International Journal on Social Science, Economics and Art, 13 (4) (2024) 214-221

Published by: Institute of Computer Science (IOCS)

International Journal on Social Science, Economics and Art

Journal homepage: www. ijosea.isha.or.id

Juridical Analysis of Artificial Intelligence-Based Patient Personal Data Protection

Vera Dumonda Silitonga [1], Sidhi Laksono [2]

[1] Akademi Kesehatan Gigi Pusat Kesehatan Angkatan Darat (PUSKESAD)., STHM, Indonesia

[2] Rumah Sakit Jantung Diagram, Indonesia

Article Info

Article history:

Received: Jan 15, 2024
Revised: Feb 17, 2024
Accepted: Feb 28, 2024

Keywords:

Privacy Infringement;
Artificial Intelligence;
Personal Data Protection;
Hospital Law.

ABSTRACT

Confidentiality of patient personal data is also a patient's right which is regulated in Law number 29 of 2004 and Law number 44 of 2009. Along with the development of technology, some loopholes can be exploited by cybercrime perpetrators. in general, they use malware programs to hack the target's computer system. The Information and Electronic Transactions Law (UU ITE) articles 30 and 31 regulate illegal access to systems belonging to other people or the public. Articles 32 and 34 also regulate illegal access and transactions with electronic documents owned by other people or the public. Violators can be charged using article 48 of the ITE Law. To date, no law specifically regulates the crime of hacking using malware on artificial intelligence technology used in hospitals. This research method is normative juridical with descriptive research methods. The specific legal basis (lex specialis) that regulates the protection of patient personal data concerning the illegal buying and selling of patient data (information business and electronic technology) that uses AI does not yet exist in the law, the closest thing is Article 67 of the Personal Data Protection Law in a general context. In this case, it can result in a legal vacuum, legal uncertainty or uncertainty about statutory regulations, or legal chaos.

Corresponding Author:

Vera Dumonda Silitonga,
Akademi Kesehatan Gigi Pusat Kesehatan Angkatan Darat (PUSKESAD)., STHM,
Indonesia.
Email: veradumonda966@gmail.com

1. INTRODUCTION

The protection of people's data by the government is formulated in the 1945 Constitution (UUD) Article 28 F, namely that every person has the right to communicate and obtain information to develop their personal and social environment, and has the right to seek, obtain, own, store, process and convey information by using all types of channels available. Advances in science and technology (IPTEK) in the medical field with artificial intelligence technology (AI) aim to improve the quality of health services in hospitals, increasingly being used as a private hospital business (Davenport & Kalakota, 2019). AI technology has the potential to transform many aspects of patient care, as well as administrative processes in healthcare providers, payers, and pharmaceutical organizations (Morley & Floridi, 2020). AI technology can also help health practitioners treat disease and track the success of preventative and intervention measures. AI technology, especially machine learning, can change and

reform health services. People responsible for making policies, legislators, and other decision makers must be aware of the changes that the implementation of AI technology can bring and create rules to regulate them. Computing to describe the capacity of computer programs to carry out tasks related to human intelligence, such as reasoning and learning is a term from AI7, including processes such as adaptation, sensory understanding, and interaction (Miller & Brown, 2018). Thus, AI is able to change its own algorithms based on the data obtained, and is able to develop and adapt based on the exposure it receives.

Some of the unique characteristics that AI has in analyzing are accountability and responsibility so that it is different from traditional health technology (Smith, 2020). In particular, this technology is susceptible to certain types of errors and biases, and sometimes cannot be easily removed or even need to be supervised by professional medical personnel. Many hospitals in Indonesia are currently using artificial intelligence in running their health services. , one of which is the Diagram Heart Hospital. Diagram Heart Hospital uses big data in computing patient personal data that will be used by doctors. Patients can use the hospital application which is integrated with other services such as doctor's schedules, laboratories, radiology, teleconsultations with doctors. When registering for the hospital application, patients are required to fill in their data first, such as entering their name, age, gender, name of parents/guarantor, and identity card. Law Number 44 of 2009 concerning Hospitals (UURS) article 32 letter i regulates that every patient has the right to the confidentiality of their personal information, including the patient's medical records. also states that every patient has the right to privacy and confidentiality regarding their illness and their medical data. According to Law Number 36 of 2009 concerning Health (UUK), Article 57 paragraph (1) reads: 14 "Every person has the right to the confidentiality of his health condition which has been disclosed to health service providers".

Provisions in the formulation of Law no. 27 of 2022 concerning Personal Data Protection, Article 1 number 1 reads: 15 "Personal Data is data about natural persons who are identified or can be identified individually or in combination with other information, either directly or indirectly through electronic or non-electronic systems". There are differences between general and specific personal data. General personal data includes full name, gender, citizenship status, marital status, religion, and/or personal data combined to identify a person. Meanwhile, examples of specific forms of personal data are Health information, life and sexual orientation, crime records, child data, political views, and other data regulated by law. The health sector is not immune from cybercrime, where the impact of crime in the health sector in cyberspace is very worrying, crime Selling patient personal data to third parties is a cyber crime that has very serious consequences and can significantly affect the health sector. Therefore, it is necessary to understand the various types of internet crime and it is important to note the impact they have on the health sector. Contributing factors are the extensive use of technology, patient records, and involvement in the medical field. Research conducted before Law No. 27 of 2022 concerning Personal Data Protection (PDP) was passed, there was a legal vacuum regarding the protection of personal data, especially in cybercrime (Novita & Santoso, 2021). There are even inconsistencies between regulations, so it is important to push for more specific laws for the protection of personal data.

2. RESEARCH METHOD

This research method uses a normative juridical research method (legal research) to find the truth of coherence, whether there are legal rules per legal norms and whether there are norms in the form of orders or prohibitions per legal principles, as well as whether a person's actions are under legal norms (not just according to law) or legal principles (Soekidjo, 2010). This research is descriptive and perspective research. Descriptive analysis research is an explanation and aims to provide a detailed, clear, systematic picture which as a whole concerns all problems related to the object of the thesis which will be researched by the author, applies in a certain place and at a certain time, or concerns existing juridical problems and related to legal events that occur in society, this problem is related to the protection of patient personal data in health services using artificial intelligence in hospitals

(Benni, 2009). The prescriptive analysis research that the author conducted has the aim of obtaining legal advice and legal rules that apply in society or whether there are no legal rules that regulate this research, due to the phenomena that occur in society, in the future there must be protection of personal data health (patients) in artificial intelligence-based health services (Zainuddin, 2011).

The approaches to this research are the Legislative Approach, Conceptual Approach, and Limited Empirical Approach. The Legislative Approach is a method applied in all laws relating to the protection of personal data, especially for patients receiving AI-based health care in hospitals. The Conceptual Approach uses a conceptual approach where researchers do not deviate from existing legal regulations. This was done because the issues discussed do not yet have or do not have legal regulations, especially the protection of patient personal data in AI health services. A limited empirical approach was carried out with direct interviews with sources who understand, master and indeed have expertise in legal regulations regarding the personal data of patients who provide AI-based health services.

The primary data for this research was obtained by conducting interviews with key informants who are experts in law regarding the relationship between information technology and health. Meanwhile, secondary data comes from literature and legal materials related to the main problem of this research. This secondary data consists of the legal basis (UUD 1945 Article 1 paragraph 3, 28 C paragraph 1, 28 F paragraph 4, 28 G paragraph 1, 31 paragraph 5; Law no 44 of 2009 concerning Hospitals Article 32 letter i; Law no 17 of 2023 concerning Health Article 57 paragraph 1; Law no 27 of 2022 concerning Protection of Personal Data, Article 1 paragraph 1, paragraph 2; Law no 11 of 2008 concerning Electronic Information and Transactions, Article 32 paragraph 1; Law no 8 of 1999 concerning Consumer Protection. Secondary legal materials come from legal materials that explain primary legal materials such as legal books, books about health, journals, theses, theses, legal dissertation or health law dissertation, including the latest information and not hoaxes circulating in online media. Tertiary legal materials come from legal materials that explain primary legal materials and secondary legal materials, which include the Dutch-Indonesian Law Dictionary, Medical Dictionary, Dictionary English Indonesian. Processing research data qualitatively, because it is easier to adapt and can be presented about matters related to juridical concepts and those that will be studied directly. This makes this research method sharper towards the value patterns that occur (Asikin, 2012).

3. RESULTS AND DISCUSSIONS

Insecurity of consumer data protection in the eHealth sector, “data breaches” can occur due to “carelessness” or “bad faith” on the part of service providers. Thus, bad faith behavior can intentionally process data for illegal commercial purposes, either by processing it or by collaborating with other parties who use the data. Meanwhile, "data theft" is caused by "illegal access" activities carried out by perpetrators, causing data to be changed, damaged and deleted. The absence of a specific legal basis (lex specialist) in protecting patient data using artificial intelligence application-based health facilities requires service providers to create "self-regulation" (Edy & Andriana, 2023). Therefore, Law no. 11 of 2008 concerning Information and Electronic Transactions, and its amendments to Law no. 19 of 2016 is a form of regulation for the development and progress of information technology in Indonesia (Bambang, 2012). Not only that, it is a crime (cybercrime) that has the potential to be carried out easily and effectively by taking advantage of developments in technology and information, also in the data and information management sector, especially in the management of personal data that requires data protection. Because with advances in information and communication technology, the boundaries of privacy are getting thinner so that various personal data is easier to spread (Normand, 2023). Personal data protection is related to the concept of privacy which requires protection for its confidentiality. Warren and Brandeis were figures who put forward the concept of privacy for the first time in a scientific journal entitled "The Right to Privacy" which means the right not to be disturbed. In the journal, it is said that every person carrying out activities has the right to have their privacy protected (Latumahina, 2014). This is also following the contents of the ITE Law article 32 paragraphs 1 to 3.

In this case, patients as individuals can be harmed and can sue according to the Criminal Code (KUHP) and Civil Code (KUHPer). Under Lex specialis derogat legi generalis (specific laws override laws of a specific nature and/or electronic documents that violate decency, gambling, insults and/or defamation, as well as extortion and/or threats, as regulated in Article 27 of the ITE Law paragraphs 1 to 4. In this case, the patient as an individual can be harmed and can sue by the Criminal Code (KUHP) and Civil Code (KUHPer). Under Lex specialis derogat legi generalis (specific laws override general laws), the Personal Data Protection Law (PDP) and ITE which are lex specialis (specific) take precedence over the Criminal Code and the Criminal Code which are lex generali (general) so that demands will be adjusted to the PDP and ITE Laws.

3.1. Implementation of Legislation on the Protection of Patient Personal Data in Health Services Using AI in Heart Hospitals Diagram

Siloam Diagram Heart Hospital (RSJD) is located on Jl. Cinere Raya No.19, Pangkalan Jati, Kec. Cinere, Depok City, West Java 16514. This is a type B hospital with dr. Hoyi Siantoresmi MARS, 75 beds, focuses on heart health services. It has emergency facilities, blood laboratory, radiology services (thoracic photo, ultrasonography, CT scan, transthoracic and transesophageal echocardiography), cardiac catheterization laboratory, cardiac surgery room, semi-intensive and intensive care units and ordinary care rooms (Walskaar et al., 2023). RSJD collaborates with the Heart Center Isala Klinieken, Zwolle, Netherlands, and Radboud University Medical Center Nijmegen, Netherlands, which already have an international reputation in the fields of service, research and education. In addition, RSJD will collaborate with many service centers and educational institutions in Indonesia to achieve greater synergy and cooperation.

RSJD has a digital-based service application that follows the Siloam group, namely mySiloam. The mySiloam application stores patient personal data, both general and specific. Contains services for doctor's appointments (doctor's video call, doctor's chat), lab examinations, radiology, medical check-ups, hospital information, emergency, homecare, or COVID-19 examinations. Artificial intelligence (AI) applied to health services at Diagram Heart Hospital can have problems in terms of leakage of patient personal data. Thus, research results were obtained regarding the implementation of personal data protection for patients who use AI-based health services at RSJD.

3.2. Interview Results

Through the mySiloam application, patients download the application on their cell phone and enter the patient's data, either general or specific. This personal data can be leaked and traded in electronic transactions. So researchers find out about AI-based applications in their implementation of protecting patient personal data by conducting normative juridical research by collecting primary and secondary data (interviews with key informants). Secondary data collection for interviews was carried out using 3 key informants who have a relationship in AI-based patient data protection, in this case the mySiloam application. The informants were from the information communications technology section, the hospital ethics and legal committee and the hospital administration section. Interviews were conducted in a quiet room and took place according to the questions asked. Key informants provide responses and answers according to their knowledge. The three key informants gave similar or the same answers, starting from the form of the mySiloam application service, patient personal data contained and stored in the mySiloam application, personal data in the form of general and specific laboratory results or procedures, regarding security which is quite safe because so far it has not been there is a leak, in the application there are Standard Operating Procedures (SPO).

3.3. RSJD Standard Operational Procedures Relating to AI-Based Patient Personal Data Protection

Policy regulations (beleidsregel) are essentially the product of organs, bodies or administrative officials based on the use of the free authority (freies Ermessen) they have in the context of implementing public interests (bestuurszorg). This Standard Operating Procedure (SPO) is a form of legal product.

RSJD's SPO relating to the protection of patient personal data based on the AI-based mySiloam application is regulated in the information and communication technology section. There are 31 SPOs contained in ICT and only 5 SPOs relate to the protection of patient personal data. These SPOs are handling security incidents, managing periodic user access activities, penetration testing, managing security risks, and managing security gaps. RSJD ICT also has a hospital unit information technology management policy.

SPO for Handling Security Incidents with no. SPO-SHG-ICT-021, 2 pages, with the content that a security incident is an operational incident involving the use of information that can result in a decrease in system integrity, disruption of availability and disclosure of information confidentiality. Meanwhile, the effort carried out is containment, which is an action in handling security incidents where hosts suspected of experiencing a security incident are localized and disconnected from the network to limit the spread of the action. Any incident can be reported by all users by creating a ticket in the helpdesk or manually filling in the security incident form. Included in the security incident report are database hacked, RansomWare, email compromised, user account compromised, denial of service (DoS), unauthorized use/disclosure, unauthorized access, unplanned downtime, or laptop loss/theft. The ICT security team will carry out an analysis of entry tickets and ensure returns are related to the incident and carry out localization (containment) actions.

SPO Management of Periodic Access User Activities, no SPO-SHG-ICT-032, 2 pages, contains a clear understanding of the process for managing periodic user access checks, as well as providing information on the authority and responsibilities of each party in the process of managing user checks Regular access and user checking process is carried out every 3 months. SPO Penetration Testing, no SPO-SHG-ICT-046, 2 pages, is used to ensure the system is safe from hacker attack bugs and becomes standard for the system before going live. A penetration test is a security testing activity that aims to ensure a system is safe from gaps or bugs that can be exploited by hackers. All applications that will go live or are already running must be informed to the IT security department for regular testing. The pentester will provide a sign in the form of a safe digital certificate.

SPO Management of Security Gaps, SPO-SHG-ICT-016, 5 pages, to guide the information security team and infrastructure team in managing security gaps (vulnerabilities), patching and hardening. The team assesses security gaps by carrying out vulnerability scanning using predetermined tools/scripts periodically every month, as well as monitoring security patching information from patch management. The security team collaborates with the infrastructure team to implement mitigation action plans according to the reports made. Implementation of the action plan is carried out based on a priority scale.

SPO Information Security Risk Management, SPO-SHG-ICT-017, 5 pages, is useful for guiding risk management activities in IT, which include risk identification, risk assessment, risk prioritization and risk mitigation plans. Prepare a mitigation plan/risk treatment plan, action plan and identify the parties involved in it. IT internal audit monitors and reviews each identified risk and its treatment process. The mySiloam application can access patient data from location, camera, gallery and folders, calendar, microphone and Bluetooth. This application contains patient personal data, both general and specific, so when registering patients must read the terms and conditions and privacy policy. From the terms and conditions of this application there is a clause that the hospital is not responsible for theft of patient data (no guarantee), so the hospital will not be blamed for the act of data theft.

3.4. AI-Based Juridical Analysis of Patient Data Protection

The confidentiality of patient data is under Law Number 14 of 2008 concerning Openness of Public Information. Protection of personal identity is guaranteed in Article 29G of the 1945 Constitution of the Republic of Indonesia. Every patient has the right to privacy and confidentiality of the disease they are suffering from, including their medical data. This is regulated in Article 32 letter i of Law Number 44 of 2009 concerning Hospitals (UU 44/2009). Concerning patient rights and hospital obligations, every hospital must keep medical secrets, which can only be disclosed in the interests of the patient's

health, to fulfill requests from law enforcement officials in the context of law enforcement, with the patient's consent, or based on the provisions of statutory regulations (Art. 38 paragraphs (1) and (2) Law 44/2009). The urgency of protecting personal data can be seen from the protection of personal data as part of human rights regulated in Article 12 of the Universal Declaration of Human Rights (UDHR) which provides a legal basis for member countries in terms of the state's obligation to protect and respect personal rights. individual citizens of their respective countries. Apart from that, in the International Covenant for Civil and Political Protection or International Covenant on Civil and Political Rights (ICCPR). This convention was born on 16 December 1966 through Resolution 2200 A and has been in effect since 23 March 1976. This international legal instrument provides more explicit protection for human personal rights. Article 17 paragraph (1) of the ICCPR states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence or unlawful attacks on his honor and reputation, everyone has the right to legal protection against such interference or attacks. Protection of personal data is part of respecting the right to privacy and must begin with providing legal certainty. Therefore, the guarantee for the protection of data privacy must be placed in a legal instrument that has the highest power, namely the constitution, because the Basic Law or Constitution is the highest legal instrument in a country. Legal certainty (the principle of legality) is necessary and cannot be ruled out in the context of law enforcement by every country. The state's step in providing legal certainty is by establishing and guaranteeing these rights in the constitution, so through this instrument the character of a country can be seen in terms of what is put forward, what legal system is used and how the government is organized (Rudi & Stefany, 2019).

According to Philipus (1987), legal protection is the protection of honor and dignity, as well as recognition of human rights possessed by legal subjects based on legal provisions against arbitrariness or as a collection of rules or rules that will be able to protect one thing from another. Concerning consumers, this means that the law protects customer rights from something that results in non-fulfillment of these rights. Regulatory efforts related to the right to privacy over personal data are a manifestation of the recognition and protection of basic human rights. Therefore, laws and regulations relating to personal data have a strong philosophical basis and can be accounted for. Rudolf Stamler stated that legal ideals are useful as leitsern (guiding stars) in realizing society's ideals. From this legal ideal, legal understanding and politics in the state are created. The legal ideal is normative and constitutive. Normative means functioning as a transcendental prerequisite which is the basis of dignified positive law, as well as being the basis of legal ethics and also the benchmark for the positive legal system. A constitutive legal ideal means that rechtsidee has the function of directing the law to the goals to be achieved. Gustaf Radbruch stated that legal ideals function as a constitutive basis for positive law, giving meaning to law. Rechtsidee is a regulatory benchmark, namely testing whether positive law is fair or not. Legal ideals will influence and function as general principles that provide guidance, norms of criticism (evaluation rules), and motivating factors in the administration of law (formation, discovery, application of law and legal behavior)(Gunawan & Kristian, 2015).

Confidentiality of personal data is every person's human right. Article 1 number 1 and 2 of the Minister of Communication and Information Technology Regulation no. 20 of 2016 concerning Protection of Personal Data in Electronic Systems states that personal data is intended as a clear and clear identity of a person which is a determination of personal evidence about him that is maintained, kept true and kept securely and confidentially. Meanwhile, Article 2 number 1 regulates the acquisition, collection, processing, analysis, storage, display, announcement, sending, dissemination and destruction of personal data, which constitutes the protection of personal data in an electronic system that respects personal data as privacy. Article 1 number 27 Government Regulation no. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions, defines personal data as certain individual data that is stored and maintained as correct and protected as confidential. People who cause harm to other people can be sued as long as the harm is the result of a violation of a norm (an act that violates the law) and the perpetrator can be regretted for violating that norm (a mistake). The person can be held legally responsible as long as they fulfill 4 (four) elements, namely the existence of an act, the existence of an element of error, the existence of a loss and the existence of a causal

relationship between the error and the loss. Cases related to theft of patient personal data can refer to more specific laws (Lex Specialis) such as the Law on Health, Hospitals, Medical Practices, Electronic Information and Transactions and Personal Data Protection based on "lex specialis derogat lege generali".

In the doctor-patient relationship, a therapeutic transaction occurs which is an inspirational agreement between the doctor and the patient, and both parties must carry out their respective rights and obligations. Patients as consumers who receive services (Anggra, 2021), have rights as regulated in Article 4, Law Number 8 of 1999 concerning Consumer Protection, which reads: "consumer rights are: the right to comfort, security and safety in consuming goods and/or services; the right to choose goods and/or services and obtain said goods and/or services in accordance with the exchange rate and conditions and guarantees promised; the right to correct, clear and honest information regarding the condition and guarantee of goods and/or services; the right to have opinions and complaints heard regarding the goods and/or services used; the right to obtain appropriate advocacy, protection and efforts to resolve consumer protection disputes; the right to receive consumer guidance and education; the right to be treated or served correctly and honestly and not in a discriminatory manner; the right to receive compensation, compensation and/or replacement, if the goods and/or services received are not in accordance with the agreement or are not as they should be; rights regulated in other statutory provisions." This right is further clarified in article 32 of Law no. 44 of 2009 concerning Hospitals, where patients have the right to obtain quality health services by professional standards and standard operational procedures, obtain effective and efficient services so that patients avoid physical and material harm and obtain privacy and confidentiality of the disease they are suffering from, including medical data.

Technological advances in the health sector have shifted the storage of patient data from physical form to electronic form. Personal data stored in electronic form will be vulnerable to computer crime (cybercrime). Cybercrime is described as a crime committed in online media using computers as the main medium for searching for targets/victims. This crime is growing in parallel with the rapid use of the Internet, especially in developing countries. This crime is not much different from the concept of ordinary crime, however, cybercrime perpetrators exploit differences across countries to prevent, detect, investigate and prosecute these crimes (Alfiyan & Dian, 2022). Law as a tool of social reform (a tool of social engineering) must be able to provide a way for developments that occur in society, especially in technological developments. For this reason, the regulation of technology transfer as a benchmark for the progress of poor and developing countries must be regulated in a separate legal manner. Cybercrime perpetrators want to access someone's data to use for the perpetrator's interests. 95 This causes losses to the victim and on this basis, the perpetrator can be sued by Article 1365 of the Civil Code. However, various kinds of obstacles will be faced in dealing with cybercrime, for example difficulties in tracking down the main perpetrators and proving them, difficulties in handling them, etc.

4. CONCLUSION

The specific legal basis (lex specialis) that regulates the protection of patient personal data in relation to the illegal buying and selling of patient data (information business and electronic technology) that uses AI does not yet exist in the law, the closest ones are the Personal Data Protection Law and the Information and Electronic Transactions Law in the context of general. In this case, it can result in a legal vacuum, legal uncertainty or uncertainty about statutory regulations, or legal chaos. Legal implementation of patient personal data in AI-based health services at the Heart Hospital. There is no diagram for legal certainty for patients. If RSJD carries out preventive measures according to the standards determined by law for preventing cybercrime, the mySiloam AI-based application is not responsible for the theft of personal data in the application.

REFERENCES

Alfiyan, U., & Dian, A. S. (2022). *Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19*. Unisba Press.

Anggra, Y. R. (2021). Perlindungan Hak Pasien Sebagai Konsumen Untuk Mendapatkan Isi Rekam Medis Dalam Pelayanan Kesehatan. *Jurnal Surya Kencana Satu Dinamika Masalah Hukum Dan Keadilan*, *12*(2).

Asikin, Z. (2012). *Pengantar Tata Hukum Indonesia*. Rajawali Press.

Benni, A. S. (2009). *Metode Penelitian Hukum*. Pustaka Setia.

Davenport, T., & Kalakota, R. (2019). *The potential for artificial intelligence in healthcare*. Future Healthc J.

Edy, S., & Andriana. (2023). Ketidakamanan perlindungan data konsumen di sektor eHealth. *Jurnal Penelitian Hukum De Yure*, *23*(1), 115–130.

Gunawan, Y., & Kristian. (2015). *Perkembangan Konsep Negara Hukum Dan Negara Hukum Pancasila*. Refika Aditama.

Latumahina, R. E. (2014). *Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya*. Gema Aktualita.

Miller, D. D., & Brown, E. W. (2018). Artificial Intelligence in Medical Practice: The Question to the Answer? *Am J Med* , *131*(2), 129–133.

Morley, J., & Floridi, L. (2020). An ethically mindful approach to AI for health care. *The Lancet Journal*, *395*(10220), 254–255.

Normand, E. E. (2023, October 19). *Perlindungan Data Pribadi Tersebar Di 32 UU. Indonesia Perlu Regulasi Khusus*. Www.Hukumonline.Com.

Novita, Y. D., & Santoso, B. (2021). Urgensi Pembaharuan Regulasi Perlindungan Konsumen di Era Bisnis Digital. *Jurnal Pembangunan Hukum Indonesia*, *3*(1), 46–58.

Rudi, N., & Stefany, M. (2019). *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*. LPPM.

Smith, H. (2020). Clinical AI: opacity, accountability, responsibility and liability. *AI & SOCIETY*, *36*, 535–545.

Soekidjo, N. (2010). *Metodologi Penelitian Kesehatan*. Rineka Cipta.

Walskaar, I., Tran, M. C., & Catak, F. O. (2023). *A Practical Implementation of Medical Privacy-Preserving Federated Learning Using Multi-Key Homomorphic Encryption and Flower Framework*. Cryptography.

Zainuddin, A. (2011). *Metode Penelitian Hukum*. Sinar Grafika.