http://ejournal.seaninstitute.or.id/index.php/Ekonomi
Jurnal Ekonomi, Volume 12, No 03, 2023
ISSN: 2301-6280 (print) ISSN: 2721-9879 (online)

THE URGENCY OF REGULATING THE USE OF PERSONAL DATA IN THE BUSINESS AND POLITICAL AGENDA IN INDONESIA

Aurellia Shinta Purnamasari
Political Science, Faculty of Social and Political Sciences, Padjadjaran University

ARTICLE INFO

Keywords:
Business; Human Security;
Personal Data; Politics

E-mail:
aurellia19003@mail.unpad.ac.id

ABSTRACT

The scope of geopolitics is no longer limited to state security, but also include human security. Coupled with globalization and the industrial revolution 4.0, the business and political sectors see personal data as a valuable resource. However, utilization without adequate regulation has the potential to threaten guarantees of privacy rights that can harm data owners, and even compromise the security of the country in the future. Therefore, this article wants to know the extent of limitations on the use of personal data in the business and political sectors in Indonesia in the implementation of Law No. 27 of 2022 on Personal Data Protection. This article uses an exploratory qualitative approach with secondary data sources in the form of literature and reports relevant to the problem being studied. The results show that so far the implementation of the PDP Law is still ineffective and there is no regulation limiting the use of personal data for business and political purposes, making it prone to misuse. In addition, there were inequalities in handling data leaks in line with low public awareness regarding the protection of personal data. Therefore, Indonesia needs to develop regulations referring to the GDPR in a comprehensive form where these regulations can ensuring the protection of personal data as a manifestation of a constitution that guarantees the right to privacy of citizens.

1. INTRODUCTION

The concept of security has undergone an expanded of meaning and has begun to pay attention to non-traditional issues. The scope of geopolitics is no longer limited to state security, but also include human security. The change from high politics to low politics also created a new constellation. The complexity of the existing problems makes the focus of security no longer limited to power competition, supported by globalization, the industrial revolution, economic integration, and other socio-political issues that have given rise to so-called non-traditional security that concerns human security.

The era of the industrial revolution and information disclosure has the potential to threaten the guarantee of privacy rights, especially those controlled by various digital companies to their use for political purposes. At an already integrated stage of life, about 196 million people are now connected to the internet. There are four forms of technology that significantly influence the current era, including mobile internet, cloud technology, the internet of things, and big data (McKinsey, 2016). However, it is still very unfortunate that many Indonesian people lack of literacy and knowledge about the digital world so they do not realize the importance of protecting credential data. Some personal data, such as national identity numbers, telephone numbers, domicile addresses, and so on have the potential to be misused by irresponsible individuals for unilateral benefits. This clearly a detrimental social impact on the owner of the associated data.

Technological advances indirectly affect the working mechanisms of most industries, including government agencies. The data management process continues to experience innovation in line with the development of information technology that occurs. This is also proportional to the complexity of data management, processing, accountability, security, and disposition. In the realm of government institutions, personal data sets are used as a consideration factor in decision making. Government agencies manage existing data and information for the purpose of make it as a source of information in compiling targeted government programs for community empowerment. Broadly speaking, there are several objectives of using big data for the government, namely improving government performance, increasing state revenue, and upholding transparency in each sector.

Not only government institutions, political parties in this case also use personal data collections for political purposes under the pretext of implementing the industrial revolution 4.0. This activity that using personal data collection for political purposes is considered to shape the image of political parties as modern organizations that are adaptive to technological developments. For example, the use of social networks and mass media in political campaigns that aim of collecting the latest information circulating in society and intensifying competition between candidates is the use of the hashtags #2019GantiPresiden and #JokowiTigaPeriode. The concept arises from none other than the results of processing circulating information. In addition, political parties also use personal data to determine the characteristics of voters as a basis for developing strategies to attract voters' attention.

Furthermore, in the business sector, personal data is used to determine market trends through consumer preferences as well as information related to other businesses. It aims to achieve marketing targets, increase revenue opportunities, show competitiveness, and so on. Big data is seen as a potential resource with great influence on some groups with specific interests. The digital era makes capitalists increasingly hungry for consumer data, people's behavior patterns, and all forms of interaction in the mass media (Schonberger, et al., 2018).

The existence of e-commerce to e-government that utilizes technological systems is able to collect, store, and process data. In business, personal data is an asset that meets the criteria in trade secrets and has the potential to cause thorny conflicts without proper management of data processing and protection (Radon, 2015). Databases on personal identity are also not infrequently traded or exchanged for other benefits for political purposes, one of which is for campaign purposes and voter mapping. Quoting the statement of the Director of the Geopolitical and Global Future Area Study Program, Arief Pranoto (2020) that the meeting of global or local elite interests that focus on accommodating all corporatist to oligarchic interests through the control of big data by establishing cooperation through infrastructure and political superstructure. The reality is that all of these activities are still in the poor quality of data processing and protection management, both by the state and the private sector. In recent years, Indonesia has been hit by various problems regarding data leakage. Reporting on the KrAsia news channel, there are at least seven major cases of personal data leaks involving large technology companies, such as Tokopedia and Bukalapak, to government agencies, such as BPJS Kesehatan and the General Election Commission.

Indonesia, which is one of the largest internet user countries, should have regulations regarding personal data protection. The regulation is a manifestation of Article 28 G paragraph 1 of the Constitution of the Republic of Indonesia which states that respect, protection, and enforcement of the right to privacy is essentially the responsibility of the state. The concept of personal data protection implies that a person has the right to determine whether he or she will join an online community, share, or even exchange personal data with others, as well as the right to determine the conditions that must be met to do so (Mangku et al., 2020). The ratification of the Personal Data Protection Law as an effort to deal with the problem of leakage of personal data seems to be insufficient. Quoted in databoks, data leakage cases in Indonesia jumped by 143% in the second quarter of 2022, which means that there were three accounts that experienced data leaks every three minutes during January-March 2022. The number continues to increase to eight accounts per minute in April-June 2022. Until the third quarter of 2022, as many as 12,742,013 accounts were leaked. Fluctuating chart patterns indicate that the problem of leakage of personal data has not been fully resolved.

Data leakage that occurred proves that the level of industry readiness is still mostly below average, so it does not have adequate standards regarding data security and management. In addition, there are still regulatory vacancies regarding the establishment of authorized institutions as supervisors as a whole, details of sanctions provisions, and arrangements regarding the extent of the use of personal data, especially in the business and political sectors. This reality has the potential for inequality in handling data leakage cases and confusion of institutional involvement, both in data processing matters and handling personal data protection. Director of the Institute for Community Studies and Advocacy (ELSAM) Wahyudi Djafar stated that there is overlap and synchrony between articles (Wahyudi and Djafar, 2014). Political compromises that occur will ultimately affect the quality of the substance resulting in inconsistent handling by the state in terms of guaranteeing the privacy rights of Indonesian citizens.. Based on the existing problems, the author is interested in analyzing loopholes in Law No. 27 of 2022 and analyzing the urgency of regulating the use of personal data in the business and political sectors in Indonesia.

2. METHODS

This article uses an exploratory qualitative approach with data collection techniques in the form of literature studies. And also this research stands on the basis of primary data through interviews that aim

to explore broadly about the causes or things that affect something with data leakage cases and their handling in Indonesia as an analysis unit. As for Mestika Zed (2003), literature studies are defined as a series of activities related to data collection methods, review, recording and processing of research materials obtained through various references, such as books, literature, and reports related to the problem to be studied. The data sources used are secondary data, in the form of journals relevant to related topics and reports on data leakage cases and their handling, both in Indonesia and abroad. After the entire data is collected and validated, the researcher will analyze the data to obtain a conclusion and validate it through data triangulation techniques.

3. RESULTS AND DISCUSSION

Privacy is the right of every individual which is very important to protect in order to maintain integrity and human dignity (Wahyudi and Djafar, 2014). All data and information of a person fall into the category of secrets that become a unified right of privacy from the concept of human rights. From a Human Rights point of view, the protection of personal data is a crucial aspect in realizing the guarantee of privacy rights that are also regulated in international law, such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). McDermott (2017) suggests several instruments related to personal data protection, including privacy, transparency, autonomy, and non-discrimination. Alan Westin (1967) defines the right to privacy as the claim of an individual, group, or institution to determine for itself regarding when, how, and to what extent information about them is communicated to others. The initial concept of personal data protection was first initiated by Germany in 1970, followed by several other countries, such as Sweden, the United States, France, the United Kingdom, and several others countries as part of privacy protection. It has been regulated into international norms which are then derived and adopted as part of national law, so that the guarantee of the protection of personal data is under the responsibility of the state. Schoeman (1984) identifies the right to privacy as a measure of an individual's control over a number of elements of personal life, which include personal information, the confidentiality of identity, as well as the accessibility of certain parties to such information.

The spread of personal data is becoming increasingly uncontrollable, especially in economic activities. This reality is accompanied by low public awareness of the importance of guaranteeing the right to privacy. In everyday life, it is not uncommon for people to get short messages from unknown parties even though they feel that they have never disseminated a telephone number to related parties. Seeing the existing situation, the public is trapped by the Terms of Use in certain applications or sites and unknowingly agrees to the use and dissemination of user personal data to third parties for marketing purposes. The current situation of data leakage in Indonesia may not be too different from that in other countries in the world. Data leakage can occur for various reasons, such as failure to maintain information security, theft of information by irresponsible parties, or even due to accidental human error. Data leakage can cause losses to the affected individuals or companies, such as financial loss, reputational damage, or even lawsuits.

UNCTAD or the United Nations Conference on Trade and Development mentions personal data recorded in e-commerce activities and collected in the marketplace, such as password encryption, credit or debit card numbers, and several other data related to purchases. The latest data recorded that as many as 53% of business actors commit personal data breaches only for business purposes. The existence of data leaks illustrates the weak cybersecurity system in Indonesia. Coupled with the uncertainty of policies that result in violators can easily get out of hand over data leakage events that can actually harm the community in the future. In a broader scope, personal data that has been misused is often used to commit crimes that include the creation of fake accounts, online fraud, money laundering and illicit transactions. The consequence of this incident is the threat of national security. Based on these threats, it can implicitly be said that the purpose of these attacks is based on economic motives (to benefit from the data attacks obtained) as well as political motives. Thus, data protection efforts are crucial, especially for governments that actually hold various data belonging to their people.

The state has actually shown efforts to protect personal data in reaction to the escalation of data leakage and its misuse by certain individuals that has the potential to harm some parties. Regulations currently in force regarding the protection of personal data include Article 26 paragraph 1 of the ITE Law, Minister of Communication and Informatics Regulation Number 20 of 2016, PP Number 80 of 2019 concerning Trade through Electronic Systems. However, these regulations have not been able to handle cases of data leaks that often occur. By considering the threats and potential violations, an arrangement was formed regarding the protection of personal data, namely Law No. 27 of 2022 concerning the Protection of Personal Data. The Personal Data Protection Law consists of 16 chapters and 76 articles regulating the rights of personal data subjects or the rights of natural persons to whom personal data is

attached; terms of processing of personal data, including the obligations of the controllers and managers of personal data; establishment of personal data protection agencies; as well as the imposition of sanctions. There are also two types of sanctions for violators, in the form of administrative and criminal sanctions such as written warnings, temporary suspension of activities, destruction of personal data, to fines as high as two percent of annual income for variable violations that will be imposed on individuals or corporations. Illegal use will be subject to criminal penalties or fines, as well as deprivation of profits until the dissolution of the business if carried out by the corporation. It is enforced to prevent unauthorized data access and data processing outside the destination. The PDP Law also regulates the approval of the use of personal data which is only carried out on the consent of the owner of the personal data.

Until now, the regulation has not been implemented effectively, so the cyber climate in Indonesia has certainly not experienced significant improvement. In the 2022 Databoks report, citing the National Cyber Security Index, Indonesia's score was only 38.86 out of 100 points. This resulted in Indonesia being ranked 3rd bottom among G20 member countries and 83rd out of 160 countries within the scope of the report. Despite demonstrating cybersecurity-related commitments, programs, and initiatives, technically there are still some shortcomings, such as low cybersecurity standards for organizations, both private and government. Meanwhile, in terms of the format of legislation, Indonesia still needs substantial improvement. This is evidenced by the prosecution of judicial review of several articles in the PDP Law by civilians. So far, there are several reasons underlying the civil desire for judicial review of the PDP Act. The current regulations are not comprehensive enough, especially in terms of corporate oversight that can be linked to political interests. Considering that corporations are the business actors that have the most direct contact in business activities, from collecting to processing consumer personal data.

The need for personal data protection regulations has not been in line with public awareness of the importance of protecting personal data. This is evidenced by the public's incomprehension of the privacy policy and terms of service of the application on the online platform. The scope of personal data may vary by country. Indonesia itself defines personal data as certain individual data that is stored, maintained, and maintained truthfully and protected by confidentiality. That way, name, NIK, address, and genetic data are included in personal data. Based on GDPR regulations and the Personal Information Protection Law, personal data is classified into two, namely personal data and sensitive data, such as ideology, beliefs, sexual orientation, and others. Differences in interpreting the scope of personal data are important because they affect the country's strategy in formulating policies to combat data leakage.

The focus of security in the concept of individual security still leans towards two main components, namely economic and political which ultimately causes problems that are non-military or asymmetric warfare, such as proxy war, cyber crime, and so on. It is said to be asymmetric warfare because there is no direct physical contact, but it has an impact on the economic, social and political stability of a country. The data that was hacked, including state-owned companies, ministries, to personal data. The sectors that experience the most data breaches are crucial sectors, namely the financial and professional sectors, including health, information, public administration, and so on. In addition, the state's handling of data leakage cases is still considered lame and indiscriminate. This is evidenced by efforts to desecuritize the problem of data leakage when business actors are partners or even the country itself and the victims are ordinary people. On the other hand, the state responsively takes concrete steps if the leakage of personal data is experienced by important figures, as happened to President Joko Widodo some time ago, when his NIK was spread due to a data leak in the peduli lindungi application. Not stopping there, the threat of data leaking by Bjorka hackers also succeeded in making the government take a stand on data leaks. Given that, the disseminated data is suspected to be classified data and has the potential to disrupt the stability of the country. Desecuritization efforts are also seen in how countries allow the use of big data without clear restrictions and guarantees of protection.

Business Sector

Violations of privacy rights do not only occur among private parties. Programs and policies initiated by the state also do not guarantee the confidentiality of customer personal data, for example e-KTP. The existence of e-KTP has resulted in the state easily tracking the personal life of every Indonesian citizen. This certainly violates the provisions of civil liberties. In addition, Minister Tjahjo Kumolo said that the server used is still in the possession of other countries so that all data in it can be easily accessed by irresponsible individuals. This practice makes consumers disturbed by their privacy, thus implying the emergence of consumer distrust of corporations as data managers (Dewi, 2018).

Regulations related to personal data protection, especially in the business sector involving corporations are still explicitly spread and differentiated at various levels of legislation in Indonesia, as

contained in several articles in Law No. 8 of 1997 concerning Corporate Documents, Law No. 10 of 1998 concerning Banking, Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE), Law No. 14 of 2008 concerning Public Information Disclosure, and so on.

Activities to collect personal data by business actors are often misused for selling data, marketing, profiling data, and espionage. The magnitude of the violation is also due to the rampant number of corporations that do not comply with the standardization applied based on Government Regulation No. 71 of 2019, Government Regulation No. 80 of 2019, and Regulation of the Minister of Communication and Informatics No. 20 of 2016 which as a whole regulates the standardization of electronic system security.

The risk of misuse of private data also affects the security and peace of the community in a wider scope. The situation is factually true, due to personal data being in the hands of irresponsible third parties. Hacking and theft of personal data for crimes has the potential to harm data owners, even countries. However, the use of personal data for political purposes, through marketing and buying and selling information, will cause a domino effect.

Laws regarding the protection of personal data in Indonesia tend to be general in nature so that it can be seen as a weakness that causes some companies not to choose Indonesia as a location for their data storage centers. In fact, the development of personal data protection arrangements will support Indonesia's future development as a global data center. This non-specific regulation leads to the ineffectiveness of the supervision system by the Ministry of Communication and Informatics. In its implementation, Kominfo is still relatively passive, especially in terms of investigations that lead to the escalation of data theft cases and violations by business actors, such as illegal data access to trade consumer data. Consumers as data owners are often the object of direct marketing from business actors that have the potential to derogate peace and comfort to consumers, such as the terror of short messages about products and services. This can adversely affect public trust, as well as hinder the provision of a clear road map on the concept of personal data protection in Indonesia. This has implications for the unclear concept of supervision of corporations as parties who collect, process, and process personal data of consumers.

Detailed arrangements regarding the limitations of the use of personal data as well as the form of accountability of data processors are very necessary because they regulate the collection, use, disclosure, transmission and security of personal data and in general the regulation of personal data is to find a balance between the need for protection of personal data of individuals with the need for governments and businesses to obtain and process personal data for legitimate purposes. Regulatory arrangements regarding personal data will indirectly place Indonesia with other countries with advanced economic levels because it has the potential to strengthen Indonesia's position as a trusted business and investment center. In this case, the interests of consumers in the business sector become valuable, so it requires certainty that the data is well protected and is in a conducive management and data processing environment.

Until now, Kominfo is still the leading sector as well as a personal data supervisory agency that indirectly implements the provisions in the PDP Law. However, this is seen as a fallacy. The designation of the communications and information technology as a personal data supervisory agency will raise questions about its partiality, given that it is still in state control. The imposition of sanctions on business actors, between private and state-owned or state-owned enterprises may be biased. In addition, there is no provision regarding the coordination mechanism between the sub-field of personal data protection of Kominfo and the data officer of the corporation who makes the annual report not run as it should.

Not only that, the authority of the Ministry of Communication and Informatics regarding the mechanism for investigating findings of violations from the supervision process is still not regulated in the Minister of Communication and Informatics. This has implications for the discrepancy of sanctions imposed on corporations due to the non-implementation of a holistic investigation mechanism. Various problems in the sub-field of personal data protection of the Directorate of Applications and Informatics make corporations non-compliant, thus implying the insecurity of electronic systems as a center for consumer personal data management activities. The disobedience of the corporation has very serious implications in the form of opening security loopholes that can be exploited by criminals. From data reported by the State Cyber and Password Agency (BSSN) in 2020, there were 88.4 million cyberattacks in Indonesia, 83% of which were vulnerable to corporations.

Political Sector

Today, political campaigning is one of the activities that also adopts technology through profiling voter data. Compared to Norway, which regulates profiling with state approval and does not apply to children, Indonesia has not yet established arrangements regarding profiling restrictions, especially those

related to political purposes. The implications of profiling itself have the potential to create an unfair democratic party, as well as violate guarantees of people's right to privacy.

The Cambridge Analytica case is seen as a lucrative business by undermining the country's political system. As a result of this phenomenon, profiling data in elections has become a topic of widespread discussion. The utilization of Big Data has taken political campaigning techniques to another level. Technology makes political campaigns more effective and significant. Politicians manage to predict the latest personality, financial condition, political beliefs, and trends among voters to then strategize a targeted campaign. Unfortunately, profiling is done by certain parties without being noticed by the data subject, from how the data is retrieved, managed, processed, and analyzed to what decisions can later be made.

The problem became even more complicated after learning that data analysis for political purposes was carried out by data brokers. These parties usually collect consumer data that is public and non-public, offline or online. , political campaigns have been able to combine public voter files with commercial information, to develop detailed and comprehensive voter profiles and subsequently create customized campaign messages (Chester and Montgomery, 2017). It is this business model that undermines the realization of protection of the right to privacy because it is so non-transparent. Data brokers tend to collect, manipulate, and disseminate consumer data without the data subject's consent. Information disclosure is the right of data subjects is even defeated by trade secret rules by business actors.

In Indonesia itself, the practice of data profiling was clearly carried out by two parties, namely Golkar and Gerindra. Golkar has publicly stated that his campaign strategy for the upcoming 2019 elections is the use of Big Data Analysis combined with Political Micro – Targeting. Then, Gerindra blatantly wanted to access the personal data of the voter list containing uncensored KTP and KK numbers (Farisa, 2018), and even sent a warning letter to the Election Commission for rejecting the access application. In fact, Gerindra's request clearly violates the rules for the protection of personal data.

In general, data profiling is carried out for several purposes, namely to predict information, assess a person, make or inform decisions about individuals, as well as decisions that personalize the individual's environment. When inaccurate or biased profiles are systematically used to inform or encourage decisions that affect individuals, such inaccuracies can result in losses later on. The Human Rights Council states that the automated processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights.

The increasingly central role of commercial digital marketing in political campaigns contemporary reshaping modern politics in a fundamental way, namely changing the relationship between candidates, parties, voters, and the media. In order to effectively convey the campaign message to individual constituents, political candidates and parties have long identified their voter markets. Political Micro Targeting (PMT) demonstrates partial retreats of undifferentiated mass audiences in order to tailor the "needs, wants, hopes, beliefs, preferences, and interests" of the target audience as determined by the data profile. This mechanism allows political parties to allocate their resources efficiently while still adopting technological novelty.

Furthermore, namely Political Behavioural Targeting (PBT) which refers to profiling voters based on the online behavior of voters and other data provided by data intermediaries, as well as the use of these profiles to target individual voters with customized political ads. This mechanism originated from the commercial marketing system. The rise of big data has prompted campaign operators to leverage digital technologies and tools to mobilize voter turnout, engage young people, raise money and support operations down to the smallest community groups. Electoral politics has now been fully integrated into the evolving global commercial digital media and marketing ecosystem that has changed the way companies market their products and influence consumers.

However, there are several risks associated with PMT and PBT practices, including profiling causing a loss of user privacy, targeting opening the door to selective information exposure, potential manipulation, and allowing campaigns to send customized messages directly to citizens, making them unaffordable for media surveillance. As a result, the campaign has the potential to deviate and is only limited to sweet promises without any real realization. The implementation of the principles of fairness and transparency in the GDPR as well as the right to information and access by data subjects can be one of the efforts to minimize unilateral and manipulative data profiling practices. The European Union in the context of protecting privacy rights has agreed to issue a comprehensive General Data Potection Regulation (GDPR) that covers almost all processing of personal data. Referring to these provisions, several rights of data subjects arise, including the right to information; the right to access; the right to rectification, blocking and

deletion of data; the right to object; the right to data portability; the right of profiling and automated decision making; the right to recovery; and the right to compensation and responsibility.

If the state has regulations related to data profiling, even businesses providing information related to profiling will prevent data brokers from using and processing the data subject's personal data in an unauthorized manner, help data subjects to better understand how their data is used for identification purposes, and what are the risks and consequences of such activities because data profiling has the potential to lead to exclusion or discrimination of individuals (International Privacy, 2018). In addition, the absence of an independent oversight mechanism would open the door for data profiling actors to use and process Indonesians' personal data in unauthorized means for political purposes, as happened in the case of Cambridge Analytica, about 50 million data on the Facebook accounts of United States voters was illegally collected in 2014 to win over Donald Trump as President of the United States (Faisal, 2018).

In the PDP Law, several exceptions are regulated, namely exceptions in terms of national security, the interests of the law enforcement process, and the interests of the press as long as personal data is obtained from information that has been published and agreed upon by the owner, and the interests of scientific and statistical research as long as personal data is obtained from information that has been published, which needs to be reconfirmed for research purposes (Araf, 2021). Many parties note the points of national security and the importance of the law enforcement process that seem too general in nature and can cause many multi-interpretations so there needs to be specific things and clear interpretations so as not to be misused by the state or the ruling government regime (Araf, 2021). Even with restrictions, data protection regulations that have not been comprehensive in providing data subjects with the right to information related to data profiling will make Indonesia vulnerable to unfair and non-transparent data profiling for political purposes. In contrast to the GDPR which specifically gives data subjects the right to information relating to profiling and establishes mechanisms of the independent supervisory authority.

4. CONCLUSION

Contemporary sociopolitical and security defense developments require the development of a national security paradigm that is not centered solely on military and territorial security. The national security paradigm undergoes an expansion from comprehensive security a la national security that rests on military security to comprehensive security that rests on human security. The meeting of the interests of the global elite and the local elite with the aim of accommodating the interests of corporatism or oligarchy through normative rules and technological adaptation by changing the system and weakening the ideology of the state through infrastructure and political superstructure to eliminate national independence and control the country's wealth has the potential to disrupt the stability of economic, social, and other aspects.

Daily life is inseparable from the use of technology that indirectly collects personal data to then become big data that is traded or used for business and political purposes. Therefore, the state passed the PDP Act. There are four aspects of concern in the PDP Law, namely data sovereignty, data security, and data for the benefit of the state; data owner; user data as a processor; and data traffic regulation, especially those of a cross-country nature. The PDP Act has accommodated the right to be forgotten with some pressing exceptions. However, the PDP Law still does not contain details on the mechanisms and limitations in the exemption of personal data protection, especially the use of business and political sectors. This makes people unaware of the implications of data dissemination and personal data buying and selling activities that can actually be a boomerang for them, or even national security in the future. There need to be detailed arrangements regarding the limitations of the use of personal data and the form of accountability of data processors are needed to find a balance between the need for the protection of individual personal data with the needs of the government and business people to support their respective activities. The establishment of an independent supervisory agency is no exception to ensure the implementation of the PDP Law as a form of guarantee of the right to privacy.

REFERENCES

[1] Aditya, G. (2021). Big Data dan Komunikasi Politik di Indonesia : Studi Kasus PILPRES 2019 dan RUU Perlindungan Data Pribadi. *ResearchGate*, *May*. https://www.researchgate.net/publication/351307911_Big_Data_dan_Komunikasi_Politik_di_Indonesia_Studi_Kasus_PILPRES_2019_dan_RUU_Perlindungan_Data_Pribadi

[2] Annur, C. M. (2022). *Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20*.

[3] Arditya, A., & Nugraha, I. R. (2021). *RUU PDP masih memiliki banyak kekurangan dibandingkan standar internasional dalam melindungi data pribadi*. The Conversation.

https://theconversation.com/ruu-pdp-masih-memiliki-banyak-kekurangan-dibandingkan-standar-internasional-dalam-melindungi-data-pribadi-151212

[4] Ayu, A., Anindyajati, T., & Ghoffar, A. (2019). Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital. *Pusat Penelitian Dan Pengkajian Perkara, Dan Pengelolaan Perpustakaan Kepaniteraan Dan Sekretariat Jenderal Mahkamah Konstitusi*.

[5] Daniswara, F., & Rahman, F. (2018). Perlindungan Data Pribadi: Studi Komparasi terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia. *Center For Digital Society*, *31*, 24.

[6] Djafar, W. (2019). Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan. *Jurnal Becoss*, *1*(1), 147–154.

[7] Juaningsih, I. N., Hidayat, R. N., Aisyah, K. N., & Rusli, D. N. (2021). Rekonsepsi Lembaga Pengawas terkait Perlindungan Data Pribadi oleh Korporasi sebagai Penegakan Hak Privasi berdasarkan Konstitusi. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, *8*(2), 467–484. https://doi.org/10.15408/sjsbs.v8i2.19904

[8] Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2013). *THE PERSONAL DATA PROTECTION OF INTERNET USERS IN INDONESIA*.

[9] Nugroho, A. A., Winanti, A., & Surahmad, S. (2020). Personal Data Protection in Indonesia: Legal Perspective. *International Journal of Multicultural and Multireligious Understanding*, *7*(7), 183. https://doi.org/10.18415/ijmmu.v7i7.1773

[10] Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi. (2019). Keamanan Big Data di Era Digital di Indonesia. *Jurnal Informa*, *5*(1), 28–34.

[11] Nugroho, I. I., Pratiwi, R., & Az Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2), 115–129. https://doi.org/10.15294/ipmhi.v1i2.53698

[12] Puspa, D., Soegiharto, A., Nizar Hidayanto, A., & Munajat, Q. (2020). Data Privacy, What Still Need Consideration in Online Application System? *Jurnal Sistem Informasi*, *16*(1), 49–63. https://doi.org/10.21609/jsi.v16i1.941

[13] Rosadi, S. (2018). Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia. *Brawijaya Law Journal*, *5*(2), 143–157. https://doi.org/10.21776/ub.blj.2018.005.01.09

[14] Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384. https://doi.org/10.24815/kanun.v20i2.11159

[15] Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, *2*(2), 2–9. https://doi.org/10.18196/iclr.2219

[16] Susetyo, H. (2008). Menuju Paradigma Keamanan Komprehensif Berperspektif. *Lex Jurnalica*, *6*(1), 1–10. https://ejurnal.esaunggul.ac.id/index.php/Lex/article/view/287/260

[17] Suwana, F. (2018). *Indonesia sangat memerlukan undang-undang perlindungan data pribadi*. The Conversation. https://theconversation.com/indonesia-sangat-memerlukan-undang-undang-perlindungan-data-pribadi-92607

[18] Yofira Karunian, A., Halme, H., & Söderholm, A.-M. (2019). Data Profiling and Elections: Has Data-Driven Political Campaign Gone Too Far? *Udayana Journal of Law and Culture*, *3*(1), 95. https://doi.org/10.24843/ujlc.2019.v03.i01.p05

[19] Yudhi Priyo Amboro, F., & Puspita, V. (2021). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia) | CoMBInES - Conference on Management, Business, Innovation, Education and Social Sciences. *CoMBInES*, *1*(1), 415–427. https://journal.uib.ac.id/index.php/combines/article/view/4466