

Personal Data Protection Policy during Covid-19 Pandemic Era

Moh. Indra Bangsawan

Universitas Muhammadiyah Surakarta
mib136@ums.ac.id

Budi Santoso

Universitas Muhammadiyah Surakarta
bs143@ums.ac.id

M. Junaidi

Universitas Muhammadiyah Surakarta
m.junaidi@ums.ac.id

Dewi Kusuma Diarti

Universitas Muhammadiyah Surakarta
ddiarti31@gmail.com

Sandya Mahendra

Universitas Muhammadiyah Surakarta
c100190078@ums.ac.id

Engine Kubota

Universitas Muhammadiyah Surakarta
c100200386@ums.ac.id

DOI: 10.23917/laj.v8i1.1558

Submission Track:

ABSTRACT

Received:

25 January 2023

Final Revision:

14 April 2023

Available Online:

7 June 2023

Corresponding Author:

Moh. Indra Bangsawan
mib136@ums.ac.id

Advances in technology and information demand that the law can accommodate all forms of need for legal protection in the future.

Objective: This research aims to describe the picture of threats to data resources during the COVID-19 pandemic as well as describe personal data protection policies during the Covid-19 pandemic.

Methods: This research uses the literature review method. The literary materials obtained are in the form of scientific papers, online media, books, etc. that concerns the analyzed object.

Findings: Previously, the personal data protection policy was based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. But now Law No. 27 of 2022 concerning Personal Data Protection has been passed. Even though it has been passed, the law still has loopholes, especially those related to cyber security, so special regulations need to be stipulated. Data reports from the National Cyber and Crypto Agency show that until 2020 cyber attacks in Indonesia have increased to reach 190 million cyber attacks.

Function: This research provides an explanation of the urgency of the need for legislation that specifically regulates the protection of personal data.

Novelty : There has not been any researches that studies the same topic as that discussed in this article.

Keywords: Policies, Personal Data, Covid-19.

INTRODUCTION

New crimes appearing in society can be interpreted as an increase in criminal activities and attitudes, the pattern of which was easily changed before, but is not so easy today (Gumbira, 2019). One is technological crime because of globalization, the impact of which has penetrated almost every aspect of people's lives, including economy, politics, science culture, education, and others. Smart data, information, and general population data can be accessed through technology, so it should be paid attention to and carefully considered because it is a way to bring down the country (Azizah, 2020). In order to protect rights in the sphere of technology, particularly those of users of Internet services, one of the tasks of the law is to maintain the smooth operation of the national development process (Arifah, 2011). Along with the discovery of copyrights and new patents in information technology, the internet is widely utilized as a channel for electronic information and communication. These activities include surfing, searching for data and news, exchanging emails, and trading. Since the Internet is currently the most effective medium, almost all items can be traded over it (Moonti, 2012).

Indonesia has a growing number of online users every year. Indonesia has 132 million Internet users in 2016, making it the third-largest country in Asia behind China and India, according to Internet World Statistics data. Data on Internet users in Indonesia reached 88.1 million in January 2016, of whom 79 million are active social media users, 15% of them are regular Facebook users. This represents approximately 50%, according to a survey by We Are Social. The user is a teenager between the ages of 13 and 29. (Marwan, 2018). There are now 140 million internet users in Indonesia as of 2018, and at least 28 million of them are continually active users of the internet for online transactions (Sinaga, 2020). The issue of how important it is to protect personal data is growing along with the rise in internet users. Through internet media, many crimes, including threats, theft, defamation, pornography, gambling, and fraud, as well as illegal acts of terrorism, can now be committed by individuals or groups without

elevated risk of detection and repercussions. Bigger losses for the state and community (Mufid, 2018).

The globe is currently experiencing a coronavirus (Covid-19) pandemic, which is weakening all aspects of life and having an impact comparable to World War II (Ministry of Social Affairs, Republic of Indonesia, 2020). Additionally, the COVID-19 epidemic has altered the way of life of Indonesians, increasing their reliance on the internet and the frequency of cyberattack attempts. According to data from the National Cyber and Crypto Agency (BSSN), from January to August 2020, Indonesia had almost 190 million attempts at cyberattacks (Compass, 2020). In its ASEAN Cyber Threat Assessment 2020, Interpol revealed that cybercrime related to Covid-19 is also anticipated to increase, particularly if a vaccination or his Covid-19 remedy becomes available. To preserve trust in the use of electronic communications and services, Interpol stressed the necessity for nations to create robust cybersecurity ecosystems. In order to tackle cybercrime, national and commercial law enforcement and cybersecurity teams must be proactive, build plans, and recognize and evaluate attack trends (Tirto, 2020).

Although Indonesia is one of the nations that has experienced the economic, social, and political effects of this pandemic, including the legislation, the Indonesian government is highly conscious of this (Kriswibowo, 2020). As a result, the previous administration created laws and regulations that can satisfy the demands for restricting internet use. All facets of the information cycle and electronic transactions are governed by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 Concerning Information and Electronic Transactions, also known as UU ITE. But now Law No. 27 of 2022 concerning Personal Data Protection has been passed. Even though it has been passed, the law still has loopholes, especially those related to cyber security, so special regulations need to be stipulated.

RESEARCH METHOD

This research is normative legal research conducted by examining library materials or secondary data. This research is descriptive in nature. Descriptive research is research which is a problem-solving procedure that is investigated by describing the current state of the subject or object of research based on the facts seen. In legal research, the research approach can be used statutory approach. The statutory approach is an approach taken to various legal regulations relating to personal data protection and cybersecurity.

RESULTS & DISCUSSION

Artificial intelligence (AI), supercomputers, genetic engineering, nanotechnology, self-driving automobiles, and innovation are characteristics of the Fourth Industrial Revolution. Business, industry, government, and politics are all being affected by these developments, which are happening at an exponential rate. At this moment, it is becoming clearer that we live in a global village (Satya, 2018). The role of information technology in people's daily lives has increased significantly in the age of informatization and globalization. In addition to being the product of human work, information technology also aspires to integrate itself into daily life and enhance human welfare (Mahfudz, 2005). There are several ramifications that must be expected and considered because of the tendency toward continued technological advancement. The Information and Electronic Transactions Act No. 11 of 2008 is the result of these efforts, and it is now a legally binding document (UU ITE). The ITE Act's adoption, however, does not fully address all ITE-related difficulties. There are many causes for this issue, including the following:

First off, the public is now informed about Law No. 11 of 2008 on Information and Electronic Transactions using more than just attorneys and information technology. To foresee solutions to various technical issues that are thought to be novel, as well as to serve as a resource for the development of various implementation rules, it is possible to identify the many types of technological progress that result in new implementations and services. Third, the expansion of the legal system will strengthen the living dynamics of the laws incorporated into the national legal framework (Ramli, 2014).

Law and technology are two factors that interact with one another and have social implications. According to Heidegger, technology can be viewed as both a human activity and a tool for achieving a certain objective. Therefore, it is clear from the nature of the interaction between technology and law that each technology is created to address a specific need and then offers advantages and services to humans, including improving the efficiency and productivity of work. The highest authority in a country has the power to impose coercive consequences for violations of the law, which also serves as a behavioral restriction (Sitompul, 2012). Law is employed as a tool of politics, or as a means to accomplish aims (means of political engineering). In a society designed by law, law is described as a political category and a weapon to enforce equitable living conditions (Siregar, 2018).

It is not negotiable to attempt to create a legislative instrument that is consistent with the evolution of the information and telecommunications industries. Experience from many democracies shows that positive privacy law and jurisprudence predated the inclusion of privacy as a fundamental principle in international human rights law frameworks. The protection of the right to privacy in the digital era is the subject of Resolution 68/167, which was approved by the UN Human Rights Council. One of the provisions highlights the need to defend everyone's online rights, including their offline rights, such as their right to privacy (Indriani, 2017). The foundation of Indonesian legal protection is Pancasila, the country's official ideology and philosophy. *Rechstaat* and the Rule of Law are the foundations upon which the idea of legal protection for persons in the west is built. using the western conception as a mental framework and the Pancasila on Pancasila foundation. In Indonesia, the Pancasila-based notion of legal protection is the principle of acknowledging and defending human dignity. Because historically in the West, the genesis of conceptions surrounding the recognition and preservation of human rights was focused on the limitations and abuses of those rights, the principle of legal protection against government actions based on and comes from this notion (Puspitasari, 2018).

When this personal data transforms into Big Data once the firm succeeds in collecting significant amounts of data, this is one crucial issue that requires special attention. This personal information is gathered in large part from users like you and me. The internet ecosystem has information such as names, personal cell phone numbers, birthdays, nationalities, addresses, shopping preferences, and even the pharmaceuticals we purchase online, which can be used to benefit such organizations financially. This raises questions regarding the use of personal data. Therefore, a data protection system to control the gathering, using, and showing of personal data is crucial to addressing these issues and preserving public confidence in the institutions and governments that collect, keep, and use such data (Anggraeni, 2018).

The University aims to make this goal a reality by collaborating with all stakeholders—individuals or groups with an interest in decisions and organizations—through the Ministry of Information and Communication of Indonesia. After much debate, a law known as Law Number 11 of 2008 Concerning Information and Electronic Transactions was finally enacted on April 21, 2008, addressing the issues around information and electronic transactions (Maskun, 2013). Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Information and Electronic Transactions has been modified throughout its development and is

currently in effect in society. Personal data are not adequately protected under the rules and regulations that are now in place in Indonesia regulating its protection. The Law on Electronic Information and Electronic Transactions (UU ITE) just briefly mentions the topic of protecting personal data without going into further detail about how that protection will be put into practice. The facts show that regulations on data protection are regulated in sectoral regulations as described in the following chart:

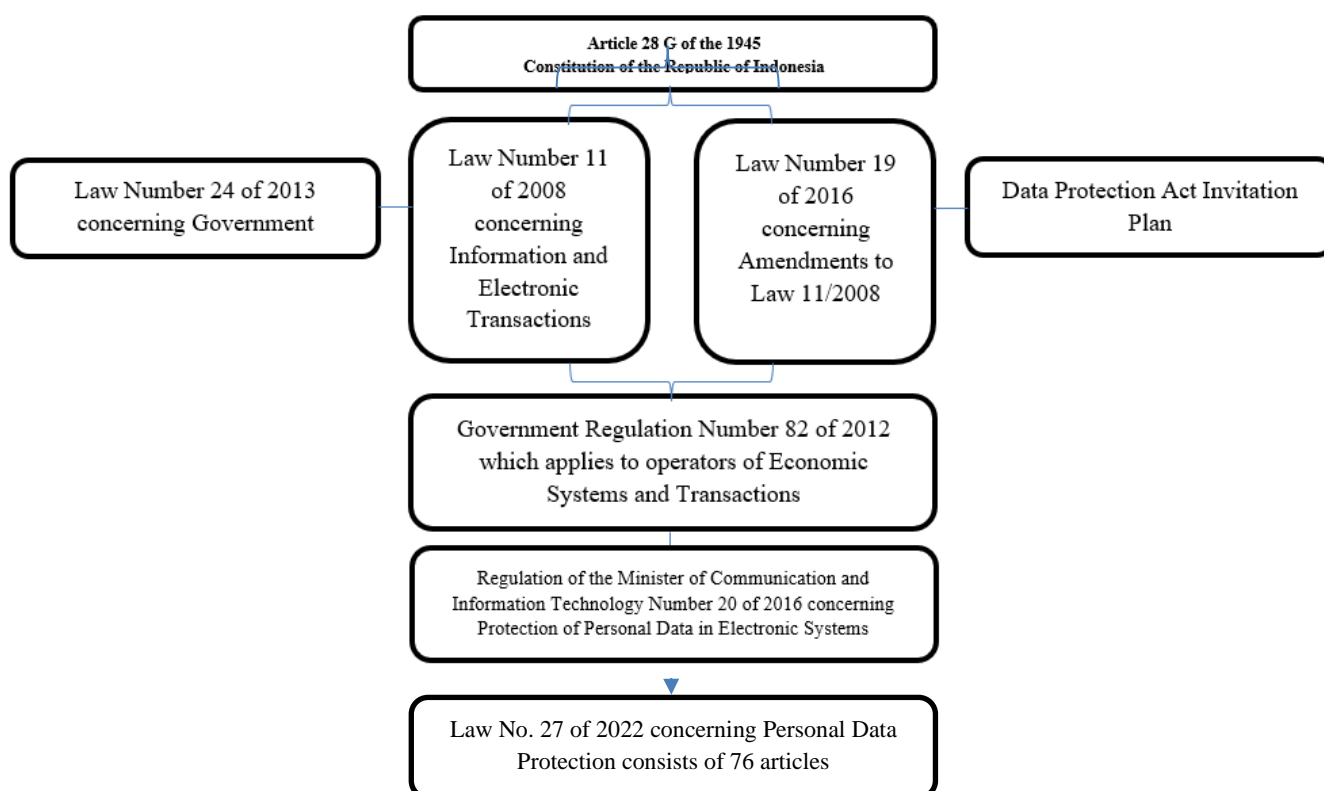


Figure 1. Data Resource Legal Arrangements

According to the illustration above, the legal basis of data resources has been independently governed in several regulations based on sectoral interests, including:

1. The 1945 Constitution of the Republic of Indonesia

Everyone has the right to personal safety, family, honor, dignity, and property under his control, according to Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. They also have the right to a sense of security and protection from threats of terror. Whether to exercise human rights.

2. Law Number 24 of 2013 concerning Population Administration

In the context of population administration Article 84 of this regulation governs the protection of data for citizen registration including: 1) Information on physical and/or

mental disability; 2) A fingerprint; 3) an eye's iris; 4) a signature; and e) any other element that brings shame to a person.

3. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.

The ITE Law underlines that protected personal rights include the right to personal information. According to the explanation provided in Article 26 Paragraph 1 of Law 19/2016, personal rights comprise the following: 1) Personal rights include the freedom to live a private life free from interference; 2) Personal rights include the right to speak freely with others; and 3) Personal rights include the right to access information pertaining to a person's personal life and data.

According to Indonesian legal regulations based on Law Number 18 of 2008 concerning ITE and PP Number 28 of 2012 concerning PSTE, victims of privacy rights violations are allowed to file a civil lawsuit for damages, which means that the legal system demands compensation from online users to e-commerce providers. There is a procedure in the new economy for requesting civil damages. It is vital to have more explicit legislative laws and broaden legal remedies for customers whose privacy rights are breached, even though this violation of personal data is general in nature and not restricted solely to civil elements (Indriani, 2017).

Only in the 2008 ITE Law, before it was judicially reviewed by the Constitutional Court of the Republic of Indonesia, was it unclear whether it is a complaint offense or an ordinary offense. Article 27 paragraph 3 of the ITE Law does not significantly differ between the 2008 concept and the 2016 concept. The 2016 concept is apparent in terms of the offense's form, specifically as a complaint offense, and this only considers the judicial review decision of the Indonesian Constitutional Court No. 50/PUU-VI/2008 (Gumbira, 2019).

4. Government Regulation no. 82 of 2012 which applies to System Operators and Electronic Transactions.

Regulation Governing Electronic System and Transaction Operators No. 82 of 2012.

5. Law Number 27 of 2022 concerning Personal Data Protection Consists

This law, which consists of 16 chapters and 76 articles, regulates basic matters for protecting individual personal data. Among other things, this Law regulates the rights of every individual to whom personal data is attached, provisions for processing personal data

and the obligations of controllers of personal data, plans to establish a personal data protection institution, and implementation of prohibitions and sanctions. However, despite the importance and necessity of this regulation, there are still some weaknesses which are suspected to threaten openness to information and have the potential to become rubber regulations, such as the Law on Information and Electronic Transactions (The Converaation, 2022).

Personal data is one of the objects that must be protected by a cybersecurity mechanism. The goal of a cybersecurity system is to protect networks, computers, programs and data from attacks and unauthorized access. These attacks can vary from hardware attacks, network attacks, and application attacks. As personal information is increasingly stored and processed online, privacy protection is becoming increasingly reliant on effective security systems. Cybersecurity measures also support critical infrastructure that protects data and safeguards confidential information (Detik, 2022). Currently, Indonesia does not yet have specific regulations for cybersecurity. Most of the laws that touch on cybersecurity are still fragmented and overlapping. The ratification of the PDP Law has been able to cover this legal loophole. However, this is still not sufficient and there is an urgency to immediately establish special regulations for cybersecurity in Indonesia.

Due to the COVID-19 pandemic's rising trend of cybercrime, the government must put it on its agenda in order to preserve its data resources. The government's agenda is viewed as a set of issues that require thoughtful consideration by public leaders at specific times (Nurhayati, 2019). The lack of ideal legal protection for data resources during the COVID-19 epidemic is the issue brought up in this paper, which encourages the creation of a legal protection model for data resources. The problems mentioned above can be included in the government's agenda, according to Cobb and Elderr (Basyarahil, 2011) if at least 3 (three) conditions are met:

1. Issuance of Personal Data Protection Derivatives

Even though the Personal Data Protection Bill has been passed (Law Number 27 of 2022 concerning Personal Data Protection Consists), there are still some weaknesses that need to be closed through derivative regulations from the law. These weaknesses, among others, are related to efforts to accommodate the private sector, which previously had public data so that it could protect its customer data. Then, this law must be ensured that it can be understood by the public so that they are not ensnared because of their ignorance.

Furthermore, stronger guarantees are needed for the protection of the personal data of children and vulnerable groups due to their position that is not yet competent at law, so they need further assistance (Kompasiana, 2022).

2. The public believes that certain steps must be taken to address the issue. Digitalization-related technological advancements need the use of big data and laws, particularly regarding the security of personal data (Palinggi, 2020);
3. The public shares the opinion that it is the government's duty and responsibility to address the issue. It is evident from a study done in Makassar that the ITE Law is unable to control such intricate cybercrime challenges. This is because information technology is advancing quickly and becoming more complex, yet conventional positive law's guiding concepts are still used in the legal system (Gani, 2019). Therefore, as a kind of future public policy, the government must develop a legal framework for protecting data resources that actively incorporates all facets of society.

CONCLUSION

In order to prevent the issue of personal data protection from emerging, threats to data resources have grown along with the annual increase in internet users. According to information from the National Cyber and Crypto Agency, Indonesia had approximately 190 million cyberattack attempts in 2020, an increase of more than four times compared to the 39 million or so cyberattacks that occurred in 2019. In response, the government must create laws and rules that can satisfy the demands for personal data protection and internet usage management.

Law Number 27 of 2022 concerning Personal Data Protection Consists serves as the foundation for the present personal data protection policy. However, This law is a good first step in terms of data security development policy in Indonesia. Whether law enforcement will be effective or not depends on its implementation. Even so, it needs to be an important note to cover the weaknesses of the law that has been passed, especially to deal with the era of the Covid-19 pandemic which could increase again at any time. This is a shared responsibility as the next step to optimize data protection.

REFERENCES

- Anggraeni, S. F. (2018). Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia. *Jurnal Hukum & Pembangunan*, 48 (4), 814-825.
- Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, 18 (2).
- Azizah, N., & Aquarisma, C. (2020). Diskursus Kebebasan Berpendapat dalam Ranah Publik Studi Kasus: Penerapan UU ITE Terhadap Kasus Ahmad Dhani. *Communitarian*, 2 (2).
- Bambang Poernomo dalam Gumbira, S. W. (2019). Problematika, Implementasi Undang-Undang Informasi dan Transaksi Elektronik dalam Menanggulangi Cyberbullying di Sosial Media Pasca Judicial Review Mahkamah Konstitusi RI, *Jurnal Pro Justice: Kajian Hukum dan Sosial*, 1(1).
- Basyarahil, A. (2011). Kebijakan Publik Dalam Perspektif Teori Siklus Kebijakan. *Publika: Jurnal Ilmiah Administrasi Negara*. Tahun II, Nomor, 2, 3-18.
- Detik, (2022). Langkah-Langkah Konkret Pasca UU Perlindungan Data, (online), (<https://news.detik.com/kolom/d-6419526/langkah-konkret-setelah-uu-perlindungan-data-pribadi-disahkan>, di akses pada 11 April 2023)
- Gani, H. A., & Gani, A. W. (2019). Penyelesaian Kasus Kejahatan Internet (Cybercrime) dalam Perspektif UU ITE No. 11 TAHUN 2008 dan UU No. 19 Tahun 2016. In *Seminar Nasional LP2M UNM*.
- Gumbira, S. W. (2020). Problematika Implementasi Undang-Undang Informasi dan Transaksi Elektronik Dalam Menanggulangi Cyberbullying di Sosial Media Pasca Judicial Review Mahkamah Konstitusi RI. *Jurnal Pro Justice: Kajian Hukum dan Sosial*, 1(1), 50-71.
- Indriani, M. (2017). Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System. *Justitia Jurnal Hukum*, 1 (2)
- Indriani, M. (2017). Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System. *Justitia Jurnal Hukum*, 1 (2).
- Kementerian Sosial Republik Indonesia, (2020). Persepsi Masyarakat dalam Menghadapi Pandemi Covid-19 . Online, (<https://puspensos.kemsos.go.id/serba-serbi-perilaku-dan-persepsi-masyarakat-indonesia-dalammenghadapi-pandemi-covid-19> di akses pada 1 September 2022)
- Kompas, (2020). Kejahatan Naik Empat Kali Lipat Selama Pandemi, (online), (<https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selamapandemi>, di akses pada 2 September 2022)
- Kompasiana, (2022). Kelemahan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi, (online),(<https://www.kompasiana.com/leohamonangan200700/635a214608a8b56a773aaaf2/kelemahan-undang-undang-nomor-27-tahun-2022-tentang-perlindungan-data-pribadi>, di akses pada 12 April 2023)
- Kriswibowo, A., & Utomo, S. A. P. (2020). *Ekonomi Politik Indonesia di Tengah Pandemi Covid-19*. Penerbit Cakradewa Ilmu.
- Mahfudz, S., & Nasution, M. K. (2005). Konsep hukum untuk teknologi informasi. *Al-Khawarizmi: Journal of Computer Science*, 1(1).
- Marwan, M. R., & Ahyad, A. (2016). Analisis penyebaran berita hoax di Indonesia. *Jurusan Ilmu Komunikasi, Fakultas Ilmu Komunikasi Universitas Gunadarma*.

- Maskun, S. H. (2014). *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Prenada Media.
- Moonti, R. M. (2012). Pengaruh Internet dan Implikasinya terhadap perjanjian jual beli. *Jurnal Legalitas*, 5 (01).
- Nurhayati, N., & Bangsawan, M. I. (2019). The Sustainable Development Licensing Policy Of Creative Industry In The Era Of Asean Economic Community (AEC) In Surakarta, Indonesia. *Humanities & Social Sciences Reviews*, 7(3), 25-31..
- Olisias dalam Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2).
- Palinggi, S., & Limbongan, E. C. (2020, January). 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)*.
- Petrus Reinhard Golose dalam Mufid, F. L. (2018). Kebijakan Integral Hukum Pidana dengan Technology Prevention dalam Upaya Pencegahan Kejahatan Cyberbullying. *Jurnal Rechtsens*, 7(2).
- Puspitasari, I. (2018). Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online dalam Hukum Positif di Indonesia. *Humani (Hukum dan Masyarakat Madani)*, 8 (1), 1-14.
- Ramli, A. M. (2018). Dinamika Konvergensi Hukum Telematika dalam Sistem Hukum Nasional. *Jurnal Legislasi Indonesia*, 5(4).
- Satya, V. E. (2018). Strategi Indonesia Menghadapi Industri 4.0. *INFO Singkat*.
- Siregar, K. M. (2018). Integrasi Politik Hukum Terhadap Tindak Pidana Pemberitaan Palsu (Hoax) Di Indonesia. *FITRAH: Jurnal Kajian Ilmu-ilmu Keislaman*, 4(2), 227-242.
- Sitompul, J. (2012). *Cyberspace, cybercrimes, cyberlaw: tinjauan aspek hukum pidana*. PT Tatanusa.
- Theconversation, (2022). UU Perlindungan Data Rentan Makan Koban, (Online), (<https://theconversation.com/panel-ahli-uu-perlindungan-data-pribadi-rentan-makan-korban-dan-belum-jamin-proteksi-data-yang-kuat-191018>, di akses pada 12 April 2023)
- Tirto, (2020). Meningkatnya Ancaman di Tengah Pandemi Covid 19, (online) (<https://tirto.id/meningkatnyaancaman-cybercrime-di-tengah-pandemi-covid-19-f51P>, di akses pada 2 September 2022)