IJLSSM
INTERNATIONAL JOURNAL OF LAW SOCIAL SCIENCES AND MANAGEMENT
E-ISSN: 3048 - 1317
Volume 1, No. 3
July 2024

Personal Data Protection in Technological Developments Era

Farrel Ardan Biantoro

Prodi Ilmu Hukum, Sekolah Tinggi Ilmu Hukum Adhyaksa

*Corresponding Author:
Farrel.biantoro@stih-adhyaksa.ac.id

Abstract

This research examines the legal impacts of the development of Artificial Intelligence (AI) technology. This paper employs a juridical normative research method. Data sources include legislative regulations and policies related to the discussed legal issues. Artificial intelligence aims to understand that AI technology not only creates tools and systems capable of performing tasks once done by humans but also enters realms that carry profound legal implications. With its ability to process and analyze vast amounts of data, legal questions arise concerning individual privacy, system security, legal accountability, and more. The legal challenges in the development of AI technology are highly complex and layered, encompassing various aspects from data privacy to legal responsibility, ethics, security, and reliability. Existing regulations often struggle to keep pace with AI innovation, creating legal gaps that need prompt attention.

Keywords: *Technology Integration, Law, Artificial Intelligence*

1. INTRODUCTION

There has been significant progress in the era of globalization, especially in communication and technology. Several sectors of society are starting to be impacted by technology, including the government sector (Astawa & Dewi, 2018). The rapid advancement of technology and information has significantly impacted every facet of life. The emergence of various technical tools is transitioning numerous human activities from analog to digital. Undeniably, technology and information growth have been pivotal in driving globalization forward. The majority of community activities in the current era of globalization are conducted through digital platforms.

However, it is important to stress that the economic advancements in technology and information must serve the greater good outlined in the Indonesian constitution. The evolution and advancement of the digital realm have the potential to alter behavior and lifestyles, making the safeguarding of personal data and identity vital for various online activities. It involves personal information, including details such as name, date of birth, address, identification number, financial status, medical history, and other sensitive data. (Suari and Sarjana, 2023). The digital revolution has impacted various aspects of life, including the way we communicate, work, shop, and run business (Panggabean, 2022).

Electronic systems that control the integration of personal data with information technology, media, and telecommunications are aimed at the data itself (Makarim, 2010). The Personal Data Protection Law, which took effect in 2019, was officially ratified that same year in response to numerous instances of personal data breaches. This law aims to uphold citizens' privacy rights, raise public awareness about the importance of safeguarding personal information, and ensure the recognition and enforcement of these rights.

It is anticipated that this law will establish a robust legal framework for the management and safeguarding of personal data for individuals and public officials. The protection of personal information is one of the human rights associated with personal security, as stipulated in Article 28G of the 1945 Constitution. As widely recognized in many countries, personal security and privacy are universal rights. Since the creation of mankind, individuals have inherently possessed information about themselves, especially biometric information. (Kindt, 2013).

The definition of personal data as stipulated in Article 1 Paragraph 1 of the Minister of Communication and Information Technology Regulation Number 20 of 2016 concerning Personal Data Protection encompasses specific personal data that is stored, maintained, and upheld as accurate and confidential. Article 3 of Law Number 43 of 2009 concerning Archives highlights the necessity of orderly arrangement to ensure data protection and security. The UK Data Protection Act 1998 provides an alternate definition, where personal data refers to any information related to a living

individual that allows for their identification, either directly or in conjunction with other available information. Personal data may also pertain to characteristic details of the individual, such as gender, age, or name.

In Indonesia, the awareness of safeguarding personal data has surged, particularly with the widespread use of the internet and technology-based applications. The right to privacy is fundamental, primarily due to its association with an individual's personal information and identity. Consequently, instances of personal data breaches have emerged as a significant concern. The repercussions of personal data leaks can result in financial losses, identity fraud, and further misuse of data. Governments, organizations, and individuals must promote consciousness about data security and undertake appropriate measures to shield personal data. Staying abreast of current developments is vital to understanding the evolving panorama of data security.

In the contemporary era, the protection of personal data entails establishing operational standards for electronic system operators. These standards necessitate electronic systems to be dependable, secure, and accountable. Article 15 of Law Number 11 of 2008, amended to Law Number 19 of 2016 concerning Information and Electronic Transactions underscores the protection of electronic system administrators from data theft and cybercrime. Furthermore, safeguarding personal information assumes paramount importance, as highlighted in Article 2 of Law Number 23 of 2006 concerning Population Administration. This article emphasizes the state's obligation to safeguard its entire territory and its inhabitants. Therefore, the government must protect the personal information of its citizens. The author is then motivated and feels compelled to discuss the value of data protection in more detail as well as serve as a reminder that new crimes have occurred and must be dealt with immediately.

2. METHOD

The research method applied in this study is normative juridical focuses on qualitative analysis to link existing problems with relevant types of analysis. This approach certainly involves identification and in-depth analysis of the questions that arise in connection with the legal issues that are at the center of attention. Based on the

views of Sugiyono (2016), the qualitative descriptive method is a research method that relies on postpositivist philosophy and is used to investigate the natural conditions of the research object. Data sources used in this research include legal regulations and policies related to the legal issues being discussed. Apart from that, the literature used as a reference also includes books, journals, articles, and papers related to the use and implementation of blockchain technology. Furthermore, the references used also include legal encyclopedias and legal dictionaries.

3. RESULTS AND DISCUSSION

Principles of Privacy Rights regarding Personal Data

The principle of the right to privacy regarding personal data is a critical aspect in this increasingly advanced digital era. Every day, we interact with technology and provide personal data online. Personal data refers to any information that can directly or indirectly identify an individual. It includes, but is not limited to, name, address, telephone number, email address, date of birth, identification number, financial data, and medical information (Mahira & Emilda, 2020). However, by providing this information, we also open up opportunities for potential data misuse and privacy violations.

The right to privacy concerning personal data encompasses an individual's entitlement to understand how their data is handled, who can access it, the purposes for which it is utilized, and the methods by which it is processed and stored. Additionally, this principle includes the right to provide consent for the use of personal data, as well as the right to request the removal (right to be forgotten) or correction of inaccurate data. The principle of the right to privacy regarding personal data is designed to safeguard human rights and individual dignity and to ensure that personal data is used responsibly and transparently. This is pertinent not only to organizations that gather data but also to governments and other entities involved in the collection, processing, and utilization of personal data. (Latumahina, 2014).

The concept of privacy, also referred to as the right to be left alone has become increasingly pertinent with the advancement of technology. This heightened awareness

has led to the recognition that everyone is entitled to lead a life free from unwarranted intrusion. Warren and Brandeis argued that privacy is the right to enjoy life and be left alone, and contended that its legal acknowledgment is both inevitable and imperative. Safeguarding privacy is essential as it is a fundamental right that every individual should enjoy.

Moreover, the freedom to choose whether to keep personal data private or share it is protected by the laws of Indonesia. Indonesian citizens have a constitutional right to safeguard their privacy, including the protection of their personal information. The constitution mandates the state to afford legal protection across various facets of its citizens' lives. In upholding constitutional rights, the legal objectives must encompass ensuring legal benefits, justice, and clarity. (Erna, 2019). Privacy data protection is enshrined in Article 28, letter G, paragraph (1) of the 1945 Constitution, which affirms every person's entitlement to safeguard themselves, their family, honor, dignity, and property under their control. It also guarantees the right to a sense of security and protection from the threat of fear, crime, or the deprivation of human rights.

Data protection safeguards individuals' freedom to choose whether to disclose or exchange their data. It also grants individuals the right to determine the terms for the transfer of their data. The development of privacy rights has led to the establishment of the right to protect personal data. Every individual has the freedom to choose to keep their data private or to share it, a freedom protected by the prevailing laws in Indonesia. (Anggraeni, 2018). Based on this legal basis, Indonesian citizens have a constitutional right to protection of their privacy rights, which includes the right to privacy of their personal information. The state is obliged based on its constitutional rights to provide legal protection for various aspects of the lives of Indonesian citizens. The legal objectives for constitutional rights must include legal benefits, justice, and clarity (Erna, 2019).

Protection of Personal Data According to Indonesian Law

In today's digital age, the Indonesian government is confronted with an immediate challenge in safeguarding its citizens' privacy rights. With the widespread

adoption of information and communication technology, the threat of personal data misuse is on the rise. Therefore, the government bears both a moral and legal obligation to establish and enforce comprehensive and effective regulations about personal data protection. Effective regulation should encompass not only the establishment of clear and strong rules but also the education of the public about their privacy rights and methods for safeguarding their data. Additionally, the government must establish a robust monitoring mechanism to identify and take decisive action against all types of data privacy breaches.

Despite demonstrating its dedication to safeguarding personal data through the drafting of related laws, the Indonesian government has yet to enact specific and comprehensive regulations governing the protection of personal data. This absence of robust regulations creates an opportunity for cybercriminals to exploit individuals' data vulnerabilities. Hence, reinforcing the legal framework and legal protection concerning data privacy is crucial in upholding public trust and ensuring the security of Indonesian society against the prevalent theft and misuse of personal data.

Many individuals continue to share their personal information on social media platforms without recognizing the potential risks. Furthermore, inadequate enforcement of laws against perpetrators of data privacy violations serves as a barrier. The penalties imposed on perpetrators often fail to act as a deterrent, thus failing to prevent similar violations from occurring in the future. To address this issue, the government needs to intensify public education initiatives through various channels, including schools, mass media, and social campaigns. Furthermore, reforming the legal system to impose stricter and more certain penalties on perpetrators of data privacy violations is essential. In essence, enhancing data privacy protection represents a long-term investment that yields significant societal benefits in the current era of intricate digitalization.

4. CONCLUSION

Legal challenges in the development of artificial intelligence (AI) technology are highly intricate and multifaceted, encompassing a wide range of issues including data privacy, legal accountability, ethics, security, and reliability. Current regulations often struggle to keep pace with the rapid advancements in AI, resulting in a pressing need to

address the resulting legal gaps. Data privacy presents a significant obstacle, as AI relies on extensive data sets to operate effectively, while regulations like the GDPR in Europe impose strict constraints on the collection and use of personal data. Furthermore, determining legal liability in cases of AI errors or damage raises the crucial question of who should be held accountable, the developer, the data provider, or the end user.

Ethical use of AI is also a significant concern, particularly regarding algorithmic bias and transparent decision-making, as inadequate regulation in these areas can perpetuate social and economic injustices. Additionally, ensuring AI security is imperative, especially in vital sectors such as cybersecurity and defense, to prevent misuse and attacks. On the other hand, overly stringent regulations could stifle innovation, necessitating balanced and adaptable policies that support technological progress without compromising security, privacy, and ethics. International cooperation, flexible regulation, education and awareness, and public involvement are pivotal in establishing an effective and equitable regulatory framework. With the right approach, regulation can catalyze AI innovation, safeguarding public interests and ensuring responsible AI usage. Therefore, addressing these legal challenges requires not only technical solutions but also collaborative efforts from diverse stakeholders to create an environment conducive to the safe and sustainable advancement of AI technologies.

References

Anggen Suari, K. R., & Sarjana, I. M. (2023). "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum, 6*(1), 132-142. https://doi.org/10.38043/jah.v6i1.4484

Anggraeni, SF, 2018, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia." *Jurnal Hukum & Pembangunan, Vol. 48 No. 4*, 814 – 825

Astawa, I & Dewi, Kadek. (2018). "E-government Facilities Analysis for Public Services in Higher Education." *Journal of Physics: Conference Series Vol. 953(2).012061*. Doi: 10.1088/1742-6596/953/1/012061.

Erna, P 2019, "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online (The Urgency of Personal Protection in Peer to Peer Lending)", *Majalah Hukum Nasional, No.2,* 1-27

Kindt, Els J. (2013). *Privacy and Data Protection Issues of Biometric Applications : A Comparative Legal Analysis*. Germany : Springer.

Latumahina, RE, 2014, "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya", *Jurnal GEMA AKTUALITA, Vol.3, No. 2*, 14-25

Mahira, DF, Emilda Y Lisa NA, 2020, "Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept." *Legislatif, Vol.3 No.2,* 287 -302

Makarim, E. (2010). *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: Rajajawali Pers.

Panggabean, A. N. (2021, October 22). MEMAHAMI DAN MENGELOLA TRANSFORMASI DIGITAL. https://doi.org/10.31219/osf.io/s36wq

Suari, K., R., A. & Sarjana, I., M. (2023). "Menjaga Privasi di Era Digital:Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum, Vol. 6 No. 1,* 132-146.

Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif dan R&D,* 24th Edition. Bandung: Alfabeta