International Journal of Law Dynamics Review
Volume 3, Number 1, May 2025
Online ISSN: 2987-7075
DOI: 10.62039/ijldr.v3i1.80

HUMAN RIGHTS AND CYBERSECURITY: REINFORCING LEGAL PROTECTIONS FOR PERSONAL DATA

Siti Rahmadani*
Universitas Duta Bangsa, Surakarta, Central Java, Indonesia
Email: ramadanisiti2020@gmail.com

Rina Arum Prastyanti
Universitas Duta Bangsa, Surakarta, Central Java, Indonesia
Email: Rina_arum@udb.ac.id

Article info

Keywords:
Human Rights,
Legal Certainty,
Personal Data Protection,
Privacy Law

Abstract

In light of international law and the challenges posed by the digital age, this study examines the protection of personal data as a fundamental human right. The protection of personal data is recognized as a form of human rights protection in several legal documents, including the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights. Human rights are universal rights that are inherent in every individual. To examine the regulation of personal data protection and its consequences for human rights, this study employs a normative juridical approach with an analytical descriptive nature. The findings demonstrate that, despite laws protecting personal information, problems such as invasions of privacy, a lack of public awareness, and lax law enforcement remain serious issues. To establish a secure framework, governments, the private sector, and society must work together. The state's role in ensuring legal certainty and safeguarding the right to personal data through effective legislation was also highlighted. The protection of personal data should be a top concern in the digital age to respect the privacy and dignity of individuals, as well as to increase public trust in institutions and companies.

Page: 20-29

* Corresponding Author.

Article history:
Received: January 15, 2025; Received in revised form: March 1, 2025; Available online: May 24, 2025.

Introduction

Human Rights are rights that every individual has naturally and are universal and eternal. For a country, human rights serve as a basis for drafting regulations that govern the life of the community and the nation (Marelli, 2023). One form of human rights protection is the protection of personal data, which is recognized as a human right in various countries, including

in Article 8: Protection of personal data by the European Union Charter of Fundamental Rights Human Rights (*EU Charter of Fundamental Rights*, 2021), EU General Data Protection Regulation (GDPR) (*General Data Protection Regulation (GDPR) – Legal Text*, n.d.) and Article 21 the Association of Southeast Asian Nations (ASEAN) Human Rights Declaration (Naldi & Magliveras, 2014). The Universal Declaration of Human Rights (UDHR 1948), created in 1948, finally recognized the right to protect personal data as part of human rights after a long evolutionary process, in which this right arose from a combination of the right to privacy and the right to information (Mantelero, 2018).

Personal data is legitimate and genuine information that is connected to a person so that it can identify that individual (Kun, 2025). The protection of personal data is important to ensure that the information obtained by individuals is used for the purposes for which it was collected, to prevent misuse of data. The right to privacy must be protected by the state (Pangrazio & Bunn, 2024), which includes the protection of personal information in such a way that it cannot be accessed, used, or disclosed without the consent of the individual concerned. When such information is not properly protected, the risk of human rights violations increases, ranging from illegal surveillance, and information collection for political or economic interests, to discrimination based on the information in its possession (Ye et al., 2024). The protection of personal data is the right of individuals, groups, or organizations to have protection for their data, as well as to provide excuses in case of errors in the data. Data privacy protection is not just a technical issue, but also part of legal protection for citizens (Kumalaratri & Yunanto, 2021). In international law, the right to privacy is guaranteed in Article 12 of the Universal Declaration of Human Rights, which states that no one has the right to interfere in matters of privacy, family, residence, or personal communication. This is also reinforced in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which obliges states to provide legal protection against unlawful invasions of privacy.

The state's position on privacy protection as the right of all and every citizen is very clear. This is stated in the Preamble to Human Rights Law Number 39 of 1999, which states in the fourth point: "As a member of the United Nations, the Indonesian people have moral and legal responsibilities, namely the Universal Declaration of Human Rights. Rights created by the United Nations to be observed and exercised, and other rights related to human rights accepted by the Republic of Indonesia. Various international documents. Therefore, the state as a government organizer is responsible for the citizens under its control, who are solely responsible for taking care of them, according to international law (Mahieu et al., 2019), responsible for the right to a healthy environment due to climate change Conceptually, the state is the only party that should be responsible for protecting human rights. Regarding personal rights as human rights, the protection of personal rights or personal rights will increase human values, improve the relationship between individuals and their communities, increase independence or autonomy to control and obtain conformity, as well as increase tolerance and distance from discrimination and limit government power (Shehu & Shehu, 2023).

In the ever-evolving digital era, personal data has become one of the most valuable assets in modern society. Violation of privacy rights exists not only in online activities but also in offline activities. Some violations of online activation rights can be in the form of large-scale personal data collection (digital dossier), direct marketing (direct-selling), social media, the implementation of the e-KTP program, e-health, and cloud computing activities (Kumalaratri & Yunanto, 2021). With the advancement of information and communication technology, the process of collecting, storing, and processing personal data has become easier and faster. However, behind this convenience, there are major challenges related to personal data protection that must be faced. The importance of personal data as a human right cannot be

ignored, as the right to privacy and data protection is an inseparable part of the dignity and freedom of the individual. The right to personal data has been widely recognized in various international legal instruments. For instance, everyone has the right to legal recognition and protection from rights violations, according to the 1948 United Nations Universal Declaration of Human Rights. Furthermore, the International Covenant on Civil and Political Rights highlights how crucial it is to safeguard people's privacy. Everyone in this situation has the right to be in charge of their personal data and is shielded from abuse or unapproved disclosure.

The protection of personal data as a human right is covered in greater detail in this study. The development of personal data protection arrangements and personal data protection from a human rights perspective are the topics of this study. This theme has been covered in some earlier research, and Indonesia has laws and regulations protecting the privacy of personal data, but there are still some barriers, including a lack of understanding of the significance of data privacy, uneven enforcement of the law, and the need for a more thorough legal framework that is adaptable to new technology. Public knowledge of personal information To adapt to the evolving digital age, policies must be modified, law enforcement must be bolstered, and privacy rights must be expanded. Furthermore, creating a secure and reliable environment requires the active involvement of all governments, corporations, and civil society (Muzairoh et al., 2024; Parihin, 2023). It is crucial to note that Article 25 of Law No. 27 of 2022 does not expressly regulate the procedures and types of legal protection for children who are the victims of data misuse. To ensure the protection of children's data, Indonesia must be able to learn from nations in the European Union, the United Kingdom, and the United States (Rohmansyah et al., 2023). Ultimately, Indonesia should have the ability to enact comprehensive legislation based on human rights. This will provide legal certainty on personal data protection and a clear mechanism for law enforcement collaboration. In this regard, the researcher suggests that a law regulating criminal sanctions and their enforcement as a preventive measure be created. In addition, the current laws on personal data protection should be amended and rebuilt (Situmeang, 2021).

Research Method

A normative juridical approach is used in this study (Nurhayati et al., 2021). Research that employs a positivist understanding of legis is known as normative juridical research. According to this theory, written standards created and issued by sanctioned organizations or officials are the same as laws. The purpose of this study is to examine personal data protection and personal data protection from the standpoint of human rights. This study is both analytical and descriptive. Research that describes, investigates, clarifies, and evaluates legal regulations is known as descriptive-analytical research. The rule of law in this study can be suitably described and examined by the study's objectives by employing this descriptive nature. The information used comes from books and journals that are pertinent.

Results and Discussions

The Role of the State and Society in Ensuring the Protection of Digital Rights

Urgency can be interpreted as an obligation or interest that is urgent and must be carried out immediately to realize something so that the matter can be interpreted effectively. The urgency in the protection of personal data can be seen from the existence of personal data protection as part of human rights regulated in Article 12 of the Universal Declaration of Human Rights which provides a legal basis for its member states in terms of the state's obligation to

protect and respect the privacy rights of their respective citizens. In addition, in the International Covenant on Civil and Political Rights (ICCPR). This convention was born on December 16, 1966, through Resolution 2200 A and entered into force on March 23, 1976. These international legal instruments provide more explicit protection of human personal rights. Article 17 paragraph (1) of the ICCPR states that no person shall be subjected to arbitrary or unlawful interference with his/her privacy, family, home, or correspondence or unlawful attacks on his/her honor and reputation, everyone shall have the right to legal protection against such interference or attack. Internationally recognized principles of privacy and personal data. These principles are the basis for modern national data protection laws. One of the international instruments that protects privacy and personal data is issued by the Organization for Economic Co-operation and Development (OECD). In addition, the Council of Europe (CoE) adopted the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1950 (*European Convention on Human Rights*, 1950).

23.0 billion email accounts have been hacked since 2004. About 7.7 billion of them have unique email addresses (*Data Breach Statistics Globally*, 2025). In the ASEAN region, Vietnam is the country with the most data leaks in 2024 with 37,608,041 email account data breached. The Philippines came second with 23,970,155 email account breaches, and Indonesia came third with 21,769,496 email account breaches (*Data Breach Statistics in 2024*, 2025).

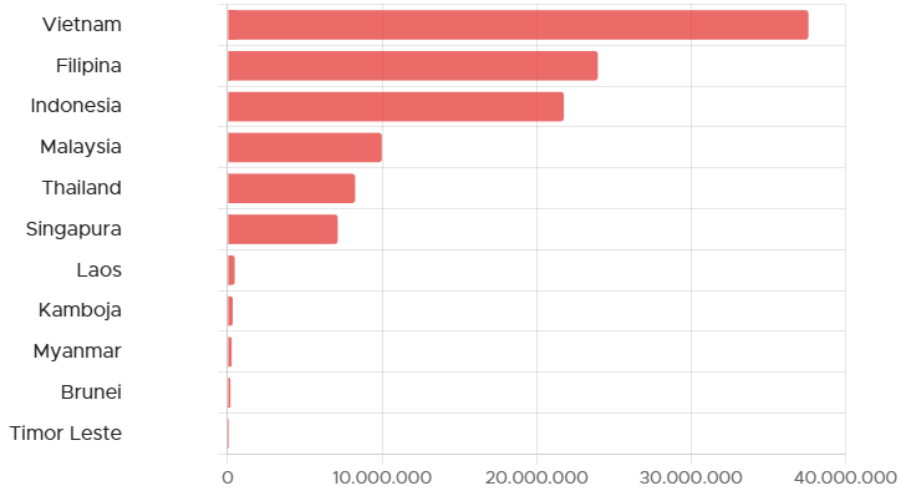

Table 1: ASEAN data leaks in 2024
Source: Surfshark (*Data Breach Statistics in 2024*, 2025).

Indonesia, the country with the most data leaks, moved up from 8th to 3rd place. Even the superpower United States is now in a higher position. From July to September 2022, a total of 108.9 million Indonesian accounts were breached (Q3). Russia and China are the countries with the highest data leakage in the world, with Indonesia contributing 12%. The United States and Brazil are below Indonesia (*Kebocoran Data Indonesia Tertinggi Ke-3 - Hypernet*, 2023). When data is leaked, not only are individuals harmed, but also people's trust in the government may decline. People who feel their data is protected may not participate in government programs or provide accurate information (Ombudsman Republik Indonesia, 2024).

In addition to hurting people, these data dumps have the potential to erode public confidence in the government. People might not give correct information or take part in government programs if they believe their personal information is not safe. Data indicates that maintaining data accessibility, confidentiality, and integrity is a challenge for public entities. The

next step is to safeguard sensitive and private data from both government and private entities, including identity numbers, home addresses, medical histories, and financial information (Y. Li & Saxunová, 2020). In addition to preserving public safety and national stability (Tan, 2024), this is crucial for stopping fraud and cyber abuse that careless people can exploit to carry out illegal activities (Ali & Mohd Zaharon, 2024).

Human rights protection of personal data faces a number of obstacles, such as low public awareness of their rights and privacy violations brought on by unethical data collection. While data leak incidents involving sensitive information demonstrate the vulnerability of current systems, privacy breaches may arise from technology companies' collection and analysis of personal data (Sultana et al., 2020). It is difficult for people to protect themselves because many people are not aware of their rights regarding the protection of personal data and because they are not taught or socialized about these rights. Laws governing the protection of personal data do exist, but their application is still beset by some issues, such as lax enforcement and regulatory gaps that permit data leaks.

Furthermore, the security of personal data is at greater risk due to technological advancements like ransomware and eavesdropping; cyberattacks that target corporate and government infrastructure show how vulnerable such data can be. In addition to hurting people, data leaks can cause businesses to suffer significant financial losses. In the long run, a company's reputation may suffer as a result of losing customers' trust (Predescu & Bălan, 2023). Therefore, the protection of personal data from a human rights perspective requires serious attention from all parties, including governments, companies, and society, with collaboration to raise awareness, strengthen regulations, and adopt safer technologies to protect human rights in the digital age.

Because personal information can be readily accessed and shared in the digital age, protecting personal data is becoming more and more crucial. Furthermore, current laws are frequently insufficient and poorly enforced, leaving gaps that careless people can take advantage of. Many nations still lack sufficient data protection laws, even though some have passed them, such as the European Union's General Data Protection Regulation (GDPR) (W. Li et al., 2025). Human rights principles, such as the right to privacy and the right to access personal data, must be adhered to when protecting personal information (Finck & Pallas, 2020). Effective personal data protection has several benefits, such as boosting public confidence in organizations and businesses, promoting economic stability, and fortifying the government's resolve to uphold individual rights. Therefore, the protection of personal data from a human rights perspective requires serious attention from all parties, including governments, companies, and the public (Bharti & Aryal, 2023).

Since its enactment in 2016, GDPR has been the strictest privacy and security law in the world. Breaking it can result in heavy fines of up to tens of millions of euros. GDPR regulates security, accountability, and data protection by design and default. Ultimately, data subjects may have rights that protect their privacy. These rights include the right to obtain information; the right to rectify or delete information; the right to restrict processing; the right to data portability; the right to object; and the right to automated decision-making and profiling processes (*General Data Protection Regulation (GDPR) – Legal Text*, n.d.).

Regulations related to the right to privacy of personal data are a manifestation of the recognition and protection of basic human rights. Therefore, the drafting of the Personal Data Protection Law has a strong philosophical foundation and can be accounted for. The philosophical foundation in question is Pancasila which is rechtsidee (legal ideals) and the idea of realizing the law to what it aspired to. Forms of personal data protection are divided into two forms, namely forms of data protection in the form of physical data security, visible data, and invisible data. The enactment of Law Number 27 of 2022 concerning Personal Data Protection

is an expectation of legal protection from many criminal cases of misuse of personal data derived from data leakage and theft of personal data. Penalties are imposed in criminal form and general penalties for people who misuse personal data. Criminal penalties can be imposed on any individual who steals or falsifies any personal data for criminal purposes. Both imprisonment and fines are punishments for such crimes. In addition to the imposition of criminal penalties, those who feel disadvantaged due to the misuse of their data by a certain amount of personal data can file a claim in the general court. Data subjects may, initially, report the misuse of their data to the supervisory committee, and the committee is obliged to facilitate a solution and provide assistance to the subject (Kröger et al., 2021). The presence of the Personal Data Protection Law gives the government authority to supervise the governance of personal data carried out by electronic system providers (Brown & Marsden, 2013). The Personal Data Protection Act defines personal data as data about an individual that is identified or can be identified individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. Meanwhile, what is meant by personal data protection is an overall effort to protect personal data in a series of personal data processing in order to guarantee the constitutional rights of personal data subjects (Richards & Hartzog, 2019).

The protection of private data as part of respect for the right to privacy must begin by providing legal certainty. Therefore, the guarantee of privacy data protection must be placed in a legal instrument that has the highest power, namely the Constitution, because the 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 each country. The state's steps in providing legal certainty are a principle of legality, very important, and cannot be ignored in the context of law enforcement in every country (Puluhulawa et al., 2022). Without legal certainty, individuals will have difficulty understanding their rights and how they are protected (Citron & Solove, 2022). Therefore, the steps taken by the state to provide legal certainty are to establish and guarantee these rights clearly in the Constitution. This legal instrument will reveal a nation's character, including its emphasis on human rights protection, the application of the law, and how the government's structure and organization fulfill its duties to the people.

The more data breaches and information leaks that happen across different industries, the more urgent it is to protect personal data. Examples of how vulnerable people's data can be include identity theft, online fraud, and data misuse by big businesses. Furthermore, the possibility of personal data being misused has increased due to technologies like artificial intelligence and big data analytics (Bainbridge, 2007). Governments, businesses, and the general public must give careful consideration to develop a framework that effectively protects the right to personal data. To control the gathering and use of data, numerous nations have enacted laws protecting personal information. Nonetheless, there are still issues with the law's consistent application and enforcement (Nissenbaum, 2017; Yudas Swastika et al., 2023). However, people must also emphasize how important it is to protect their data. In light of current threats, it is crucial to educate people about their right to privacy and how to safeguard personal data.

Therefore, it is crucial to have a thorough understanding of the significance of personal data as a human right. This has to do with both public trust in the expanding digital system and individual protection (Chen et al., 2025). In this article, we will discuss more about the implications of the right to personal data, the challenges faced, and the steps that can be taken to ensure the effective protection of these human rights. Thus, it is hoped that a collective awareness can be created of the importance of maintaining and protecting personal data as part of fundamental human rights.

With an increase of 0.05 points from 3.49 to 3.54 in 2022, Indonesia's digital literacy index shows improvement, especially in digital culture and digital ethics. Indonesia's digital literacy mapping results provide an overview of the strengths and weaknesses of digital skills and knowledge levels, as well as insights into the country's situation and potential (Kementerian Komunikasi dan Digital (Kemkomdigi), 2024). During the period from 2019 to 14 May 2024, the Ministry of Communication and Information handled 124 cases of alleged violations of personal data protection, 111 of which were cases of personal data leakage (Mediana, 2024). Thus, the placement of privacy data protection guarantees in the constitution not only reflects the state's commitment to respect for human rights but also provides a solid foundation for fair and transparent law enforcement. This will build public trust in the legal system and government, and encourage the active participation of citizens in safeguarding and protecting their rights, including the right to privacy and personal data protection.

Conclusion

The study highlights how various international legal documents, such as the ICCPR and the Universal Declaration of Human Rights, recognize the protection of personal data as a fundamental component of human rights. Even though data protection laws are in place, there are still many significant issues, including unethical privacy violations, a lack of public awareness, and lax law enforcement—especially as technology advances and data security threats rise. In addition to upholding public confidence through efficient oversight and law enforcement, the state plays a critical role in ensuring legal certainty and safeguarding the right to personal data through laws like Law Number 27 of 2022. To encourage people to take more proactive measures to protect their data, it is also critical to raise public awareness and educate them. To establish a safe and reliable framework, governments, businesses, and society must work together to protect personal data effectively. Good protection has the effect of boosting economic stability, public trust, and the state's dedication to individual rights. Therefore, to establish an atmosphere that respects each person's privacy and dignity, protecting personal data as a human right must be a top priority, particularly in the digital age.

Bibliography

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A Cyber Fraud: The Types, Implications and Governance. *International Journal of Educational Reform*, *33*(1), 101–121. https://doi.org/10.1177/10567879221082966

Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. *Computer Law & Security Report*, *23*(3), 276–281. https://doi.org/10.1016/j.clsr.2007.03.001

Bharti, S. S., & Aryal, S. K. (2023). The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the companies. *Journal of Contemporary European Studies*, *31*(4), 1391–1402. https://doi.org/10.1080/14782804.2022.2130193

Brown, I., & Marsden, C. T. (2013). *Regulating code: Good governance and better regulation in the information age*. The MIT Press.

Chen, J., Cai, W., Luo, J., & Mao, H. (2025). How does digital trust boost open innovation? Evidence from a mixed approach. *Technological Forecasting and Social Change*, *212*, 123953. https://doi.org/10.1016/j.techfore.2024.123953

Citron, D. K., & Solove, D. J. (2022). Privacy Harms. *Boston University Law Review*, *102*, 793.

Data breach statistics globally. (2025). Surfshark. https://surfshark.com/research/data-breach-monitoring

Data breach statistics in 2024. (2025). Surfshark. https://surfshark.com/research/study/data-breach-recap-2024

Eu charter of fundamental rights: A commentary (First edition). (2021). HART PUBLISHING. https://doi.org/10.5040/9781509933495

European Convention on Human Rights. (1950). https://www.echr.coe.int/documents/d/echr/convention_ENG

Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1).

General Data Protection Regulation (GDPR) – Legal Text. (n.d.). General Data Protection Regulation (GDPR). Retrieved April 22, 2025, from https://gdpr-info.eu/

Kebocoran Data Indonesia Tertinggi Ke-3—Hypernet. (2023, March 3). https://www.hypernet.co.id/id/kebocoran-data-indonesia-tertinggi-ke-3/

Kementerian Komunikasi dan Digital (Kemkomdigi). (2024). *Indeks Literasi Digital Indonesia Tahun 2021-2022—Satu Data KOMDIGI*. https://data.komdigi.go.id/opendata/dataset/indeks-literasi-digital-indonesia

Kröger, J. L., Miceli, M., & Müller, F. (2021). How Data Can Be Used Against People: A Classification of Personal Data Misuses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3887097

Kumalaratri, G., & Yunanto, Y. (2021). Urgency of the personal data protection bill on privacy rights in Indonesia. *Jurnal Hukum*, *37*(1), 1. https://doi.org/10.26532/jh.v37i1.13604

Kun, E. (2025). Searching for the appropriate legal basis for personal data processing for cybersecurity purposes under the NIS 2 Directive: Legal obligation and/or legitimate interest? *Computer Law & Security Review*, *56*, 106098. https://doi.org/10.1016/j.clsr.2024.106098

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2025). Mapping the empirical literature of the GDPR's (In-)effectiveness: A systematic review. *Computer Law & Security Review*, *57*, 106129. https://doi.org/10.1016/j.clsr.2025.106129

Li, Y., & Saxunová, D. (2020). A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations. *Procedia Computer Science*, *170*, 1110–1115. https://doi.org/10.1016/j.procs.2020.03.060

Mahieu, R., van Hoboken, J., & Asghari, H. (2019). *Responsibility for Data Protection in a Networked World – On the Question of the Controller, 'Effective and Complete Protection' and Its Application to Data Access Rights in Europe* (SSRN Scholarly Paper 3256743). Social Science Research Network. https://doi.org/10.2139/ssrn.3256743

Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, *34*(4), 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

Marelli, M. (2023). The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. *Computer Law & Security Review*, *50*, 105849. https://doi.org/10.1016/j.clsr.2023.105849

Mediana. (2024, June 3). *Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024*. kompas.id. https://www.kompas.id/baca/ekonomi/2024/06/03/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024

Muzairoh, E., Suharso, S., Noviasari, D. T., & Syafingi, H. M. (2024). Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi di Era Digital dalam Prespektif Hak Asasi Manusia. *Borobudur Law and Society Journal*, *3*(1), 31–36. https://doi.org/10.31603/11824

Naldi, G. J., & Magliveras, K. D. (2014). *The asean Human Rights Declaration*. https://doi.org/10.1163/22131035-00302003

Nissenbaum, H. (2017). Protecting Privacy in an Information Age: The Problem of Privacy in Public. In K. W. Miller & M. Taddeo (Eds.), *The Ethics of Information Technologies*. Routledge.

Nurhayati, Y., Ifrani, I., & Said, M. Y. (2021). Metodologi Normatif dan Empiris Dalam Perspektif Ilmu Hukum. *Jurnal Penegakan Hukum Indonesia*, *2*(1), 1–20.

Ombudsman Republik Indonesia. (2024). *Keamanan Data dan Kepercayaan Warga pada Pelayanan Publik (Memperingati Hari Pelayanan Publik Internasional)*. https://ombudsman.go.id:443/artikel/r/pwkinternal--keamanan-data-dan-kepercayaan-warga-pada-pelayanan-publik-memperingati-hari-pelayanan-publik-internasional

Pangrazio, L., & Bunn, A. (2024). Assessing the privacy of digital products in Australian schools: Protecting the digital rights of children and young people. *Computers and Education Open*, *6*, 100187. https://doi.org/10.1016/j.caeo.2024.100187

Parihin, N. mardiana. (2023). Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, *5*(1), Article 1. https://doi.org/10.52005/rechten.v5i1.108

Predescu, P.-A., & Bălan, D. (2023). The Implications and Effects of Data Leaks. *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)*, 170–177. https://doi.org/10.19107/CYBERCON.2023.22

Puluhulawa, F., Rusdiyanto Puluhulawa, M., & Adelina Harun, A. (2022). Good Environment as Part of Human Right: A Case Study on Plastic Waste Post Pandemic. *KnE Social Sciences*. https://doi.org/10.18502/kss.v7i15.12071

Richards, N. M., & Hartzog, W. (2019). Privacy's Constitutional Moment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3441502

Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilasasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), Article 2. https://doi.org/10.37680/almanhaj.v5i2.3054

Shehu, V. P., & Shehu, V. (2023). Human rights in the technology era – Protection of data rights. *European Journal of Economics, Law and Social Sciences*, *7*(2), 1–10. https://doi.org/10.2478/ejels-2023-0001

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, *20*(1), 256. https://doi.org/10.1186/s12911-020-01275-y

Tan, W. (2024). National security as the trump card: Assessing China's legal regime on cross-border data transfer. *Information & Communications Technology Law*, *33*(3), 368–383. https://doi.org/10.1080/13600834.2024.2375125

Ye, X., Yan, Y., Li, J., & Jiang, B. (2024). Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. *Telecommunications Policy*, *48*(10), 102851. https://doi.org/10.1016/j.telpol.2024.102851

Yudas Swastika, I. G. B., Sri Rahayu Gorda, A. A. A. N., Gorda, Aaa. Ngr. T. R., & Kurniawan, I. G. A. (2023). Misuse of Personal Data as a Crime from a Cyber Law Perspective. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *22*(2). https://doi.org/10.31941/pj.v22i2.3073