja.ac.id/index.php/jimih/article/view/536

[14] M. Tzanou, *The Fundamental Right to Data Protection Normative Value on The Context of Counter Terrorism Surveillance*. Oregon: Hart Publishing, 2017.

[15] I. Kaļķe, "The Challange of Personal Data Protection in The Era of Digital Economy," Riga Graduate School of Law, 2018.

[16] Y. H. Sirait, “General Data Protection Regulation (GDPR) dan Kedaulatan Negara Non-Uni Eropa,” *Gorontalo Law Rev.*, vol. 2, no. 2, pp. 60–71, 2019.

[17] Riza Roidila Mufti, *A Policy Brief EU General Data Protection Regulation (GDPR)*, 2021st ed. Brussels: Kedutaan Besar Republik Indonesia di Brussel, 2021. [Online]. Available: https://kemlu.go.id/download/L1NoYXJlZCUyMERvY3VtZW50cy9icnVzc2VsL3Jlc2VhcmNoJTIwc2VyaWVzL0dEUFIlMjAtJTIwdXBkYXRlZC5wZGY=

[18] N. Tsamara, “Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara,” *J. Suara Huk.*, vol. 3, no. 1, p. 53, 2021, doi: 10.26740/jsh.v3n1.p53-84.

[19] H. Li, L. Yu, and W. He, “The Impact of GDPR on Global Technology Development,” *J. Glob. Inf. Technol. Manag.*, vol. 22, no. 1, pp. 1–6, 2019, doi: 10.1080/1097198X.2019.1569186.

[20] C. Wang, N. Zhang, and C. Wang, “Managing Privacy in The Digital Economy,” *Fundam. Res.*, vol. 1, no. 5, pp. 543–551, 2021, doi: 10.1016/j.fmre.2021.08.009.

[21] A. Acquisti, C. Taylor, and L. Wagman, “The economics of privacy,” *J. Econ. Lit.*, vol. 54, no. 2, pp. 442–492, 2016, doi: 10.1257/jel.54.2.442.

[22] R. P. Romansky and I. S. Noninska, “Globalization and Digital Privacy,” *Electrotech. Electron. E+E*, no. August, pp. 2008–2011, 2016.

[23] Organisation for Economic Co-Operation and Development (OECD), *The OECD Privacy Framework*. 2013, pp. 1–154.

[24] Tetiana L. Syroid, T. Y. K. V. M, Shamraieva, Olexander S. Perederii, I. B. Titov, and Larysa D. Varunts, “The Personal Data Protection Mechanism in the European Union,” *Int. J. Econ. Bus. Adm.*, vol. VIII, no. Special Issue 1, pp. 190–201, 2020, doi: 10.35808/ijeba/536.

[25] A. Lukacs, “What Is Privacy? The History and Definition of Privacy,” *Tavaszi Szel 2016 Tanulmanyköoet I, Budapest, 15-17 April*, vol. 2, no. 3, pp. 256–265, 2017, [Online]. Available: http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf

[26] G. Zanfir-Fortuna, T. Troester-Falk, and M. McCluskey, “Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases.”

[27] D. P. Commission, “Guidance Note: Legal Bases for Processing Personal Data,” 2019. [Online]. Available: https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance on Legal Bases_Dec19_1.pdf

[28] European Commission, “Opinion 06/2014 onTthe Notion of Legitimate Interests of The Data Controller Under Article 7 of Directive 95/46/EC,” Brussels, 06/2014, 2014. [Online]. Available: https://ec.europa.eu/newsroom/article29/news.cfm?item%7B_%7Dtype=1360

[29] Riduan Syahrani, *Rangkuman Intisari Ilmu Hukum*. Bandung: Citra Aditya Bhakti, 1999.

[30] Sidharta, *Moralitas Profesi Hukum: Suatu Tawaran Kerangka Berpiki*. Bandung: Refika Aditama, 2006.

[31] Sidharta, “Reformasi Peradilan dan Tanggung Jawab Negara,” in *Bunga Rampai Komisi Yudisial, Putusan Hakim: Antara Keadilan, Kepastian Hukum, dan Kemanfaatan*, Jakarta: Komisi Yudisial, 2020.

[32] Mochtar Kusumaatmadja, *Pengantar Ilmu Hukum, Suatu Pengenalan*. Bandung: Alumni, 2000.

[33] A. F. Westin, “Social and Political Dimensions of Privacy,” *J. Soc. Issues*, vol. 59, no. 2, p. 911, 2003, doi: 10.2307/3479272.

[34] P. Nonet and P. Selznick, *Law & Society in Transition Toward Responsive Law*. New York: Taylor & Francis, 2001.

[35] S. B. Soedjono, “Hukum Represif dan Sistem Produksi Hukum yang Tidak Demokratis,” *J. Huk. IUS QUIA IUSTUM*, vol. 7, no. 13, pp. 157–169, 2000, doi: 10.20885/iustum.vol7.iss13.art13.

[36] A. Podgorecki and V. Olgiati, Eds., *Totalitarian and Post-Totalitarian Law*. Aldershot, UK: Dartmouth, 1996.

[37] Soehino, *Ilmu Negara*. Yogyakarta: Liberty, 1981.

[38] S. K. Christmas and E. Purwanti, “Perkembangan Sistem Pemerintahan dan Konsep Kedaulatan Pasca Revolusi Perancis Terhadap Hukum Internasional,” *J. Pembang. Huk. Indones.*, vol. 2, no. 2, pp. 222–235, 2020, doi: 10.14710/jphi.v2i2.222-235.

[39] E. Carolan, “The Concept of a Right to Privacy,” *SSRN Electron. J.*, pp. 1–30, 2012, doi: 10.2139/ssrn.1889243.

[40] I. Cahyadi, “Tata Kelola Dunia Maya Dan Ancaman Kedaulatan Nasional,” *Politica*, vol. 7, no. 2, pp. 210–232, 2016.

[41] A. Makarychev and E. Wishnick, “Anti-Pandemic Policies in Estonia and Taiwan: Digital Power, Sovereignty and Biopolitics,” *Soc. Sci.*, vol. 11, no. 3, 2022, doi: 10.3390/socsci11030112.

[42] P. Hummel, M. Braun, M. Tretter, and P. Dabrock, “Data sovereignty: A review,” *Big Data Soc.*, vol. 8, no. 1, 2021, doi: 10.1177/2053951720982012.

[43] K.-L. Tan, C.-H. Chi, and K.-Y. Lam, “Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization,” vol. 637533, pp. 1–18, 2022, [Online]. Available: http://arxiv.org/abs/2202.10069

[44] R. Á. Pinto, “Digital sovereignty or digital colonialism?,” *Sur*, vol. 15, no. 27, pp. 15–27, 2018.