Hakim: Jurnal Ilmu Hukum dan Sosial
Vol.2, No.2 Mei 2024
e-ISSN: 2987-7539; p-ISSN: 2987-6737, Hal 315-336
DOI: https://doi.org/10.51903/hakim.v2i2.1821

Legal Protection of Private Platform in Carrying Out the Responsibility of Maintaining User Privacy Rights

Dini Mardhatillah
UIN Syarif Hidayatullah
Korespondensi penulis: Ddmrdhsz15@gmail.com

Abel Parvez
UIN Syarif Hidayatullah
E-mail: Abelparvezjustice@gmail.com

Abstract. This research focuses on examining the legal protection of Electronic System Operators (PSE) in order to be consistently responsible for maintaining the privacy rights of users from state intervention that is too much into the private sphere also interferes freedom of digital business activities. This study purposed to analyze the problem of the defects legal protection provided by the state against the private rights of User because application of surveillance state and provide solutions regarding the ideal legal protection. The Research methodology use normative legal research with statute approach and conceptual approach. This study concluded that there is a threatening regulation related to private PSE and can be categorized as a form of Surveillance state in digital business world. As a result, PSE feels dilemma between wanting to protect the privacy rights of users but being subject to administrative sanctions or injuring terms&references that formed by both for submit to the state.

Keywords: Private PSE; State Surveillance; User

INTRODUCTION

The development of digital technology for information dissemination becomes a double arrow effect which in addition to providing positive things to the digital business, but also threatening the interests of consumers or *Users* by the competent authority as a supervisor. Countries that used to have restrictions on monitoring now have the potential to know all the activities of their people by utilizing cyberspace whose function is vital in various privacy activities or personal data to use digital business services. Such threats can dehumanize privacy rights in cyberspace that include when, how, and to what extent information can be communicated to others.[1] The concrete evidence of surveillance that led to privacy losseswas seen in the case of complete data leakage including the phone number of a Covid-19 Patient in Cilegon in the form of a Microsoft Excel file circulating, making the Patient terrorized.[2]

Apart from the right to privacy as part of Human Rights (HAM) which is closely related to other rights of freedom, the state continues to carry out cyber surveillance which leads to losses to users and even Private Electronic System Operators (Private PSE). This is shown based on data obtained from Surfshark, a Netherlands-based cybersecurity company, that

[1] William Prosser In DeCew, Judith, "Privacy", 2012, *The Stanford Encyclopedia of Philosophy,* http://plato.stanford.edu/archives/fall2012/entries/privacy/.
[2] Banpos.co, "Pasien Covid-19 Merasa Diteror, Data Pribadi Bocor," June 14, 2020, https://banpos.co/2020/06/14/pasien-covid-19-merasa-diteror-data-pribadi-bocor/., diakses pada tanggal 14 September 2022

Received Februari 10, 2024; Accepted Maret 14, 2024; Published Mei 28, 2024
*Dini Mardhatillah, Ddmrdhsz15@gmail.com

Indonesia is in fourth place on the list of countries that have experienced the most data leaks globally, from January to August 2022, namely there are 13.89 million accounts whose data has been leaked.[3]

The supervision carried out by the state becomes even greater and more dangerous if you look at the establishment of the Minister of Communication and Information Regulation No. 5 of 2020 concerning Private Scope Electronic System Operators(Permenkominfo No. 5 Tahun 2020) which shows that excessive intervention is carried out by the state in the cyber world against Private PSE and *Users*. The regulation that raises the legal issue has injured the substance of protecting the privacy rights of *Users* managed by PSE, threatening both. Users are threatened with their privacy rights being violated. Meanwhile, PSE is in danger of being in a dilemma between fulfilling its obligations to the *User* or to the State.

As in Article 21 of Permenkominfo No. 5 Tahun 2020 which requires the PSE to provide access to Traffic *Data* and Electronic System User Information (*subscriber information*) to the State under the pretext of Supervision. This reason is very ambiguous and not specific so it can be indicated that there is excessive state supervision that can interfere with the contract between the PSE and the *user*. The impact is that there are major interruptions in the business world, especially Business and Human Rights and good corporate governance. Of course that's just one problematic one of the other issues in Article 12 Paragraph 3 jo Article 46, Part Two Chapter V, and Article 43 of Permenkominfo No. 5 Tahun 2020. Broadly speaking, there is still a lot of blurring in the "surveillance" provisions intended in this ministry of communication and information regulation.

Atthis time, PSE is an important forum for the life of cyber people in their daily activities. Given the adagium "where there is a society there is a law" (*Ubi Societas Ibi Ius*) makes the existence of laws governing PSE really very much needed, including regarding the protection of personal data as one of the rights of privacy. It is in this case that the State should immediately fix a number of articles *a quo* in Permenkominfo No. 5 Tahun 2020 to ensure the protection of the privacy rights of its citizens in this case PSE and Users by making specific rules to serve as implementation guidelines and making changes to the substance of the problematic article so as not to cause excessive state oversight or surveillance state. Referring to the concept of “Big Brother” in the 1984 novel by George Orwell's which produced an Orwellian understanding where the state can become an authoritarian figure by utilizing the

[3] (Sadya, n.d.)

development of mass surveillance technology.[4] Permenkominfo No.5 Tahun 2020 and increasingly vital digital technologies can make surveillance states like *Orwellian* a reality.

The state as a protector of people's rights should not turn into an authoritarian surveillance state which is the main threat. If we review the existence of Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which essentially states that "no man shall be disturbed by his personal affairs, his family, his household or his correspondence relationship arbitrarily." proving that the right to privacy is a fundamental right that each country needs to respect. This is in line with Article 28G Paragraph (1) of the Constitution of the Republic of Indonesia of 1945 (UUD NRI 1945) which states "Everyone is entitled to the protection of personal self, family, honor, dignity, and property under his control, and is entitled to a sense of security and protection from the threat of fear of doing or not doing something that is a human right".

As a consequence, everyone has the right to legal protection against interference or misconduct. In this case, the state should provide legal protection and safeguard each of the privacy rights of its citizens. According to Philipus M. Hadjon, such legal protection can be both preventive and repressive. In terms of repressive protection, it aims to resolve disputes, such as the handling of legal protection by courts in Indonesia. Whereas in preventive matters, legal subjects are given the opportunity to raise their objections or opinions before a government decision gets a definitive form. The goal is to prevent disputes from occurring.[5] Again, one of the realizations that can be taken by the State (Government) is to formulate regulations that are carried out to provide legal certainty (*rechtzekerheid*) to produce legal protection (*rechtbescherming*).

Based on the problems that have been presented, the presence of Perkominfo Nomor 5 Tahun 2020 this threatens the right to privacy for Users and the freedom to do business based on consumer protection by Private PSE. In addition, excessive state intervention can also occur due to the absence of surveillance restrictions that lead to surveillance states. Therefore, the author considers that the problem is very crucial and needs to be studied further. This study aims to analyze and examine **"How the problem of legal protection of private rights of PSE and Users in the form of supervision by the state?"** In addition, this study also wants to analyze **"How the legal protection of private rights of PSE and Users is ideal?"**

[4] Julie A Dilmac and Özker Kocadal, 2019, *Exchanging Glances with Big Brother: Diffuse Surveillance in Orwell's Nineteen Eighty-Four and Today* (Sciences et Actions Sociales, No. 12). pp.2.
[5] Philipus M Hadjon, 1987, *Perlindungan Hukum Bagi Rakyat Indonesia.* (Surabaya: Bina Ilmu). pp. 30

RESEARCH METHOD

The type of research used in this paper is normative legal research by placing laws and regulations as a system construction[6] and the rules contained therein.[7] Furthermore, the approach used is the statute approach[8] and conceptual approach.[9] The sources of legal materials used in this study are divided into 3 (three) namely primary legal materials in the form of official legal documents which are the main material,[10] secondary legal materials in the form of explanations of primary legal materials such as books and journal articles,[11] as well as tertiary legal materials such as the Legal Dictionary and the Big Indonesian Dictionary (KBBI) which contain explanations that give additional instructions to the two previous legal materials.[12] Furthermore, the data analysis method used is descriptive-analytical to describe the problem in detail and find solutions and prescriptive in order to get an assessment of what should be done according to the law.[13] The conclusion drawing uses a deductive way of thinking where starting from general to specific.[14]

RESULT AND DISCUSSION

1. Problems of Legal Protection of Private Rights of PSE and Users in the form of Supervision by the State

Legal protection by the state must essentially be directed at all aspects of life, especially in the cyber domain which is a new vital source of livelihood. It is as stated by Fitzgerald who states that "*legal protection that law aims to integrate and coordinate various interest in society as a traffic interest, the protection of certain interests can only be done by limiting the various interests on the other*".[15] In line with this paradigm, Prof. Satjipto Rahardjo is of the view that legal protection must provide protection for the human rights of everyone who is harmed by others in order to enjoy the rights granted by law.[16] Based on the opinions of the two experts, the main essence of legal protection should be directed at preventing or correcting losses to the

[6] Asikin Zainal and Amiruddin, 2012, *Pengantar Metode Penelitian Hukum*, Cet. keenam (Jakarta: Rajawali Pers). pp. 118.
[7] Soerjono Soekanto, 1984, *Pengantar Penelitian Hukum* (Jakarta: UI Press). pp. 20.
[8] Peter Mahmud Marzuki, 2011, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group). pp. 24
[9] Peter Mahmud Marzuki, 2013, *Penelitian Hukum (Edisi Revisi)* (Jakarta: Kencana Prenada Media Group). pp. 135-136.
[10] Johnny Ibrahim, 2007, *Teori & Metodologi Penelitian Hukum Normatif, Malang* (Malang: Bayumedia Publishing). pp. 141.
[11] Mukti Fajar ND and Yulianto Achmad, 2015, *Dualisme Penelitian Hukum Normatif & Empiris* (Yogyakarta: Pustaka Pelajar). pp. 318.
[12] Peter Mahmud Marzuki, 2005, *Penelitian Hukum : Edisi Revisi* (Jakarta: Kencana Prenada Media Group). pp. 183-184.
[13] Sri Soemantri Martosoewignjo, 1987, *Presepsi Terhadap Prosedur Dan Sistem Perubahan Konstitusi Dalam Batang Tubuh Undang-Undang Dasar 1945* (Bandung: Alumni). pp. 8-9
[14] Soerjono Soekanto and Sri Mamudji, 2001, *Peneltian Hukum Normatif* (Jakarta: Rajawali Pers). pp. 65
[15] Satjipto Raharjo, 2000, *Ilmu Hukum* (Bandung: PT. Citra Aditya Bakti). pp.54
[16] Satjipto,…2000, pp. 54.

interests of everyone to whom they are entitled, especially regarding vital branches, if there are still losses then the state fails to realize legal protection.

As an effort by the state to realize legal protection, especially in vital business and economic interests such as in cyberspace, there are several roles that can be carried out. Referring to the Constitutional Court Decision Number 001-021-022/PUU-I/2003 which provides an interpretation of the conception of "controlled by the state" in Article 33 may include *beheersdaad* (management), *bestuursdaad* (management), and *toezichthoudensdaad* (supervision). This conception is actually a manifestation of legal protection in the interests of Economic, Social, Cultural Human Rights (EKOSOB) which are positive rights with the embodiment "*right* to" and not "*freedom from*" so as to demand the active role of the state.[17] However, it is worth knowing that the active role of the state in the protection of the law does not always have to be actively manifested, but rather some must be passive.

If EKOSOB human rights demand the active role of the state, then the opposite is the case with Civil and Political Human Rights with its embodiment "freedom from″ so that the further the role of the state in intervening in this freedom, the better.[18] Furthermore, personal data as a derivative of the right to privacy becomes part of civil and political rights as stated in Article 17 of the International Covenant on Civil and Political Rights (KIHSP) which in its outline guarantees the right to legal protection for its privacy from any intervention or attack. Although Article 4 Paragraph (2) of the KIHSP does not list the right to privacy in the category of non-derogable rights, the state still has an obligation to formulate human rights limits based on the law, legitimate reasons, and the need for a democratic society.[19] As for if it refers to the restriction of legal protection on the right to privacy through Permenkominfo No.5 Tahun 2020 has not met these three criteria.

Legal protection of the right to privacy is so important that it requires a clear and comprehensive legislative ratio if restrictions are to be held. This statement is based on the thoughts of Samuel D. Warren and William Brandeis who put forward the theory of the *right to privacy* which is categorized into 6 (six) parts, namely right to be alone, limited access to the self, secrecy, control over personal information, personhood, dan intimacy.[20] In line with that, Alan Westin also stated that privacy became a necessity that existed from the very

[17] Manfred Nowak, 2003, *Introduction to The International Human Rights Regime* (Leiden: Martinus Nijhoff Publishers). pp. 24.
[18] Eko Riyadi, 2018, *Hukum Hak Asasi Manusia Perspektif Internasional, Regional, Dan Nasional* (Depok: RajaGrafindo Persada). pp. 43.
[19] See in ketentuan "Prinsip Siracusa Bagian B", angka 15-38
[20] (Solove 2002) pp.1087- 1155.

beginning of human beings[21] Where it is urgently needed for personal autonomy, emotional release, limited and protected communication, self-evaluation, and load minimization.[22] All these categories have become such a vital part of human life that without them, man would not live as himself or simply the more open his privacy the more vulnerable and lost the sovereignty of an individual. When associated with personal data which essentially includes all information data that can be identified directly or indirectly to an individual (not a legal entity) based on digits / identification codes, physiological, psychological, social and cultural identification.[23]

Considering that the owner of the right to privacy and its derivatives, namely personal data, is an individual or individual, then in the context of digital business, of course, consumers or often referred to as Users are *right*-holders. The personal data submitted to the Electronic System Operator (PSE) who acts well as a Personal Data Controller or Personal Data Processor provided under an agreement that must meet the principle of consumer protection so that in the event of losses such as leakage and/or misuse of it there must be compensation.[24] Achievements created from the privacy policy between the PSE (Personal Data Controller or Personal Data Processor) and the User which is usually in the form of a standard agreement must be prioritized for its fulfillment so that there is no default that can harm both parties. If there is a default in the form of a large-scale leakage of personal data, of course, it will have an impact on the economy and investment because PSE as a business actor must pay a large amount of compensation and reduce the level of user trust .

Protection of Users' personal data by PSE with a *legis ratio* from rights threats and activities that are increasingly dependent on cyberspace encourages the birth of new rights, namely digital rights covering all rights that exist in the real world but are implemented in cyberspace.[25] The formulation of law enforcement that injures *digital* rights without being accompanied by justification of derogation or limitation can lead to active human rights violations or acts of commission. This axiom is based on the meaning of human rights violations as "acts or omissions that are not yet a violation of national criminal law but are internationally recognized rules in relation to human rights".[26] This means that state actions

[21] Alan F. Westin, Prologue: Of Technological Visions and Democratic Politics, dalam buku (Westin 1971) pp. 1.
[22] Alan F. Westin, 1984, The Origins of Modern Claims to Privacy, dalam buku: Philosophical Dimensions of Privacy: an Anthology (ed. Schoeman, F. D.), (Cambridge: Cambridge University Press). pp. 56.
[23] (Djafar and Santoso 2019) pp.8.
[24] (S, n.d.)pp. 206 – 212.
[25] Katz, I.T.; Weintraub, R.; Bekker, L.-G.; Brandt, A.-M. 2021. From vaccine nationalism to vaccine equity—Finding a pathforward. N. Engl. J. Med. 384, 1281–1283.
[26] (Rover 2000) pp. 456.

that have not been or have been legalized within a legal framework that are not in accordance with international rules that are accepted by all nations are considered human rights violations.

Over-intervention from the government can lead to the application of the concept of surveillance state. As a first step to understand the concept of surveillance state, it is necessary to know in advance the limitations of the definition of surveillance itself. According to Proffesor Lyon, supervision is a focused, systematic, and routine attention given in order to get detailed information that will be used to influence, manage, protect, or direct.[27] Furthermore, supervision has elements in the form of: a) As an effort to learn information about individuals; b) As a systematic and deliberate effort rather than randomly or semborono; c) As a routine effort that is part of the activities of the apparatus that is characteristic of modern society;[28] d) Surveillance has such a broad purpose that it is not always for totalitarian domination, but rather rather for subtle influence or control.[29] This clear definition gives a bright spot to the concept of surveillance state, which is a state that conducts surveillance of each individual systematically and routinely carried out by officials for certain purposes.

The concept of surveillance state itself was created not when the state faced precarious circumstances or wars considering that these two situations were temporary. This concept is actually created in ordinary circumstances because of its systematic and routine nature so that it becomes a permanent activity carried out everywhere by the state in line with the development of legal needs and the legal mind of the welfare state.[30] The reason why it becomes a legal need and an effort to realize the legal ideals of the welfare state is that the collection and management of personal data in the community is very important to research the fulfillment of the interests of administrative or social services (social services) in policy formulation.[31] In addition, the collection of people's personal data can also help improve security from terrorist attacks and law enforcement against common criminal acts.[32] At first glance, this concept does look very good because it utilizes law and technology for the common good, but there are actually harmful effects.

If we refer to the Neil M. Richards paradigm which posits 4 (four) threats from state surveillance that can be carried out by state, private, or collaborative actors between the two.

---

[27] (Lyon 2007) pp. 14.
[28] David Lyon, 2007…, pp. 14.
[29] David Lyon, 2007…, pp. 15-16.
[30] (Balkin and Levinson 2006)
[31] Jack M Balkin & Sanford Levinson, 2006, …, pp. 520-23
[32] Fred H. Cate, 2008, Government Data Mining: The Need for a Legal Framework, Havard Civil Rights-Civil Liberties Law Review, Vol. 43, (Cate 2008)

These threats include the vulnerability of privacy interventions, especially intellectual privacy, and the disruption of the balance of power between individual sovereignty and oversight. In the second threat, it is fragmented again into 3 (three) dangers, namely blackmail, the risk of subtle persuasion (commonly used for the use of personal data for covert marketing purposes), and the misuse of sensitive personal data for various interests by various parties.[33] In line with the threat mapping, Jack M. Balkin also shared the negative impact of the surveillance state concept from : a) law enforcement emphasizes ex *ante* rather than *ex post* so that preventive efforts can be contrary to punishment in general, namely prioritizing *actus reus rather* than just *mens rea*; b) social services and law enforcement would resemble pressure-inducing parallel tracking; c) Private-state co-operation in surveillance states tends to be more burdensome for private parties given that they have the technology and resources to encourage the sale of personal data to cover losses.[34]

All vulnerabilities and threats to the concept of *surveillance state* have of course become the nature of technological developments that are double-edged swords. The development of surveillance technology ranging from cheap sensors, CCTV cameras, thermal cameras, GPS trackers, and RFID chips. As for web bugs and software tools commonly used by PSE, they can be digital monitoring tools as well. This abuse of the power of cutting-edge technology can certainly harm the large audience and business climate. Looking at the grassroots level, where the acquisition of data by the state without being accompanied by good capabilities and responsibilities has resulted in massive losses.

Based on a report by Dark Tracer which is a cyber research agency, in January 2022 there was a leak of user credential data from BPJS Ketnaker, BKN, Kemdikbud, and the Directorate General of Taxes reaching 502,000 data. Still according to a Dark Tracer report, in March 2022 the djponline.pajak.go.id failed to protect Users' credential data reached 17,585.[35] In addition, according to Kominfo in August 2022, the State Electricity Company (PLN) has been negligent in protecting 17,000,000 of its Users' personal data so that hackers @lolyta stolen and sold on the Breach Forum.[36] Furthermore, in September 2022 there was a leakage of personal data of Indonesian citizens at the Ministry of Social Affairs (Kemensos) to reach 102,533,221 data.[37] It doesn't stop there, in November 2022 there was a larger case of personal data leakage by the Ministry of Health (Kemenkes) due to data that was not detected by it so

[33] (Richards 2013)
[34] (Balkin 2008)
[35] (Ashari 2022)
[36] (Rizkinaswara 2022)
[37] (CNBC Indonesia 2022)

that it was easily leaked by Bjorka hackers. The leakage of personal data reached 3,250,144,777 data.[38] The presentation of this data shows that 2022 is proof that the government has not been able to protect the personal data of *Users* it manages.

People's personal data that should have been protected by the government was actually left unattended without a clear restoration effort. For example, the personal data of employees of the Ministry of Education and Culture (Kemendikbud) as users has been leaked up to 1,300,000 data ranging from names, places of birth dates, full names of parents, addresses, family card numbers, and national identity numbers. The response from the Ministry of Education and Culture was more about dissenting than real legal protection. In addition, the hacking of the Police Personnel Information System of the Republic of Indonesia is also sought to be hidden from the public where it should be responded to with real legal protection.[39] Leakage of personal data without being accompanied by good faith and protection responsibility for it results in unstoppable losses.

Misuse of personal data will have an impact on other parts of privacy, which in general include social media piracy, online loan terror or other spam, and hacking of digital financial services.[40] Impacts on Users' privacy can be material and immaterial. In modern times, almost all *Users* using fin-tech and e-commerce services can suffer material losses due to deprivation of access to finances. Daily life such as sending electronic messages, GPS location-specific data, camera and microphone access, and others. The privacy of users can be misused by third parties. Among these, the most affected by governments that are less responsible in managing personal data is the derogation of intellectual privacy, namely privacy to reflect on ideas and develop them without outside intervention which is closely related to the right to free speech.[41]

In addition, the adverse impact is also experienced by Private PSE because Users who get losses can have an effect on losing their trust to continue using the services or products offered. Considering that the main essence of consumer protection which is closely related to a good digital business climate is to maintain consumer awareness and dignity and increase the sense of responsibility of business actors[42] in this case Private PSE. In the world of digital business, consumers are increasingly critical in choosing the products or services offered due to the rapid dissemination of information. The worse the protection of users′ rights by Private

[38](CNN Indonesia 2022)
[39] (WAFI 2020)
[40] (Edu 2022)
[41] (Richards, 2008)
[42] (Barkatullah 2016) pp. 23.

PSE, will have an impact on decreasing profits due to being abandoned by Users. If this happens massively, it will have an impact on the country's economy.

It should be noted that Indonesia is one of the countries with the largest digital industry in the world with 204.7 million internet users.[43] Furthermore, the number of startups as of December 2021 in Indonesia reached 2,324 so that it occupied the fifth position and the number of online transactions reached 2.36 million units per 2020. Even Indonesia's digital economy is growing to 70 billion USD per year 2021.[44] If the state intervenes which leads to private PSE losing the trust of Users or even amputating a free digital business climate, it will have a major negative effect on Indonesia's digital industry which has contributed greatly to the national economy. Considering the requirements of the development of the digital business world is that all parts of digital rights are fulfilled, including the privacy rights of Users to protect the benefits of Private PSE as well.

Seeing the reality of the digital industry world which is very unfriendly to the PDP, of course, it has denied the right to privacy guaranteed protection which is contained in Article 28G Paragraph (1) of the Constitution of the Republic of Indonesia of 1945 (UUD NRI 1945) that "Everyone has the right to the protection of personal self, family, honor, dignity and property under his control, and is entitled to a sense of security and protection from the threat of fear of doing or not doing something that is a human right." The implication of this constitutional right according to Manfred Nowak is that human rights are relative as understood by Jimly Asshidiqie, that is, they apply as long as the constitution regulates them or is called absolutely human.[45]

In addition, at the level of international rules, human rights violations that have occurred due to regulations that do not accommodate denying Article 12 of the Universal Declaration of Human Rights (UDHR) reads "*No one shall be subjucted to arbitrary interference with his privacy, family, home or correspondence , nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*". The provisions of the UDHR are also adopted in Article 17 *verse* 1 of the International Convenant Civil and Political Rights (ICCPR) where the substance is equal and corroborating. Even the ICCPR has been ratified by Indonesia through Law Number 12 of 2005 concerning the Ratification of the ICCPR. Finally, the social and juridical realities in PDP regulation in Indonesia's digital business industry are not aligned with Article 11 of the Organisation for

[43] (Annur, n.d.)
[44] (15Februari2022)
[55](Matompo 2014)

Economic Co-Operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which regulates that PDP must be protected with protection derived from one of the threats is data disclosure. All of these international regulations are aligned to protect the protection of privacy rights as part of human rights that correlate with other rights.

The protection of personal data whose transfer flows are often carried out in private PSEs certainly requires legal protection that prioritizes the sovereignty of user privacy. However, on Permenkominfo No.5 Tahun 2020 in fact, there are many provisions that give the State excessive intervention and authority in the supervision of Users' personal data, resulting in the loss of people's privacy sovereignty. Some problematic provisions that lead Indonesia to surveillance state and injure the business climate that is free of excessive state intervention include Article 12 Paragraph 3 jo Article 46, Article 21 jo Article 23 Paragraph (2), Part Two Chapter V, and Article 43 of Permenkominfo No. 5 Tahun 2020.

First, Article 12 Paragraph 3 jo Article 46 of Permenkominfo No. 5 Tahun 2020 which requires the Cloud Computing Organizer[46] to provide electronic data of its service users to the authorities in the context of supervision, if they do not share access, they will get administrative sanctions from the Ministry of Communication and Information. The purpose of monitoring the electronic data of users or users is not explained at all and there is no arrangement regarding the permission of Users as the owner of personal data. To make matters worse, cloud computing is very often used in today's cyber age such as: a. Software as a Service with e.g. Gdocs, Adobe Creative Cloud, Spreadsheet; b. Infrastructure as a Service with e.g. Azure and Google Compute Engine; c. Platform as a Service with e.g. AWS Elastic Beanstalk, Google Cloud Platform, and IBM Bluemix.[47] Given that there are so many users of cloud computing services and the intensity of activities is high, the threat of misuse of personal data due to the absence of a clear surveillance purpose is very high. On the other hand, cloud computing operators are forced to violate Users′ privacy due to the threat of administrative sanctions.

Second, Article 21 jo Article 23 Paragraph (2) Permenkominfo No. 5 Tahun 2020 which requires the PSE to share access to electronic data (including Users' personal data) and its electronic systems with other ministries or state agencies for supervisory purposes. This, of course, invites the issue of PDP Users who are not clear what will be used for post-surveillance. Surveillance is a "process" carried out for a "purpose", so making the collection of personal

[46] (Susatyono 2021) Diakses pada Tanggal 16 Desember 2022
[47] Jarot Susatyono, 2021,…*id*

data a "purpose" is a logical fallacy. It should be explained "what for" the personal data collected post-surveillance, which is what is newly called "purpose". Furthermore, supervision in Article 23 Paragraph (2) is also stated to be the type of electronic data based on the relevant ministry so that various kinds of personal data can be collected including specific personal data such as for example health, physical, and mental data by the Ministry of Health.

Third, Part Two Chapter V (Article 22-Article 31) Permenkominfo No. 5 Tahun 2020 which describes the arrangements regarding procedures for sharing access from electronic systems and/or data for supervisory purposes. In this section there is a problem in the form of lack of *consent* (concern) from *Users* as the owner of personal data so that the most authorized in deciding on dissemination or restrictions is himself. Even in Article 28, the agreement related to how to regulate the granting of access to electronic data (personal data) is also only carried out between the ministry or state institution and the private PSE. In addition, the PSE was also not given the option to refuse so it was normatively powerless to resist.

Fourth, Article 43 Permenkominfo No. 5 Tahun 2020 which regulates the obligation to submit audit track records of system access and/or electronic data for supervision. Article 43 Paragraph (2) provides flexibility to accompany the audit track record with an assessment of the impact of access by the Ministry or Institution. This provision is actually more aimed at protecting Private PSEs and *Users* so that State Ministries or Agencies are not arbitrary in using access authority for supervision. However, logical fallacy again occurs when connected with Article 45 of Permenkominfo No. 5 Tahun 2020 where if a track record is not provided, it will be given administrative sanctions to the private PSE concerned. This is a mistake because sanctions should be given to those who can violate rights, instead of those who get rights. In this context, private PSEs are the exercise of the right of protection from the existence of Article 43 so they need to be protected and not threatened with sanctions.

Problems in the provisions Permenkominfo No. 5 Tahun 2020 has resulted in conflicts with the customary formulation of agreements between Private PSE and Users which are often spelled out in terms & references. As it is known that terms & references are standard agreements that are usually given by Private PSE to Users when providing their personal data in order to use the services and management of the webpage or application. This standard agreement itself usually discusses the use of users' personal data by Private PSE so that it is not misused. As long as this standard agreement does not violate Article 18 of Law Number 8 of 1999 concerning Consumer Protection (UU PK) Where broadly speaking, it has set certain clauses. The existence of Permenkominfo No. 5 Tahun 2020 resulting in a Private PSE dilemma between inserting a clause disseminating consumer personal data to an authority

without its consent and without knowing its final purpose or not notifying at all. Whichever choice is taken, will force Private PSE Article 18 UU PK.

When we associate Permenkominfo No.5 Tahun 2020 with Law Number 27 of 2022 concerning Protection of Personal Data (UU PDP) then there can be found conflicts with him. Based on Article 20 Paragraph (2) juncto Article 21 UU PDP then broadly explained that the controller of personal data Have the obligation to carry out explicit consent-based processing of personal data and convey it to Users starting from the legality, purpose, relevance of personal data, retention period, details of the info collected, period of processing, and rights of the personal data subject. This provision shows that the PDP Law is very concerned with the approval and transparency of the processing of users personal data so that active involvement of Users must exist. Especially in Article 47 and Article 51 Paragraph (3) UU PDP also imposes responsibility on the Personal Data Controller and the Personal Data Processor if obligations are violated so that oversight by the state that harms Users can drag Private PSE to disputes that can hinder the development of the digital industry.

Based on the presentation of these legal issues, it can be seen that the state that should be the duty-carrier of human rights through one of its duties to fulfil by formulating laws that provide protection of privacy rights to Users, actually creates surveillance regulations that can kill the right to privacy and the right to freedom of expression. Moreover, this can threaten the progress of the business climate and good human rights in the world of digital industry so that the state can be said to be an active human rights violator or act by commission. However, PSE that can be entangled in responsibilities that lead to administrative sanctions and have an effect on the digital economy weaken. Although it is undeniable that protection by the state can only work well if it has a lot of information through supervision where this creates a dilemma. It is necessary to formulate legal protections for the private rights of PSE and Users through surveillance oriented surveillance oriented into a democratic information state as implemented by South Korea, european union countries, and the United States.

2. Legal Protection of PSE Private Rights and Ideal Users

The development of technology should not ultimately be responded to with cynicism or rejection given the purpose for which it was created for a good thing and not for abuse. On the contrary, the law must be able to find solutions to problems arising from changes caused by the phenomenon of surveillance through digital technology in a massive, systematic, and structured manner. As stated by Soedikno Mertokusumo that the written law is always hobbled behind changes /events (*het recht hink achter de feiten aan*) to adjust the circumstances to

correct it.[48] Given that digital surveillance technology accompanied by information needs that are urgently needed by the state cannot be ignored, the concept of right to be forgotten can be erased.

In essence, the concept of right to be forgotten is the right for individuals to have all their data or information restricted, altered, or deleted because it can create shame, is irrelevant to the data owner, is anachronistic (inconsistent with the development of time), misleading, excessive, or misleading. This right is realized by making it difficult for individual information to be found in cyberspace so that it can be considered forcible neglect or oblivion.[49] As part of the right to privacy, the right to be forgotten is created due to the rapid development of digital technology for the dissemination of information and parties who often violate these interests such as private PSE itself or the state (Government or Company brought by the government). The difficulty of the *right to be forgotten* is implemented if the government directs to a new concept of supervision, namely the Democratic Information State.

Broadly speaking, surveillance states can be categorized into 2 (two) namely "Authoritarian Information State" and Democratic Information State. In the first model, namely the authoritarian information state, the State conducts supervision to obtain as much information as possible through confidential supervision and creates rules and regulations that give them the authority to obtain data without the imposition of accountability. The ultimate goal is of course to strengthen the influence and power of the state in controlling everything such as by misusing the information it has.[50] At Permenkominfo No. 5 Tahun 2020, liability charges are thrown at Private PSEs when the state can obtain as much data as possible behind the ambiguous "oversight" clause.

The second model, namely the Democratic Information State, the State conducts supervision to obtain as much information as possible through supervision under a legal umbrella that ensures transparency, participation, and clear accountability. The purpose of obtaining such information is for public administration services, development for agricultural purposes, education, scientific research, security and resilience, and other public interests. The acquisition of information data will be deleted regularly at predetermined intervals to protect privacy rights. If the data is difficult to delete because there is too much storage and is scattered everywhere, it will be destroyed[51] As long as the reason is that the right to be forgotten cannot

[48] (Mertokusumo 1966) pp. 99.
[49] Michael J. Kelly and David Satola, 2017, "The Right to Be Forgotten," *University of Illinois Law Review* 1, no. No.1, pp. 3-4.
[50] Stanley K and Laughlin Jr, 1968, "Westin: Privacy and Freedom," *Michigan Law Review* 66, no. 5. pp. 23-26.
[51] (Balkin 2008) pp. 18.

be applied is valid and indeed privacy data is not misused. This view is according to Alan Westin as further described by Stanley K. Laughlin Jr. as "Permissible Deviation."[52]

Supervision can still be carried out by the state on Private PSE along with privacy information belonging to the User provided that there needs to be a clear purpose of the supervision held, notification and approval of related parties, imposing liability on the right party, and implementing rules governing detailed and clear technical procedures. All of this is done in accordance with the principle of user centric in the world of digital business expressed by Edmon Makarim as a result of his analysis of the OECD Guidelines for Consumer Protection in the E-Commerce. The user's centric principle requires several things which include: *First*, the implementation of business activities efficiently and effectively in order to reduce economic burdens; *Second*, the application of business activities with the principle of trust and the principle of good faith in electronic systems whose security has good accountability; *Third*, prevention, convenience, and protection of consumer/user rights.[53] Given that the supervision carried out by the state on the activities of the digital business world affects Private PSE and user's which also have an effect on economic development, the legal protection formulated in the rules must use a good business and human rights approach.

In an effort to improve the charge material from Permenkominfo No. 5 Tahun 2020, then it can be started from the improvement of the level of detail and technicality as the implementing regulations that should be appropriate UU P3. If you look at the enactment of Law No. 11 of 2008 concerning Electronic Transaction Information (UU ITE) whose original p charges are still multi-interpreted such as Article 27 Paragraph (1) and Paragraph (3) regarding decency and defamation. Joint Decree (SKB) between the Minister of Communication and Information, the Attorney General of the Republic of Indonesia, and the Chief of Police of the Republic of Indonesia on Implementation Guidelines for a number of such Articles were issued to eliminate multi-interpretation. So to overcome the problems in the Ministry of Communication and Informatics here, a guideline is needed as a form of further regulation, for example in the form of S KB between the Minister of Communication and Informatics and all relevant ministries or state institutions in the implementation of supervision of private scope PSE.

The second option is the establishment of Permenkominfo others that focus on the implementation of mass supervision. As in Articles 36-40 Permenkominfo No. 5 Tahun 2020

[52] (K and Jr 1968)… , pp.1070.

[53] Edmon Makarim, 2014 , "Kerangka Kebijakan Dan Reformasi Hukum Untuk Kelancaran Perdagangan Secara Elektronik (E-Commerce) Di Indonesia," *Jurnal Hukum Dan Pembangunan*, Edisi No. 3, 44, pp. 320.

in essence, the Private Scope PSE is also required to provide access to Traffic Data and Electronic System User Information (Subscriber Information) requested by Law Enforcement Officials. which actually still needs an explanation regarding its implementation. However, granting access to Law Enforcement Officers is only used when an incident or suspected criminal act occurs, which is concerned with digital evidence, where there will be procedures for taking digital evidence. After being traced, there is already a Minister of Communication and Information that has been designed related to the Procedures for First Handling Electronic Evidence which is a reference for ministries, agencies, and law enforcement, However, the rule is still in draft form and has not been passed and enforced. This is also a task for the government, but at least it is better and clearer than data access to Private PSEs and their Users for the benefit of "Supervision" which still has a blur and there has been no follow-up at all.

As a way to find better ideas, it is also necessary to make comparisons with several countries in dealing with surveillance states. When we refer to the regulations in the United States regarding digital surveillance, there is a significant difference between mass surveillance and targeted surveillance. The term mass surveillance refers more to surveillance in the wider community, while targeted surveillance is more to reconnaissance individuals who have been determined for the benefit of law enforcement.[54] The United States also has regulations that can grant it immunity in carrying out surveillance activities under its legal umbrella, namely the Foreign Intelligence Surveillance Act 1978 (FISA Act) which is the domain of the Federal government in the name of *national security*.[55] The FISA Act is more of an intelligence activity on outside parties that could endanger the national interest. Meanwhile, targeted surveillance is carried out by law enforcement. The United States has made a clear distinction in the term "surveillance" so that the objectives and authorities under the appropriate legal umbrella to carry out such supervision provide more legal certainty.

The regulatory reference of a good privacy protection relationship between countries, Private PSE as the controller of personal data, and Users can also be clearly seen in the European Union through the European Union General Data Protection Regulation (EU GDPR). Based on Article 13 and Article 14 of the EU GDPR broadly states that there is a right to be informed or the right to be informed of the acquisition and use of personal data on the owner either obtained directly from the owner or indirectly. Furthermore, in Article 77 and *Article* 78 of the EU GDPR also states the existence of a right to lodge a complaint with a supervisory

[54] (Sharma 2021) pp. 17.
[55] Bureau of Justice Assistance U.S Department of Justice, *The Foreign Intelligence Surveillance Act of 1978 (FISA) Justice Information Sharing*, , https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286

authority and a right to an effective judicial remedy against a supervisory authority if the supervisory authority is suspected of violating the use of personal data. In addition to the right to self-defense when a supervisory authority (state) violates the use of personal data, there is a derogation provided for in Article 89 of the EU GDPR applicable to public interest, science, historical research, and statistical interests. Of course, all access and storage of user information by the state is based on the principles of lawfully, fairly, transparent and specified, explicit, compatible, legitimate purposes.

Some of these country comparisons add to the distinctiveness in the formulation of the Democratic Information State. When adjusted to the establishment of laws and regulations in Indonesia, the Minister of Communication and Informatics is friendly to user privacy and the implementation of the obligations of Private PSE in protecting consumers with two options. Either with the SKB or the establishment of a new Minister of Communication and Informatics that focuses on supervisory arrangements where later the objectives will be narrowed down to several interests such as monitoring the spread of certain diseases within a predetermined period and data needed to deal with health issues in the community. Another example is the monitoring of community stunting in an area by looking at the average height data where the data is managed in a predetermined period. Furthermore, a right to lodge a complaint mechanism will also be set up on the supervision that has been carried out. All of this is done by relevant ministries or state agencies that have been determined, except for law enforcement agencies, state tools, or intelligence agencies where the mass surveillance they carry out needs to be regulated in law because it has different impacts and objectives from other national interests.

Based on the presentation of this o-0i0o0-idea, it is hoped that the formulation of good surveillance state regulations in accordance with the democratic information state and the principle of Users centric can be realized ideally. The realization of this *ius constituendum* can create a more user-friendly digital business world and especially Private PSE so that it can encourage the country's economic development. In line with the legal postulate of Satjipto Rahardjo that the law must seek to protect the interests of everyone by ensuring that their rights can be in power/sovereign for their own interests.[56] Therefore, ensuring state intervention/supervision in the business world in the business world as necessary accompanied by procedures that provide legal certainty is the key to the success of protecting the rights of Private PSE and Users.

[56] (Rahardjo 2003) pp. 121.

CONCLUSIONS

This research has implications and contributions to ensure knowledge regarding state surveillance which endangers the state, including the privacy rights of the people, in this case PSE and its users. Article 12 Paragraph 3 jo Article 46, Article 21 jo Article 45, Part Two Chapter V, and Article 43 of Permenkominfo Nomor 5 Tahun 2020 can be categorized as an act of the concept of Surveillance state or excessive state intervention in the form of mass surveillance that violates the right to privacy for Users with the core of the legal problem being the blurring or ambiguity of the meaning of substance. The implications of a surveillance state that are not accompanied by credibility and clear accountability from the state can lead to adverse impacts on digital business due to forcing Private PSE to provide access to users' personal data to the state which can injure terms & references which is formed by both parties so as to create a dilemma between violating user privacy or being subject to administrative sanctions if it refuses to grant access. Therefore the concept of a surveillance state in the digital business era can be used as a state promotion if it is directed to become a democratic information state juxtaposed with the protection of privacy rights and user centric principles. The concrete embodiment of this idea can be created by creating a new Permenkominfo or SKB that is detailed and detailed as the implementing rules in general. Absorption of concern from users in the submission of access to information data, clarity of surveillance objectives, transparency, determination of authorized state parties, right to be lodge complaints, and time intervals of data utilization, as well as its elimination, and Differentiation between mass surveillance and targeted surveillance is the key to the success of legal protection to Users and Private PSE. Apart from that, this research is here to urge the government to revise Article 12 Paragraph 3 in conjunction with Article 46, Article 21 in conjunction with Article 45, Part Two Chapter V, and Article 43 of Minister of Communication and Information Regulation Number 5 of 2020 concerning Private Scope Electronic System Operators which is problematic because it does not provide legal certainty. Also formulate a draft of a new Permenkominfo or by forming a SKB on procedures for implementing supervision over Private PSE and Ratify the draft Permenkominfo on Procedures for First Handling of Electronic Evidence.

REFERENCES

Book

Barkatullah, Abdul Halim. Framework Sistem Perlindungan Hukum Bagi Konsumen Di Indonesia. Bandung: Nusa Media, 2016.

Djafar, Wahyudi, and M.Jodi Santoso. Perlindungan Data Pribadi Konsep, Instrumen, Dan Prinsipnya. ELSAM, 2019.

Hadjon, Philipus M. Perlindungan Hukum Bagi Rakyat Indonesia. Surabaya: Bina Ilmu, 1987.

Ibrahim, Johnny. Teori & Metodologi Penelitian Hukum Normatif, Malang. Malang: Bayumedia Publishing, 2007.

Lyon, David. Surveillance Studies. Oxford: Polity Press, 2007.

Martosoewignjo, Sri Soemantri. Presepsi Terhadap Prosedur Dan Sistem Perubahan Konstitusi Dalam Batang Tubuh Undang-Undang Dasar 1945. Bandung: Alumni, 1987.

Marzuki, Peter Mahmud. Penelitian Hukum. Jakarta: Kencana Prenada Media Group, 2011.

———. Penelitian Hukum : Edisi Revisi. Jakarta: Kencana Prenada Media Group, 2005.

———. Penelitian Hukum (Edisi Revisi). Jakarta: Kencana Prenada Media Group, 2013.

Mertokusumo, Soedikno. Mengenal Hukum Suatu Pengantar. Yogyakarta: Liberty, 1966.

ND, Mukti Fajar, and Yulianto Achmad. Dualisme Penelitian Hukum Normatif & Empiris. Yogyakarta: Pustaka Pelajar, 2015.

Nowak, Manfred. Introduction to The International Human Rights Regime. Leiden: Martinus Nijhoff Publishers, n.d.

Prosser, William. The Stanford Encyclopedia of Philosophy, 2012.

Rahardjo, Satjipto. Sisi-Sisi Lain Dari Hukum Di Indonesia. Jakarta: Kompas, 2003.

Raharjo, Satjipto. Ilmu Hukum. Bandung: PT. Citra Aditya Bakti, 2000.

Riyadi, Eko. Hukum Hak Asasi Manusia Perspektif Internasional, Regional, Dan Nasional. Depok: RajaGrafindo Persada, 2018.

———. Scott Davidson Dalam Eko Riyadi, Hukum Hak Asasi Manusia Perspektif Internasional, Regional, Dan Nasional. Depok: RajaGrafindo Persada, 2018.

Rover, C. de. To Serve & To Protect, Acuan Universal Penegakan HAM. Jakarta: Rajawali Press, 2000.

Soekanto, Soerjono. Pengantar Penelitian Hukum. Jakarta: UI Press, 1984.

Soekanto, Soerjono, and Sri Mamudji. Peneltian Hukum Normatif. Jakarta: Rajawali Pers, 2001.

Westin, Alan F. Information Technology in a Democracy. Massachusetts: Harvard University Press, 1971.

———. Philosophical Dimensions of Privacy: An Anthology (Ed. Schoeman, F. D.). Cambridge: Cambridge University Press, 1984.

.Westin, Alan F. Privacy and Freedom, 1967.

Zainal, Asikin, and Amiruddin. Pengantar Metode Penelitian Hukum. Cet. keenam. Jakarta: Rajawali Pers, 2012.

Regulation

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Deklarasi Universal Hak Asasi Manusia 1948

European Union General Data Protection Regulation (EU GDPR)

Kovenan Internasional tentang Hak-hak Sipil dan Politik (ICCPR) tahun 1966

Peraturan Menteri Komunikasi dan Informatika tentang Tata Cara Penanganan Pertama Bukti Elektronik

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem Transaksi Elektronik, LN.2019/NO.185,TLN NO.6400

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem Transaksi Elektronik, LN.2019/NO.185,TLN NO.6400

Permenkominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat BN.2020/No.1376

Surat Keputusan Bersama Menteri Komunikasi dan Informatika RI, Jaksa Agung RI, dan Kepala Kepolisian RI Nomor 229 Tahun 2021 Nomor 154 Tahun 2021 Nomor KB/2/VI/2021

Undang-Undang No. 11 Tahun 2008 tentang Informasi Transaksi Elektronik, LN.2008/NO.58, TLN No.4843

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, LN. 1999/ No. 22, TLN NO. 3821

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, LN.2022/No.196, TLN No.6820

Verse 1 International Convenant Civil and Political Rights, Resolusi 2200A (XXI) (n.d.).

Jurnal

Balkin, Jack M. "The Constitution in the National Surveillance State." Minnesota Law Review 93, no. 1 (2008): 18.

———. "The Constitution in the National Surveillance State." Minnesota Law Review 93, no. 1 (2008): 15,16,17.

Balkin, Jack M, and Sanford Levinson. "The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State." Fordham Law Review 75, no. 2 (2006): 520–23.

Cate, Fred H. "Government Data Mining: The Need for a Legal Framework." Havard Civil Rights-Civil Liberties Law Review 43 (2008): 440.

Dilmac, Julie A, and Özker Kocadal. Exchanging Glances with Big Brother: Diffuse Surveillance in Orwell's Nineteen Eighty-Four and Today. Sciences et Actions Sociales, No. 12, 2019.

Jolly, R. D. "Mannosidosis of Angus Cattle: A Prototype Control Program for Some Genetic Diseases." Advances in Veterinary Science and Comparative Medicine 19 (1975): 1–21.

K, Stanley, and Laughlin Jr. "Westin: Privacy and Freedom." Michigan Law Review 66, no. 5 (1968): 1070.

Kelly, Michael J., and David Satola. “The Right to Be Forgotten.” University of Illinois Law Review 1, no. No.1 (2017): 3–4.

Kreuzer, W. “Ecological Observation of the 137Cs-Contamination in Beef of Animals from the Southern-Bavarian Area.” Environmental Quality and Safety 4 (1975): 24–36.

Makarim, Edmon. “Kerangka Kebijakan Dan Reformasi Hukum Untuk Kelancaran Perdagangan Secara Elektronik (E-Commerce) Di Indonesia.” Jurnal Hukum Dan Pembangunan, Edisi No. 3, 44 (2014): 320.

Matompo, Osgar R. “Pembatasan Terhadap Hak Asasi Manusia Dalam Perspektif Keadaan Darurat.” Jurnal Media Hukum, No.1, 21 (2014): 64.

Richards, Neil M. Intellectual Privacy. 87 Tex. L. Rev. 387, 2008.

Richards, Neil M. “The Dangers of Surveillance.” Havard Law Review 126, no. 7 (2013): 1945.

Romdoni, M., Fatma, M., Nurdiansyah, R., Suyanto, S., & Fahmi Lubis, A. (2023). A critique and solution of justice, certainty, and usefulness in law enforcement in Indonesia. Journal of Law Science, 5(4), 174-181. https://doi.org/10.35335/jls.v5i4.4269

S, Dewi. “Prinsip – Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya.” Sosiohumaniora 19, no. No.3 (n.d.): 206–12.

Solove, Daniel J. “Conceptualizing Privacy.” California Law Review, Article 2, 90, no. 4 (2002).

Website

Annur, Cindy Mutia. “Ada 204,7 Juta Pengguna Internet Di Indonesia Awal 2022.” Accessed March 23, 2022. https://databoks.katadata.co.id/datapublish/2022/03%20/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022.

Ashari, Mahmud. “Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga Adalah Data Pribadi,” March 22, 2022. https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html.

———. “The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State.” Fordham Law Review 75, no. 2 (2006): 520–23.

Banpos.co. “Pasien Covid-19 Merasa Diteror, Data Pribadi Bocor,” June 14, 202AD. https://banpos.co/2020/06/14/pasien-covid-19-merasa-diteror-data-pribadi-bocor/.

DataIndonesia.id. “Rangkuman Data Perkembangan Ekonomi Digital Indonesia Artikel Ini Telah Tayang Di Bisnis.Com Dengan Judul "Rangkuman Data Perkembangan Ekonomi Digital Indonesia,” 15Februari2022. https://finansial.bisnis.com/read/20220215/563/1500443/rangkuman-data-perkembangan-ekonomi-digital-indonesia.

Edu, Heylaw. “Mafia Jual Belikan Data Pribadi WNI Di Tengah Pandemi Covid-19! Bagaimana Perlindungan Hukumnya?,” March 14, 2022. https://heylawedu.id/blog/mafia-jual-belikan-data-pribadi-wni-di-tengah-pandemi-covid-19-bagaimana-perlindungan-hukumnya\.

Gardos, G., and J. O. Cole. “Maintenance Antipsychotic Therapy: Is the Cure Worse than the Disease?” The American Journal of Psychiatry 133, no. 1 (January 1976): 32–36.

https://doi.org/10.1176/ajp.133.1.32.

Indonesia, CNBC. "102 Juta Data Warga RI Di Kemensos Dilaporkan Bocor," September 14, 2022. https://www.cnbcindonesia.com/tech/20220914164253-37-372099/102-juta-data-warga-ri-di-kemensos-dilaporkan-bocor.

Indonesia, CNN. "Data PeduliLindungi Tak Dienkripsi? Pakar Sindir Beda Ucap Dan Fakta Baca Artikel CNN Indonesia "Data PeduliLindungi Tak Dienkripsi? Pakar Sindir Beda Ucap Dan Fakta," November 16, 2022. https://www.cnnindonesia.com/teknologi/20221116133010-192-874507/data-pedulilindungi-tak-dienkripsi-pakar-sindir-beda-ucap-dan-fakta.

Radley-Gardner, Oliver, Hugh Beale, and Reinhard Zimmermann, eds. Fundamental Texts On European Private Law. Hart Publishing, 2016. https://doi.org/10.5040/9781782258674.

———, eds. Fundamental Texts On European Private Law. Hart Publishing, 2016. https://doi.org/10.5040/9781782258674.

Rizkinaswara, Leski. "Data Pelanggan PLN Bocor, Kominfo: Sudah Dipanggil Dan Terus Dipantau," August 22, 2022. https://aptika.kominfo.go.id/2022/08/data-pelanggan-pln-bocor-kominfo-sudah-dipanggil-dan-terus-dipantau/.

Sadya, Sarnita. "Peta Kebocoran Data Global Sepanjang 2022, Termasuk Indonesia." Accessed September 15, 2022. https://dataindonesia.id/digital/detail/peta-kebocoran-data-global-sepanjang-2022-termasuk-indonesia.

Sharma, Ishan. A More Responsible Digital Surveillance Future: Multi-Stakeholder Perspective and Cohesive State & Local, Federal, and International Actions. Federation of American Scientists, 2021.

Susatyono, Jarot Dian. "Apa Itu Cloud Computing? Beserta Manfaat, Cara Kerja Dan Contoh." Universitas STEKOM, November 1, 2021. http://sistem-komputer-s1.stekom.ac.id/informasi/baca/Apa-Itu-Cloud-Computing-Beserta-Manfaat-Cara-Kerja-dan-Contoh/cf2ad82fb83125f83dfcac83ec61a3807a9ac126.

WAFI, RANGGA NAVIUL. "Pemerintah Tidak Serius Melindungi Data Pribadi Kita," December 7, 2020. https://www.remotivi.or.id/mediapedia/609/pemerintah-tidak-serius-melindungi-data-pribadi-kita.