Journal of Business, Social and Technology
Volume 7, Issue 3, 1-9
e_ISSN: 2807-6362
https://bustechno.polteksci.ac.id/index.php/jbt/index
DOI: doi.org/10.59261/jbt.v7i3.666

Protection Of Social Media Users' Personal Data From An International Law Perspective and Its Application In Indonesia

***Rezti Aisyahbella**[1]
Universitas Diponegoro, Indonesia

Adya Paramita Prabandari[2]
Universitas Diponegoro, Indonesia

***Corresponding author:**
Rezti Aisyahbella, Universitas Diponegoro, Indonesia, ✉reztiaisyahbella@gmail.com

Article Info :

Article history:
Received May 07, 2026
Revised June 03, 2026
Accepted June 09, 2026

Keywords:
implementation; international law; protection of social media user

Abstract

Background: The rapid development of digital technology has enabled widespread communication through social media, yet it has simultaneously exposed millions of users to serious risks of personal data leakage and misuse.
Objective: This study aims to analyze personal data protection for social media users from an international law perspective and examine its application within the Indonesian legal framework.
Methods: This research employs a normative juridical approach using statutory, conceptual, and comparative methods, analyzing primary, secondary, and tertiary legal materials through descriptive-qualitative techniques.
Results: International personal data protection law is governed by a range of international legal frameworks, including the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Both the UDHR and ICCPR apply globally and emphasize that the right to privacy is a fundamental aspect of human rights. Indonesia ratified the ICCPR through Law No. 12 of 2005, which pertains to the ratification of the International Covenant on Civil and Political Rights. Furthermore, the safeguarding of personal data is addressed in Law Number 11 of 2008 on Information and Electronic Transactions, and further detailed in Law Number 27 of 2022, which focuses on the Protection of Personal Data. However, challenges in implementation remain, particularly regarding the classification of children's data and the establishment of an independent supervisory authority for personal data protection.
Conclusion: Strengthening legal implementation, ensuring social media platform compliance, and developing derivative regulations are essential to effectively protect social media users' personal data in Indonesia.

To cite this article: Aisyahbella, R., & Prabandari, A. P. (2026). Protection of social media users' personal data from an international law perspective and its application in Indonesia. *Journal of Business, Social and Technology*, 7(3), 1–9. https://doi.org/10.59261/jbt.v7i3.666

INTRODUCTION

Today's technological developments have shown rapid progress, with increasing sophistication and diverse innovations that arguably make life easier. These advancements have significantly impacted the fabric of daily life. One of the positive outcomes of this rapid technological growth is the ease of long-distance communication and online access to information (De Wet et al., 2016; Deb, 2014). Among these technologies is the availability of social networking services, which people can use and access via the internet (Hodge et al., 2017; Villanti et al., 2017).

According to Troussas (2020), social networking sites are characterized as internet-based

platforms that enable individuals to: first, establish a public or semi-public profile within a confined system; second, indicate a list of other users with whom they share a connection; and third, access and navigate the list of connections associated with themselves as well as the connections of other users within the system (Albarran & Albarran, 2013).

The convenience of communication and information access also presents adverse effects for users, including the risk of personal data breaches and other criminal activities, which are often unavoidable due to the ease of internet access via social media (Tudorel & Vintila, 2020). One of the objectives of the state in advancing information and communication technology is manifested in the form of personal data protection for all citizens (Ahmed & Ahmed, 2023; Calzada, 2022).

The significance of personal data protection has grown with the increase in internet and social media users (Mahmoodi et al., 2018). Numerous incidents have arisen involving the misuse of personal data, such as data breaches, data trading, and even the embezzlement of customer accounts (Abidin et al., 2019). These occurrences have sparked discussions regarding the necessity of implementing legal frameworks to safeguard personal data. Personal data protection is intrinsically linked to the notion of privacy (Purtova, 2018). Privacy encompasses the preservation of personal integrity and dignity (Guimarães, 2023). The right to privacy also pertains to an individual's capacity to control who possesses information about them and how that information is utilized (Djafar & Komarudin, 2014).

In international legal frameworks, the right to privacy is articulated in the Universal Declaration of Human Rights (UDHR) of 1948. This declaration has established a legal foundation for member states concerning their obligation to safeguard and honor the personal rights of their citizens.

In the fourth amendment of the 1945 Constitution of the Republic of Indonesia, Article 28G paragraph (1) stipulates that every individual is entitled to protection for themselves, their families, their honor, dignity, and property under their control. Additionally, individuals possess the right to a sense of security and protection against threats that induce fear regarding their actions or inactions, which is recognized as a fundamental human right. Regarding human rights, Youvan (2024) explained that the protection of personal rights, or private rights, enhances human values, fosters improved relationships between individuals and their communities, encourages independence or autonomy in exercising control and achieving appropriateness, and nurtures tolerance while limiting discriminatory practices and constraining governmental power.

Upon examining the description, it becomes evident that the protection of personal data, as delineated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, is intrinsically linked to the safeguarding of personal rights or private rights. Historically, the concept of privacy is universal and recognized across various nations, both in codified legal frameworks and in unwritten moral principles.

METHOD

This study was conducted utilizing a normative juridical approach alongside a statutory approach, which involved an examination of laws and regulations pertinent to the legal issue at hand. The data collection method employed in this research involved gathering legal materials through library research and document analysis, specifically concerning personal data protection from an international legal standpoint and its implementation in Indonesia.

RESULTS AND DISCUSSION

Results

Personal Data Protection for Social Network Users from an International Legal Perspective

Personal data is data that reflects an individual's identity, symbols, codes, numbers, or letters, but is private (Latumahina, 2014). The term "personal data" is used by European countries; in the United States, the term "personal information" is used. However, when discussing the transfer of personal information, policymakers and citizens worldwide use the appropriate term "privacy".

The concept of privacy itself was developed in research conducted by Warren and Brandheis in their article entitled "*The Right to Privacy*". This article explains that with the

advancement and development of technology, there will be a public awareness that every person has the right to enjoy life, or in other words the right that a person has so that his or her private life is not interrupted by the state or other people (Latumahina, 2014).

Regulations regarding the right to privacy and protection of personal data in international legal instruments include:

1. Universal Declaration of Human Rights (UDHR)

The 1948 Universal Declaration of Human Rights (UDHR) establishes a legal framework for its member states concerning their responsibilities to safeguard and uphold the privacy rights of their citizens. Article 12 specifically addresses the safeguarding of the right to privacy:

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

The UDHR asserts that every individual possesses the right to privacy, family life, housing, association with others, and a good reputation. Consequently, all these aspects must be legally protected. The Universal Declaration of Human Rights stands as the most significant international document, having effectively consolidated the agreements of nearly all nations. The adverse legacy of World War II was a pivotal factor that led to the ratification of this Charter.

Article 12 does not explicitly mention personal data, but it serves as an " *umbrella term* " because it is related to other articles. The UDHR itself contains 30 articles that are provisions related to the most fundamental rights, including civil rights, political rights, economic rights, social rights, and cultural rights.

2. International Covenant on Civil and Political Rights

Article 12 of the UNHCR provides comprehensive protections for the right to privacy. This led to the formulation of more specific safeguards, which ultimately resulted in the establishment of the International Covenant on Civil and Political Rights (ICCPR). This convention was adopted on December 16, 1966, through resolution 2200A, and it came into force on March 23, 1976. This international legal framework details the safeguarding of human privacy rights. Article 17, paragraph (1) of the ICCPR states that: 1) *No individual shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor shall they face unlawful attacks on their honor and reputation.* 2) *Everyone is entitled to legal protection against such interference or attacks.*

The distinction between Article 12 of the UDHR and Article 17 of the ICCPR is found in paragraph 2 of Article 17, which affirms the protection of the right to privacy. The ICCPR emphasizes that no person shall experience arbitrary or unlawful intrusions into their privacy, family, home, or correspondence. Furthermore, this convention empowers each state to create legal structures for their national protection. Therefore, it is the responsibility of countries that have ratified and signed the ICCPR to implement the provisions of the convention.

While the ICCPR does not specifically state that personal data is included within the right to privacy, the United Nations Human Rights Committee (HRC) provides extensive guidelines concerning the scope of this right, as outlined in the ICCPR General Comment No. 16: Article 17 (Right to Privacy). This General Comment emphasizes that to ensure the highest level of protection for one's private life, every individual should possess the right to know what personal data is stored in automated data files and the purposes for which it is used. Additionally, individuals should be able to ascertain which public authorities, individuals, or private entities may have access to their data. If the data contains personal information that is incorrect or has been unlawfully collected, processed, or managed, individuals have the right to request its deletion or correction. This statement leads to the conclusion that personal data is a fundamental aspect of the right to privacy that requires safeguarding against violations (Khadzhiradieva et al., 2024).

Indonesia's ratification of this treaty was formalized through Law No. 12 of 2005, which relates to the International Covenant on Civil and Political Rights (ICCPR). The ICCPR includes essential provisions regarding the protection of privacy rights, which are closely linked to the broader issues of personal data protection. Articles 17 paragraphs (1) and (2) of the ICCPR clearly state that no individual shall face arbitrary or unlawful interference in their private life, family, home, or correspondence. Furthermore, the ICCPR empowers member states to create domestic

legal frameworks to support privacy rights.

Implementation of Personal Data Protection in Indonesia

The International Covenant on Civil and Political Rights (ICCPR), ratified by Indonesia through Law Number 12 of 2005 concerning the Ratification of the International Covenant on Civil and Political Rights, remains a primary reference for numerous experts discussing the right to privacy.

The safeguarding of personal rights in Indonesia is enshrined in the fourth amendment of the 1945 Constitution of the Republic of Indonesia, particularly in Article 28G paragraph (1). This provision affirms that every person has the right to protect themselves, their family, their honor, their dignity, and their property under their control, along with the right to feel secure and protected from threats that could violate their fundamental human rights. The right to personal data protection is a derivative of the right to respect for private life. The concept of private life relates to individuals as sentient beings. Therefore, individuals are acknowledged as the primary holders of the right to personal data protection (Erdos, 2022).

Regarding personal data protection in Indonesia, it is regulated by Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Article 26 of the ITE Law stipulates that the utilization of personal data in electronic media necessitates the consent of the data owner, and any breach of this requirement may lead to legal repercussions for damages incurred. In the realm of information technology, the protection of personal data is essential to the right to privacy. Consequently, to provide a sense of security for users of electronic systems, the ITE Law includes provisions on personal data protection and the right to privacy, as detailed in Article 26 paragraph (1) of the ITE Law. In this regard, the personal rights mentioned encompass: a) Privacy rights are the right to enjoy a private life and be free from all kinds of interference. b) Privacy rights are the right to be able to communicate with other people without being spied on. c) Privacy rights are the right to control access to information about one's personal life and data.

The unauthorized use of personal information and data via electronic media is deemed a breach of privacy rights (Ahmad, 2023). While the Electronic Information and Transactions Law acknowledges the safeguarding of privacy rights and personal data in electronic contexts, as specified in Article 26 and its accompanying explanation, the necessary protective measures and responsibilities that should be undertaken by relevant entities, such as electronic system administrators or governmental bodies, are not yet encompassed within the ITE Law.

Moreover, alongside the ITE Law, Indonesia's efforts to protect personal data are regulated by Law Number 27 of 2022 concerning Personal Data Protection. This law provides a more extensive framework, which includes definitions of personal data, categories of personal data, international cooperation in the realm of personal data protection, and further details (Babikian, 2023).

As defined in Article 1 number 1 of the Personal Data Protection Law, personal data is described as information related to an individual who can be identified, either directly or indirectly, whether alone or in combination with other information, through both electronic and non-electronic systems. This legislation guarantees the safeguarding of personal data rights, based on eight fundamental principles: legal certainty, protection, benefit, prudence, public interest, accountability, balance, and confidentiality, as specified in Article 3. The personal data that is protected includes information capable of identifying individuals, either directly or indirectly, across various formats.

The Personal Data Protection Law grants individuals, known as data subjects, significant rights as owners of personal data (Veale et al., 2018). These rights include the right to information, the right to correct, delete, or withdraw personal data, also the right to file a complaint in the event on a violation. In order to these rights to be effectively enforced, the public needs to be aware of the existence and importance of personal data protection. Most of Indonesians still do not fully understand the concept od “personal data” Many are still unaware of the right to refuse to provide data and how to file a complaint in the event of misused of personal data. Therefore, increased public awareness of the Personal Data Law needs to be increased, focusing on specific groups, especially particularly key industry stakeholders and vulnerable groups.

Law Number 27 of 2022 regarding Personal Data Protection marks a crucial development in the evolution of privacy safeguards in Indonesia. This legislation was introduced due to the inadequacies of earlier regulations, including the Electronic Information and Transactions Law (ITE Law), which were deemed ineffective in offering thorough protection for personal data and privacy.

Under the Law Number 27 of 2022 concerning Personal Data Protection, criminal sanctions are applied as *ultimum remedium* and are stipulated in Articles 67 and 68. These provisions regulate 4 (four) prohibited acts that are subject to criminal penalties, namely: 1) Acquiring or gathering personal information that is not one's own with the aim of gaining an advantage for oneself or another individual, particularly when such actions may deliberately inflict harm on others. 2) Revealing personal information that is not one's own. 3) Utilizing personal information that is not one's own. 4) Fabricating false personal information or altering personal data with the purpose of benefiting oneself or another individual, especially when such actions may result in harm to others.

A key issue that has arisen concerns whether violations of the criminal provisions stipulated in the Personal Data Protection Law should be classified as "complaint-based offenses" or "ordinary offenses". This distinction is crucial, as it directly influences the operation of criminal justice mechanisms and the protection of fundamental rights. Specifically, the issue centers on whether state, acting through law enforcement agencies, is authorized to commence criminal proceedings only upon the submission of a complaint by the personal data subject whose rights have been violated.

The classification of offenses under the Personal Data Protection Law appears to nomenclature contained in Article 60 letters (i) and (j), which regulate the authority of the personal data protection supervisory institution. These previous authorize the institution to conduct examinations and investigations based on complaints, reports, and supervisory findings concerning alleged violations of personal data protection. Such nomenclature indirectly indicates that the criminal provisions under the Personal Data Law may possess a dual classification, encompassing both complaint-based offenses and ordinary offenses.

According to R. Tresna (1959) in Azas-Azas Hukum, there is a fundamental distinction between a report and a complaint. In the case of an ordinary offense, a report is not a prerequisite for prosecution. By contrast, in a complaint-based offense, a complaint constitutes an essential condition for initiating prosecution. Furthermore, a key distinction between these two categories lies in the standing of the complainant and the consequences of withdrawal. In ordinary offenses, any person may submit a report, even if the alleged criminal act has not caused direct harm to them. Moreover, the withdrawal of such a report does not prevent investigators from continuing the investigation and prosecution process. Consequently, if the complaint is withdrawn, the case can no longer be pursued through the criminal justice process (Tresna, 1959).

The classification of personal data is regulated under Article 4 of Law Number 27 of 2022 concerning Personal Data Protection. Pursuant to this provision, personal data is classified into two categories: 1) Specific personal data. 2) General personal data.

Specific personal data refers to personal data that, when processed, may result in greater impacts on the data subject, including discriminatory treatment and more substantial harm. The categories of specific personal data include: 1) Health data information. 2) Biometric data. 3) Genetic data. 4) Criminal records. 5) Children's data. 6) Personal financial data. 7) Other categories of data as provided by applicable laws and regulations.

Meanwhile, general personal data includes: 1) Full name. 2) Gender. 3) Nationality. 4) Religion. 5) Marital status. 6) Personal data that, when combined, may identify an individual, such as mobile phone and an IP address. This classification reflects the legislator's recognition that certain categories of personal data require a higher level of protection due to the greater risks associated with their misuse, unauthorized disclosure, or unlawful processing.

One example of a case involving a violation of personal data protection is the decision of the Karanganyar District Court Number 5/Pid.Sus/2023/PN Krg. This case is noteworthy because it demonstrates the practical application of criminal law provisions in addressing the unlawful use and dissemination of personal data. Furthermore, the court decision provides insight into the interpretation regulations within the Indonesian legal system, particularly concerning the

protection of individual privacy rights in the digital era.

In decision Number 5/Pid.Sus/2023/PN Karg, the defendant, HI, was charged with creating and using false personal data to deceive victims. The defendant, a daily wage laborer, allegedly falsified his identity by impersonating a police officer for fraudulent purposes. The defendant used his Whatsapp account, which displayed a profile picture featuring the Indonesian national flag, to send messages to the victim's Whatsapp account. In those messages, he introduced himself as a police official. To facilitate the scheme, the defendant searched Google for information regarding police officers serving in Central Java and subsequently used the name and identify of an actual police official to convince others, including victim, to transfer money to him.

For these actions, the court found HI guilty of violating Article 68 in conjunction with Article 66 of Law Number 27 of 2022 on Personal Data Protection for intentionally creating false personal data for personal gain. Consequently, the court sentenced the defendant to four years of imprisonment and imposed a fine of IDR 1 billion. This case illustrates the application of the criminal provisions of the Personal Data Protection law in addressing the misuse and falsification of personal data, particularly where such conduct is intended to obtain unlawful financial benefits through deception and identity misinterpretation.

Implementation Challenges

Law No. 27 of 2022, which pertains to Personal Data Protection, comprises 16 chapters and 76 articles, establishing fundamental principles for safeguarding individual personal data. Nevertheless, this legislation exhibits various shortcomings that necessitate further scrutiny, including:

1. Regarding "Children's Data": Under the Personal Data Protection Law, children's data is classified as specific personal data, which requires a higher level of protection. The processing of children's personal data may only be carried out with the consent of a parent or legal guardian. Such processing includes the collection, storage, use, and dissemination of children's data by both public authorities and private entities. Consent must be given explicitly and knowingly, based on complete information regarding the purpose and scope of the data processing. For example, a school that intends to publish students' photographs for promotional purposes must obtain written consent from their parents or legal guardians. In Chapter III, Types of Personal Data, Article 4, paragraph (2) mentions specific personal data, including child data. However, this Law does not yet define the age thresholds that classify "child data." This lack of specification may lead to confusion during implementation, considering the varying definitions of children in different Indonesian laws and regulations. Consequently, this could create the potential for differing interpretations. Moreover, many digital platforms, particularly social media services and online gaming applications, collect children's personal data without obtaining clear parental consent. In some cases, such data collection practices are hidden within privacy policies that are difficult for parents and children to understand. Accordingly, effective personal data protection requires not only a robust legal framework but also targeted safeguards for vulnerable individuals who face heightened risks of exploitation and discrimination.
2. Institutional: Articles 58 through 60 of the Personal Data Protection Law regulate the establishment of a new agency to oversee data control and processing. This agency must be independent of the ministry because the Law applies not only to the private sector and individuals but also to public bodies. However, the institutional structure, authority, and operational mechanisms of this supervisory body remain unclear. The Law merely provides a general mandate for the establishment of a supervisory authority without specifying its organizational form or the extent of its independence. This ambiguity has given rise to several challenges, including overlapping authority with the Ministry of Communication and Digital Affairs, delays in responding to personal data breach incidents, and a lack of transparency in enforcement practices. The uncertainty also affects private sector entities, which often face difficulties in determining the appropriate reporting standards and compliance requirements. Furthermore, the absence of a clearly defined supervisory authority hampers international cooperation, particularly since many personal data breaches involve cross-border actors and transactions. Therefore, the government should promptly establish a fully

operational and independent personal data protection supervisory authority with clearly defined powers, responsibilities, and accountability mechanisms. These measures are essential to strengthen legal certainty, enhance public trust, improve regulatory compliance, and facilitate effective domestic and international cooperation in the enforcement of personal data protection law.

3. Low Public Digital Literacy: A significant challenge in the implementation of the Personal Data Protection Law is the prevalence of low digital literacy among vulnerable groups. Limited digital literacy may hinder public awareness and understanding of the rights and protections provided under the Law. Consequently, the growing number of fraud and personal data theft cases is partly attributable to insufficient awareness that personal data constitutes an asset requiring adequate protection. The effective implementation of the Law depends not only on a robust legal framework but also on public awareness and active participation. To address this challenge, comprehensive and sustainable digital literacy campaigns should be conducted through both formal and informal educational channels. The government, private sector, and educational institutions should collaborate to provide training programs and public awareness initiatives that are accessible and easily understood by the public. Therefore, policymakers should prioritize the development of a national digital literacy strategy that integrates personal data protection education into school curricula, community outreach programs, and professional training initiatives. Such efforts are essential to strengthening public capacity, enhancing compliance with data protection regulations, and ensuring the long-term effectiveness of Indonesia's personal data protection regime.

Constitutional Court Decision Regarding Personal Data Protection

One of the rulings issued by the Constitutional Court regarding personal data protection before the enactment of Law Number 27 of 2022 is Constitutional Court Decision No. 5/PUU-VIII/2010. In this decision, the Constitutional Court examined the application of Law Number 11 of 2008 concerning Electronic Information and Transactions in the context of the 1945 Constitution of the Republic of Indonesia.

In the decision, it was concluded that Article 31, paragraph (4) of Law Number 11 of 2008 was inconsistent with Article 28G, paragraph (1), and Article 28J, paragraph (2) of the 1945 Constitution of the Republic of Indonesia. As a result, it was ruled that Article 31, paragraph (4) of Law Number 11 of 2008 regarding Electronic Information and Transactions did not possess binding legal authority. This ruling clarifies that the right to privacy is a component of human rights (a derogable right) that relates to information or the right to privacy of information, commonly known as data privacy (data protection).

Moreover, the Court acknowledged that the right to privacy includes the safeguarding of personal information and individual autonomy from unlawful interference. In this context, privacy rights are intricately linked to the notion of information privacy, which underpins personal data protection. Therefore, this decision marks a significant milestone in the evolution of Indonesia's personal data protection framework, as it established constitutional recognition of privacy and personal data protection even prior to the enactment of the Personal Data Protection law in 2022.

Thus, this Constitutional Court Decision can be viewed as a constitutional foundation for the safeguarding of personal data in Indonesia, reinforcing the principle that any limitations on privacy rights must be explicitly regulated by law and executed in accordance with the constitutional guarantees of human rights.

CONCLUSION

International personal data protection is regulated through various international legal instruments, including the UDHR and ICCPR. Both the UDHR and ICCPR are universally recognized instruments that affirm the right to privacy as an inseparable component of human rights that must be safeguarded. In Indonesia, the right to privacy is enshrined in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Indonesia has also ratified the ICCPR through Law Number 12 of 2005 concerning the Ratification of the International Covenant on Civil

and Political Rights. Previously, Indonesia had the ITE Law, which regulated Electronic Information and Transactions; subsequently, Law Number 27 of 2022 concerning Personal Data Protection provides more detailed and specific regulations regarding personal data protection. Furthermore, the Karanganyar District Court Decision Number 5/Pid.Sus/2023/PN Krg illustrates that the criminal provisions of the PDP Law can be effectively applied to acts involving the creation and use of false personal data for fraudulent purposes and personal gain.

The implementation of the Personal Data Protection Law, however, remains constrained by several challenges, including an unclear age threshold for children, ambiguity surrounding the supervisory authority, and low public awareness and literacy regarding personal data protection. Therefore, regulatory refinement, institutional strengthening, and continuous public education are necessary to ensure the effective enforcement of personal data protection in Indonesia.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the Faculty of Law, Universitas Diponegoro, for providing the academic environment and institutional support that made this research possible. The authors also extend their appreciation to the reviewers and editors of the Journal of Business, Social and Technology for their constructive feedback and scholarly guidance throughout the review process. Special thanks are owed to colleagues and fellow researchers at the Department of International Law and Cyber Law, Universitas Diponegoro, whose discussions and insights greatly enriched the analytical depth of this study. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors and was conducted independently as part of the authors' academic scholarly activities.

AUTHOR CONTRIBUTION STATEMENT

Rezti Aisyahbella: Conceptualization, literature review, data collection, formal analysis of international legal instruments (UDHR, ICCPR), drafting of the original manuscript, and preparation of the final submission. Adya Paramita Prabandari: Supervision, methodology, validation of legal analysis, comparative analysis of Indonesian national law framework (ITE Law and UU PDP 2022), and revision of the manuscript, and overall academic guidance throughout the research process.

REFERENCES

Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization's experience. *Information & Computer Security*, *27*(1), 81–100. https://doi.org/10.1108/ICS-04-2018-0043

Ahmad, N. (2023). Data privacy issues and risks with sharing on social media: An inquiry. *Russian Law Journal*, *11*(4), 597–611.

Ahmed, M. M., & Ahmed, A. M. (2023). Citizens' data protection in E-government system. *International Journal of Innovative Computing*, *13*(2), 1–9. https://doi.org/10.11113/ijic.v13n2.389

Albarran, A. B., & Albarran, A. B. (2013). *The social media industries*. Routledge New York.

Babikian, J. (2023). Securing rights: legal frameworks for privacy and data protection in the digital era. *Law Research Journal*, *1*(2), 91–101.

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129–1150. https://doi.org/10.3390/smartcities5030057

De Wet, W., Koekemoer, E., & Nel, J. A. (2016). Exploring the impact of information and communication technology on employees' work and personal lives. *SA Journal of Industrial Psychology*, *42*(1), 1–11.

Deb, S. (2014). Information technology, its impact on society and its future. *Advances in Computing*, *4*(1), 25–29.

Djafar, W., & Komarudin, A. (2014). Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci. *Elsam, Jakarta*.

Erdos, D. (2022). Identification in personal data: Authenticating the meaning and reach of another broad concept in EU data protection law. *Computer Law & Security Review*, *46*, 105721.

Guimarães, J. A. S. A. (2023). Preserving personal dignity: The vital role of the right to be forgotten. *Brazilian Journal of Law, Technology and Innovation*, *1*(1), 163–186. https://doi.org/10.59224/bjlti.v1i1.163-186

Hodge, H., Carson, D., Carson, D., Newman, L., & Garrett, J. (2017). Using Internet technologies in rural communities to access services: The views of older people and service providers. *Journal of Rural Studies*, *54*, 469–478.

Khadzhiradieva, S., Bezverkhniuk, B., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. *Social and Legal Studios*, *3*(7), 245–256. https://doi.org/10.32518/sals3.2024.245

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

Mahmoodi, J., Čurdová, J., Henking, C., Kunz, M., Matić, K., Mohr, P., & Vovko, M. (2018). Internet users' valuation of enhanced data protection on social media: Which aspects of privacy are worth the most? *Frontiers in Psychology*, *9*, 1516. https://doi.org/10.3389/fpsyg.2018.01516

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Tresna, R. (1959). *Azas-azas hukum pidana: disertai pembahasan beberapa perbuatan pidana jang penting*.

Troussas, C., & Virvou, M. (2020). Advances in social networking-based learning. *Intell. Syst. Ref. Libr*. https://doi.org/10.1007/978-3-030-39130-0

Tudorel, O. I., & Vintila, M. (2020). The benefits and consequences of using modern information and communication technology. *Revista de Asistenţă Socială*, *1*, 169–175.

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, *8*(2), 105–123. https://doi.org/10.1093/idpl/ipy002

Villanti, A. C., Johnson, A. L., Ilakkuvan, V., Jacobs, M. A., Graham, A. L., & Rath, J. M. (2017). Social media use and access to digital technology in US young adults in 2016. *Journal of Medical Internet Research*, *19*(6), e196.

Youvan, D. C. (2024). *The Tension Between Freedom and Security: Navigating Autonomy and Interdependence in Human Society*.