The Jurisprudence Regarding the Protection of Personal Data for the Communities and Business Actors in Indonesia

Bagus Satrio Utomo Prawiraharjo[1], F.X. Joko Priyono[2], Nanik Trihastuti[3]
{bagussup@students.undip.ac.id[1]}

Universitas Diponegoro, Indonesia[1, 2, 3]

Abstract. The Covid-19 pandemic has had a global influence on humanity; with restrictions on home-based social activities, a transition to digital media is unavoidable. After the Covid-19 outbreak, a surge in internet activity has led to a spike in cybercrime. One of them is personal data breaches, such as the unauthorised disclosure of personal information to the public or the bulk trade of personal data. The purpose of this paper is to comprehend that the misuse and trafficking of sensitive personal data and its misuse can pose a threat to personal security, which is a violation of human rights, from the perspective of legal sociology theory and a philosophical examination of the formation of the PDP Bill. Although, in principle, the state is obligated to ensure the confidentiality of personal data, several Indonesian laws and regulations governing the management of personal data are deemed insufficient. In addition, the Personal Data Protection Bill (RUU PDP), the legislative framework for addressing the breach and misuse of personal data, was not passed due to worries that the PDP Bill would be a double-edged sword for MPs and their constituents. This issue is analysed using the empirical legal technique, a socio-legal perspective, and a socio-philosophical foundation. Because even though personal data protection is a part of Human Rights, the private sector and the Indonesian government have little motivation and competence to handle personal data. In addition, worldwide underground commercial groups functioning via the dark web, one of the driving causes behind private data unlawful trade regulations, will continue to exist despite removal efforts.

Keywords: Law and Society, Personal Data Protection, Jurisprudence

1 Introduction

The emergence of information technology has drastically and profoundly altered human life. The existence of technology has rendered human society unduly dependent on it. Post-industrial society arose due to technological advancements central to human existence.

Globally, people's behaviour and way of life have been modified by information technology. In addition to making the world borderless, its expansion has brought about significant changes in social, cultural, economic, and law enforcement practices. From the original to the most recent wave, technological advancements are constantly supported by legal papers and statutes.

The world is entering the fourth phase of the industrial revolution, which has altered every element of human existence. This era is characterised by the expanding use of information technology in all fields, which has altered our way of life. This revolution was characterised by the automation of computer and electrical equipment, which had been made possible by

IWLEG 2022, July 27, Semarang, Indonesia

DOI 10.4108/eai.27-7-2022.2326264

Industrial Revolution 3.0. It turns out that revolution and renewal will continue to accompany the advancement of science and technology until the birth of cyber-physical systems. This system permits the integration of human contact with the computer. The digitalisation of technologies involving cyber-physical systems marks the beginning of the 4.0 phase of the Industrial Revolution.

There has been a movement in how people live, from physical to smartphones and laptops with internet access. Additionally, the COVID-19 pandemic impacts people globally. It restricts their social activities at home and forces them to turn to digital media. As digital activity grows, so do cyber-crimes and infractions [1] [2]. According to the 2018 APJII poll, Indonesia has 171,17 million Internet users, with a 64.8% penetration rate. Based on the 2017 APJII poll, which examined 143.26 million internet users at a penetration rate of 54.68 per cent, this number is anticipated to increase. Nearly all Internet users in Indonesia use smartphones; nonetheless, cell phone or cell phone users have reached 59.59 per cent [3]. This suggests that more than half of the population of Indonesia is susceptible to cybercrimes.

In its evolution, particularly after the constitutional amendment (the 1945 Constitution of the Republic of Indonesia), the right to privacy, including the protection of personal data, has been acknowledged as one of the citizens' constitutional rights. This is consistent with including a special human rights provision (Bill of Rights) in the revised Constitution (Chapter XA-Article 28 A-J). In particular, Article 28G, paragraph "The right to feel secure against and receive protection from the threat or fear to do or not do something constitutes a human right", has requirements to guarantee the security of personal data.

In addition to the Constitution, Indonesia's ratification of the International Covenant on Civil and Political Rights (IPCPR) through Law No. 12 of 2005 demonstrated the government's commitment to privacy and personal data. Protecting the honour, dignity, and property rights of citizens, individuals, and families is the purpose of this activity. Not only does this protection apply to direct relationships but also personal information and data. Article 14, paragraph 2 specifies that one of the rights to self-development is the freedom to seek, receive, store, process, and transfer information by all methods available. This relates to Article 31 of the Human Rights Law, which also provides that the confidentiality of communication by electronic means is guaranteed, excluding instructions from courts or other judicial officials under the law.

As an intrinsic individual right, maintaining one's right to privacy initially arose in court decisions in the United Kingdom and then the United States. Before that time, a legal understanding of the right to privacy originated in an article titled "The Right to Privacy," which was the first to conceptualise the right to privacy as a legal right [4]. The misuse and trafficking of sensitive personal data pose a threat to individual security and is a violation of human rights. This is also by the Human Rights Law no. 39/1999, which protects citizens' privacy rights in several clauses, such as Article 14 (2), Article 29 (1), and Article 31. Article 29, paragraph 1 stipulates: Individuals' right to defend themselves is acknowledged.

Several Indonesian laws and regulations governing the management of personal data are deemed insufficient, even though the state is required to preserve the confidentiality of personal data in principle. In addition, the Personal Data Protection Bill, the legislative foundation for addressing the breach and misuse of personal data, was not passed out of worry that it would be a double-edged sword for MPs and their constituents.

In addition, even though preserving personal data is a component of Human Rights, the private sector and the Indonesian government have limited preparation and capability in handling personal data. In addition, despite ongoing eradication, the cyber underground economy syndicate is anticipated to continue to expand. This syndicate has become one of the primary engines for the trafficking of personal data. Therefore, it is required to examine the

phenomena of the low level of personal data protection in Indonesia utilising legal sociology theory and to build a personal data protection law in Indonesia from a philosophical standpoint.

2 Method

The study of the problem is related to protecting personal data, particularly electronic transactions and other related regulations. The empirical legal method with a socio-legal approach and socio-philosophical basis are used to analyse this problem. This paper also uses secondary data such as legal documents, books, and articles.

3 Finding and Discussion

3.1 Personal Data Trafficking in Indonesia in Terms of Legal and Societal Aspects

Non-physical personal data is frequently neglected, particularly by society as a whole. Data security is susceptible; therefore, individuals must safeguard their personal information to prevent misuse. The hospitality of the Indonesian people and their culture of politeness provide numerous loopholes for crimes involving the possession of personal data. The forgiving habit of Indonesians is also why fraud is rarely reported, as indicated by the head of the Research Department of the Ministry of Communications and Information Technology. This lenient disposition influences the number of fraud cases worldwide, particularly online. However, the majority of victims of online fraud prefer not to disclose it to the authorities. The victims will likely disclose the crimes only if the loss surpasses IDR 500,000.

Indonesia is reputed to be the most hospitable nation in the Asian region, proving the veracity of its forgiving attitude. The Legatum Institute is a UK-based research institution. The 2016 Legatum Prosperity Index classified Indonesia as the friendliest and most sociable country in Asia, scoring 61.88. The indicated community outreach encompassed personal ties, community involvement, and social network support [5].

If there are only one or two victims, digital data trafficking instances are typically not reported. This, however, does not apply to prominent political or public figures who frequently appear in the media. The public is aware of pornographic recordings, "sexual" photographs, and the data trafficking or publication of various personal, intimate data belonging to several artists and government officials. For example, an artist with the initials GA whose video became viral and spread throughout Indonesia, attacks on various local agencies, such as the recent ransomware epidemic and the hacking of the National Cyber and Crypto Agency (BSSN) [6] and the Indonesian National Police [7]. They were victims of hacking and trafficking that were either intentionally or unwittingly triggered by a faulty system.

The greatest vulnerability for cybercrime is human carelessness. For example, do not establish passwords that are simple to guess, change your passwords frequently, allow others to access your smartphone, or disclose your phone number to strangers. Commonly known as social engineering attacks, [8] they are the greatest threat to information security today. Even personnel with a hand in data security in the IT industry are prone to making mistakes and being attacked in various methods, much less the general population with minimal knowledge of digital data protection. In light of such, as long as humans are involved, social crime can occur there, exploiting the flaws of neglect, security, and trust.

Who is behind the crime and why specific data types are stolen determine the intent of data trafficking? For example, suppose a data thief is driven to ruin an individual's or organisation's reputation, uncover undisclosed fraud, or improve cybersecurity. In that case, the culprit is likelier to release sensitive information to the public. In 2014, for instance, a hacker supported by North Korea obtained sensitive personnel information from Sony Pictures Entertainment, including social security numbers, financial records, payroll information, and emails of top executives. The hacker then uploaded an email to bring down the corporation in retribution for producing a comedy about a plan to assassinate North Korean ruler Kim Jong Un dubbed "The Interview" [9].

Additionally, if a government steals data, it is never revealed nor sold. They are instead utilised for spying. In 2018, Marriott's hotel company suffered a data breach in which 500 million guests' personal information was compromised. In this case, the primary suspect was a hacker supported by the Chinese government. One idea suggests that the Chinese government took these records to collect information on US government officials and corporate leaders.

Frequently, stolen data is sold on the dark web. In 2018, for instance, a hacker offered to sell over 200 million personal records from China. Even though data breaches threaten national security, 86% of cases involved money, and organised crime groups were responsible for 55%.

Buyers can choose and buy the data they want. The most common payment methods for transactions are Bitcoin or Western Union. The type of data and supply and demand determines prices. For instance, the cost of trafficking personally identifiable information is $4, the cost of an email dump containing 100,000 to millions of email addresses is $10, and the cost of a voter database from one country is $100 [10].

Multiple uses are found for stolen personal information by purchasers. They can utilise credit card numbers or mobile phone numbers to generate counterfeit cards and conduct fraudulent transactions. People can utilise an Identification Number, home address, name, date of birth, and other personally identifying information if personal information is taken. For instance, a buyer can apply for a credit card or online loan on behalf of the victim. Marketing companies or companies engaged in spam or telemarketing can purchase stolen personal information, especially cell phone numbers and email addresses. These purchasers can also utilise stolen email addresses and passwords for phishing, social engineering, and malware dissemination.

Moreover, there appears to be no law enforcement involvement, which causes public concern and confusion. All examples of personal data breaches only reach the level of press coverage. Corporations and government entities adequately provide the general public with information and clarity. This condition indicates that criminals are free to perpetrate crimes on the dark web as a method of subsistence [11].

In general, the absence of legislation regulating personal data protection in Indonesia is a drawback, as there are no regulatory laws and legal rules that may prosecute violators [12]. Protecting personal data for information and commerce between nations is important in international relations. Several international corporations still need to select Indonesia as their major data storage location. Consequently, establishing personal data protection rules will assist Indonesia's future as a global data centre. It is vital to regulate personal data since it regulates the collection, use, disclosure, provision, and security of personal data. This law seeks to strike a balance between the protection of personal data and the ability of governments and enterprises to receive and process personal data for their reasonable and legitimate needs.

In terms of costs, rewards, and consequences, the perpetrators do not always act rationally [13]. Nonetheless, their behaviour is more rational regarding self-interest and utility maximisation (neoclassical rationality) [14] since it does not contravene Indonesian law. Although not ethically justifiable, this sensible economic behaviour frequently pushes

traffickers to do what they want or require. This concept embodies the rationality principles of Max Weber, namely reasonable behaviour based on individually held values without regard to the success or failure of the action [15].

Socially, the PDP Bill is intended to safeguard the rights of individuals and businesses regarding the acquisition, processing, management, and distribution of personal data. Proper data security and personal privacy can encourage the public to share their information for various public objectives without fear of their information being exploited or their rights being violated. Therefore, this system will strike a balance between the rights of individuals and the interests of the community as represented by the state [16]

The PDP bill should be able to raise the awareness of the government, business actors, customers, and all citizens regarding the security and protection of personal data, which provides a sense of security and comfort in buying and selling processes and online transactions, particularly on e-commerce media platforms [17].

Following the thesis established by Roscoe Pound Legislation as a weapon of social engineering, namely law as a means of social reform [18], this PDP bill will significantly contribute to establishing order and progress in the information society.

3.2 Establishment of Personal Data Protection Law in Indonesia in terms of legal philosophy

At the 2017 G20 conference in Hamburg, G20 ministers agreed on the significance of protecting personal data to the growth of the digital economy [19]. This agreement is outlined in the e-commerce roadmap required by Presidential Regulation 74/2017 in the e-commerce strategy for 2017-2019 Indonesia [20]. By this Presidential Regulation, the development of e-commerce in Indonesia encompasses finance, taxation, consumer protection, education and human resources, communication infrastructure, logistics, cyber security, and the establishment of management for the 2017-2019 implementation of the Electronic-Based National Trading System (SPNBE). Personal data protection discussion is one of consumer protection's top priorities.

The issue of international data transfer necessitates an immediate strengthening of national data protection laws. In response to the needs above, numerous ASEAN nations have initiated the development of unique personal data protection rules. Some examples are Singapore in 2012, Malaysia in 2010, the Philippines in 2012, Laos in 2017, and Thailand in 2019. Indonesia's participation in recently begun trade agreement negotiations at PTA, RCEP, and CEPA [21] Moreover, the mandatory EU GDPR, which went into effect on May 25, 2018, has had a substantial influence on Indonesian businesses in different sectors, such as transportation, e-commerce, hospitality, and others that gather personal data.

Unfortunately, the growing public awareness of the need for comprehensive legislation to protect personal data differs from the need for such regulations. In 2017, according to a poll by Mastel and APJII, 79% of respondents refused to reveal personal information without permission, and 98% wanted the Personal Data Protection Act to be passed promptly [22]. Nonetheless, this fear does not arise in actuality. The general public does not view personal information as an asset that must be protected. The quantity of posts containing personal data on various social media platforms and social networking groups is one of them. In addition, when utilising numerous electronic system platforms (e-commerce, online transportation, fintech), users typically require a comprehensive understanding of the privacy policies and terms of use of each of these applications, particularly as they pertain to the use of personal information. In this regard, the government and service providers should implement a

transparent verification process independent of the necessity for precautionary steps or vigilance on the part of all parties to secure their particular data [23].

The government participated by implementing the National Population Registration Number Program mandated by the Population Management Law (updated in 2006 and 2013); since 2011, the government has been collecting citizens' personal information electronically. Technically, this programme is supported by Presidential Decree Number 67 of 2011 on Identity Cards Based on Population Identification Numbers, which includes types of personal population data recorded in e-KTP as a National development programme, making it necessary to update population data, issue Population Identification Numbers (NIK), and apply for e-KTP [24]. Unfortunately, these standards do not control the processing, management, and protection of these personal data, including the processing performed by third parties. The NIK presently mentioned in e-KTP is an absolute and crucial prerequisite for government and commercial sector access to numerous governmental services. For instance, e-KTP is the essential criterion for gaining access to social services like health, job, pension, and other forms of social security. An e-KTP is the primary condition for opening a bank account or obtaining a bank loan. The Election Law (UU No. 7/2017) requires citizens to possess an e-KTP before exercising their right to vote in elections. In other words, all components of personal data (almost all related to e-KTP) are susceptible to hacker assaults and data breaches simultaneously.

In addition to the government, there have recently been concerns regarding the gathering of personal data by the private sector, particularly information and communication technology corporations. In recent years, there have been numerous incidents in Indonesia involving the disclosure of the personal information of users of financial technology (fintech) platforms based on peer-to-peer lending, online lending, or borrowing. Under the guise of controlling credit bureau administration, the platform provider initially accesses personal information on the user's cell phone, such as photos and phone numbers. In actuality, however, the data collected is utilised for invoicing purposes by third parties, not a party to the data collection agreement.

Several billings are conducted forcibly by threatening to distribute private photographs. The Ministry of Communication and Information Technology blocklisted at least 738 unlawful fintech in 2018. The blocked ones typically must meet the Financial Services Authority (OJK) rules and frequently misuse personal information. Moreover, debt collectors (third parties) frequently distribute users' information, such as financial transactions and photographs, to contacts or family members on the creditor's cell phone without their consent [25].

As the e-commerce industry in Indonesia grows, so does the potential for personal data loss. The 1000 startup movement, announced by President Joko Widodo as one of the foundations of the digital economy's development, has successfully fostered the creation of at least four Indonesian unicorn startups: Go-Jek, Tokopedia, Traveloka, and Bukalapak. Nonetheless, the expansion of this digital startup has resulted in a massive gathering of personal data from users, including behavioural data (shopping/activity) from consumers. This refers to the terms and conditions of e-commerce in Indonesia, which stipulate the collection of personal information from consumers, including their name, ID number, address, email address, telephone number, and some biometric information [26].

Due to the lack of personal data protection regulation, it is impossible to standardise the rules governing this problem, and the rights of data subjects must be recognised. The Institute for Community Studies and Advocacy-ELSAM (2018) discovered numerous discrepancies between privacy rules and terms of service for each platform and the principle of protecting personal data [27] in a survey of ten Indonesian information and communication technology-based enterprises.

While several organisations outside of Indonesia have attempted to comply with at least the EU GDPR data protection standards, many Indonesian enterprises must still incorporate personal data protection principles in their internal policies. The absence of regulations is the primary cause of the inconsistency of data protection norms and the problem of firms' inability to comprehend the ideas of privacy and consumer data protection [28]. According to Rudiantara, a former Minister of Communication and Information Technology, the process of discussing the PDP Bill must be expedited so that Indonesian e-commerce can expand markets in nations that require personal data protection [29].

However, discussions with data protection authorities have stopped since it was included in the national legislative programme for 2020-2021. The government desires that the Ministry of Communication and Information Technology (Kominfo) assume control. In addition, the People's Representative Council (DPR) did not entirely support forming an independent body. Some members view the approval of the PDP Bill as an urgent matter, necessitating a DPR compromise on the government's proposal. Since the government holds the data, the DPR desires autonomy from the PDP regulator. As a result, the authorities could become aware of PDP infractions. In addition, the establishment of a separate PDP Authority. It is anticipated to improve this institution's performance [30].

The existence of an independent supervisory authority is one of the most significant factors in ensuring the security of personal data. Therefore, this authority can lead to the protection of personal data and compliance with data protection requirements by individuals and legal entities under private law and governmental institutions responsible for processing personal data.

In addition, authorities are authorised to create public awareness and construct networks to safeguard private information. In addition, the PDP Bill is currently listed in the 2021 national priority legislation programme. While the PDP Bill is stalled in Senayan, the Social Security Agency of Health (BPJS Kesehatan) was accused of having their data hacked and sold on web forums in May 2021, exposing 279 million Indonesians. In 2020, 91 million Tokopedia users' data will be sold on a dark website. Tokopedia acknowledges this, despite asserting that sensitive user data, including passwords, is encrypted [31].

Philosophically, the regulation of privacy rights for personal data is an example of the acknowledgement and defence of human rights. Therefore, the development of the PDP Bill is founded on a solid and accountable philosophical basis. The philosophical basis of personal data protection is Pancasila (Indonesia's fundamental philosophical theory), the development of legal thought and reasoning by the intended law.

According to Sunaryati Hartono, Indonesia's founders' legal philosophy is that the Indonesian people as a whole and as individuals adhere to an awareness of human rights. Regarding the protection of personal data, it is essential to recognise that the protection reflects the Indonesian people's understanding of human rights protection. As the purpose of a welfare state, a democratic rule of law is a nation, together with attempts to improve the public interest and justice as the goal of the state of law.

In other words, the framers of the 1945 Constitution of the Republic of Indonesia expected more than a mere legal system. In the truest meaning of the word, it is more. In addition, the life of the nation and state is not founded merely on the rule of law but on a life that delivers social justice to all Indonesians [32]. Not only for the entire population of Indonesia as a political entity but also for individual citizens. High and low, wealthy and impoverished, young and old, regardless of ethnic or racial background, social class, or religion.

In addition to utilitarianism, Bentham asserts, "The purpose of legislation is the greatest happiness for the greatest number." The enactment of the PDP Bill, deemed an emergency or even ideal, is seen as a good law because it brings happiness to most people. Bentham argues

further that the existence of the state and law is only a means to achieve the essential good, which is the happiness of most of the population. Bentham's individualistic teachings nonetheless include the interests of the society so that the interests of one individual do not conflict with those of another; it must be limited to prevent *homo homini lupus*. According to Bentham, each individual must have compassion for others to create individual and community happiness [33].

4 Conclusion

Hackers motivated primarily by financial gain take advantage of the Indonesian people's hospitality, forgiving nature, and carelessness to commit crimes against the country. Because the personal data hackers who trade the data do not break the laws that are in effect in Indonesia, the activities that they conduct are, in principle, economically rational. This is because the regulations that are in effect in Indonesia prohibit them from doing so. To the concept of the law as a tool of social engineering put forward by Roscoe Pound, the formulation of the PDP Bill is necessary because of the need to protect individual rights in society. This idea that the law is a tool of social engineering in society means that the law is a tool of reform in society.

From a philosophical standpoint, the efforts being made to regulate the right to privacy on personal data manifest the safeguarding of fundamental human rights. In light of this, developing the PDP Bill is grounded in a robust and accountable philosophy, namely, the achievement of a national and state life that provides social justice to all Indonesian people. In addition, according to utilitarianism, legislation deemed beneficial to the greatest number of people in a community will be regarded as good law, even though it may not be without flaws. This standard applies to the PDP Bill as well. Their requirements are recognised as an urgent situation that stands apart from the legislators' political interests.

References

[1] Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

[2] Asosiasi Penyelenggara Jasa Internet Indonesia. "Hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia 2017." Retrieved from APJII: https://www. apjii.or.id/

[3] Statistik Telekomunikasi Indonesia (2017) dalam Badan Pusat Statistik (BPS). Retrieved from https://www.bps.go.id/publication/

[4] Rubenfeld, Jed. "The right of privacy." Harvard Law Review (1989): 737–807.

[5] Legatum institute. "Legatum Prosperity Index 2016" Retrieved from: www.li.com/activities/publications/2016-Legatum-prosperity-index-(10th-edition) (2016).

[6] "Peretasan Situs Badan Siber dan Sandi Negara Bikin Terheran-heran" Retrieved from https://news.detik.com/berita/d-5783999/peretasan-situs-badan-siber-dan-sandi-negara-bikin-terheran-heran

[7] https://nasional.kompas.com/read/2021/11/19/11560141/peretasan-data-internal-polri-diduga-merupakan-bentuk-pesan-politik?page=all

[8] Menyerang menggunakan kelemahan manusia. See: Kearney, P. (2010). Security: The Human Factor. Cambridgeshire: IT Governance Publishing.

[9] https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

[10] https://www.privacyaffairs.com/dark-web-price-index-2021/

[11] Makarim, E. (2020). Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi. Retrieved from https://law.ui.ac.id/v3/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh-edmon-makarim/. Fakultas Hukum Universitas Indonesia.
[12] Hisbulloh, Moh Hamzah. "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi." Jurnal Hukum 37.2 (2021): 119-133.
[13] Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? The Howard Journal of Crime and Justice, 44(4), 387–399.
[14] Firmansyah, M., et al. "Perdebatan Teori Rasionalitas dalam Menjelaskan Terbentuknya Biaya Transaksi pada Seleksi Pegawai Negeri." Jurnal Ekonomi dan Pembangunan Indonesia 13.1 (2012): 69-89.
[15] Turner, B.S. (2012). Teori Sosial Dari Klasik Sampai Postmodern. Yogyakarta: Pustaka Pelajar.
[16] Wulansari, Eka Martiana. "Konsep Perlindungan Data Pribadi Sebagai Aspek Fundamental Norm Dalam Perlindungan Terhadap Hak Atas Privasi Seseorang di Indonesia." *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan* 7.2 (2021): 265-289.
[17] Palinggi, S., & Limbongan, E. C.. Pengaruh Internet Terhadap Industri Ecommerce Dan Regulasi Perlindungan Data Pribadi Pelanggan di Indonesia. In Semnas Ristek (Seminar Nasional Riset dan Inovasi Teknologi) (Vol. 4, No. 1 th. 2020).
[18] Fuadi, M. (2013). Teori-Teori Besar (Grand Theory) Dalam Hukum. Jakarta: Kencana Prennamdeia Group.
[19] See: G20 Digital Economy Ministerial Declaration: Shaping Digitalisation for an Interconnected World, in http://www.g20.utoronto.ca/2017/170407-digitalization.html.
[20] The e-commerce roadmap is one of the Economic Policy Packages (14th package) out of the 16 Economic Policy Packages launched by President Joko Widodo.
[21] https://dailysocial.id/post/survei-mastel-apjii-pengguna-internet-butuh-campur-tangan-pemerintah-lindungi-privasi-dan-data-pribadi
[22] Asosiasi Penyelenggara Jasa Internet Indonesia. "Hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia 2017." Retrieved from APJII: https://www. apjii. or. id/content/read/39/342/Hasil-Survei-Penetrasi-dan-Perilaku-Pengguna-Internet-Indonesia-2017 (2017).
[23] Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." SASI, vol. 27, no. 1, 24 Mar. 2021, pp. 38-52
[24] Febriharini, Mahmuda Pancawisma. "Pelaksanaan Program e KTP Dalam Rangka Tertib Administrasi Kependudukan." Serat Acitya 5.2 (2017): 17.
[25] https://www.moneysmart.id/738-fintech-ilegal-diblokir-pemerintah-sepanjang-2018/.
[26] https://aptika.kominfo.go.id/2020/01/gerakan-1-000-startup-digital/
[27] https://elsam.or.id/5806-2/
[28] "Industri e-commerce terganggu bila RUU perlindungan data pribadi belum rampung", at https://nasional.kontan.co.id/news/industri-e-commerce-terganggu-bila-ruu-perlindungan-data-pribadi-belum-rampung.
[29] "Pasar Indonesia akan sulit diakses bila UU perlindungan data pribadi belum rampung", in https://nasional.kontan.co.id/news/pasar-indonesia-akan-sulit-diakses-bila-uu-perlindungan-data-pribadi-belumrampung
[30] https://nasional.kontan.co.id/news/jadi-kendala-dpr-ngotot-lembaga-otoritas-pengawas-data-pribadi-bersifat-independen
[31] https://www.voaindonesia.com/a/ruu-perlindungan-data-pribadi-tak-kunjung-disahkan-tersumbat-di-mana-/5921932.html
[32] Nasution, Adnan Buyung, Seminar Pembangunan Hukum Nasional VIII, And Badan Pembinaan Hukum Nasional. "Implementasi Perlindungan Hak Asasi Manusia dan Supremasi Hukum." *Presented at "Seminar Pembangunan Hukum Nasional VIII", Badan Pembinaan Hukum Nasional, Departemen Kehakiman dan Hak Asasi Manusia RI, Denpasar*. 2003.
[33] Besar. (2016). Utilitarianisme Dan Tujuan Perkembangan Hukum Multimedia di Indonesia. Bina Nusantara.