IUS POENALE
Volume 3 Issue 1, January–June 2022: pp.39-48.
Faculty of Law,Universitas Lampung, Bandar Lampung, Indonesia.
http://jurnal.fh.unila.ac.id/index.php/ip
P-ISSN: 2723-2638 E-ISSN: 2745-9314

Independent Supervisory Authority to Protect Social Media Users' Personal Information in Indonesia

Galang Syafta
Universitas Lampung
galang.syafta@yahoo.com

Rio Fahni
Universitas Lampung
fahnirio@gmail.com

Aprilia Fitri Ningsih
Universitas Lampung
apriliafitri.n@gmail.com

Submitted: Feb 11, 2022; Reviewed: May 19, 2022; Accepted: June 29, 2022

Article's Information

keywords:
Data Protection Abuse; Personal Data;

DOI :
https://doi.org/10.25041/ip.v3i1.2531

Abstract

Given the lack of a specific institution in Indonesia that oversees the protection of personal data, the importance of protecting personal data is frequently debated. Along with technological developments that continue to occur, it will be directly proportional to the legal risks caused. Hence, these developments need to be balanced with existing legal rules to minimize the occurrence of criminal cases, one of which is the misuse of technology today, which is related to property rights to personal data, especially personal data on social media. This paper uses a normative research method that aims to determine the essence of the formation of legal products and independent authority institutions in Indonesia in maximizing protection and law enforcement against misuse of personal data. Based on the results of the study, it is known that the urgency of establishing this independent authority greatly influences the protection of the misuse of personal data, especially personal data on social media.

A. Introduction

The advancement of information technology in the current era has become very important in terms of improving performance and productivity because it allows for the quick, precise, and accurate completion of various tasks. Globally, information and communication technology has changed human behavior, resulting in significant and rapid social changes. However, the advancement of information and communication technology has also resulted in the lack of a geographical boundary (borderless).[1]

Online social networking, also known as Social Networking Sites/ SNS, has become an inseparable part of modern society's social life. Of course, this is inextricably linked to technological advancements infiltrating community interaction patterns.[2] People must indirectly follow suit with new technology and increasingly aggressively developing innovations. Because of its quick, simple, and low-cost nature, social media is a viable option for staying in touch with others. Social Networking Sites (SNS) are one web service that allows people with similar interests, backgrounds, and activities to form a virtual network platform.[3] SNS can help people solve problems in various fields, including communication, bureaucracy, entertainment, education, and others.[4] SNS provides important benefits to its users by removing economic and geographic boundaries and can also assist in achieving goals related to job search, entertainment, and education. However, the popularity of SNS poses a significant risk to its users. Users who share personal information on social media become tempting targets for criminals such as spam, malware, social bots, and identity theft. Even attackers can find important data, such as bank account information, which is then used for crimes such as fraud, personal identity, and user location.[5]

On the other hand, it has grown in popularity because it allows users to stay connected and log in continuously, allowing them to receive messages from colleagues and relatives daily. Users can connect with other virtual communities, including family, friends, coworkers, and strangers. According to Henson et al., over the last few decades, SNS has evolved from a fun new world to a multibillion-dollar global industry with users from all walks of life.[6]

SNS can have negative consequences, such as encouraging people to disclose personal information such as their age, sexual or political orientation, date of birth, purchase of an item, etc.[7] Of course, disclosing personal information carries risks. According to research conducted by Clemens et al. in 2015, which was published in Milham & Atkin, disclosing this information is suspected to result in identity theft or sanctions at school or work for raising a sensitive issue. According to Henson et al. research, approximately 42 percent of student SNS users experience some form of privacy threat during their lifetime; this issue requires further attention.[8]

---

[1] Ahmad M. Ramli, *Cyber Law and Intellectual Property Rights in the Indonesian Legal System* (Bandung: Refika Aditama, 2015).

[2] Philippa Collin et al., "Literature Review: The Benefits of Social Networking Services," *Inspire Foundation, University of Western Sydney and Murdoch University*, no. April (2011): 29.

[3] Shailendra Rathore et al., "Social Network Security: Issues, Challenges, Threats, and Solutions," *Information Sciences* 421 (2017): 43-69., https://doi.org/10.1016/j.ins.2017.08.063.

[4] Astri Wibawanti Putri, Sutopo JK, and Andre N Rahmanto, "KOMUNIKASI KRISIS KEMENTERIAN PERTANIAN PADA KASUS PENGGEREBEKAN GUDANG BERAS PT IBU (Analisis Isi Kualitatif Menggunakan Situational Crisis Communication Theory)," *Jurnal Studi Komunikasi Dan Media* 23, no. 1 (2019): 53, https://doi.org/10.31445/jskm.2019.1765.

[5] Rathore et al., "Social Network Security: Issues, Challenges, Threats, and Solutions."

[6] Billy Henson, Bradford W. Reyns, and Bonnie S. Fisher, "Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization.," *Critical Justice Review* 36, no. 3 (2011): 253–68, https://doi.org/10.1177/0734016811399421.

[7] Mary Helen Millham and David Atkin, "Managing the Virtual Boundaries: Online Social Networks, Disclosure, and Privacy Behaviors.," *New Media & Society* 20, no. 1 (2016): 50–67, https://doi.org/10.1177/146144816654465.

[8] *Ibid.*

The novelty of this research is an independent data protection authority is one of the public institutions tasked with ensuring the protection of personal data and the compliance of controllers and processors of personal data, both individuals and private entities, as well as public institutions, with data protection laws and regulations. Analysis of the ideal format of an independent authority that is not under the government, with the task of socializing, supervising, handling administrative disputes, mediating, and providing recommendations regarding protecting personal data.

Based on the explanation above, it can be seen that the discussion regarding the supervisory authority for the protection of personal data is critical to put forward, considering that Indonesia currently does not have a particular institution that oversees the protection of personal data as a whole. The debate about the importance of protecting personal data often cannot be separated from the issue of information disclosure. Up until now, no writing has explicitly explained the essence of the establishment of an independent supervisory authority in protecting the personal data of social media users and legal protection of the personal data of social media users. As a result, the authors attempts to explain in this paper how important the establishment of an independent supervisory authority in the protection of personal data for social media users is, as well as how legal protection for personal data of social media users is.

B. Discussion

1. Independent Supervisory Authority In The Protection Of Personal Data Of Social Media Users.

An independent data protection authority is a public institution whose function is to protect personal data and ensure the compliance of personal data controllers and processors, both individuals and private entities, as well as public institutions, with data protection laws and regulations. This organization is a critical player in data protection efforts, serving as the spearhead of privacy and data protection regulators. The agency's primary role is not only to implement privacy and data protection policies but also to raise awareness, consult, and develop networks.[9] In general, there are two law enforcement models for personal data protection: the first with the establishment of an independent supervisory authority, and the second with the ministry. Five of the seven international treaties and standards relating to personal data protection require the establishment of an independent supervisory authority.[10]

Personal data monitoring agencies are the most important factor in any country's efforts to protect its citizens' personal data. This is also the state's role in providing the public with a sense of security and comfort when using social media or other platforms that require the use of personal data to access the platform. Elsam's research, Measuring the Compliance of Information and Communication Technology Companies, stated several things about social media platforms' privacy policies, as follows:[11]

a. In general, social media platforms already have a privacy policy, although the details and completeness are still very varied;
b. Some platforms have listed third-party companies for them to share information about their consumers' personal data, but the names of these third-party companies are not listed;

[9] Denico Doly, "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)," *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 12, no. 2 (2021): 223–44, https://doi.org/10.22212/jnh.v12i2.2357.

[10] Wahyudi Djafar, "Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan," *Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada* 1, no. 1 (2019): 147–54.

[11] https://elsam.or.id/id/ , accessed on October 28, 2021, at 22.00 WIB.

c. Some platforms do not state the retention period for consumer personal data, there are some that include, but still do not clearly explain the retention period for consumer personal data;
d. Most platforms do not state the company's obligation to notify data subjects of data leaks;
e. Most companies do not include a redress mechanism for consumers whose rights to privacy are violated as a result of data leaks;
f. Some terms in the privacy policy are confusing, such as, 'including without limitation', 'relevant information', 'active users', 'enrich your experience', and so on;
g. The appearance of the privacy policy is not attractive, communicative and easy to understand, only a few companies are able to explain with examples, besides that the Indonesian language used seems to be the result of machine translation.

The 2015 APEC Privacy Framework also emphasizes the need for each country to establish a personal data protection enforcement agency or agency with a model. The second reason is Indonesia's lax regulation of personal data protection in law enforcement. We must know the use of Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP) as a guideline for criminal law enforcement and coercive measures. The Criminal Procedure Code only requires confiscation action with the permission of the head of the court (Article 38 paragraph (1) KUHAP). Still, it does not require the need to protect the user's data, even in the investigation process. Things such as in the act of confiscation carried out by investigators, where although not explicitly, but implicitly personal electronic data contained in electronic devices is one of the objects of confiscation as referred to in Article 39 paragraph (1) of the Criminal Procedure Code.

Based on the presumption of innocence, personal data of social media users must be protected, not published or misused. Personal data is vulnerable to misuse by law enforcement for purposes other than law enforcement because there is no regulation governing personal data protection. Based on these two imperatives, an authority that regulates and ensures personal data protection, including in the context of law enforcement, must be established.[12] Personal data concerns human rights and privacy that must be protected, as stated in:

a. Universal Declaration of Human Rights 1948
b. Law Number 12 of 2005 concerning Ratification of the International Covenant on Civil and Political Rights
c. Law Number 36 of 2009 concerning Health regulates the confidentiality of the patient's personal condition
d. Law Number 10 of 1998 concerning Banking regulates personal data regarding depositors and their deposits.

There are several reasons why it is important to protect personal data, including:

a. Data is a high-value asset or commodity in the era of big data and the digital economy. It has been mentioned that the data volume in 2015 is estimated to reach 8 trillion GB and will increase 40 times in 2020.[13] and Data-driven AI applications are projected to contribute US$13 trillion to the global economy by 2030.[14]

[12] Ahmad Budiman, "Otoritas Pengawas Pelindungan Data Pribadi," *Info Singkat Hubungan Internasional* XII, no. 5 (2021): 2.
[13] OECD, "Programme for International Student Assessment (PISA) Results from PISA 2018.," *Oecd*, 2019, 1–10.
[14] Brian Caldwell, "The New Enterprise," *Re-Imagining Educational Leadership*, no. 4 (2012): 75–82, https://doi.org/10.4135/9781446214657.n7.

b. Violations of privacy and misuse of personal data are increasingly occurring, for example activities related to digital dossier, direct selling, location-based messaging, in addition, an example of a concrete case that has occurred relating to misuse of personal data is the Cambridge Analytica case that occurred in 2018
c. The public is not yet fully aware of the importance of protecting personal data. Public awareness of personal data protection is one of the important things given the significant increase in the number of internet users in Indonesia, but not all of them are aware of the importance of personal data protection; even based on research conducted by Apjil in 2017 more than 30% of Indonesian internet users are not aware that data can be retrieved.[15]

Accessing other people's data can interfere with individual privacy rights by distributing personal data without the person's permission, which is a type of unlawful action. There are numerous cases of privacy violations in both cyberspace and the real world. One example is the rise in cyberspace privacy violations, particularly in social media applications.[16] Furthermore, it can be seen that the perpetrators' misuse of personal data on social media platforms is an unlawful act that is contrary to the personal rights of others, where personal data is one of one's privacy rights.[17] The debate over the supervisory authority for personal data protection is critical, given that Indonesia currently lacks an extraordinary institution that oversees personal data protection. It is critical to provide legal protection to victims; in order to do so, law enforcement must be carried out correctly.[18] Furthermore, the laws that govern must be comprehensively and explicitly regulated to provide legal certainty to protect personal data, such as how other parties may collect, store, and use data, as well as the exact steps or rules in the personal data security process.[19]

In comparison to other countries that already have special rules governing personal data protection, Indonesia lags. Since 2010, Malaysia has had a Personal Data Protection Act. It has been in Singapore and the Philippines since 2012. Thailand, another Southeast Asian country, recently announced the passage of a Personal Data Protection Act.[20] As a result, special rules for personal data protection must be enacted quickly, and the existence of an independent supervisory authority will later maximize protection and law enforcement against misuse of personal data on social media or other types of platforms.[21]

2. Legal Protection Of Personal Data Of Social Media Users

Social media has a positive impact on social life, one of which is as a tool to provide convenience in communicating and interacting between users without having to face to face, which is not limited by space and time. The rapid development of social media in the current era is marked by the emergence of various social media such as Facebook, Twitter, Instagram,

[15] Marsya Nabila, "APJII: Penetrasi Pengguna Internet Indonesia Capai 143 Juta Orang," Daily Social, 2018, https://dailysocial.id/post/apjii-survei-internet-indonesia-2017.
[16] Imam Teguh Islamy et al., "The Importance of Understanding Privacy Applications in the Information Technology Era," *Journal of Information Technology and Education* 11, no. 2 (2018): 122, https://doi.org/10.24036/tip.
[17] Rosa Agustina, *Perbuatan Melawan Hukum* (Jakarta: Fakultas Hukum Universitas Indonesia, 2003).
[18] Budiman, "Otoritas Pengawas Pelindungan Data Pribadi."
[19] Lydia Kharista Saragih, Danrivanto Budhijanto, and Somawijaya Somawijaya, "Perlindungan Hukum Data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial," *De Rechtsstaat* 6, no. 2 (2020): 125–42.
[20] Husein Abdulsalam, "Sulitnya Melindungi Data Pribadi Di Indonesia," Tirto.id, 2019.
[21] Tiara Almira Raila, Sinta Dewi Rosadi, and Rika Ratna Permata, "Perlindungan Data Privasi Di Indonesia Dan Singapura Terkait Penerapan Digital Contact Tracing Sebagai Upaya Pencegahan Covid-19 Serta Tanggungjawabnya," *Jurnal Kepastian Hukum Dan Keadilan* 2, no. 1 (2020): 1–16, https://doi.org/10.32502/khdk.v2i1.3044.

Line, and other social media applications. Amid the widespread use of social media, user information on social media can be easily obtained, including user personal data information and other privacy matters. This, of course, can trigger a loophole for the misuse of personal data. Misuse of personal data becomes an effortless thing to happen, namely if the owner of personal data feels that other parties use the personal data listed or included in his social media without his permission for purposes that are considered disturbing, self-benefiting, endangering, or threatening others, which will undoubtedly provide loss to data owners.[22]

Personal data protection is specifically about how the law protects how personal data is collected, registered, stored, exploited, and disseminated. Data can be said to be personal data if the data can be used to identify or identify a person. Jerry Kang argues that personal data is used to describe information closely related to someone who can distinguish the characteristics of each individual.[23] Personal data is defined as any actual and accurate personal data attached and identifiable to the person, according to Article 1 of the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, so personal data must be stored, cared for, and kept accurate and confidential. As a result, personal data must be safeguarded.[24]

As a state of law, the Republic of Indonesia must protect the rights of its citizens. These rights are part of human rights guaranteed in the 1945 Constitution as stated in Article 28D paragraph (1) which states that: "Everyone has the right to recognition of guarantees, protection and fair legal certainty and equal treatment before the law." Personal data protection is a type of privacy protection directly mandated by the Republic of Indonesia's Constitution, which includes respect for human rights values and individual rights, so a legal basis is required to provide more security for privacy and personal data.[25]

To address the issue of personal data security and protection, the government passed Law No. 19 of 2016 amending Law No. 11 of 2008 on Information and Electronic Transactions (UU ITE). However, due to the rapid advancement of technology, these provisions are currently deemed insufficient to address legal issues, particularly the protection of personal data on social media platforms.[26] The government has drafted a regulation to protect personal data, as stated in the Personal Data Protection Bill, but the bill has yet to be ratified. This bill should be included in the government's priority list because legal issues regarding the misuse of personal data are becoming more prevalent, as is the need for personal data protection itself, given that personal data is part of privacy, which is a human right of every individual. Misuse of personal data harms the data owner. Personal data has a confidential nature that should be kept confidential. Following this, legislation governing the legal protection of personal data in Indonesia comprises several laws that do not stand alone. At least 30 laws and regulations at various levels govern personal data protection and are sectoral, governing only their domain.[27]

The legal protection of personal data and the extent to which the use of personal data can be carried out is still unclear. Therefore, the Personal Data Protection Bill that has been drafted,

[22] Saragih, Budhijanto, and Somawijaya, "Perlindungan Hukum Data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial."

[23] Nugraha, *Juridical Analysis Regarding Personal Data Protection in the Cloud Computing System Judging from the Electronic Information and Transaction Law*.

[24] Sinta Dewi Rosadi and Dinah Sumayyah, *Cyber Law: Data Privacy Aspects According to International, Regional, and National Law*, 1st ed. (Bandung: PT Refika Aditama, 2015).

[25] Sinta Dewi Rosadi and Garry Gumelar Pratama, "Urgensi Perlindungandata Privasi Dalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (2018): 88–110, https://doi.org/10.25123/vej.2916.

[26] Samuel D Warren et al., "The Right to Privacy Today," *Harvard Law Review* 43, no. 2 (1929): 297, https://doi.org/10.2307/1330091.

[27] Muhammad Iqsan Sirie, "The Mandatory Designation of a Data Protection Officer in Indonesia ' s Upcoming Personal Data Protection Law * Menerapkan Kewajiban Penunjukkan Seorang Data Protection Officer Di Dalam Undang-Undang Perlindungan Data Pribadi A . Introduction In the Past" 5, no. 1 (2018): 24–49, https://doi.org/10.22304/pjih.v5n1.a2.

according to the author, has covered essential aspects as a cover for gaps in the ITE Law and other regulations on protecting personal data. As contained in the preamble to the Personal Data Protection Bill, the regulation of personal data is currently contained in several laws and regulations. To improve the effectiveness of personal data protection implementation, personal data protection must be legally regulated.[28] Furthermore, the PDP Bill states that community participation in raising public awareness of the importance of personal data protection can be accomplished through education, training, advocacy, technical guidance, and/or socialization.[29] As a result, awareness of personal data protection can be felt and carried out by all parties, not just the government as a policymaker.

One of the most important aspects that must be prioritized in every policy formulation is the security and confidentiality of personal data. It is clear that there is a need for protection and the establishment of a firm and comprehensive law governing the use of personal data in order for its development and utilization to proceed smoothly.[30] Clear and comprehensive laws are urgently needed to establish definite steps in using and protecting personal data. As Thomas Hobbes argues, the rights and freedoms of the people have been handed over to the Primus inter ruling pares as a form of the social contract, and the government, as the party making policy, must pay more attention to this matter.[31]

The laws and regulations currently available in Indonesia regarding personal data protection have not comprehensively provided sufficient protection for personal data. By paying attention to international developments in personal data regulation, both those carried out by many countries around the world and those carried out by international organizations, the Personal Data Protection Bill, which has been completed and formed, needs to be ratified immediately because it will provide more certainty and protection law to regulate and protect personal data as a human right of every citizen.[32] In order to provide legal protection to all victims, law enforcement must be carried out correctly. Furthermore, the laws that govern must be comprehensively and explicitly regulated to provide legal certainty to protect personal data, such as how personal data may be collected, stored, and used by third parties, as well as the exact steps or rules in the personal data security process. This Personal Data Protection Regulation will also help create order and progress in the information society.

C. Conclusion

Establishing an independent authority institution is one of the most important things to do, as an independent supervisory authority will later maximize protection and law enforcement against misuse of personal data on social media or other platforms. It is critical to provide legal protection and legal protection to all victims. When special rules are required that are regulated comprehensively and precisely to provide legal certainty to protect personal data, the existence of an independent authorized agency and the laws that regulate it cannot be separated.

It is well understood that the widespread misuse of personal data requires the support of the rule of law and the agency overseeing it. The country's constitution established a framework for developing regulations to protect the personal data of mass media users, which was realized with the passage of Law Number 11 of 2008 Concerning Information and Electronic Transactions (UU ITE). Concerning personal data protection, it has been explicitly regulated in

[28]Personal Data Protection Bill.
[29]Article 60 of the PDP Bill.
[30] Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia," *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018): 369–84, https://doi.org/10.24815/kanun.v20i2.11159.
[31] Harisman Harisman, "Protection of Human Rights in the Amendment of the 1945 Constitution of The Republic of Indonesia," *Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020)* 549 (2021): 384–89, https://doi.org/10.2991/assehr.k.210506.050.
[32]Academic Draft of the PDP Bill.

the Personal Data Protection Bill, which has been completed and formed, so this bill must be ratified immediately because it will provide more certainty and legal protection to regulate and protect personal data as a human right of every citizen.

Bibliography

Abdulsalam, Husein. "Sulitnya Melindungi Data Pribadi Di Indonesia." Tirto.id, 2019.

Agustina, Rosa. *Perbuatan Melawan Hukum*. Jakarta: Fakultas Hukum Universitas Indonesia, 2003.

Budiman, Ahmad. "Otoritas Pengawas Pelindungan Data Pribadi." *Info Singkat Hubungan Internasional* XII, no. 5 (2021): 2.

Caldwell, Brian. "The New Enterprise." *Re-Imagining Educational Leadership*, no. 4 (2012): 75–82. https://doi.org/10.4135/9781446214657.n7.

Collin, Philippa, Kitty Rahilly, Ingrid Richardson, and I. Third, AmandaCollin, P., Rahilly, K., Richardson. "Literature Review: The Benefits of Social Networking Services." *Inspire Foundation, University of Western Sydney and Murdoch University*, no. April (2011): 29.

Dewi Rosadi, Sinta, and Garry Gumelar Pratama. "Urgensi Perlindungandata Privasi Dalam Era Ekonomi Digital Di Indonesia." *Veritas et Justitia* 4, no. 1 (2018): 88–110. https://doi.org/10.25123/vej.2916.

Djafar, Wahyudi. "Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan." *Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada* 1, no. 1 (2019): 147–54.

Doly, Denico. "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)." *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 12, no. 2 (2021): 223–44. https://doi.org/10.22212/jnh.v12i2.2357.

Harisman, Harisman. "Protection of Human Rights in the Amendment of the 1945 Constitution of The Republic of Indonesia." *Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020)* 549 (2021): 384–89. https://doi.org/10.2991/assehr.k.210506.050.

Henson, Billy, Bradford W. Reyns, and Bonnie S. Fisher. "Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization." *Critical Justice Review* 36, no. 3 (2011): 253–68. https://doi.org/10.1177/0734016811399421.

Islamy, Imam Teguh, Sisca Threecya Agatha, Rezky Ameron, Berry Humaidi Fuad, Evan Evan, and Nur Aini Rakhmawati. "The Importance of Understanding Privacy Applications in the Information Technology Era." *Journal of Information Technology and Education* 11, no. 2 (2018): 122. https://doi.org/10.24036/tip.

Millham, Mary Helen, and David Atkin. "Managing the Virtual Boundaries: Online Social Networks, Disclosure, and Privacy Behaviors." *New Media & Society* 20, no. 1 (2016): 50–67. https://doi.org/10.1177/1461444816654465.

Nabila, Marsya. "APJII: Penetrasi Pengguna Internet Indonesia Capai 143 Juta Orang." Daily Social, 2018. https://dailysocial.id/post/apjii-survei-internet-indonesia-2017.

Nugraha, Radian Adi. *Juridical Analysis Regarding Personal Data Protection in the Cloud Computing System Judging from the Electronic Information and Transaction Law*.

Jakarta: Rajawali Press, 2012.

OECD. "Programme for International Student Assessment (PISA) Results from PISA 2018." *Oecd*, 2019, 1–10.

Putri, Astri Wibawanti, Sutopo JK, and Andre N Rahmanto. "KOMUNIKASI KRISIS KEMENTERIAN PERTANIAN PADA KASUS PENGGEREBEKAN GUDANG BERAS PT IBU (Analisis Isi Kualitatif Menggunakan Situational Crisis Communication Theory)." *Jurnal Studi Komunikasi Dan Media* 23, no. 1 (2019): 53. https://doi.org/10.31445/jskm.2019.1765.

Raila, Tiara Almira, Sinta Dewi Rosadi, and Rika Ratna Permata. "Perlindungan Data Privasi Di Indonesia Dan Singapura Terkait Penerapan Digital Contact Tracing Sebagai Upaya Pencegahan Covid-19 Serta Tanggungjawabnya." *Jurnal Kepastian Hukum Dan Keadilan* 2, no. 1 (2020): 1–16. https://doi.org/10.32502/khdk.v2i1.3044.

Ramli, Ahmad M. *Cyber Law and Intellectual Property Rights in the Indonesian Legal System*. Bandung: Refika Aditama, 2015.

Rathore, Shailendra, Pradip Kumar Sharma, Vincenzo Loia, Young Sik Jeong, and Jong Hyuk Park. "Social Network Security: Issues, Challenges, Threats, and Solutions." *Information Sciences* 421 (2017): 43-69. https://doi.org/10.1016/j.ins.2017.08.063.

Rosadi, Sinta Dewi, and Dinah Sumayyah. *Cyber Law: Data Privacy Aspects According to International, Regional, and National Law*. 1st ed. Bandung: PT Refika Aditama, 2015.

Saragih, Lydia Kharista, Danrivanto Budhijanto, and Somawijaya Somawijaya. "Perlindungan Hukum Data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial." *De Rechtsstaat* 6, no. 2 (2020): 125–42.

Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018): 369–84. https://doi.org/10.24815/kanun.v20i2.11159.

Sirie, Muhammad Iqsan. "The Mandatory Designation of a Data Protection Officer in Indonesia ' s Upcoming Personal Data Protection Law * Menerapkan Kewajiban Penunjukkan Seorang Data Protection Officer Di Dalam Undang-Undang Perlindungan Data Pribadi A . Introduction In the Past" 5, no. 1 (2018): 24–49. https://doi.org/10.22304/pjih.v5n1.a2.

Warren, Samuel D, Louis D Brandeis, Harvard Law Review, and No Dec. "The Right to Privacy Today." *Harvard Law Review* 43, no. 2 (1929): 297. https://doi.org/10.2307/1330091.