Advances in Social Science, Education and Humanities Research, volume 549
Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020)

The Patient Data Protection from the Using of Big Data During the COVID-19 Pandemic in Indonesia

Jose Guardiola[1,*] Rica Donna[1]

[1]*Faculty of Law Atma Jaya Catholic University of Indonesia, Jakarta, Indonesia*

**Corresponding author. Email: joseguardiola9@gmail.com*

ABSTRACT
Big Data is a technology that accommodates large and complex databases to be analyzed by a computing system to construct a more concise information. Indonesia is not the only country that utilizes big data to compile databases from public, for instance, during COVID-19 Pandemic Indonesia has adopted and implemented an application named *Peduli Lindungi* as one of the effort of *The Ministry of Communication and Information Technology of Indonesia* together with *The Ministry of State Owned Enterprises* in assisting *The Ministry of Health* overcoming the COVID-19 pandemic in Indonesia. However, it will create a significant problem if there is patient's information/ *datum* leakage to the public. This is crucial for COVID-19 patients, as they may experience great injury both materially and immaterially. The publication of their data and identities through social media and news that had happened at the beginning of COVID-19's entry to Indonesia, was an important affair for the Government to handle and prevent. Therefore, realizing that there is an urgency to tighten security towards personal information, it is decisive to have a legal protection as human rights provided by the government. This paper used A normative juridical approach in this legal writing. The analytical approach adopted is descriptive analytical based on International treaties and National Personal Data Security Regulations. The result of the study can be inferred that Big data is the answer key, a perfect technology, to assist the elimination of this catastrophe that is happening all over the world, as it is used for the advancement of data management in the world during COVID-19 Pandemic so that fair inspections and states needs can be fulfilled. There is, however, a risk for data leakage that causes public damages, and yet, Indonesia still does not have regulations specifying personal data. This makes the information processing through big data a matter of concern as the security is not guaranteed. Therefore, the government needs to be prompt and responsive in harmonizing the existing laws and regulations to ensure the right to personal data privacy guaranteed by the government, especially during the COVID-19 Pandemic.

Keywords*: Data Protection, Human Rights, Big Data, COVID-19, Indonesia, Patient.*

1. INTRODUCTION

The former Vice President of European Commission responsible for the Digital Agenda, Neelie Kroes, delivered her speech at the opening of the Press Conference on Open Data Strategy in 2011 entitled with a strong message "Data is the New Gold.[1] Through the President of Indonesia's state address on August 16, 2019, Ir. H. Joko Widodo also supported the idea as he stated "Data is a new type of wealth for our nation, as data is more valuable than oil". Data has become a very important part of human civilization as well as petroleum, as Data are considered as *Black Gold.*[2]

Coping with rapid technological development nowadays, the government is required to be adaptive and responsive in envisaging the Industrial Revolution. The world has entered the Industrial Revolution 4.0, in fact, Japan has already preceded other countries as it has entered the Business Society 5.0. Thus, technological developments in the form of data must be calibrated to the constitution of each country. The presence of big data is the real example of government's adjustment as it functioned as a

Copyright © 2021 The Authors. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

receptacle and a processor regarding consumer data for companies and governments.

Indonesia has adopted big data in various government institutions, especially in handling the situation of the COVID-19 Pandemic which is currently the state's urgency to be resolved immediately, big data has become the perfect instrument in helping the government determine what decision to make in accordance with community needs. Until today, the number of COVID-19 continues to rise drastically, necessitating the government to constrain the extent of the Large-Scale Social Restrictions in order to reduce the spread rate. *Achmad Yurainto*, the spokesman of COVID-19, consistently announces the number of cases each day to the public through the media. Although it looks simple, the data collection process has gone through a series of complex activities carried out from all over Indonesia. The Ministry of Health and The Ministry of Owned State Enterprises have developed an application named *PeduliLindungi* to be used by *Kementerian Kesehatan* and the Task Force in overcoming the COVID-19 pandemic in Indonesia.

On March 23, 2020, a Twitter upload was circulated, showing a picture of COVID-19 patients list in the form of Microsoft Excel in which had been censored by one of the COVID-19 patients who was also the victim of Personal Information leakage. In fact, there were another 230 thousand COVID-19 patients who experienced data leakage and traded. It was suspected that the data have been stolen by hackers who sold the patient's data to the dark web.

The Universal Declaration of Human Rights 1948 provides a legal basis to the right of privacy for member states in regulating the state's obligation to protect and respect the rights of individual citizens of each country. This is clearly regulated in Article 12 However, Indonesia still has not specifically formulated regulation regarding protection of personal data, as the law is still being discussed by the House of Representatives and has not yet met a conclusion and has encountered obstacles in its passage. This is crucial as computerized data sovereignty is a fundamental thing that must be protected carefully as it is part of personal data of Indonesian citizens, especially during the Pandemic of COVID-19.

2. RESEARCH METHOD

This research is conducted by a juridical-empirical method which analyzes both primary and secondary data. The primary data is any regulations concerned with citizenship while the secondary data consists relevant literature related to the problems persisted in this research. Thus, this research does not only compile the materials such as theories, concepts, principles and regulations of law dealing with the topic, but also explains the reality of law in society as a law phenomenon for the subject, that data protection for patients in this Pandemic situation. All data needed are collected by literature review.

That data, then, are analyzed qualitatively by doing a deep analysis. Deep interview and Focus Group Discussion are conducted to supply the empirical data needed. The interviewees are chosen purposely from various backgrounds categorized as government and Non-Government Organization also practitioner and academics.

3. FINDINGS AND DISCUSSION

Indonesia had declared a state of emergency due to the spread of the COVID-19 virus since last February 2020, which means Indonesia has been fighting this pandemic for the past 7 months. The government has been endeavoring to diminish the spread rate of the virus while providing the people the newest update of the number of people who died due to COVID-19 each day. The site was developed by the Risk Communication and Community Engagement Team for COVID-19 countermeasures, which consists of various elements such as the government, UN Agencies (including UNICEF, WHO, and others), international development partners, civil society organizations and the business world. Although the data disclosed looks simple, the process of collecting data has gone through a complex series of activities carried out from all over Indonesia, which is known as big data. Big data is a term used to describe a technology that accommodates large and complex databases to be analyzed by a computing system to construct a more concise information.

Numerous government institutions of Indonesia have implemented big data technology to improve their performance and productivity, especially in facing the Pandemic of COVID-19. The West Java government, for instance, established an application called *Pusat Informasi dan Koordinasi COVID-19 Jawa Barat* (PIKOBAR) by using social media data,

the West Java Governor, *Ridwan Kamil*, succeeded to monitor and perceive immediately in detail per area in West Java. In order for the data to be accurate, a fast and precise tracking system based on the Big Data approach is needed, therefore, the data collection through platforms in each region such as PIKOBAR is the most effective way. Not only as a data provider for information dissemination, but big data may also be a tracking to create a good and effective control system for each person. Thus, data from the regions will be integrated with the central government data so that it may assist the government in making policies.

It cannot be denied that Big Data is a very crucial instrument in this Pandemic of COVID-19. Big Data has a massive and escalated character due to the ease and speed of access to information technology or internet media. With just one touch, data can be spread widely and change in various formats in a short time. However, Indonesia still does not have sufficient legal protection towards data privacy, whereas the confidentiality of a person's personal information is at stake.

3.1. Legal Framework

3.1.1. Domestic Legal Framework

In Indonesia, the legal protection towards personal data has not been specifically regulated by the law. The personal data protection bill is currently being discussed by the House of Representatives and still has not reached an end, yet encountered obstacles in its passage. Personal data in Indonesia has a general meaning, as defined in Law number 23 of 2006 concerning Population Administration as amended by Law number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration. Article 1 number 22 states that:

Personal Data is certain individual data that is stored, managed, and secured for the authenticity, and protection of the confidentiality

However, the development of internet-based technology and networks has urged the government to explicitly define personal data in Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Article 26 Paragraph (1), In the use of Information Technology, protection of personal data is one part of personal rights (privacy rights), which contain the following meaning:

a. Personal right is the right to enjoy personal life and to be free from all kinds distractions.

b. Personal right is the right to be able to communicate with other people without spying.

c. Personal right is the right to monitor access to information about a person's personal life and data.

Moreover, the meaning of personal data is also stated in Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions as stated in Article 1 number 29, which states:

Personal Data is any data concerning a person that is individually identified and/ or can be identified or combined with other information, either directly or indirectly through electronic and/ or non-electronic systems.

Meanwhile, the definition of personal data protection is still variously defined in several laws because there are no specific provisions regarding the protection of personal data itself, as contained in Article 54 paragraph 1 of Law number 14 of 2008 concerning Openness of Public Information which states:

Anyone who intentionally and without right accesses and / or derives and/ or provides exempt information as regulated in Articles 17 letter a, letter b, letter d, letter f, letter g, letter h, letter I, and letter j shall be sentenced to imprisonment of 2 (two) years and a maximum fine of Rp. 10.000.000,00 (ten million rupiah).

In addition, Regulation of The Ministry of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronics Systems explains the formal provisions in case there is a leakage of personal data or violation of personal data protection in Indonesia. Article 2 paragraph (1) Regulation of The Ministry of Communication and Information Technology number 20 of 2016, states that:

1. *Protection of Personal Data in Electronic Systems includes protection against the procuration, collection, processing, analysis, storage, appearance, announcement, transmission, dissemination and destruction of Personal Data.*

As we are all aware, personal data that is collected by an institution or government must have

a body or a data storage place of its own, for instance, Indonesia owns an *Electronic System Operator*. Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions explains that an *Electronic System Operator* is any person, state administrator, business entity, and society who provides, manages, and/ or operates electronic systems independently or jointly with users of electronic systems for their own needs and/ or the needs of other parties.

If there is a failure in protecting the personal data it manages, the *Electronic System Operato*r is obliged to notify the owner of the personal data in writing. The failure referred to includes the interruption of part or all of the functions of an essential electronic system so that the electronic system does not function properly. The occurrence of system failure can be caused by internal factors and external factors, one of them that often occurs is cybercrime. Judging from the type of activity, cybercrime can be in the form of hacking, cracking, phishing, identity theft, and others. The impact of losses that arise includes personal data leakage, data manipulation, privacy violations, system damage, and so forth.

Therefore, protection of personal data should be a fundamental matter that is protected by electronic system operators, both private and public, which includes clear regulations towards the form of compensation given when it comes to a failure, as it is detrimental to the people if their personal information is promulgated to the public.

3.1.2. International Legal Framework

ASEAN member[1] countries have regulated the protection towards personal data even though most of the countries do not establish the right to privacy in their constitutions. Malaysia through Personal Data Protection Act 2010, which came into effect on November 15th, 2013, stated in Article 10 that**:**

1. *The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose;*
2. *It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed*

Although the government of Singapore is considered to have failed in protecting the right to privacy, however, the provisions of law regulates the protection of personal data which stated in Article 3 of Personal Data Protection Act 2012, saying[2]:

"*The purpose of this Act is to regulate the collection, use and disclosure of personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data and the need for organizations to collect, use or disclosure personal data purposes which it would reasonably considered right in the situation"*

Brunei Darussalam's Data Protection Policy took effect from 27 August 2015. In Article 12 paragraph (1), it is explained that *"Data may not be used or disclosed to third parties for purposes other than those collected, except with the consent of the individual or required by laws".*

In the third part of the Constitution of the Kingdom of Thailand Article 35 stipulates that: *"A person's family rights, dignity, reputation and the right of privacy shall be protected. The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public. A person shall be protected fr*om the unlawful exploitation of personal information in relation to oneself as provided by law.

Protection of data privacy in the Southeast Asia region has generally been included in the national laws of each country. However, it is unfortunate that although the states have provided strict regulations, on the other hand, the state still does not recognize that the right to privacy is inherent in every citizen.

3.1.3. Protection Toward Personal Data for Covid-19 Patients in Indonesia

During the COVID-19 pandemic, the confidentiality of the patient's data is the fundamental thing that must be guaranteed by the government. The case of COVID-19 Patient's data leakage in Indonesia that happened at the beginning of the COVID-19 pandemic seemed to cause anxiety for the people regarding the data stored by the Government. Thus, it is an urgency for the government to construct a regulation regarding the protection of patient personal data processed through data centers and big data, as the Government has not issued any policy regarding the protection of personal data, furthermore, the sanctions towards any infringement is only administratively.

Indonesia provides protection of patient's personal data in several laws such as the Criminal threat in Article 26 and Article 45 of the Law on Information and Electronic Transactions, however, it does not specifically mention leakage of patient data. Moreover, Patient's personal data are also regulated in Article 32 letter i of Law number 44 of 2009[3] concerning Hospitals which reads:

> *"i) procure the privacy and confidentiality of the illness, including medical data; … "*

However, the provisions of this article do not provide a criminal threat for the perpetrator or the violator. Before the COVID-19 pandemic occurred, entire patient data were stored by the hospital where the subject was referred, but during the COVID-19 pandemic, there was an unclear system where patient's data were stored by *Kementerian Kesehatan. PeduliLindungi,* an application that was developed by *Kementerian Komunikasi dan Informatika (Kominfo)* and *Kementerian BUMN* in order to assist *Kementerian Kesehatan* and the Task Force in overcoming the COVID-19 pandemic in Indonesia, utilizes the user's Bluetooth to record the required information. Data exchange will occur when there are other gadgets within the Bluetooth radius that are also registered in *PeduliLindungi*, which then the application will identify people who have been in close proximity with people who have tested positive for COVID-19 or Patients and People under Supervision. This is immensely useful when the user cannot remember travel history and who they are in contact with. The user will also be contacted by health workers if they have been within a certain distance with positive COVID-19 sufferers, Patient under Supervision and People under Supervision. Therefore, the Hospital Law is only applied as a reference in fulfilling the patient's rights. From the *PeduliLindungi* application that we have discussed, we can see that there is the utilization of Big Data. Thus Electronic System Operator, which in this case is the *Kementerian Kesehatan*, can freely access and utilize the data according to their needs.

COVID-19 patient's data is identified with public information data, thereby, the Public Information Disclosure Law becomes one of the references in its implementation. In Article 54 paragraph of Law number 14 of 2008 concerning Freedom of Information, which reads:

> *"Anyone who intentionally and without right accesses and / or derives and/ or provides exempt information as regulated in Articles 17 letter a, letter b, letter d, letter f, letter g, letter h, letter I, and letter j shall be sentenced to imprisonment of 2 (two) years and a maximum fine of Rp. 10.000.000,00 (ten million rupiah)."*

Nevertheless, we can realize that all the articles that have been mentioned are crime by accusation. Therefore, it can be imagined if there are Leakage of COVID-19 patient's data to the public due to the negligence of electronic system administrators or because of cracking and hacking actors, there would be thousands of COVID-19 patients whose identities would be disseminated. This will obstruct the government from enforcing the law, as a crime by accusation may not allow the government to handle such abundant cases that arise through the leakage.

While Indonesia does not have any legislation that specifically regulates electronic medical records, it turns out that several countries in the world have regulated this matter due to the desire of each country to protect the privacy of every citizen including medical history. For instance, Singapore Ministry of Health has regulated the storage period for medical records in the ***Guidelines for The Retention Periods of Medical Records 2015***, as there are different rulings between the storage period for online medical records and in the form of file. Moreover, each state of the United States of America also regulates the storage of medical records in the ***Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, California Confidentiality of Medical Information Act, and California Civil Code.*** Furthermore, reviewing in December 2012, Austria issued a law regulating electronic medical records namely the ***Electronic Health Records Act (HER-Act).***

3.2. An Overview of the Human Rights

Human rights is one of the factor that the government made the regulation. In this case Patient's Covid 19 data is the part of the right to privacy that the government shoul take care. The fulfillment of the rights for every citizens have to be done.

3.2.1. Considerations of Rights to Personal Data and Protection of Indonesia and Global

The right to privacy or the right to personal data is explicitly stated in the ***Universal Declaration of Human Rights 1948.*** This declaration has provided a legal basis for member states regarding the state's

obligation to protect and respect the right to every citizen in each country, as stated in Article 12[1], which reads:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Through this article, it stipulates that all individuals have the right to privacy, rights to their families, rights to residence, rights to relate to other people, and rights to their good names. Therefore, all of these elements must receive legal protection.

The Universal Declaration of Human Rights is the most important international instrument because it has succeeded in uniting agreements from almost all countries. However, as UDHR provides a very broad protection of the right to a person, it leads to the emergence of a more specific protection, which is ***International Covenant on Civil and Political Rights (ICCPR)*** that has been in effect from March 23th, 1976, through the 2200A Resolution. ***Article 17 paragraph (1) stated that:***

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.*
2. *Everyone has the right to the protection of the law against such interference or attacks.*

   This convention emphasizes that no one may be treated arbitrarily or illegally interfered with in his personal, family, home, or correspondence matters. This convention furthermore gives authority to each country to create legal instruments to protect the nation, therefore it is an obligation for the member state to implement this convention.

This convention emphasizes that no one may be treated arbitrarily or illegally interfered with in his personal, family, home, or correspondence matters. This convention furthermore gives authority to each country to create legal instruments to protect the nation, therefore it is an obligation for the member state to implement this convention.

Therefore, protection of personal data is a fundamental matter that has to be prioritized in upholding human rights in accordance with the Universal Declaration with Human Rights 1948. However, the author cannot deny that the attitude of guaranteeing human rights protection in terms of fulfilling personal data protection has not been fully respected.

3.2.2. Considerations of Personal Data Protection in Indonesia

Data in Indonesia can be accessed by the citizens according to the 1945 Constitution, as the amendment towards the 1945 Constitution and the endorsement of Law of the Republic of Indonesia Number 39 of 1999 concerning Human Rights have contributed to the protection of fundamental rights for Indonesia citizens. Article 28F of the Second Amendment to the 1945 Constitution states that:

"Everyone has the right communicate and obtain information to develop their personal and social environment, and the right to seek, obtain, process, store, process and convey information using all available channels"

Freedom of information is a citizen's right which can be reduced when the information is a citizen's right to privacy that must be protected in society. So that the protection of the constitutional rights of information is contained in Article 28F of the 1945 Constitution also needs to be understood with other constitutional mandates which are also contained in Article 28J of the 1945 Constitution Paragraph (2):

"In exercising his rights and freedoms, everyone is obliged to comply with the restrictions established by law for the sole purpose of ensuring recognition and respect for the rights and freedoms of others and to fulfill fair demand in accordance with moral considerations, religious values, security and public order in a democratic society".

Regulation regarding privacy rights are also clearly stated as Indonesia has ratified the International Covenant on Civil and Political Rights (ICCPR) on October 28, 2005 through Law of the Republic of Indonesia Number 12 of 2005 concerning the Ratification of the International Covenant on Civil and Political Rights. Article 28 G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, the fourth amendment, reads:

"Everyone has the right to self-protection, family honor, dignity and property under his control, and the right to a sense of security and protection from the threat of fear to do or not to do something that is a human right".

Long before the ratification of the International Covenant on Civil and Political Rights was carried out, during the amendment period of the 2000

Indonesian Constitution, the Chapter on Human Rights was developed and the recognition of the right to privacy took a special place in the 1945 Indonesia Constitution. Article 28H guarantees the right to privacy by stating that *"Everyone has the right to own private property and these rights cannot be taken over arbitrarily by anyone"*. This provision is clearly a legal protection and the basis for the Laws and Implementing Regulations under it to give authority to protect the right to privacy, including the protection of personal data.

4. CONCLUSION

The world has entered the Industrial Revolution 4.0 and in fact, Japan has already preceded other countries as it has entered the Business Society 5.0. Therefore, an adjustment of technological developments, especially in the form of data, becomes an urgency to be implemented to the constitution of each country. The rapid development is proven by the presence of big data as a container which processes consumer data for companies and government. During the COVID-19 Pandemic, Big Data or data processing systems has become a perfect instrument in assisting the government to collect and process the covid-19 patient data, both patients under surveillance or people under surveillance. The processed data will later be accommodated and stored by an electronic system organizer. Regarding health matters, patient data will be stored and guarded confidentially by the Hospital in accordance with the provisions in the Hospital Law, however, it is different during the COVID-19 Pandemic. Through *PeduliLindungi* application, it is easier to find the point of spread of the virus as every hospital in the province of Indonesia is obliged to provide the medical record to the health office, which later will be managed and stored by the *Kementerian Kesehatan. PeduliLindungi* helps the user to identify the people who have been in close proximity with people who have tested positive for COVID-19 or Patients Under Supervision and People Under Monitoring, whenever the user cannot remember travel history and who they have contact with.

Indonesia still has not specifically formulated regulation regarding protection of personal data, as the law is still being discussed by the House of Representatives and has not yet met a conclusion and has encountered obstacles in its passage. Policies regarding personal data are broadly defined and regulated, therefore, legislation that specially governing personal data is required. This legislation is expected to be the standard of protecting personal data in general, whether data that is processed in part or in whole by electronically or manually, where every form of data can apply the protection of Personal data according to the characteristics of the sector concerned. The fact that Indonesia has not been able to construct a legislation concerning personal data protection is a setback for our country as a member of ASEAN. As we all aware, countries on Southeast Asia have been successfully rule about personal data protection, such as Malaysia, Singapore, Brunei Darussalam, Philippines and Thailand. Therefore, Indonesia needs to reflect from neighboring countries to actualize this regulation as to protect personal data, whether related to data regarding any field and in any form. This is an urgency for the government to be cope with, as the country is dealing deal with COVID-19 Pandemic amidst rapid technological advances.

During the COVID-19 pandemic, patient data is very crucial that the Government must be able to guarantee its security. However, the leakage of COVID-19 patient's data has raised public concerns about the safety of data storage performed by the government. As yet, the government has not issued any policy on personal data protection and only provides administrative sanctions, as we believe there must be a legal certainty regarding sanctions for perpetrators if any failure occurred. Even though there are legal instruments provided by ministers, these formal regulations are deemed unable to cope with the dynamics of technological development, differ from Southeast Asian countries that already have regulations related to the protection of personal data.

The construction of Personal Data Protection, especially for COVID-19 patients, has to be immediately as the regulation for medical records storage which regulated in Hospital Law are not yet based on technology, meanwhile patient's data during this Pandemic has been encrypted so that users of *PeduliLindungi* can exchange data and medical records. According to the author, this construction of regulation becomes a main urgency so that the fulfillment of human rights towards privacy must be put forward as a guarantee, especially during the COVID-19 Pandemic.

The government is demanded to be able to guarantee the protection of the rights to privacy, so that the citizens may get compensations accordingly, whenever the data owner experiences material and immaterial losses. It is unfortunate that criminal sanctions only applied for cracking and hackers,

meanwhile people who suffer personal data leakage only be notified by the government or electronic system administrators, which is not worth the losses incurred by the owner when their data was leaked to the public. Therefore, the Electronic System Operator is required to provide appropriate compensation to build a sense of security towards people who store their personal data in the system (big data, cloud computing, *et cetera*.)

REFERENCES

[1] R. Natamiharja, "Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN Fakultas Hukum Universitas Lampung."

[2] Republic of Singapore, "Personal Data Protection Act 2012," vol. 2012, no. 26, p. 77, 2016, [Online]. Available: https://sso.agc.gov.sg/Act/PDPA2012.

[3] N. F. Octarina, M. B. N. Wajdi, M. I. Setiawan, A. Sukoco, T. Purworusmiardi, and N. Kurniasih, "Tinjauan terhadap UU ITE untuk Penerapan Rekam Medis Berbasis Online pada Penduduk Muslim di Indonesia," *Ejournal.Kopertais4.or.Id*, vol. 5, no. 2, pp. 78–94, 2017, [Online]. Available: http://ejournal.kopertais4.or.id/mataraman/index.php/tahdzib/article/view/3253.

[4] T. Indonesia. "Peran Penting Big Data di Masa Wabah Corona." Telkom Metra. https://www.telkommetra.co.id/en/publication/insight/peran-penting-big-data-di-masa-wabah-corona (accessed Oct. 12, 2020).

[5] The Republic of Indonesia, *"Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions," State Gazette of the Republic of Indonesia. 2016 Number 251, pp. 1689-1699, 2016.*

[6] *The Law number 23 of 2006 concerning Population Administration as amended by Law number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration.* The Republic of Indonesia, 2013.

[7] *The Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions*, The Republic of Indonesia, 2016.

[8] The *Law number 14 of 2008 concerning Openness of Public Information*, The Republic of Indonesia, 2008.

[9] *The* Government Regulation of *Menteri Komunikasi dan Informatika* Number 20 of 2016 concerning Protection of Personal Data in Electronics Systems, The Republic of Indonesia, 2016.

[10] *The government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions*, The Republic of Indonesia, 2019.

[11] The 1959 Constitution of Brunei Darussalam with Amendments through 2006

[12] *The law Number 44 of 2009 concerning hospitals*, The Republic of Indonesia, 2009.

[13] 1945 Constitution of The Republic of Indonesia.

[14] AFP, "230 Ribu Data Pasien Covid-19 di Indonesia Bocor dan Dijual", CNN Indonesia. https://www.cnnindonesia.com/teknologi/20200620083944-192-515418/230-ribu-data-pasien-covid-19-di-indonesia-bocor-dan-dijual, (accessed Oct.12, 2020).

[15] Aurelia, Bernadetha. "Dasar Hukum Perlindungan Data Pribadi Pengguna Internet". Hukumonline.com https://www.hukumonline.com/klinik/detail/ulasan/lt4f235fec78736/dasar-hukum-perlindungan-data-pribadi-pengguna-internet (accessed Oct. 13, 2020)

[16] A. Permana. "Pemanfaatan Big Data untuk Penanganan Pandemi COVID-19". Institut Teknologi Bandung. https://www.itb.ac.id/news/read/57556/home/pemanfaatan-big-data-untuk-penangan-pandemi-covid-19 (accessed Oct. 12, 2020)

[17] Dr. Danrivanto Budhijanto, S.H., LL.M, *Big Data Yurisdiksi Virtual: Legislasi dan Regulasi di Indonesia*, Indonesia: LoGoz Publishing, 2017, pp 99-100.

[18] https://www.pedulilindungi.id, PeduliLindungi.id.

[19] Law of the Republic of Indonesia Number 39 of 1999 concerning Human Rights, The Republic of Indonesia, 1999.

[20] Law of the Republic of Indonesia Number 12 of 2005 concerning the Ratification of the International Covenant on Civil and Political Rights, The Republic of Indonesia, 2005.

[21] M. Arnani. "Virus Corona di Indonesia, Ini 6 Layanan Informasi yang Bisa Diakses". Kompas.com. https://www.kompas.com/tren/read/2020/03/20/090200165/virus-corona-di-indonesia-ini-6-layanan-informasi-yang-bisa-diakses (accessed Oct. 12, 2020).ection Objectives," *Privacy-Respecting Intrusion Detect.*, no. June, pp. 31–42, 2007, doi: 10.1007/978-0-387-68254-9_5.

[22] N. F. Octarina, M. B. N. Wajdi, M. I. Setiawan, A. Sukoco, T. Purworusmiardi, and N. Kurniasih, "Tinjauan terhadap UU ITE untuk Penerapan Rekam Medis Berbasis Online pada Penduduk Muslim di Indonesia," *Ejournal.Kopertais4.or. Id*, vol. 5, no. 2, pp. 78–94, 2017, [Online]. Available: http://ejournal.kopertais4.or.id/mataraman/index.php/tahdzib/article/view/3253.