INTI

eISSN 2830-795X

Relevance of Privacy within the Sphere of Human Rights: A Critical Analysis of Personal Data Protection

Fayola Issalillah, Rommy Hardyansah

Universitas Sunan Giri Surabaya

Email: fayola.issalillah@gmail.com

ABSTRACT – Privacy and personal data protection are increasingly important issues in today's digital era. This article highlights the importance of recognizing privacy as a fundamental human right that must be protected by the state in accordance with applicable human rights principles and the constitution. Protection of personal data is becoming increasingly crucial because it is often a target for irresponsible parties. International regulations, such as the Universal Declaration of Human Rights and the General Data Protection Regulation (GDPR) in the European Union, provide a framework for the protection of personal data. This article also highlights a key challenge to protecting privacy, namely finding a balance between the need for security and individual privacy. Efforts such as developing specific laws on personal data protection, increasing public awareness, and enhancing international cooperation are urgently needed.

Keywords: privacy, data protection, human rights, regulations, challenges.

A. INTRODUCTION

Human Rights are natural or natural rights that are lasting and universal for every human being. Sen (2009) states that human rights are considered rights that cannot be abolished or ignored by anyone. In national and state life, human rights are the basis for the formation of legal regulations that regulate interactions between individuals, society and the government. The state is expected to recognize, respect and protect human rights in all aspects of life, whether political, social, economic or cultural.

The formation of national laws must be in line with human rights principles, because laws that conflict with human rights can become instruments of oppression and violations of human dignity. Reidenberg (1998) emphasized that although formal legislators do not have absolute power or authority, the constitution must guarantee the protection of human rights as a fundamental right for every individual.

In Indonesia, the state philosophy of Pancasila is recognized as a source of human rights for the Indonesian people. As the philosophical foundation of the state, Pancasila views that the implementation of human rights must be in harmony with the noble values of the Indonesian nation. The Pancasila concept emphasizes that the implementation of human rights must not be absolute, but must consider the interests of society and uphold the moral norms contained in Pancasila (Sen, 2009).

Thus, the implementation of human rights is not only the responsibility of the state, but also involves the active participation of society to ensure that every action taken does not violate the rights of other people and is in accordance with the principles contained in Pancasila.

One of the protections for human rights is the protection of personal data. Personal data protection is a form of human rights protection that is recognized internationally. The European Charter of Human Rights and the ASEAN Declaration of Human Rights expressly recognize the protection of personal data as an integral part of human rights (Maniadaki et al., 2021). Furthermore, the Universal Declaration of Human Rights recognizes personal data protection as a human right after going through a long evolutionary process in recognizing basic human rights (Newman, 2008; Seubert & Becker, 2021).

Personal data refers to information that can directly or indirectly identify a specific individual. This may include information such as name, address, identification number, and other information related to a person's identity. Protection of personal data to ensure that it is only used for the purposes for which it was originally collected. This aims to prevent misuse of data that could threaten individual privacy

and rights. Thus, the protection of personal data is not only a technical issue, but is also an important part of efforts to protect human rights as a whole (De Hert, 2012).

Privacy consists of two main types, namely psychological privacy and physical privacy. Psychological privacy focuses on an individual's thoughts, plans, beliefs, and desires, while physical privacy deals with the physical aspects that reveal a person's private life. Allan Westin's definition of data protection emphasizes that it is the right to safeguard personal information that can be linked to an individual's desire to communicate or maintain the privacy of other parties (Westin, 2003).

The importance of psychological privacy is that it protects important aspects of an individual's inner life, such as thoughts, feelings, and beliefs that may be sensitive or private. Meanwhile, physical privacy relates to control over physical exposure that could reveal personal information, such as a person's location or activities. Thus, the protection of personal data and efforts to maintain privacy are an integral part of human rights, which include both psychological and physical dimensions of privacy (Solove, 2013; Quinn & Malgieri, 2021).

Privacy protection is becoming increasingly important in the increasingly advanced digital era. In the midst of rapid advances in information and communication technology, individual personal data often becomes a potential target for irresponsible parties. Therefore, privacy protection is not only important to safeguard the human rights of every individual, but also to maintain democratic stability (Rosen, 2012; Gstrein & Beaulieu, 2022).

Article 17 of the Covenant states that private affairs, including communications and private life, should be protected from unlawful interference. This shows the importance of the right to privacy in international law as an integral part of human rights. Without adequate privacy protections, individuals are vulnerable to violations of their rights and abuse of power by parties with access to their personal data.

Additionally, privacy protection has far-reaching implications for maintaining a healthy democracy. Privacy functions as a regulator in communication between individuals, sets expectations in interpersonal relationships, and regulates when individuals want to be with other people or choose to be alone. Thus, privacy is not only an individual issue, but also a foundation for healthy social interactions and a balance of power between individuals and larger institutions or organizations (Nissenbaum, 2010; Swire, 2011).

Amid emerging issues such as mass monitoring, online tracking, and the use of data for commercial purposes, privacy protection has become increasingly urgent. Concerns about misuse of personal data, including individual identities, preferences and behaviour, have increased, given the fact that such data can be used for manipulation, fraud or even discrimination. The state has a great responsibility to protect the privacy rights of its citizens.

In addition, privacy protection is also needed to support innovation and sustainable economic growth (Pincus & Johns, 1997; Tao et al., 2019). When individuals feel safe to share information without fear of misuse, they are more likely to engage in various economic activities, such as e-commerce or online purchases. With this trust, businesses and organizations can develop better and more innovative services without compromising individual privacy.

However, the main challenge to preserving privacy is finding a balance between the need for security and the need for privacy (Darmawan, 2024). In the midst of increasingly complex security threats, some parties may feel the need to collect and analyse personal data to protect society from security threats (Mantelero, 2016; Wahyudi et al., 2021). However, these steps must be taken with caution and in line with human rights and privacy principles.

To face these challenges, it is important for countries to have a strong and effective legal framework to protect individual privacy. This includes clear privacy policies, efficient law enforcement mechanisms, and strict data protection (Kuner, 2013; Lynskey, 2019). Additionally, public education and awareness about the importance of privacy is also critical to encourage individuals to protect their own privacy rights and support government efforts to safeguard privacy as a whole.

Thus, privacy protection is not only an individual issue, but also a social and political issue that affects the stability of democracy, economic growth, and the welfare of society as a whole. By recognizing the importance of privacy, we can move towards a more just, open and empowering society.

The aim of this study is to explore the legal framework that recognizes the importance of privacy as a fundamental human right, with a particular focus on the protection of personal

data. This study aims to identify widely recognized international instruments and national legal frameworks governing privacy protection, and to understand how these frameworks are implemented on a global scale.

In addition, this study also aims to analyse the various strategies and approaches used by countries to achieve the right balance between ensuring national security and protecting individual privacy rights. Taking into account rapid technological developments and increasingly complex security threats, this research will explore how countries can face these challenges without compromising the privacy rights of their citizens.

Through a deeper understanding of the existing legal framework and effective strategies in protecting privacy, it is hoped that this research can contribute to increasing awareness of the importance of privacy as an integral part of human rights, as well as providing guidance for policy makers to develop policies that comply with the needs of a modern society that is increasingly connected digitally.

B. METHOD

This research applies normative juridical research methods (legal research) as its main methodological framework. This approach allows researchers to systematically examine the norms or rules that apply in positive law related to the protection of personal data and human rights. Using this method, researchers will analyse various legal regulations relevant to the research topic, aiming to understand the legal framework that regulates the protection of personal data related to human rights.

The normative juridical approach allows researchers to identify gaps or lacunae in existing regulations, as well as evaluate the consistency and effectiveness of the legal protection provided for individual privacy rights. Apart from that, this method also involves descriptive-analytical analysis to explain the legal implications of the various regulations analysed, as well as to develop a critical framework for the issue of personal data protection related to human rights.

Thus, through a normative juridical approach, this research aims to provide a better understanding of the complexity of the legal framework that regulates privacy in relation to human rights.

C. RESULTS AND DISCUSSION

The Main Legal Frameworks and International Instruments Related to Personal Data Protection

The importance of privacy as a fundamental human right has been widely recognized in various international instruments and legal frameworks (Edwards, 2016; Milkaite & Lievens, 2019; Solove, 2022). At the international level, there are several main documents that recognize the right to privacy, especially in the protection of personal data. Some of them are:

1. Universal Declaration of Human Rights (UDHR): This document, adopted by the United Nations in 1948, expressly declares the right to privacy as part of fundamental human rights. Although it does not specifically mention the protection of personal data, the UDHR affirms the right to privacy in Article 12, which recognizes that “no one shall have an attack on his or her dignity” and that “everyone has the right to the protection of the law against interference with or attacks on his or her private, family, or personal life.” household, and letters."
2. International Covenant on Civil and Political Rights (ICCPR): This document, adopted in 1966, specifically recognizes the right to privacy in Article 17. The article states that "No arbitrary interference in private life, one's family, household, and correspondence."
3. European Charter of Human Rights (ECHR): This instrument, adopted by the Council of Europe in 1950, expressly recognizes the right to privacy in Article 8. The article confirms that "everyone has the right to respect for his private and family life, his residence, and his correspondence."
4. General Data Protection Regulation (GDPR): This is a European Union regulation that came into force in 2018, which provides a comprehensive framework for the protection of personal data. GDPR gives individuals the rights to control their personal data and places obligations on organizations to protect that data.

In addition to these documents, many countries also have national laws that affirm the right to privacy and provide a legal framework for the protection of personal data. As an example:

1. California Consumer Privacy Act (CCPA): This is a United States state law that provides California consumers with additional privacy rights, including the right to know what information is collected about them and the right to object to the sale of their personal information.
2. Future EU Personal Data Protection Laws: In addition to the GDPR, the European Union is also developing additional laws to protect personal data, such as the Digital Services Act (DSA) and the Digital Markets Act (DMA), which aim to strengthen privacy rights and giving individuals greater control over their data.

Enforcement of key legal frameworks and international instruments governing privacy and personal data protection has become a key focus for many countries and international organizations. Below is an overview of how the main legal framework is operating so far:

1. Implementation and Enforcement: Many countries have adopted national laws that align with the standards set out in international documents such as the GDPR in the European Union, the CCPA in California, and other privacy laws in various countries. Law enforcement against privacy violations and violations of personal data protection laws is a priority for privacy monitoring bodies and law enforcement agencies in many countries (Koops & Leenes, 2014).
2. Strengthening Personal Data Protection: Many countries and regions have stepped up their efforts to strengthen personal data protection through legislative and regulatory updates (Zalnieriute, 2015). An example is the revision and expansion of the GDPR in the European Union, which introduced additional requirements to strengthen the rights of individuals over their personal data and increase the obligations of organizations that collect and process data.
3. International Cooperation: Cooperation between countries and international institutions in terms of exchanging information and coordinating law enforcement is increasingly important regarding privacy and protection of personal data that crosses national borders. The European Union, for example, has strengthened cooperation with other countries outside its territory to ensure compliance with high data protection standards.
4. Increased Public Awareness: Many initiatives have been launched to increase public awareness about the importance of privacy and personal data rights. Civic organizations, government agencies, and private companies often serve to provide information and resources to help individuals understand their rights and how to protect their privacy online.
5. Technological Developments: Technological developments, especially in terms of artificial intelligence and data analytics, have given rise to new challenges for protecting privacy and personal data (Masrichah, 2023). Many countries and institutions have attempted to keep pace with these developments by designing new regulations or updating existing ones to address privacy issues arising from new technologies.

Although there has been significant progress in the enforcement and implementation of the international legal framework on privacy and personal data protection, there are still challenges that need to be overcome. One of the main challenges is overcoming differences in privacy regulations between countries and regions, which can create barriers for companies operating across borders (Gonçalves & Jesus, 2013). Additionally, consistent and effective law enforcement remains a challenge in some countries (Halpert, 2016).

Overall, implementation of key legal frameworks and international instruments on privacy and personal data protection continues to move forward, but there is still room for improvement and innovation to overcome existing challenges. With solid cooperation between states, international institutions and the private sector, it is hoped that individual privacy rights will continue to be respected and protected in the ever-evolving digital era.

Legal Approaches to Striking a Balance between National Security and Protection of Individual Privacy

The legal approach to achieving a balance between national security and protecting individual privacy involves several important principles and strategies (Rosadi, 2016). Some legal principles and approaches that can help countries strike a balance between national security and protecting individual privacy are as follows:

1. Compliance with Human Rights Principles: States must ensure that every step taken to ensure national security does not violate human rights, including the right to privacy. This means that actions such as the collection and use of personal data by governments or security agencies must comply with the principles of proportionality, equality and non-discrimination.
2. Transparency and Accountability: States should ensure that national security policies and practices involving the use of personal data are carried out with a sufficient level of transparency to the public. This includes providing adequate information about how data is collected, stored and used, as well as the mechanisms available for individuals to access and correct their data and file complaints if violations occur.
3. Regulatory and Legal Updates: Amid technological developments and ever-evolving security threats, countries need to regularly update and adapt existing regulations and laws to address new challenges. This may involve revising data protection laws, establishing new policies on the use of monitoring technologies, or developing new regulations on cybersecurity.
4. International Cooperation: In the era of globalization, cooperation between countries is very important to face complex security threats. Countries need to work together to develop common standards and principles for the use of personal data for national security purposes, as well as facilitating the exchange of information necessary for those purposes.
5. Responsible Use of Technology: The development and implementation of technology must be carried out with due regard for its impact on individual privacy. Countries need to introduce strict security and privacy standards in the development of new technologies, as well as adopt effective oversight mechanisms to ensure that these technologies are used responsibly.
6. Public Education and Awareness: Public awareness of their privacy rights and the impact of the use of personal data for national security is essential. Countries need to develop education programs and public awareness campaigns to increase public understanding of privacy and the importance of protecting personal data.

To implement this approach, countries can strike the right balance between national security and protecting individual privacy. However, there is no one-size-fits-all approach, and each country must consider its own circumstances and ensure that actions taken are consistent with legal and human rights principles.

Legal Framework for Personal Data Protection in Indonesia

The right to personal protection has been regulated in Indonesia, as stated in Article 28 G Paragraph (1) that citizens have the right to personal protection as part of Human Rights. This personal right has its own sensitivity because it relates to personal data or individual identity listed in official documents such as Resident Identification Card, Parpor, Driver's License, Family Card, Taxpayer Identification Number, Bank Account Number, and even fingerprints. Protection of personal rights is also protection of the right to freedom of speech, which guarantees freedom from the threat of fear of doing or not doing something which is a human right. The concept of personal data protection emphasizes that every individual has the right to control when and with whom their data will be shared, as well as establishing conditions that must be met during the process of sharing data within a community.

Regarding personal data protection, there are several examples of cases that often occur in society. One of them is copying ATM card data and information, which is known as skimming. In skimming, the perpetrator can steal someone's ATM card information and then use this data to withdraw funds from other places without the card owner's knowledge. Apart from that, cases of online loans also often occur, where a person's identity can be misused to borrow money online without the identity owner's consent. Another example is the case related to online motorcycle taxi services, where number owners or consumers often experience terror via WhatsApp messages. Misuse of personal data in cases like this often fulfils the elements of criminal acts such as theft and fraud. Therefore, the criminal act of misuse of personal data can be considered a very serious form of crime (Situmeang, 2021).

Indonesia faces challenges in regulating personal data protection because it does not yet have a law that specifically regulates this.

The unavailability of explicit laws regarding personal data protection creates confusion in handling cases of personal data breaches. This shows the need to draft special and comprehensive laws regarding personal data protection in Indonesia. It is hoped that the existence of this law will provide a clear and strong legal basis for protecting individual privacy. Without proper regulation, the risk of misuse of personal data by irresponsible parties can increase significantly (Van Dijk et al., 2016). However, this aspect is spread across several related regulations, including:

a. Banking Law Number 10 of 1998 recognizes the concept of "bank secrets" as stated in Article 1 Paragraph 28. According to this article, everything related to customers and their deposits is considered bank secrets, and this information must be kept confidential by the bank except in a few cases. certain circumstances regulated in Article 40.
b. Telecommunications Law Number 36 of 1999 also has provisions regarding the protection of personal data. Article 42 (1) of the Telecommunications Law mandates telecom operators to maintain user confidentiality, except for trial purposes with approval from the Attorney General/Chief of Police. Article 57 regulates penalties for misuse of information.
c. Consumer Protection Law Number 8 of 1999, although it does not specifically regulate the protection of personal data, is based on the interests of justice, safety, security and legal certainty. However, this law is considered not strong enough to protect consumers' personal data because of its lack of clarity in regulating this matter.
d. Human Rights Law Number 39 of 1999 provides the legal basis related to the right to information and personal protection. Article 14 (1) confirms everyone's right to obtain the information they need to develop themselves and their environment. Article 29 paragraph (1) of the Human Rights Law states the right of every person to receive equal treatment in accordance with their dignity, including the right to personal protection. This is also in line with Article 28 of the 1945 Constitution which provides every person with the right to personal protection, with the exceptions regulated in Article 32.

Despite efforts in existing regulations, there are still shortcomings and lack of clarity in regulating personal data protection as a whole. This indicates the need to review and refine existing regulations to more effectively protect individual privacy rights (Mantili & Dewi, 2020). A thorough evaluation of existing regulations is key to ensuring that the policies implemented can address the challenges faced in protecting personal data. Concrete steps are needed to close gaps in regulations that allow misuse of personal data. Without these steps, risks to individual privacy may continue to increase as technology advances and data use becomes more widespread.

Personal Data Protection Framework in Indonesia

Protection of personal rights in Indonesia is regulated in the 1945 Constitution, especially Article 28G paragraph (1), which confirms that safety and protection for doing or not doing something is part of human rights. The right to protection of personal data, which comes from the right to privacy, is an important aspect for individuals and institutions (Mutiara & Maulana, 2020). Violations of privacy can result in both material and non-material losses, making the protection of personal data important as part of human rights.

Personal data protection not only affects individuals directly, but also has a significant impact on institutions and institutions. For example, financial losses caused by identity theft or data breaches can harm an institution's reputation and public trust. Therefore, protecting personal data is key to maintaining the integrity and sustainability of these institutions.

Constitutional Court Decision No.5/PUU-VIII/2011 also confirms that the right to privacy is an inviolable part of human rights, including the right to information or information privacy, which is also known as data protection. Furthermore, the regulatory rules regarding personal data in Indonesia are explained in several regulations, such as the ITE Law and PP Number 82 of 2012, which regulate the storage and confidentiality of certain individual data.

The importance of clear and integrated rules in personal data protection not only creates legal certainty for individuals and institutions, but also provides a foundation for effective law enforcement (Rahman, 2021). With a strong legal framework, law enforcement efforts against personal data violations can be carried out more efficiently and effectively, thereby providing better protection for the community.

Personal data protection is also covered in various other laws, such as Law Number 11 of 2008, Law Number 7 of 1971 concerning Archives, and others. To ensure the protection of citizens' privacy rights, integrated regulations are needed, considering that Indonesia is a member of ASEAN which has adopted the ASEAN Human Rights Declaration, as well as the development of personal data protection policies at the international level, such as GDPR in the European Union.

International law, including human rights declarations, increasingly emphasizes the need for transparency in the collection of personal data. Several countries, such as Australia and Singapore, already have personal data protection laws that regulate transparency and citizens' rights to their personal data (Rachovitsa, 2016; Rawal & Patel, 2023). Comprehensive personal data protection, as regulated in the GDPR, confirms the principle of transparency in the use of personal data, which gives individuals the right to access, change or delete their personal data in the company's systems at any time.

Thus, implementing laws related to personal data protection in Indonesia requires effectively planned and coordinated efforts. An important first step is strengthening the legal framework. Renewing and improving legal regulations, including the revision of the ITE Law and its derivative regulations, is a very crucial first step in providing a solid foundation for personal data protection. With a clear and comprehensive legal framework, society and institutions have strong guidelines for managing and protecting personal data.

Furthermore, effective law enforcement is a top priority. It is necessary to establish a special institution or unit that focuses on dealing with personal data breaches, and there is a need to increase coordination between law enforcement agencies to ensure effective and consistent legal action. Without strong law enforcement, personal data protection regulations will be ineffective in protecting the rights of individuals and institutions.

Apart from that, increasing public awareness and education is also very important. Through education and outreach campaigns, the public needs to be given a better understanding of the risks of personal data breaches and their rights regarding privacy. Close collaboration between government and the private sector also needs to be improved. This collaboration can establish standards and best practices in the management and protection of personal data, as well as strengthen existing regulatory frameworks.

Finally, regular monitoring and evaluation is essential. Audits of personal data management practices by companies and institutions, as well as evaluation of policies that have been implemented, are important instruments to strengthen the implementation of personal data protection in Indonesia. By taking these steps, it is hoped that personal data protection in Indonesia can be improved, providing better protection for society and companies, and ensuring that individual privacy rights are maintained in this digital era.

D. CONCLUSION

Privacy is considered a fundamental human right and must be protected by the state in accordance with applicable human rights principles and the constitution. Protection of personal data is becoming increasingly important in the increasingly advanced digital era because it often becomes a potential target for irresponsible parties. International regulations such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the General Data Protection Regulation (GDPR) in the European Union provide a framework for the protection of personal data. The main challenge to protecting privacy is finding a balance between the need for security and the need for individual privacy. A legal approach that includes principles such as compliance with human rights, transparency, accountability, regulatory reform, international cooperation, responsible use of technology, and public education and awareness can help countries strike the right balance between national security and individual privacy.

In Indonesia, personal data protection is regulated in several different laws, but there is no specific law that regulates this comprehensively. The preparation of explicit laws regarding personal data protection in Indonesia is necessary to provide a clear and strong legal basis for protecting individual privacy. Therefore, countries must continue to strengthen the enforcement and implementation of the international legal framework on privacy and personal data protection. Countries need to develop specific

and comprehensive laws on personal data protection according to their region. Efforts are needed to increase public awareness about their privacy rights and the importance of protecting personal data through education and public awareness campaigns. International cooperation in exchanging information and coordinating law enforcement also needs to be improved to overcome challenges that cross national borders.

The preparation of laws regarding personal data protection must be carried out by considering the principles of human rights, transparency and accountability, as well as taking into account technological developments and increasingly complex security threats.

REFERENCES

Covenant on Economic, Social, and Cultural Rights. 1966. 993 UNTS 3.

Darmawan, D. 2024. Distribution of Six Major Factors Enhancing Organizational Effectiveness. Journal of Distribution Science, 22(4), 47-58.

De Hert, P. 2012. A Human Rights Perspective on Privacy and Data Protection Impact Assessments. in Privacy Impact Assessment (Pp. 33-76). Dordrecht: Springer Netherlands.

Edwards, L. 2016. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. Eur. Data Prot. L. Rev., 2, 28.

Gonçalves, M. E. & I. A. Jesus. 2013. Security Policies and the Weakening of Personal Data Protection in the European Union. Computer Law & Security Review, 29(3), 255-263.

Gstrein, O. J. & A. Beaulieu. 2022. How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches. Philosophy & Technology, 35(1), 3.

Halpert, J. 2016. Privacy and Security Issues in Data Mining and Machine Learning: International Ecamlaw. Cham, Switzerland: Springer.

Koops, B. J. & R. Leenes. 2014. Privacy Regulation Cannot be Hardcoded. A Critical Comment on the 'Privacy by Design'provision in Data-Protection Law. International Review of Law, Computers & Technology, 28(2), 159-171.

Kuner, C. 2013. Transborder Data Flows and Data Privacy Law. Oxford, UK: Oxford University Press.

Lynskey, O. 2019. Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. Theoretical Inquiries in Law, 20(1), 189-220.

Maniadaki, M., A. Papathanasopoulos, L. Mitrou, & E. A. Maria. 2021. Reconciling Remote Sensing Technologies with Personal Data and Privacy Protection in the European Union: Recent Developments in Greek Legislation and Application Perspectives in Environmental law. Laws, 10(2), 33.

Mantelero, A. 2016. Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. Computer law & security review, 32(2), 238-255.

Mantili, R. & P. E. T. Dewi. 2020. Prinsip Kehati-Hatian Dalam Penyelenggaraan Sistem Elektronik dalam Upaya Perlindungan Data Pribadi di Indonesia. Jurnal Aktual Justice, 5(2), 132-145.

Masrichah, S. 2023. Ancaman dan Peluang Artificial Intelligence (AI). Khatulistiwa: Jurnal Pendidikan dan Sosial Humaniora, 3(3), 83-101.

Milkaite, I. & E. Lievens. 2019. Children's Rights to Privacy and Data Protecton Around the World: Challenges in the Digital Realm. European Journal of Law and Technology, 10(1).

Mutiara, U. & R. Maulana. 2020. Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. Indonesian Journal of Law and Policy Studies, 1(1), 42-54.

Newman, D. E. 2008. European Union and United States Personal Information Privacy, and Human Rights Philosophy-Is There a Match. Temp. Int'l & Comp. LJ, 22, 307.

Nissenbaum, H. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.

Pincus, L. B. & R. Johns. (1997). Private Parts: A Global Analysis of Privacy Protection Schemes and a Proposed Innovation for Their Comparative Evaluation. Journal of Business Ethics, 16, 1237-1260.

Quinn, P. & G. Malgieri. 2021. The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework. German Law Journal, 22(8), 1583-1612.

Rachovitsa, A. 2016. Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue. International Journal of Law and Information Technology, 24(4), 374-399.

Rahman, F. 2021. Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia. Jurnal Legislasi Indonesia, 18(1), 81-102.

Rawal, M. S. & H. Patel. 2023. A Critical Analysis of National and International Legal Framework for Protection of the Right to Privacy and Data Protection. RES MILITARIS, 13(1), 4042-4057.

Reidenberg, J. R. 1998. Data Privacy Law: A Study of United States Data Protection. Columbia Law Review, 98(7), 2487-2574.

Rosadi, S. D. 2016. Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia. Yustisia, 5(1), 35-53.

Rosen, J. 2012. The Right to be Forgotten. Stanford Law Review, 64(1), 88-104.

Sen, A. 2009. The Idea of Justice. Cambridge, MA: Harvard University Press.

Seubert, S. & C. Becker. 2021. The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection. German Law Journal, 22(1), 31-44.

Solove, D. J. 2013. Understanding Privacy. Cambridge, MA: Harvard University Press.

Solove, D. J. 2022. The Limitations of Privacy Rights. Notre Dame L. Rev., 98, 975.

Swire, P. 2011. Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment. NCL Rev., 90, 1371.

Tao, H., M. Z. A. Bhuiyan, M. A. Rahman, G. Wang, T. Wang, M. M. Ahmed, & J. Li. 2019. Economic Perspective Analysis of Protecting Big Data Security and Privacy. Future Generation Computer Systems, 98, 660-671.

Van Dijk, N., R. Gellert, & K. Rommetveit. 2016. A Risk to a Right? Beyond Data Protection Risk Assessments. Computer Law & Security Review, 32(2), 286-306.

Wahyudi, W., R. N. K. Kabalmay, & M. W. Amri. 2021. Big Data and New Things in Social Life, Studi Ilmu Sosial Indonesia, 1(1), 1-12.

Westin, A. F. 2003. Privacy and Freedom. New York, NY: Routledge.

Zalnieriute, M. 2015. An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance. International Journal of Law and Information Technology, 23(2), 99-133.