

## The urgency of establishing a special agency of personal data protection and supervision to ensure the Indonesian citizens' privacy rights

Ferina Widyawati Ayu Silvi<sup>1</sup> and Anom Wahyu Asmorojati<sup>2</sup>✉

<sup>1,2</sup>Faculty of Law, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

✉ anom.asmorojati@law.uad.ac.id

### Article info

Submitted:  
2022-April-20

Reviewed:  
2022-May-7

Accepted:  
2022-July-28



This work is licensed under  
a Creative Commons  
Attribution-NonCommercial  
4.0 International License

### Publisher

Universitas Muhammadiyah  
Magelang

**Keywords:** Personal Data,  
Protection, Supervision,  
Agency

### ABSTRAK

Perlindungan Data Pribadi merupakan hak asasi manusia, secara konstitusional kewajiban negara untuk dihormati, dipenuhi, dan dilindungi sebagaimana amanat Pasal 28 C ayat (1) UUD 1945. Namun, karena kebocoran data besar-besaran membuktikan bahwa hak tersebut belum sepenuhnya dilindungi. Penelitian ini bertujuan untuk mengetahui perlindungan hukum terhadap data pribadi warga negara Indonesia dengan mendirikan badan khusus dan dimaksudkan untuk menemukan format untuk instansi khusus perlindungan dan pengawasan data pribadi yang ideal untuk diterapkan di Indonesia. Metode penelitian yang digunakan adalah yuridis normatif melalui penelitian kepustakaan. Data dianalisis secara kualitatif dan disajikan dengan metode deskriptif-analisis. Penelitian ini juga bersifat doktrinal dengan bahan hukum primer dan sekunder. Hasil penelitian menyimpulkan bahwa perlindungan data pribadi tergolong isu yang muncul akibat kekosongan hukum. Apalagi belum adanya badan khusus yang berperan penting dalam melindungi atau mengawasi data pribadi warga negara Indonesia. Apalagi urgensinya untuk membentuk badan khusus perlindungan dan pengawasan data pribadi telah menjadi isu global mengacu pada regulasi dan konvensi internasionalnya, luasnya konflik kepentingan dalam pengawasan dan pengelolaan data, dan akibat terjadinya kebocoran data pribadi secara masif.

Kata Kunci: Data Pribadi, Perlindungan, Pengawasan, Instansi

### ABSTRACT

Personal Data Protection is the right of humans, constitutionally the state's obligation to respect, fulfill, and protect as mandates in Article 28 C paragraph (1) of the 1945 Constitution. However, due to the massive data leaks prove that the rights have not been protected. The research is aimed to know the legal protection for the Indonesian citizens' personal data by establishing a special agency and intended to find the ideal format of the special agency for personal data protection and supervision to be implemented in Indonesia. The research methods used is the juridical normative through library research. The data were analyzed qualitatively and presented using the descriptive-analysis method. The research is also doctrinal with primary and secondary legal materials. The research concluded that the personal data protection classified as the emerge issues due to the vacuum of law. Moreover, the absence of special agency which plays the important rules to protect or supervise the personal data for the

Indonesians. Moreover, its urgency for establishing a special agency for personal data protection and supervision has become the global issues refer to its international regulation and convention, wide conflict of interests in data supervision and management, and due to the occurrence of massive personal data leaks.

## I. INTRODUCTION

One of the goals of the Indonesian government mentioned in the 4<sup>th</sup> paragraph of the Preamble of the Indonesian 1945 Constitution (UUD 1945) stated mentioned regarding on the protection the whole Indonesian nation and the entire native land of Indonesia. It by means that UUD 1945 mandate the obligation of state to protect the Indonesian citizens including form of personal data protection. In other words, personal data protection is the embodiment of personal rights. Alan Westin in Wahyudi Djafar and Asep Komarudin defines personal rights as the rights of each individual, group, or institution to determine on its own when, how, and how far the personal information can be transferred to other parties (Djafar & Komarudin, 2014: 4).

In essence, personal data protection further mentioned as the state's responsibility through Article 28 G paragraph (1) of UUD 1945. Therefore, the state must attempt to guarantee citizens' personal rights (Doly, 2021: 225). While, in reality the state has not been able to fulfill their responsibility, it proved by the intervention of personal data through surveillance, tapping, and other disturbances amidst the high use of information and communication technology through the internet.

Based on Laws Number 24 of 2013 regarding Population Administration, personal data means the personal data stored, maintained, and of which the accuracy and confidentiality are maintained. Personal data consists of full name, address, phone number, birth date, Number of Family Card (KK), Single Identity Number (NIK), fingerprint, iris, signature, disability, or other data categorized as a personal disgrace.

During 2020-2021, was considered the dark years for Indonesia's personal data security. It is because there were data stored in the government and private parties' database was leaked. Based on the data gathered by Kompas.com, in 2020, much data from various sectors was leaked. For example, the subscribers' data of Tokopedia and Bhinneka.com (May 2020), Permanent Voter List (DPT) data of the 2014 general election (May 2020), data of the Kreditplus users (August 2020), Shopback users' data (September 2020), RedDoorz users' data (November 2020), dan platform Cermati users' data (November 2020) (Conney Stephanie, 2021).

Further, in 2021, data leaks occurred much to those in the government. Some examples are 279 million users' data of health care and social security agency (BPJS) (May 2021), 2 million of BRI life insurance clients' data (July 2021), Single Identification Number (NIK) of the 2019 general election for the president and vice president candidates (Sahara, 2021). Another, in October 2021, data leaked from the Indonesian Child Protection Commission (KPAI), especially the personal identity of the people who had filed a complaint (CNN Indonesia, 2021).

The aforementioned cases proved the poor and vulnerable personal data protection for the Indonesian citizens. Indeed, the law enforcers have not protected the people from personal data leaks. It was due to the unavailability of comprehensive and integrated regulation for personal data protection and supervision.

Indonesia has established several regulations for personal data protection. However, they are partial and sectoral, other than providing general aspects of protection (Hartadi, 2020: 291). One example is the Laws Number 19 of 2016 regarding Electronic Information and Transaction (UU ITE), which contains only the subjects of the protection without providing the procedures to implement the protection (Anggraeni, 2018: 823). Since 2019, the government has reiterated the Personal Data Protection Bill, regulating comprehensive personal data protection. However, it has not been enacted.

Further, data leak was also caused by the non-existence of a special agency focusing on supervising and protecting personal data as well as handling the data leak issues. To date, the task was assigned to the Ministry of Information and Communication. Nevertheless, when personal data leaked, the ministry found difficulties in handling the cases due to the unavailability of comprehensive regulation. Besides, personal data supervision and protection only cover the matters related to the government. It has not included private corporates, which are more vulnerable to data hacks.

The supervision for personal data protection should include all parties: government, private corporates, and individuals. They are responsible for storing and managing the people's personal data stored in their database. Therefore, a special agency becomes urgent in Indonesia. It serves to supervise personal data protection more effectively.

The present study is similar to the previous ones in terms of topic. However, it offers different issues, such as the necessity for in-depth analysis of personal data legal protection in Indonesia and the urgency to establish a special agency for personal data protection and supervision. Hence, it is interesting to study and analyze the personal data protection for Indonesian citizens, especially the urgency to establish an appropriate special agency for personal data protection and supervision.

## **II. RESEARCH METHOD**

The research is qualitative with normative method. The data were gathered through literature research/library study/document study. They were then analyzed qualitatively and presented in a descriptive-analysis manner. Besides, the research belongs to the doctrinal type using primary and secondary legal materials.

## **III. RESULT AND DISCUSSION**

### **3.1. Legal Protection for Indonesian citizens' Personal Data**

To date, Indonesia has enacted several regulations for personal data protection. However, they are sectoral and less integrated. Some are presented in the following table.

**Table 1.** Regulation regarding Personal Data Protection in Indonesia

No	Types of Regulation	Name of Regulation
1.	Laws	Laws Number 10 of 1998 regarding Banking
		Laws Number 39 of 1999 regarding Human Rights
		Laws Number 36 of 1999 regarding Telecommunication
		Laws Number 12 of 2005 regarding Ratification for International Covenant on Civil and Political Rights (UU ICCPR)
		Laws Number 24 of 2013 regarding Population Administration
		Laws Number 19 of 2016 regarding Electronic Information and Transaction
		Laws Number 14 of 2008 regarding Public Information Disclosure
		Laws Number 36 of 2009 regarding Health
2.	Government Regulation	Laws Number 43 of 2009 regarding Archives
		Government Regulation of the Republic of Indonesia Number 71 of 2019 regarding the Organization of Electronic System and Transaction
		Government Regulation of the Republic of Indonesia Number 80 of 2019 regarding Trade through Electronic System
3.	Bill	Regulation of the Ministry of Communication and Information Number 20 of 2016 regarding Personal Data Protection in Electronic Systems
		Personal Data Protection Bill

Source: various

As presented in the table, various regulations have not provided maximum protection for the Indonesian citizens' personal data. Indeed, the regulations have caused juridical problems, leading to inadequate protection. The problems are also caused by the unavailability of a comprehensive regulation for personal data protection.

The establishment of laws and regulations in Indonesia needs to be adjusted to the concepts of laws and regulation as mentioned in the Laws Number 12 of 2011 regarding the

Establishment of Applicable Laws as amended with the Laws Number 15 of 2019 regarding the Amendment of the Laws Number 12 of 2011 regarding the Establishment of Applicable Laws (UU PPP). In the discipline of law, an umbrella act or umbrella provision is known as *kadarwet* or *raamwet*, which is not a new concept in Indonesia. The concept has been implemented in the Laws Number 5 of 1960 regarding the Basic Agrarian Principles and Laws Number 32 of 2009 regarding Environmental Protection and Management.

In essence, the concept of the umbrella act in Indonesia has not been clearly identified. As a result, it is considered a tradition of the standard law adopted by Indonesia. The position of an umbrella act, viewed from Article 7 paragraph (1) of the Legislation Formulation Act, is below the constitution but higher than other kinds of laws. An umbrella act is understood as a method or concept of drafting a regulation by combining several rules containing different points. The laws will be an integrated regulation functioning as an umbrella act for all regulations regarding personal data protection, which was previously sectoral in characteristic.

The Indonesian State has not established a comprehensive regulation (umbrella act) for the citizens' personal data protection (Situmeang, 2021: 43). The regulation regarding the protection is mentioned in different sectors of regulation as mentioned previously. It is different from those practiced in other countries, such as Personal Data Protection Act 2012 in Singapore, Personal Data Protection Act 2010 in Malaysia, and General Data Protection Regulation (GDPR) since 2018 in the European Union (Tsamara, 2021).

Previously, the Indonesian Government drafted the Personal Data Protection Bill (RUU PDP) in 2016. Indeed, it was included in the 2019 and 2021 National Legislation Program (*Prolegnas*) (Maichle et al., 2021). Nevertheless, the Bill has not been enacted. Instead, the government seems to abandon personal data protection issues (E. P. Putri & Martha, 2021).

RUU PDP is a reform for personal data protection at the normative stage, creating a comprehensive regulation. The unavailability of specific regulations for personal data protection has caused several problems, such as the followings:

A. Dis-harmonization at the normative layer due to the distributed personal data to various sectors of regulation

Dis-harmonization of regulations refers to an event where two or more applicable laws regulate a similar matter, yet the procedures for each are different. Besides, it means overlapping one another regulations, both vertically and horizontally. The overlap results from various regulations applied to one matter (Zaenal & Adhi, 2020).

According to L.M Gandhi in Lutfia (2020), there are several factors causing dis-harmonization in Indonesian legal practices.

1. The disparity between the several applicable laws and regulations;
2. The contradiction between the laws and the implementing regulation;
3. The disparity between the applicable laws stipulated by the previous judge and the Circular Letter of the Supreme Court;

4. The disparity between the laws and regulations and the government policy;
5. The contradiction between the government policies;
6. The disparity between the central and regional policies; different formulations from a particular legal provision lead to an overlapping condition;
7. Conflicting authorities of the government.

Dis-harmonization in terms of personal data protection needs to be studied. First, there has been a different definition of personal data provided by several sectors of laws. For example, in the Population Administration Laws and the Ministry Regulation for the Personal Data Protection, personal data is defined as the data of an individual that is stored, maintained, and of which the accuracy and confidentiality are protected. Meanwhile, in the Regulation of the Ministry of the Organization of Electronic System and Transaction, personal data refers to each data of an individual identified and/or can be identified separately or combined with other information, either directly or indirectly, through electronic and/or non-electronic method.

Second, the personal data scope also varies. For example, in the Population Administrative Laws, the protected data include physical and mental disabilities, fingerprints, iris, signature, and other data components categorized as a person's deficiency. Meanwhile, in the Public Information Disclosure Laws, personal data of which the confidentiality must be protected include family members' history and condition, the person's history, condition, physical health treatment, and psychological condition. Besides, it also covers financial condition, assets, income, bank account, evaluation results in relation to the capability, intellectuality, and recommendation of the person's ability, as well as notes about the personality in terms of formal and non-formal education.

Based on the data, the dis-harmonization of regulations and personal data protection is caused by the different types of regulation. Similar term with different meaning/definition/scope tends to create multiple interpretations in the implementation. The differences can also lead to legal uncertainty. Therefore, comprehensive and integrated regulation serving as an umbrella act is urgent to guarantee the legal certainty for personal data protection for the people of Indonesia.

#### B. Various Issues due to the Weak regulation for Personal Data Protection

A vulnerable regulation for personal data protection has caused endless data leaks. Indeed, the government seems to abandon the issues. The Ministry of Information and Communication is assigned to handle the personal data leaks. Nevertheless, they found difficulties due to the unavailability of comprehensive regulation. What is more, the government or the institution holding the data experiencing the data leaks is freed from fulfilling any responsibility commonly attached to

personal data holders. Meanwhile, the users whose data have leaked lost their rights, such as rights to information, recovery, and compensation.

One of the cases of personal data leaks that have not been resolved is 279 data leaked from the Health care and Social Security Agency (BPJS) in May 2021. The government has not taken any action to handle the issue. Further, the data controllers, the health care BPJS, did not take responsibility, causing the people to lose their rights as the data owners.

The situation was different in Singapore. It has experienced exactly the same case. Based on [katadata.co.id](http://katadata.co.id), 1.5 million personal data of the SingHealth patients were leaked. However, SingHealth immediately took responsibility for the matter. They informed all the patients utilizing their facilities and services about the data leaks ([katadata.co.id](http://katadata.co.id), 2021).

Other than contacting the patients, SingHealth also created a mobile application named Mobile Health Buddy. The patients can use it to check if their data are secured. The application also provides complete guidelines for the data leak victims, allowing them to take immediate action ([Liputan6.com](http://Liputan6.com), 2018).

For the incident, SingHealth paid as much as S\$250.000 (2 or 3 trillion rupiahs) to compensate the patients as the data owner. Indeed, the Integrated Health Information System (IHIS), as the information system management of the Singapore health sector, was fined even greater, as much as S\$750.000 (8 or 9 trillion rupiahs) ([katadata.co.id](http://katadata.co.id), 2021). Singapore has established a comprehensive regulation to protect its citizens' personal data through the Personal Data Protection Act (PDPA). Hence, Indonesia needs to adopt the best practice implemented by other countries to protect the people's personal data.

### **3.2. The Urgency to Establish a Special Agency for Personal Data Protection and Supervision for the Indonesian Citizens**

Indonesia highly upholds human rights, including the right of personal data protection for the people. Hence, the government is responsible for respecting, fulfilling, and protecting the rights. This way, the goal to protect the whole nation and the entire native land of Indonesia will be fulfilled ([Setiawati et al.](http://Setiawati et al.), 2020).

The state's role in protecting the people's personal data has been mentioned in Article 28 G of the 1945 Constitution of the Republic of Indonesia. It confirms that "every person shall be entitled to the protection of his/her own person, family, honor, dignity, and property under his/her control, as well as be entitled to feel secure and be entitled to protection against the threat of fear to do or omit to do something being his/her fundamental right." The article has imposed the obligation on the government to exert any efforts to protect the privacy of the people, allowing it to create the most secure protection.

Further, the state's function in protecting the people's privacy cannot be separated from its' essence as a power organization. Logemann in Vanya Karunia Mulia Putri viewed the state as an organization aimed to regulate the people based on power ([Kompas.com](http://Kompas.com), 2021).

The view was followed by Miriam Budiardjo, proposing that a state is an organization within one region with the highest and most legitimate power (Budiardjo, 2008:17).

Moreover, a state as an organization establishes the government serving to control all the matters regarding the state and the life of the nation. Similarly, the concept applies to Indonesia. As the supreme organization, the Indonesian government holds power and control to regulate and manage the state through the policies to accomplish the nation's goals.

Jimly Asshidiqqie in Suhardjana (2010) suggested that Indonesia needs a mechanism through fundamental provisions and policies based on laws to fulfill the goals. Law is understood and developed into a unity of system and concept. Law consists of several elements: institutional, instrumental, and subjective and cultural (the subjects holding the rights and obligations determined by the norms).

Unfortunately, Indonesia has not protected the people's personal data, evidenced by the loose supervision and protection. Meanwhile, the massive data leaks must not be abandoned. The Personal Data Protection Bill has not been enacted because of the endless polemic about who will implement the regulation. It is expected that RUU PDP accommodates establishing a special agency for personal data protection and supervision.

The urgency of establishing a special agency for personal data protection and supervision is as follows:

1. The Mandate of International Regulations and Convention

Various international regulations and conventions have mandated the establishment of personal data protection and supervision agency. International law refers to the entire laws consisting of principles and norms to which the relevant countries are attached. (Starke, 2012: 3).

Boermauna defined an international convention as an international legal source functioning as a juridical instrument protecting the collective wills and intentions of a state or international legal subjects to achieve a particular purpose (Roisah, 2015). An international convention covers all tools and instruments arranged by international legal subjects. Besides, it has an international binding effect. The international regulation and conventions include the followings:

- a. *United Nations Guidelines for the Regulation of Computerized Personal Data* of 1990

The regulation requires personal data protection of a country assigned to an independent agency:

*"The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies."*



As regulated, each country assigns or establishes an authority to protect and supervise the people's personal data. The referred to authority is independent, having no partiality to a particular person or institution. Indeed, any breach or failure in protecting people's personal data may lead to the application of criminal and other laws.

b. *APEC Privacy Framework* (2015)

Electronic trade flows are increasing rapidly. Hence, personal data protection is necessary to improve people's trust, ensure electronic trade growth, protect information confidentiality, and strengthen information security. In the Asia Pacific region, APEC Privacy Framework has been enacted since 2015. It mandates each member country to establish an agency or legal enforcer to protect personal data.

*"Empowering privacy enforcement authorities to fulfill their mandate to protect individual privacy. Privacy enforcement authority means any public body that is responsible for enforcing privacy law and that has powers to conduct investigations and/or pursue enforcement proceedings. A privacy enforcement authority is a public body that is responsible for enforcing an APEC economy's privacy law. It will have powers to conduct investigations and/or pursue enforcement proceedings. As economy may have more than one privacy enforcement authority."*

The APEC Privacy Network (2015) concluded that the rapid electronic flows required each person to input their personal data through the internet. Hence, personal data protection is necessary. Further, the protection is carried out by assigning one or more institutions or authorities.

The international regulation and convention become the reference for the state of Indonesia to establish an institution or a special authority to protect the citizens' personal data. Indonesia, declaring to be bound to the provisions of the international convention, is obliged to implement the mandate of protecting the people's privacy.

2. Conflict of Interest within the Personal Data supervision and management

Conflict of interest means as is. According to the Corruption Eradication Commission (KPK), conflict of interests is defined as a condition in which a state organization holding the authority and power based on the applicable laws and regulations has or is suspected of having a personal interest in using the authority, raising a potential to influence the quality or the performance (KPK, 2009).

Meanwhile, the Organization of Cooperation and Development (OECD) defines conflict of interest as follows (OECD, 2003):

*"A conflict of interest involves a conflict between the public duty and the private interest of a public official, in which the official's private-capacity interest could improperly influence the performance of their official duties and responsibilities."*

Further, Article 1 paragraph (14) of Laws Number 30 of 2014 regarding Government Administration also provides the definition of conflict of interest. It is a condition of the government official holding a personal interest to benefit himself and/or other people by taking advantage of the authority that influences

the neutrality and the quality of the decision and/or action made and/or implemented.

In short, conflict of interest is a condition where the government official, either an institution or a state body, uses the power or authority for the sake of the personal interest of the institution or body, leading to affecting the performance.

To date, personal data protection for the people of Indonesia has been assigned to the Ministry of Communication and Information. However, it has the potential of experiencing a conflict of interest (*conflict of interest*).

The conflict of interest is potential because the assigned ministry collects and manages the people’s personal data. Consequently, it is not appropriate for the ministry to supervise the personal data protection for the institutions, other ministries, or private companies because they have the same interest.

Conflict of interest implies the ineffectiveness and inefficient public services. Further, it decreases the people’s trust in the institution or public officials. Stanley (Swasanany, 2014) stated that an institution or a state agency could not function without the people’s trust. Therefore, the government needs to establish one to work effectively and efficiently (Iswandari, 2021: 134).

3. Massive Personal Data Leaks

Indonesia faces some issues related to personal data leaks. A person’s private information such as name, email address, social media account password, home address, phone number, and family identity card has the possibility of leaking out. 2020-2021 is the dark period of the Indonesians’ personal data protection. The massive data leaks are presented in the following table

**Table 2.** *Personal Data Leaks in 2020*

No	Month	Database	Amount of data
1	May	Tokopedia	91 million
2	May	Bhineka.com	1,2 million
3	May	General Election Commission (KPU) (Permanent Voter List of the General Election)	2,3 million
4	August	KreditPlus	890 thousand
5	November	RedDoorz	5,8 million
6	November	Cermati	2,9 million

Source: [Kompas.com](https://www.kompas.com), 2021

**Table 3.** *Personal Data Leaks in 2021*

No	Month	Database	Amount of data
1	May	Health Care and Social Security Agency (BPJS Kesehatan)	279 million

2	July	BRI Life	463 thousand
3	August	Ministry of Health (E-HAC users)	1,3 million
4	September	General Election Commission (KPU) (data of the president and vice president candidates of 2019)	4
5	October	Indonesian Child Protection Commission (KPAI)	13 mb

Source: [CNN Indonesia, 2021](#)

The massive data leaks harm the Indonesian people because they can cause other crimes. The potential crimes of data misuse include the followings:

- a. Phishing (password harvesting fishing) is a fraudulent action committed by a person using a fake email to obtain the victim's personal data ([Vyctoria, 2013: 214](#)).
- b. Revealing the password. One of the most common hacked data is a person's birth date. People frequently use their birth date as a password to their social media accounts. A personal data hack gives access to a person to take over and misuse the victim's social media account.
- c. Creating an online loan account using another person's data. A person who succeeded in stealing the victim's personal data can create an account using the data, which then misuse it to apply for a loan online on behalf of the victim.
- d. Scamming is a fraud carried out by convincing a person through SMS, phone call, e-mail, or a direct message via social media.
- e. Telemarketing. According to Machfoeds telemarketing is a promotion or marketing of a product directly to a consumer via a systematic phone call ([Machfoedz, 2010](#)). Telemarketing is conducted repeatedly, which leads to disturbing a person.

#### IV. CONCLUSION

The legal protection for the Indonesians' personal data is mentioned in various laws, causing them to be less comprehensive and integrated. Further, it resulted in risking personal data protection. Therefore, the Personal Data Protection Bill has become an urgency to be enacted. The state needs an agency to protect and supervise the people's personal data. The urgency to establish the agency is the result of several factors. First, it has been mentioned in the international regulation and conventions. Second, there has been a conflict of interest in personal data protection and supervision. The third is massive personal data leaks. Hence, the personal data protection bill needs to clarify the material regarding the special agency for personal data protection and supervision.

#### Author Declaration

**Author contributions and responsibilities** - The contributions and responsibilities of the author-Author contribute substantially to the conception and design of the research. The

author is responsible for data analysis, interpretation, and discussion related to the results. The author also reads and approves the final manuscript.

**Funding** – There is no funding information from the author.

**Availability of data and materials** - All data and materials are available from the author.

**Conflict of interest** - The author states there is no interest in competing.

**Additional information** - There is no further information from the author.

## References

- Anggraeni, S. F. (2018). Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia. *Hukum Dan Pembangunan Tahun Ke-4*, 823.
- Budiardjo, M. (2008). *Dasar-Dasar Ilmu Politik*. Gramedia Pustaka Utama.
- CNN Indonesia. (2021). Data KPAI Bocor, Dijual di RaidForums. *Cnnindonesia.Com*.
- Conney Stephanie. (2021). Kebocoran Data yang Terjadi Sepanjang 2020. *Kompas.Com*.
- Development), O. (Economic C. and. (2003). *Managing Conflict of Interest in the Public Service: OECD Guidelines and Country Experiences*. EOCED Publishing.
- Doly, D. (2021). Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru. *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan*, Vol. 12, N, 225. <https://doi.org/https://doi.org/10.22212/jnh.v12i2.2357>
- Hacker Curi Jutaan Data Penduduk Singapura, Perdana Menteri Ikut Jadi Korban*. (2018). *Liputan6.Com*.
- Hartadi, M. H. R. dan H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik (Policy the Discontinuation of Personal Data Storage in Electronic Media). *Jurnal HAM*, vO. 11, nO, 291. <https://doi.org/http://dx.doi.org/10.30641/ham.2020.11.285-299>
- Iswandari, B. A. (2021). Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance. *Jurnal Hukum Ius Quia Lustum*, Vol. 28 No. <https://doi.org/10.20885/iustum.vol28.iss1.art6>
- Korupsi), K. (Komisi P. (2009). *Panduan Penanganan Konflik Kepentingan Bagi Penyelenggara Negara*. KPK.
- Lidwina, A. (2021). *Mengapa Indonesia Membutuhkan UU Pelindungan Data Pribadi?* *Katadata.Co.Id*.
- Lutfia, V. (2020). *Urgensi Perlindungan Hukum Terhadap Masyarakat Hukum Adat Melalui Penataan dan Harmonisasi Regulasi*. Universitas Ahmad Dahlan.
- Machfoedz, M. (2010). *Komunikasi Pemasaran Modern*. Cakra Ilmu.
- Maichle Delpiero, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, N. M. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Market Place dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjajaran Law Review*, Vol. 9, No.
- Putri, E. P., & Martha, A. E. (2021). *The Importance of Enacting Indonesian Data Protection Law as a Legal Responsibility for Data Leakage*. 17(3), 287–303. <https://doi.org/10.31603/variajusticia.v17i3.6231>
- Putri, V. K. M. (2021). *Pengertian Negara Sebagai Organisasi Kekuasaan*. Kompas.Com.
- Roisah, K. (2015). *Hukum Perjanjian Internasional*. Setara Press.
- Sahara, W. (2021). Deretan Kasus Kebocoran Data Pribadi dalam Dua Tahun Terakhir. *Kompas.Com*.
- Satria, Z. A. dan A. P. (2020). Disharmonisasi Peraturan Perundang-Undangan di Indonesia: Antara Bentuk, penyebab, dan Solusi. *Jurnal Pro Hukum : Jurnal Penelitian Bidang Hukum Universitas Gresik*, 9, No. 1.

- Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, 2(2), 2–9. <https://doi.org/10.18196/iclr.2219>
- Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber. *Jurnal Sasi*, Vol. 27 No, 43. <https://doi.org/10.47268/sasi.v27i1.394>
- Starke, J. G. (2012). *Pengantar Hukum Internasional (Kesepuluh)*. Sinar Grafika.
- Suhardjana, J. (2010). Supremasi Konstitusi Adalah Tujuan Negara. *Dinamika Hukum*, 10, No. 3.
- SwasananY, D. W. T. (2014). *Mengembalikan Kepercayaan Publik Terhadap Parlemen : Pengalaman Indonesia*.
- Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, Vol. 3, No. <https://doi.org/https://doi.org/10.26740/jsh.v3n1.p53-84>
- Vyctoria. (2013). *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*. CV Andi Offset.
- Wahyudi Djafar dan Asep Komarudin. (2014). *Perlindungan Hak Atas Privasi di Internet: Beberapa Penjelasan Kunci*. ELSAM.