

Legal Securities Against Covid-19 Patient Privacy Data in Indonesia

Eka N.A.M Sihombing¹, Cynthia Hadita², Muhammad Yusrizal Adi Syaputra³

¹ Faculty of Law, University Muhammadiyah of North Sumatera, E-mail: ekahombing@gmail.com

² Faculty of Law, University Muhammadiyah of North Sumatera, E-mail: cynthiahadita@gmail.com

³ Faculty of Law, Medan Area University, E-mail: yusrizal@staff.uma.ac.id

ARTICLE INFO

Keywords:

Privacy; Law; Data; Patient; Covid-19.

How to cite:

Sihombing, E. N. A. M, Hadita, Cynthia, & Syaputra, Muhammad Yusrizal Adi. (2021). Legal Securities Against Covid-19 Patient Privacy Data in Indonesia. *Veteran Law Review*. 4(1). 34-49

ABSTRACT

The issue of disclosure of patient data privacy covid-19 has a dilemma, on the other hand covid-19 patients must be protected data privacy so as not to spread into public consumption because it will negatively implicate patients covid-19 to economic, social, and other aspects if their medical records are disseminated without approval. Thus, this study will also describe one of the court rulings in which a covid-19 patient sued the local government for a press conference on the positiveness of covid-19 patients and also sued one of the mass media that reported about his condition. Thus, there are two sides of the currency, where on the other hand the privacy of patient data must be protected, but on the other hand, the dissemination of information with the patient's permission is needed to avoid other people being exposed to covid-19, because it takes traces of contact from covid-19 patients so that the virus does not spread. Thus, the protection of patient data privacy covid-19 needs to be reviewed to answer the dilemma with the model of protecting the privacy of patient data covid-19. The research method used in this study is normative juridical method using doctrinal approach. The purpose of the research is to analyze the settings regarding the privacy of covid-19 patient data in Indonesia and is communicated with the protection of the privacy of covid-19 patient data in other countries. The results showed that there is still a violation of patient privacy data covid-19, whereas the Constitution (Article 28 G paragraph (1)), Article 57 of the Health Law, and several international conventions that have been ratified have also essentially stated that patient privacy must be maintained but there are still central and local governments that violate the privacy of patients covid-19 by announcing clearly about the identity of covid-19 patients that have a detrimental impact on patients. Referring to the protection of data privacy of covid-19 patients in the EU, UK, US, China, India, Hongkong, Malaysia, and Singapore that guarantees firmly that there is no data leakage that can worry the public in general to really maintain the privacy of covid-19 patient data, and its tracking is integrated through an application that has been guaranteed security.

Copyright ©2021 VELREV. All rights reserved.

1. Introduction

The dilemma of disclosing patient privacy data to the public is faced with a consolidation like two sides of the currency. If opened, it will make it easier to know the contact *tracing* of covid-19 patients to minimize the potential of others infected. However, on the other hand, patient privacy data needs to be protected as guaranteed by the constitution and its various degradations.

Patients, including COVID-19 patients, have the right to privacy and confidentiality of the disease, including their medical data. The identity of COVID-19 patients is the privacy of patients, so the identity of COVID-19 patients must be kept confidential. Article 32 letter I of Law No. 44 of 2009 concerning Hospitals, mention that "The doctor is obliged to keep everything he knows about the patient confidential". This means that doctors should not share the patient's identity and illness, including COVID-19 patients. Article 51 letter c of Law No. 29 of 2014 on Medical Practice "Hospitals are obliged to respect and protect the rights of patients. If a hospital leaks patient data including COVID-19 patients, the hospital may be penalized in the form of a reprimand, written reprimand, fine, and even revocation of hospital license". Article 29 paragraph (2) of Law No. 44 of 2009 concerning Hospitals "Not just anyone can access the patient's data and identity". Article 54 paragraph (1) of Law No. 14 of 2008 concerning Public Information Disclosure, mention that "Any person who knowingly accesses a person's history, condition and treatment, physical and psychic treatment will be penalized". (Ponjong, 2020). In the first case of covid-19 patients in Depok, President Jokowi insisted that all parties should respect the code of ethics and personal rights of patients. Therefore, their identity, said Jokowi should be strictly maintained and should not be opened to the public as part of the ethics in communicating. "The media should also respect their privacy [patients] so that psychologically they are not depressed, and can go home and recover immediately (Septianto, n.d.).

This problem is increasingly raised when information about the personal data of the first two patients of Covid-19 in Indonesia is so widespread the information is precisely provided by the government. On March 2, 2020, depok regional leaders held a press conference and provided personal data information of Patients 01 and 02. In the press conference held at Depok City Hall, it was released chronologically as well as the home addresses of patients 01 and 02. Also doing the same, Former SOE Minister Dahlan Iskan released the personal information of the two patients' lives on his personal blog equipped with photos of the patient's home." Not only stopped in patients 01 and 02, the dissemination of other personal data befalls a citizen, after conducting a Covid-19 examination test at one of the hospitals and declared as ODP (Ahmad Redi, 2020).

As *early warning* since the corona virus in Indonesia, the disclosure of data should only be by mentioning the area, not specifically providing a complete identity ranging from initials, home addresses to detail to RT, RW, Kecamatan, Kelurahan, to the number of his home, which can be easily detected by the public who are infected with positive covid-19 to implicate the creation of irregularities and concerns for the community and harm the patient. Not only

during *the early warning* but until now there is still disclosure of patient privacy data is still happening, proven there is a lawsuit in court between the patient and the government that discloses his privacy data.

Proven by the sued by the government (central/regional) by covid-19 patients who are given data privacy through press conferences and also print media, thus implicating the personal of covid-19 patients in terms of social and economic relationships to the patient's psyche that should be protected personal data so as not to negatively impact him, the virality of information that is widespread through cyber networks causes patients to be depressed, shunned, ridiculed and also the condition of local people who feel unsafe with that information. One of the legal phenomena that occur over the lack of legal securities related to the privacy of covid-19 patient data is with the Civil Award No. 19/Pdt.G/2020/PN Psp SHL (initials of covid-19 patients suing) Against Irsan Efendi Nasution as Mayor of Padangsidempuan. Dkk.

The lawsuit filed by Plaintiff SHL against the Defendants of the Padangsidempuan City Local Government and the Daily Alert media. The lawsuit is based on plaintiff's objection to the defendant's statement spreading the identity of plaintiff's husband's name as a positive patient of Covid-19 in press conferences and articles in journalistic media with the title "Close Contact of Covid-19 Patients Sidempuan 'Wandering'. Plaintiff considers that the defendants' statements are provocative, arbitrary, tendential, and personally cornered the Plaintiff and the Plaintiff's family and the problems that occurred. The dissemination of the identity of plaintiff's husband as a Covid-19 patient is considered to have damaged the honor of the plaintiff's family's good name and harmed the Plaintiff's husband economically, socially, and privacy. Although the lawsuit was rejected on the grounds of *error in persona*, but the case for disclosure patient privacy data of covid-19 still continues to occur. Because, for violations of privacy rights cause covid-19 patients stigmatized from the community.

Differentiation between this study and previous research, that regarding the privacy of patient data covid-19 much discussed problems in the aspect of *contact tracing* of patients covid-19 through various applications provided by various countries. However, in the study will be more detailed review about the security of data privacy of covid-19 patients in Indonesia, the protection of patient data privacy covid-19 in some countries, and also offers a model of data protection of covid-19 patients in Indonesia with reference to various regulations in Indonesia, ranging from the Law to its relevance to policy regulations in the form of a Ministerial Circular letter relating to information relating to covid-19 patients. In addition, this study also expressed examples of cases of violating the privacy rights of covid-19 patients that boil down to the lawsuit process in the Court.

2. Method

The method used in this study is the normative juridical law research method. The normative research, must use a statutory approach (*statute Approach*), this is because what will be researched are various rules of law. Taking the term Dworkin, this kind of research is also referred to as *doctrinal research*, (Ibrahim, 2018) which is research that analyzes the law, both written in the book (law as it is written in the *book*). In this study the literature and document studies were used as the main material.

Marzuki in Eka NAM Sihombing (2019) states that the normative juridical legal research method is a method that uses an approach that is based on the main legal material by examining theories, concepts of legal principles, norms, rules of legislation, court decision, agreement. The nature of the research used in this paper is prescriptive, adhering to the characteristics of legal science as an applied science, the prescriptions given in legal research activities must be able and possible to be applied. Therefore what is produced by legal research, even if it is not a new legal principle or a new theory, is at least a new argument (Sihombing, 2019).

3. Settings on Data Privacy Protection of Covid-19 Patients in Indonesia

The recognition of the right to Privacy stems from Warren and Brandeis's thinking that in principle an individual should have full protection for himself or her property (Rianarizkiwati, 2020). More information as follows:

"That the individual shall have full protection in person and in property is a principle as old as the common law, but it has been found necessary from time to time to define anew the exact nature and extent of such protection... thus, in very early times, the law gave a remedy only for physical interference with life and property,... then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights is broadened; and now the right to life has come to mean the right to enjoy life, the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession-intangible, as well as tangible."

Warren and Brandeis further claimed that privacy is a right to be left alone is a narrow sense of privacy. Privacy means not being disturbed by others or means that one must feel safe in his or her personal life, ownership and in terms of communicating. Whereas in a broad sense, privacy in a narrow sense and the presence of a sense of comfort in social interaction, for example in terms of anonymity and confidentiality of personal data (Ibrahim, 2018).

In the early 21st century, the European Union pioneered the protection of personal data as part of basic rights through the Charter of Fundamental Rights of The European Union (2000), then ASEAN in 2012 through The ASEAN Human Right Declaration stated that personal data is part of the right to privacy, thus gaining protection as a Human Right.

In Indonesia Article 28G (1) Constitution “Everyone has the right to protection of his / her personal, family, honor, dignity and property under his control, as well as to the feeling of security and protection from the threat of fear to do or not do something that constitutes a human right”. The understanding of the text interprets that what is meant by self-protection is the right to privacy (Ibrahim, 2018).

The forerunner of the disclosure of covid-19 patient privacy data in Indonesia, starting on March 2, 2020, the Government of Indonesia announced the presence of two people in this region of the country who are positively indicated corona. The two residents are said to live in Depok, West Java, and are being treated at Sulianti Saroso Hospital, North Jakarta. On the same day, Depok city government held a press conference in its office. In the media conference, the Mayor of Depok revealed the residential address of corona positive patients and received widespread news from the national mass media. Some of media reports, the two corona positive patients felt depressed because of the massive media coverage. The government is obliged to provide accurate and timely health guidelines and prevent misinformation about the virus in a proportionate, legitimate, and absolutely necessary way so as not to violate human rights (Sari, 2020).

The privacy of information in the constitution is seen from the statement that everyone can supervise and distribute the information they have. This oversight helps protect the integrity and integrity of a person by avoiding the use of information that could damage or embarrass the owner of the information. Furthermore, even if a person has released his or her personal information, that person retains an interest in what happens next and who can access that information. The law does protect the right to personal information, but with technological advances, it has difficulty in its application. Lastly, everyone has the right to submit the right to eliminate personal data in the event of personal data misrepresentation or data collection or processing that is not in accordance with the laws and regulations (Rianarizkiwati, 2020). Article 12 of the Universal Declaration of Human Rights (DUHAM) says that no one should be disturbed by the personal affairs of his family, his household, or his correspondence, arbitrarily and entitled to legal protection for such violations. Keep in mind, Indonesia has ratified international human rights laws that require the government to ensure the health of its citizens, the availability of services, doctors and other health needs, including protecting the right to privacy. It must be obeyed by all government officials, from top to bottom (Sari, 2020).

Das sollen on the collection of patient privacy data, can be done with exceptions, not unilaterally disclose about the information experienced by patients in this case covid-19 patients, this is generally stipulated in Article 57 of Law No. 36 of 2009 on Health:

(1) Everyone is entitled to the confidential state of his/her personal health condition which has been submitted to the health care provider.

- (2) The provisions on the right to confidential personal health conditions as referred to in paragraph (1) shall not apply in the case of:
- a. statutory orders;
 - b. court orders;
 - c. relevant permissions;
 - d. the interests of the community; Or
 - e. interests of the person.

The reason used by the government is usually related to so that the public knows who is affected by covid-19 and also to stop the spread. In fact, there is an isolation mechanism that does not harm other communities. The exception of information transparency regarding patient data and medical records (e.g. positive covid-19 information) must be approved by the patients of covid-19 and/or their families.

Regulation of the Minister of Health (PMK) No. 269/MenKes/Per/III/2008 concerning Medical Records, which requires all health service providers to maintain the confidentiality of patients' medical records. In Article 10 (2) the regulation is said, that opening a medical history is possible for health purposes, fulfilling the request of law enforcement officials, the request of the patient himself, and for the purposes of research or education as long as it does not mention the identity of the patient (ELSAM, 2020).

Rizal E. Halim, Chairman of BPKN RI said, "In terms of tracing which means collecting personal data, including location tracing, it should be displayed only information about the location, without revealing the patient's personal identity in order to fulfill the public's right to public health with clarity about the location that has been visited by patients positively confirmed Covid-19 (BPKN, 2020).

For example, the release of Personal Data to the Public Regardless of the pros and cons of hrs swab test results rolling in the community, basically the patient's personal data and/or medical records are confidential, strict and limited, must be maintained and protected and can only be disclosed with the consent of the patient concerned or disclosed with the provisions of applicable law. Due to its confidential nature, the rules for opening the patient's personal data should also not be arbitrary. The patient's personal data should only be disclosed when it comes to law enforcement and with the patient's consent (Palupi Kurnianingrum, 2020) Groups with this view argue that: (Kontroversi Kerahasiaan Data Pasien Covid-19 & MK, n.d.) the interests of society should take precedence over personal interests. This view reaped a test application to the Constitutional Court against several laws in the field of Health. Applicants question the rules on doctor confidentiality in Law No. 29 of 2004 on Medical Practice, Law No. 44 of 2009 on 4 Hospitals, and Law No. 36 of 2014 on Health Workers.

Some articles submitted to the Constitutional Court are:

- a. Article 48 paragraph (2) of the Law on Medical Practice governing the obligation of doctors and dentists to maintain medical confidentiality. Medical secrets can be disclosed only for the benefit of the patient's health, fulfilling the request of law enforcement officials in the framework of law enforcement, the request of the patient himself, or based on the provisions of legislation.
- b. Article 38 paragraph (2) of the Hospital Law governing the obligation of each hospital to maintain medical confidentiality. Hospitals can only disclose patient data for the benefit of the patient's health, the request of law enforcement officials in the framework of law enforcement, the request of the patient himself, or based on legislation.
- c. Article 73 paragraph (2) of the Health Workers Act requires that every health worker keep the health care recipient confidential, and can only be opened for the benefit of the patient's health, the fulfillment of the request of law enforcement officials, the request of the recipient of health services or in accordance with the laws and regulations.

It is also contained in the Central Information Committee Circular Letter Number 2 of 2020 concerning Public Information Services in the Public Health Emergency Due to Corona Virus Disease 2019 (Covid-19). In the number 4 letter c, one of the public information guidelines related to the handling of health emergencies due to Covid-19 is to inform the spread of Covid-19 as a means of early warning for the community, which includes the distribution area for the smallest unit of the region up to the village or hamlet level while maintaining the personal data of People Under Surveillance (ODP), Patients Under Surveillance (PDP) and Covid-19 positive patients. Central Information Committee Circular Letter No. 2 of 2020 concerning Public Information Services In The Emergency Period of Public Health Due to Corona Virus Disease 2019 (COVID-19), point 4 letter b mentions in essence the Central Information Committee provides guidance to the Chairman of the Task Force on The Acceleration of Handling Covid-19, The Minister of Health, Governor, Regent/Mayor, and other government agencies related to the handling of the Covid-19 health emergency, among others strictly and limitedly, inform the spread of Covid-19 while protecting the personal data of Persons In Monitoring (ODP), Patients Under Surveillance (PDP), Covid-19 positive patients, and people who are declared cured by the authorities. The personal data in question consists of: name, home address, telephone number, and so on, which can reveal the personal identity of the person concerned. Personal data can be used by the government to mitigate the spread and confectionery of Covid-19. However, it should not be published unless approved by the concerned or the core family and in accordance with the laws and regulations. It is in accordance with the provisions in Article 2 paragraph (2) of Law No. 14 of 2008 concerning Public Information Disclosure which states that public information that is excluded is strict and limited. As previously stated, that Covid-19 patient data is information that is excluded in the public information disclosure service, so that based on the Article the spread is carried out strictly and limited.

Regarding the binding power of regulation / policy under the Regulation of the Minister of National Development Planning / Head of Bappenas As a "policy regulation" that is not a rule of law, according to Bagir Manan the policy regulation is not directly legally binding but contains legal relevance (Soebroto, n.d.).

The first group assessed that some of these articles were considered to hinder the constitutional interests of applicants to obtain information about patients who have been affected by Covid-19. The applicants think that opening covid-19 patient data has a positive impact, namely early detection and reduced spread, because citizens can do early anticipation. In contrast to the first view, the second view holds that the patient's personal data is confidential information, i.e. information that is excluded in the public information disclosure service, as stipulated in Article 17 letter h number 2 of Law No. 14 of 2008 concerning Public Information Disclosure. The article stipulates that a person's history, condition and treatment, physical and psychic health treatment are information that is excluded because when disclosed and provided to the applicant public information, it can reveal private secrets. Thus, normatively patient data should not be opened except for some exceptions stipulated in the legislation. This group is of the view that if Covid-19 patient data is opened to the public, there is a chain effect that is revealed also the personal data of people who have interacted with the patient.

While there is an opportunity to disclose data and health conditions of Covid-19 patients for the reasons set out in the legislation as outlined earlier, it cannot be used other than for the purposes set out. In other words, the dissemination of Covid-19 patient data based on Article 2 paragraph (2) of Law No. 14 of 2008 concerning Public Information Disclosure adheres to the principle of restriction based on a specific purpose (purposive limitation), in this case the purpose as stipulated in the legislation. One of the limited opportunities in the dissemination of Covid-19 patient data is also seen in Article 5 paragraph (2) of Regulation of the Minister of Health No. 36 of 2012 concerning Medical Secrets, which contains the provision that the opening of medical secrets is limited as needed. As outlined earlier, the legislation provides an obligation for health workers to keep medical secrets, in this case including data and the condition of Covid-19 patients. In this case, Article 5 paragraph (2) provides an opportunity to unlock medical secrets, but must be done on a limited basis as needed. It can be said that this Article adheres to the principle of necessity and proportionality, where the disclosure of personal data of Covid-19 patients must be done minimally and as needed in the control and handling of Covid-19. This minimalist pattern of data also needs to underlie the selection of the personal data portion of Covid-19 patients that can be opened, i.e. only data that if opened, not to reveal the patient's personal secrets, such as anonymous use, age, gender, or the provision of identification codes for Covid-19 patients.

4. Comparison of Covid-19 Patient Data Privacy Protection with Some Other Countries

The information that we know is also known by others, regardless of whether the other person stores or remembers the information, then the end of one's autonomy over his/her personal information. That others already know will not be with information easily covered back. One of the concepts of privacy in terms of information focuses on the right to control information about a person. Loss of control over privacy occurs when information about a specific thing is passed on to others. In addition to being associated with information collected by the public sector, the loss of control over privacy also occurs when individuals fear information disclosure. Information collection should not allow information disclosure (Rianarizkiwati, 2020).

In UK, personal data regulation is relevant with General Data Protection Regulations (GDPR), in India, they regulate it in Data Empowerment and Protection Architecture (DEPA). In China, there is a cybersecurity law. In Malaysia and Singapore, it has the similar act nomenclature for data privacy, Personal Data Protection Act 2010 (PDPA).

In EU countries collecting personal data as part of their COVID-19 response will be required to comply with the GDPR (as well as their own laws). For example, Italy's data protection authority, the Garante, adopted a decree addressing the intersection between the GDPR and COVID-19, the need for processing special categories of personal data, and how some data protection rights could be suspended to combat the virus. The Garante has issued further guidance prohibiting "do-it yourself" data collection. DPAs in France and Ireland have likewise taken positions on the handling of personal data in the context of responding to COVID-19 (*COVID-19 Response and Data Protection Law in the EU and US*, 2020).

In US, Although there is no omnibus data protection law at the federal level in the U.S., several federal and state laws offer privacy protection to certain types of data. Given the sectoral approach to privacy under the U.S. legal system, it is worth exploring the protections that exist under U.S. law for certain types of data relevant to this discussion, namely protected health information, employment data, and location data (*COVID-19 Response and Data Protection Law in the EU and US*, 2020).

Other risks from the spread of Covid-19 patients identities can reap citizen rejection and other social impacts such as refusal to live in their neighborhood, even the refusal of funerals of people known to have died as covid-19 patients. In practice, some countries apply the openness of some types of Covid patient data, such as age, gender, and nationality. In Indonesia, the Regional Government of DKI Jakarta Province opened covid-19 distribution data to the Village level. So that the community knows if in a village there are Covid-19 positive patients or not.

If we analysis from the act of some country about the privacy data, health is a human right (the right of self determination) that must be realized through the

guarantee of providing safe and quality health by the government and health services including during the Covid-19 Pandemic situation that has hit almost all countries in the world including Indonesia. One of the things that causes public unrest is the circulation of covid-19 patient data on social media and in the community that leads to negative stigma in victims including victims' families as happened in Aik Mel Village, Cimahi, Cianjur and some other places even there is rejection from the community even though the patient has been declared cured (Ariany & Ningsih, 2019).

The main obstacle in effective media communication of the Covid-19 pandemic is the controversy over patient privacy v.s. public interest in efforts to prevent the spread of pandemics. Efforts to prevent the spread of the Covid-19 pandemic require the disclosure of information especially related to patients who have been declared positive for Covid-19. But on the other hand, it is contrary to patient privacy (Ardiyanti, 2020).

The construction of regulations regarding legal protection of personal data which is a right to privacy in Indonesia is very behind when compared to countries in the European continent, this can be seen from several regulations that were initiated first, one of which is the General Data Protection Regulation (GDPR) or GDPR 2016/679 which has now been updated with the 2018 GDPR, which is seen as a charter regulating the protection rights of personal data in the European Union, for example and a comparison of several countries in the European continent that have responded quickly to the importance of protecting personal data is Belgium, which has had regulations regarding the protection of personal data since 1992, which became known as the "Law of 1992 on privacy protection when processing personal data", then in 2018 the Belgian Government has replaced the regulations with the Belgian Law of July 2018 on protection of natural persons with regard to the processing of personal data. Apart from Belgium, the Netherlands also has regulations regarding personal data known as *Wet Bescherming Persoonsgegevens*, the rest of the Netherlands has also established a Personal Data Protection Authority named *Autoriteit Persoonsgegevens (AP)* which is in accordance with most Data Protection Laws which require the establishment of a supervisory authority, AP as a Personal Data Protection Authority is subject to and based on the law on the GDPR, the General Data Protection Implementation Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming*) and several other regulations. The Netherlands also has regulations regarding personal data known as *Wet Bescherming Persoonsgegevens*. The rest of the Netherlands has also formed a Personal Data Protection Authority called *Autoriteit Persoonsgegevens (AP)*, which is under most Data Protection Laws which require the establishment of the supervisory authority, AP as the Authority Protection of Personal Data is subject to and based on the law in the GDPR, the General Data Protection Implementation Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming*) and several other regulations (Haganta, 2020).

4.1 Covid-19 Patient Privacy Data Protection In UE Countries

Dijkstra & de Ruijter explains that if the public health threat increases to a security threat, then public health interventions begin to resemble security interventions. The threat of COVID-19 certainly enters the realm of this threat. In this case, an emerging trend was identified in the EU context of public health "safeguards," leading to the integration of public health policy and public safety. The "Health Threat Decision" is a good example of public health securitization in the EU as it links EU public health and security policies. It has a wide range of applications, taking an "all-hazard approach" by defining threats of biological origin (such as infectious diseases), threats of chemical origin, and unknown threats of origin all as "serious cross-border threats to health." The decision, in this case, opens the door to bringing infectious disease devices from contact tracking to the realm of security. On contact tracking privacy restrictions, Greene explains that "In the COVID-19 crisis, member states and the EU have indeed turned to freedom restriction measures in the interests of public health protection. This lack of clarity for complex proportionality tests precludes consistent and high-level protection of the basic rights of individuals in EU (van Kolfschooten & de Ruijter, 2020).

Many, if not all, EU countries are currently working on apps aimed at facilitating the fight against the COVID-19 crisis. Some are based on geolocation, such as Coronamadrid and StopCovid19 in Spain, while others are based on Bluetooth technology known as 'digital handshakes', such as Stopp-CoronaApp in Austria, StopCovid in France, ProteGo in Poland, or apps being developed by the National Health Service ('NHS') in the UK (Bradford et al., 2020).

4.2 Covid-19 Patient Privacy Data Protection In UK Countries

With legal considerations in mind, there is no doubt that all existing tracking technologies have broad implications for people's privacy. The implications of "public health surveillance" have sparked a lot of attention among some scholars. In the UNITED Kingdom, more than 170 cybersecurity and privacy experts signed an open letter in April 2020, warning governments not to use centralized tracking apps for mass surveillance. What is not known, however, is how specific features of candidate technology affect people's attitudes, what safeguards can reduce privacy concerns, and how political views and risk perceptions determine views on actions that violate privacy (Id et al., 2021).

4.3 Covid-19 Patient Privacy Data Protection In US

Prior to the COVID-19 emergency declaration, blue cities preferred privacy over red cities. This is consistent with recent studies showing that Republicans care less about privacy than Democrats. Distance practices (higher number of contact quantiles) have a lower willingness to share location data (higher allowance rates) compared to blocks with better social distance practices. We also observed that in Virginia and San Francisco beaches, the opt-out rate trend remained relatively the same for people practicing lower social distances even after the declaration (Ghose et al., 2020).

In the United States, privacy advocates propose strict procedures for keeping personal information safe, including deletion, after data is no longer used to prevent abuse by law enforcement agencies. A typical use case that is sensitive to data privacy concerns is the use of information related only to visits to public facilities, including public transport systems, parks, churches, mosques, or malls, by COVID-19 positive individuals (Ekong et al., 2020).

4.4 Covid-19 Patient Privacy Data Protection In China and India

Tracking and tracing covid-19 patients in China and India has similarities, because it is inseparable from the consensus mechanism (CM) which is very important to achieve the unique advantages of blockchain. Commonly used CM include Proof of Work (PoW), Proof of Stake (PoS), and CM-based directed acyclic graphs (DAG). This can also be a challenge, where user privacy is at stake. By design, a more balanced weighting scheme in the coin age can solve such problems. Both PoW and PoS CM work on single chain architecture. To maintain a single version of the blockchain among users, CM must reduce the access level of new blocks. This can cause some bottlenecks in applying PoW and PoS CMs to a large number of participant contact tracking (Xu et al., 2020).

4.5 Covid-19 Patient Privacy Data Protection In Hongkong, Malaysia, and Singapore

Hong Kong already has the Personal Data Privacy Ordinance of 1995 (PDPO) as the first national legislation to comprehensively regulate privacy and personal data issues. The privacy of Malaysians' personal data is protected through The Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia). Meanwhile, Privacy and personal data in Singapore are sectorally protected by The Personal Data Protection Act No. 26 of 2012 Singapore (PDPA 2012 Singapore) (Dewi Rosadi & Gumelar Pratama, 2018).

Frequent misuse of personal data by the government and private parties, therefore, there is a need for accommodating laws and regulations that can provide guarantees and security of personal data so that the use of personal data can not be misused. Each country uses different terminology between personal information and personal data. However, substantively the two terms have almost the same definitions so that the two terms are often used interchangeably. For example, the United States, Canada, and Australia use the term personal information while the countries of the European Union, Malaysia and Indonesia itself in the ITE Law use the term personal data. This legal issue is very important because if a person's personal data is misused by a data provider or a third party, then this is contrary to the basic human right of protection of the privacy and personal data of a person who has been protected by international, regional and national instruments. Indonesia until now has not had regulations that specifically protect citizens from the practice of arbitrary use of personal data, whether carried out by governments, private companies or individuals¹. Currently, there is a draft of law about Personal

¹ Dewi, Sinta. (2009). CyberLaw: Protection of Privacy of Personal Information in E-Commerce According to International Law. *Widya Padjadjaran*

Data Protection (RUU PDP) in Indonesia. Hopefully, it will cover all of the privacy data problem especially in the disaster or non natural disaster situation.

5. Legal Securities Model Offer on Covid-19 Patient Data Privacy and implementation description

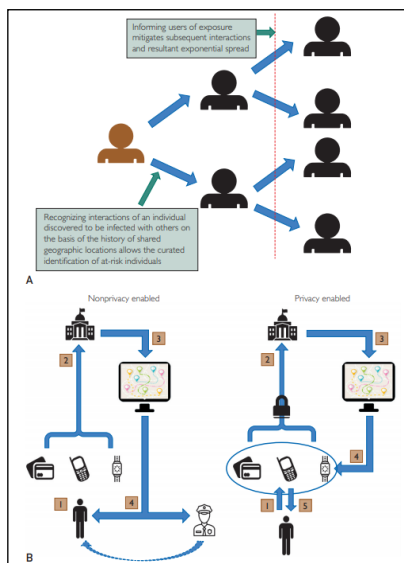
Philosophy and principles of privacy, principles of Anonymity / Pseudonymity Media development, both communication media and technology media is growing rapidly, even sometimes the data in the media does not have a name. Seeing the development of media, communication and technology can unite into a large entity. Privacy As a Right In its developmental history, privacy is a concept that is universal and known in various countries both written in the form of laws and not written in the form of moral rules. Pancasila's second principle, "A just and civilized humanity" is a philosophical foundation of personal data protection, this is given that the protection will create justice and form a human civilization that respects and respects personal data (Wulansari, 2018).

Based on these contemplations, a territorial direction that does not apply or reflect formal and material standards within the definition of a territorial control will not be canceled in the event that there's no loss or potential misfortune of a legitimate subject who submits an examination of territorial regulation. To guarantee compliance with these standards, an expectant step is required so that territorial regulation formulated by the competent educate stay steady in implementing the standards of the definition of legislation. Because the rule of law (in this setting the guideline of detailing of enactment) contains a measure of esteem and as it was indirectly provides rules, the guideline of law isn't always posited in the rule of law, then it gets to be troublesome to implemented within the run the show of law (Eka N.A.M. Sihombing, Eddy Purnama, Budiman Ginting, 2020).

The content of information containing medical records and personal data of non-medical covid-19 patients becomes excluded information is strict and limited to be published to the public. This data can only be opened with the permission of the owner or based on the order of the legislation, if anyone violates this provision can be penalized in accordance with the prevailing laws and regulations. Covid-19 positive patient medical data information should be protected and set aside to be disclosed to the public. A number of potential risks occur due to the opening of personal medical data to Persons In Monitoring (ODP), Patients In Surveillance (ODP), Positive Patients and Patients cured by parties who do not have competence to cause violations of individual human rights. The negative stigma embedded in the four types of subjects above is the carrier of the virus. So many of those who are expelled from the place of residence and Even for the dead get rejected when to be buried (Prananda, n.d.).

Such a privacy-first approach may still be met with skepticism but ideally will allow the implementation of tools to mitigate the current pandemic and

potentially future outbreaks. By enabling individuals to understand exposure history, to have full control over their data, and to share their data privately, it may be possible to balance privacy and public health. Contact Tracing and Personal Privacy:(Kapa et al., 2020)



Moreover, global instantaneous statistics could be made available to epidemiologists as well as precise people's covid infection status. From the privacy perspective, such an additional functionality would introduce the notion of "online tracking" (i.e., custodians will share in an ongoing manner their contacts or their location to a central database) as opposed to "offline tracking", the former being considered even more severe from a privacy standpoint. One could of course also envision supplementary (domain specific) activity for MCTA (e.g., for restaurants, beaches) (Zeinalipour-Yazti & Claramunt, 2020).

Discussions about the protection of personal data cannot be separated from the concept of privacy. The law has recognized the concept of privacy in relation to physical interference in the form of trespass (entering the yard of another person without permission) known in criminal law. In its development, the law also provides protection for human emotional and intellectual (Yuniarti, 2019).

According to Savigny, if the lawmakers want to formulate the law in technical juridical principles, then the legislators must remain positioned as organs of public awareness. Legislators are tasked with giving shape to what is found in raw materials. The raw material in the formation of law according to Savigny is the duty of legal scientists to provide it. While the legislators formulated technically in the form of formal rules (Muhammad Yusrizal Adi Syaputra, 2019). 3 (three) principles as referred to are important pillars in understanding the construction of statutory law in Indonesia in detail, it can be explained that: a) The principle of *lex superior de rogat lex inferior*, higher regulations will override lower regulation when regulating the same and conflicting substances; b) *As a lex specialist derogat lex generalis principle*, more specific rules

will override general rules when regulating the same and contradictory substances; c) The principle of *lex posterior de rogat lex priori*, the new regulation will override the old regulation (Sihombing, Eka N.A.M, 2019).

Providing protection of the right to privacy, means also providing protection of the right to free speech. For example, in a democratic society, it is important to maintain privacy in communication between communities, concerns about monitoring members of the public from irresponsible parties will result in inability to argue. Such circumstances can result in constructive ideas in the life of democracy cannot be voiced. That is, the right to privacy guarantees protection from the threat of fear to do or not do something that is a human right.(Cynthia Hadita, 9 C.E.)

Personal data should not be made public. It's our ethics in communication. The media must also respect their privacy. The offer of the model needed in Indonesia is strict protection of patient privacy data covid-19 because it is not currently in an *early warning* situation, because there is already a health protocol system that must be adhered to by all citizens, thus, for covid-19 patients must be protected data privacy so as not to negatively affect patients. So that in the future, the central and local governments do not unilaterally conduct press conferences or preach in print media related to covid-19 patient data in detail and complete that can be easily accessed and detected by the public that can negatively impact covid-19 patients on aspects of economic and social relations.

6. Conclusion

The personal data of Covid-19 patients based on the laws and regulations is a medical secret and the information is excluded in the public information disclosure service so that it must be kept confidential. There are several arrangements that provide opportunities to disclose the personal data of Covid-19 patients for the reasons set out in the legislation, but the disclosure of such data must be done strictly and limited based on purposive limitation principles, necessity principles, and proportionality principles, the dissemination of personal data of Covid-19 patients needs to be done with a minimalist pattern of data or the selection of the personal data part of Covid-19 patients that can be opened, namely the type of data that if opened, not until revealing the patient's personal secrets. Comparatively with some countries, that the EU, UK, US, China, India, Hongkong, Malaysia, and Singapore strictly maintain the privacy of covid-19 patients there are even countries that form a special commission to protect the personal data of covid-19 patients so it is necessary to consider the adoption or modification of the system against the protection of patient privacy data covid-19.

References

Books

- Ahmad Redi, I. S. C. (2020). *Segi Hukum Terhadap Implikasi Covid-19 di Indonesia*. Jakarta: Kencana.
- Ibrahim, J. E. and J. (2018). *Metode Penelitian Hukum (Normatif Dan Empiris)*. Jakarta: PrenadaMedia.
- Rianarizkiwati, N. (2020). *KEBEBASAN INFORMASI versus HAK ATAS PRIVASI, Tanggung Jawab Negara dalam Perlindungan Data Pribadi*. Depok: Infermia Publishing

Journal Articles

- Ardiyanti, H. (2020). Komunikasi Media Yang Efektif Pada Pandemi Covid-19. *Info Singkat: Kajian Singkat Terhadap Isu Aktual Dan Strategis Dpr Ri*. 7(7), 25–30.
- Ariany, F., & Ningsih, M. (2019). Perlindungan Hukum Terhadap Identitas Pasien Covid 19. *Journal of Chemical Information and Modeling*. 53(9). 1689–1699.
- Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps : a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*. 7(1). 1–21.
- Dewi Rosadi, S., & Gumelar Pratama, G. (2018). Urgensi Perlindungan data Privasi dalam Era Ekonomi Digital Di Indonesia. *Veritas et Justitia*. 4(1). 88–110.
- Ekong, I., Chukwu, E., & Chukwu, M. (2020). COVID-19 Mobile Positioning Data Contact Tracing and Patient Privacy Regulations: Exploratory Search of Global Response Strategies and the Use of Digital Tools in Nigeria. *JMIR Mhealth Uhealth*. 8. 1–7.
- Ghose, A., Li, B., Macha, M., Sun, C., & Foutz, N. Z. (2020). Trading Privacy for the Greater Social Good: How Did America React During COVID-19? *arXiv*.
- Hadita, Cynthia. (2018). Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia (Provision of Personal Information in Prepaid SIM Card Registration from Human Rights Perspective). *Jurnal HAM*. 9(2). 191-204.
- Haganta, R. (2020). Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic. *Lex Scientia Law Review*. 4(2). 77-90.
- Kapa, S., Halamka, J., & Raskar, R. (2020). Contact Tracing to Manage COVID-19 Spread – Balancing Personal Privacy and Public Health. *Mayo Clinic Proceedings*. 95(7). 1320–1322.
- Lewandowsky, S., Dennis, S., Perfors, A., Kashima, Y., White, J. P., Garrett, P., Little, D. R., & Yesilada, M. (2021). Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom. *PloS one*. 16(1). 1–23.
- Palupi Kurnianingrum, T. (2020). Pelindungan Data Pribadi: Dapatkah Hasil Tes Swab Rizieq Shihab Dibuka? *Info Singkat: Kajian Singkat Terhadap Isu Aktual Dan Strategis DPR RI*. 24(7). 1–6.

- Prananda, R. R. (2020). Batasan Hukum Keterbukaan Data Medis Pasien Pengidap Covid-19: Perlindungan Privasi VS Transparansi Informasi Publik. *Law, Development & Justice*. 3(1). 142-168.
- Sihombing, Eka N. A. M. (2019). Eksistensi Paralegal dalam Pemberian Bantuan Hukum bagi Masyarakat Miskin (The Existence of Paralegals in Providing Legal Aid to the Poor). *Jurnal Ilmiah Penegakan Hukum*, 6(1). 70-77.
- Sihombing, Eka N.A.M. & Hadita, Cynthia. (2019). Analisis Wacana Hukuman Pancung Di Provinsi Aceh. *Jurnal Legislasi Indonesia*, 16(4). 514-523.
- Sihombing, Eka N.A.M., Purnama, E., Ginting, B., F. A. N. (2020). The Regional Regulation Concerning Management of Zakat Viewed from The Principles of Formulation of Legislation. *International Journal of Advanced Science and Technology*. 29(6). 1098 - 1103.
- Syaputra, Muhammad Yusrizal Adi & Sintara, Dani. (2019). Revitalization of Malay Cultural Values in Regional Regulation of Spatial and Region in Medan City. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*. 2(3). 353-366.
- van Kolfschooten, H., & de Ruijter, A. (2020). COVID-19 and privacy in the European Union: A legal perspective on contact tracing. *Contemporary Security Policy*. 41(3). 478-491.
- Wulansari, E. M. (2018). Konsep Perlindungan Data Pribadi Sebagai Aspek Fundamental Normdalam Perlindungan Terhadap Hak Atas Privasi Seseorang Di Indonesia. *Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*. 5(1). 332-351.
- Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W. B., & Imran, M. A. (2020). BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and Beyond. *ArXiv*. 8(5). 3915-3929.
- Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*. 1(1), 147-154.
- Zeinalipour-Yazti, D., & Claramunt, C. (2020). COVID-19 Mobile Contact Tracing Apps (MCTA): A Digital Vaccine or a Privacy Demolition?. 1-4.

Website Material

- Hukum Online. (2020). *Kontroversi Kerahasiaan Data Pasien Covid-19, Advokat Ini Daftarkan Uji Materi ke MK*. Form <https://www.hukumonline.com/Kontroversi-Kerahasiaan-Data-Pasien-Covid-19-Advokat-Ini-Daftarkan-Uji-Materi-Ke-MK>.
- Kelurahan Ponjong. (2020). *Perlindungan Hukum Terhadap Identitas Pasien Covid-19*. From <https://www.ponjong.desa.id/>.
- Kompas.com. (2020). *Amnesty: Pengungkapan Data Pasien Virus Corona Langgar Hak Privasi*. From <https://nasional.kompas.com/>.
- Lembaga Studi & Advokasi Masyarakat. (2020). *Data Privasi Pasien Covid-19*. From <https://elsam.or.id/Perlu-Kesetimbangan-Perlindungan-Privasi-Dan-Kesehatan-Publik-Dalam-Penanganan-Covid-19/>.

- Penatausahaan Berkas Kasus Piutang Negara. (2020). Perlindungan Data Pribadi Pasien Covid-19 Menjadi Hak Privasi Konsumen. From <https://bpkn.go.id/posts/show/id/2020>.
- Soebroto, A. C. (n.d). *Kedudukan hukum peraturan/kebijakan dibawah peraturan menteri perencanaan pembangunan nasional/kepala bappenas*. 3, 1-15.
- The International Association of Privacy Professionals. (2020) *COVID-19 response and data protection law in the EU and US*. From <https://iapp.org/News/a/Covid-19-Response-and-Data-Protection-Law-in-the-Eu-and-Us/>.
- Tirto.id. (2020) *Jokowi Minta Privasi Pasien Positif Corona COVID-19 Dijaga*. From <https://tirto.id/jokowi-minta-privasi-pasien-positif-corona-covid-19-dijaga>