HORIZON PUBLIC LEGAL STUDIES
Vol 2 Issue 1 Tahun 2025
Doi : https://doi.org/10.56087/hegels.v2i1

Artificial Intelligence and the Data Protection Crisis: When the Absent State Faces the Threat of Personal Data Abuse

Afdal Mubarak[1], Andi Sri Amlinawaty Muin[2], Salmawati Salmawati [3]

[1]Faculty of Law, Muslim University of Indonesia
[2]Faculty of Law, Muslim University of Indonesia
[3]Faculty of Law, Muslim University of Indonesia

Surel Koresponden: afdalmubarak040@gmail.com

Abstrak: Penelitian ini bertujuan Untuk mengetahui dan menganalisis kecukupan peraturan perundang-undangan di Indonesia dalam mengatur pemanfaatan teknologi kecerdasan buatan (*Artificial Intelligence*) yang mengakses dan mengolah data pribadi masyarakat. Dan mengetahui dan merumuskan upaya hukum yang diperlukan untuk menutup kekosongan regulasi demi pencegahan penyalahgunaan kecerdasan buatan (A.I.) terhadap data pribadi. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang dianalisis secara preskriptif untuk menjelaskan ketentuan hukum yang berlaku serta memberikan argumentasi dan rekomendasi normatif. Hasil penelitian ini mengindikasikan bahwa Peraturan perundang-undangan di Indonesia belum secara khusus mengatur pemanfaatan *Artificial Intelligence* yang mengakses data pribadi masyarakat. Meskipun UU Perlindungan Data Pribadi telah memberikan dasar hukum, belum terdapat regulasi khusus yang mengatur karakteristik AI, sehingga pengaturan yang ada belum sepenuhnya memadai. Serta Upaya Hukum Yang Diperlukan Untuk Menutup Kekosongan Regulasi Agar Mencegah Penyalahgunaan A.I Terhadap Data Pribadi yaitu, Pembentukan Undang-Undang *Artificial Intelegence*, Penguatan Dan Harmonisasi Peraturan Perundang-Undangan Yang Telah Ada, Peningkatan Teknologi Forensik Digital, Penguatan Kewajiban Transparansi Dan Akuntabilitas Penyelenggara Sistem AI. Serta Penguatan Mekanisme Pengawasan Dan Penegakan Hukum

Kata Kunci: *Kecerdasan Buatan, Data Pribadi, Regulasi Hukum.*

Abstract*: This study aims to find out and analyze the adequacy of laws and regulations in Indonesia in regulating the use of artificial intelligence technology (Artificial Intelligence) that accesses and processes people's personal data. And knowing and formulating the necessary legal remedies to close the regulatory gap for the prevention of the misuse of artificial intelligence (A.I.) on personal data.This research is a normative law research with a legislative and conceptual approach. The legal materials used consist of primary, secondary, and tertiary legal materials that are analyzed prescriptively to explain the applicable legal provisions and provide normative arguments and recommendations. The results of this study indicate that laws and regulations in Indonesia do not specifically regulate the use of Artificial Intelligence that accesses people's* *personal data. Although the Personal Data Protection Law has provided a legal basis, there is no specific regulation that regulates the characteristics of AI, so the existing regulations are not fully adequate. As well as the legal measures needed to close the regulatory gap to prevent the misuse of personal data, namely, the establishment of the Artificial Intelligence Law, the strengthening and harmonization of existing laws and regulations, the improvement of digital forensic technology, the strengthening of transparency and accountability obligations of AI system operators. As well as strengthening the supervision and law enforcement mechanism*

Keywords: *Artificial Intelligence, Personal Data, Legal Regulation*

A. INTRODUCTION

Cybercrime is a new phenomenon in criminal activity that has emerged as a direct result of the rapid development of information and communication technology. Advances in digital technology facilitate data exchange, information access, and various internet-based activities. However, these developments also open up opportunities for irresponsible parties to commit various forms of cybercrime, such as hacking, personal data theft, online fraud, malware distribution, and misuse of information systems.[1]

Furthermore, the reliance on big data to train artificial intelligence (AI) models also raises various ethical issues. The data used to train AI systems is often obtained from diverse sources that may not be accurate, relevant, or free from bias. If the data contains imbalances or certain tendencies, the decisions made by AI have the potential to be non-objective and even discriminatory. This is because AI systems essentially learn from the data patterns they are given.[2]

For example, in healthcare or finance, AI algorithms trained on unrepresentative data can reinforce stereotypes or make decisions that disadvantage certain groups. For example, an AI-based credit scoring system might favor certain groups if its training data is dominated by specific economic groups. Similarly, in healthcare, if the data used does not reflect the diversity of the population, the medical recommendations generated by AI could be less accurate for certain groups.[3]

In Indonesia, although laws such as Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) have been enacted, their implementation is often not strict enough to anticipate the rapid development of AI technology. This creates legal loopholes that allow companies or individuals to collect data without adequate oversight, increasing the potential for exploitation. [4]

Furthermore, the limitations of current legal regulations in managing the complexity of artificial intelligence algorithms often pose substantial moral risks, such as algorithmic bias and over-reliance on machine-based systems. Experts highlight the need to revise the regulatory structure to be more flexible, incorporating self-auditing processes and strict penalties for violations. Without such interventions, innovative advances in artificial intelligence may be hampered by public concerns, which in turn will limit the technology's role in supporting sustainable national development.

The absence of such regulations is crucial to identify the shortcomings of the current legal system, assess the potential impacts of technology misuse, and encourage the development of more effective and comprehensive policies. This study aims to examine existing policies and their regulatory gaps in Indonesia, compare them with legal practices in various countries, and assess the potential risks of Artificial Intelligence (AI) misuse, particularly as they relate to personal data protection.[5]

B. METHOD

Penelitian ini merupakan penelitian hukum normatif dengan pendekatan yuridis normatif yang menempatkan hukum sebagai sistem norma berupa asas, kaidah, dan peraturan perundang-undangan. Tujuan penelitian adalah menganalisis kecukupan pengaturan hukum di Indonesia terkait pemanfaatan teknologi Artificial Intelligence dalam mengakses data pribadi serta potensi penyalahgunaannya. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) melalui telaah regulasi terkait perlindungan data pribadi dan kejahatan siber, serta pendekatan konseptual (conceptual approach) melalui kajian doktrin dan teori hukum. Bahan hukum yang digunakan terdiri atas bahan hukum primer seperti KUHP, UU ITE beserta perubahannya, dan UU Perlindungan Data Pribadi, bahan hukum sekunder berupa buku, jurnal, dan pendapat ahli, serta bahan hukum tersier seperti kamus hukum. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan, yang kemudian dianalisis secara kualitatif dengan metode deskriptif-analitis untuk menjelaskan, menafsirkan, dan mengevaluasi ketentuan hukum terkait pemanfaatan Artificial Intelligence dalam mengakses data pribadi.

C. DISCUSSION

1. Indonesian Legislation Concerning the Regulation of the Use of AI Technology That Accesses People's Personal Data.

In practice, these various potential violations have given rise to complaints and legal issues that can have serious consequences for the public. Personal data breaches can result in material and immaterial losses for data subjects, while copyright infringement can harm creators and undermine legal certainty in the intellectual property sector. Therefore, the use of AI technology that is not balanced with compliance with laws and regulations has the potential to give rise to legal conflicts and injustice.[6]

In the context of positive law in Indonesia, there are currently no laws and regulations that specifically and comprehensively regulate the use of Artificial Intelligence technology. However, the use of AI to access personal data remains subject to various general laws and regulations, particularly those governing electronic systems and personal data protection. Indonesia requires a more specific legal instrument to address these crimes. Currently, existing Indonesian law, specifically the Criminal Code (KUHP), only covers theft, fraud, extortion, and threats. These are regulated in Articles 335, 476, and 492 of the Criminal Code. [7] Article 335 of the Criminal Code regulates the crime of unpleasant acts, particularly those related to unlawful coercion of will, accompanied by threats or violence. This article is often used in the context of criminal law to prosecute acts such as threats, intimidation, or coercion, which are not explicitly covered by other specific articles of the Criminal Code. However, the application of this article is often criticized because it is considered to have broad elements and multiple interpretations, and therefore must be applied carefully to avoid excessive criminalization of expression or dissent. Article 335 of the Criminal Code reads: "Anyone who unlawfully forces another person to do, not to do, or to tolerate something, by using violence, the threat of violence, or any other act, whether against that person or against another person, shall be punished by a maximum imprisonment of one year or a maximum fine of four thousand five hundred rupiah." In the context of cybercrimes using Artificial Intelligence (AI), Article 335 of the Criminal Code can be associated if AI is used to: Send automated threats to someone; Force someone to provide personal data through digital threats. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is the main legal instrument in providing protection for people's personal data. Article 1 number 1 of the PDP Law defines personal data as any data about an individual who is identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic and/or non-electronic systems. Thus, data processed by an AI system, as long as it can identify the data subject, is included in the scope of protection of the PDP Law. [8]

Furthermore, Article 20 of the PDP Law stipulates that processing of personal data may only be carried out based on the valid consent of the data subject, unless otherwise stipulated by law. This provision also applies to the processing of personal data through AI technology, requiring every AI system operator to ensure a lawful basis for processing. Furthermore, Article 35 of the PDP Law regulates the data subject's right to obtain information regarding the clarity of their identity, the basis for their legal interest, the purpose of the request, and the use of their personal data. This normatively can be interpreted as an obligation for transparency in data processing, including AI-based processing.

In cases where personal data processing is carried out automatically and may have legal consequences or significant impacts on the data subject, Article 39 of the PDP Law grants the data subject the right to object to decisions based solely on automated processing, including profiling-based processing. This provision is relevant to the use of AI, particularly in automated decision-making, such as credit assessments, administrative selection, and behavioral monitoring. In addition to the PDP Law, regulations related to the use of AI can also be traced in Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 (the ITE Law). Article 15 of the ITE Law requires Electronic System Providers to operate electronic systems reliably, securely, and responsibly. This provision implicitly includes the obligation to secure personal data processed through AI systems. Furthermore, Article 26 paragraph (1) of the ITE Law emphasizes that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. [9]

However, although the PDP Law and the ITE Law provide a legal basis for personal data protection, these regulations are still general in nature and do not specifically address the specific characteristics of AI technology. There are no explicit provisions governing algorithm audits, AI system accountability, explainability requirements for AI decisions, or oversight mechanisms for the use of adaptive and self-learning AI.As in the case in Indonesia, the PeduliLindungi application was widely used for COVID-19 tracking and processed large amounts of personal data, such as names, National Identification Numbers (NIK), telephone numbers, locations, and health histories. In practice, the application system used algorithm-based automated processing to track and classify user data. In 2021–2022, reports emerged of user data leaks and misuse, including findings that data on the President and state officials was improperly accessed. This case demonstrates that electronic systems using automated processing (which conceptually aligns with AI) have not been balanced with specific regulations regarding system accountability, oversight, and audits. Legally, the handling of this case still relies on Article 26 paragraph (1) of the ITE Law and general data protection principles, because there are no specific provisions governing the use of AI or automated systems in managing personal data in the public sector. [10]

Furthermore, in recent years, facial recognition technology has begun to be used by law enforcement officials, local governments, and the private sector for security, surveillance, and public service purposes. This technology represents a concrete application of Artificial Intelligence that processes biometric data, which, according to Article 4 paragraph (2) of the PDP Law, is considered specific/sensitive personal data. However, to date, there are no laws and regulations specifically governing the limitations, procedures, and oversight of the use of facial recognition AI, including: Click or tap here to enter text. The use of this technology still relies on the general provisions of the PDP Law and the ITE Law, without specific technical regulations regarding AI. Various cases of leaks and misuse of personal data related to the use of electronic systems based on automated processing demonstrate that the use of technology with Artificial Intelligence (AI) characteristics has occurred in practice. However, legal handling of these cases still relies on the general provisions contained in the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law, because to date there are no laws and regulations that specifically and comprehensively regulate the use of Artificial Intelligence technology in processing people's personal data.[11] The absence of specific regulations regarding AI indicates a legal vacuum in addressing the rapid and dynamic development of technology. Current regulations still utilize a technology-neutral regulation approach, which does not specifically target any particular technology. While this approach provides flexibility in its application, in practice it has not fully addressed the various risks and legal challenges arising from the use of AI technology, particularly those related to the processing and protection of personal data.[12]

2. Laws Needed To Close Regulatory Gaps To Prevent AI Abuse Of Personal Data.

Although regulations regarding cybercrime already exist and are outlined in greater detail in the latest Criminal Code, this does not eliminate the need for regulations regarding artificial intelligence. Legislative bodies and their derivatives are still needed to regulate Artificial Intelligence Cybercrime or AI-based cybercrime. The current legal vacuum significantly impacts law enforcement and preventative measures taken by the government, law enforcement, and legal practitioners. There are also concerns that this legal vacuum could lead to an increase in the misuse of Artificial Intelligence for various types of cybercrime and other crimes in Indonesia. Therefore, legal reconstruction is needed to provide criminal law reform that clearly, in detail, and comprehensively regulates Artificial Intelligence and its law enforcement.[13]

Based on the explanation above and considering current legal and societal facts, there are several legal recommendations for reforming laws to combat Artificial Intelligence

Cybercrime, particularly in Indonesian jurisdictions. These legal reforms and actions that can be implemented immediately include the following:

1) Pembentukan Undang-Undang *Artificial Intelegence*

   Hingga saat ini, Indonesia masih belum memiliki produk hukum yang secara spesifik mengatur mengenai *Artificial Intelegence*. Tanpa adanya regulasi khusus yang mengatur mengenai kecerdasan buatan, sangat sulit untuk membedakan penggunaan *Artificial Intelegence* yang sah dan diperbolehkan serta yang dilarang dalam konteks kejahatan siber. Dalam Undang-Undang *Artificial Intelegence* tersebut, nantinya terdapat beberapa hal yang harus diatur. Beberapa hal yang direkomendasikan untuk diatur dalam undang-undang tersebut diantaranya:

   a. *Establishment of the Artificial Intelligence Act*
   b. Legal liability if AI is used as a medium and tool to commit crimes
   c. Technology monitoring and auditing that requires special state institutions or agencies to ensure that the development and use of AI is carried out in accordance with applicable legal norms.

2) Strengthening and harmonization of existing laws and regulations,

   Specifically, Law Number 27 of 2022 concerning Personal Data Protection. This strengthening can be achieved through the development of implementing regulations that explicitly regulate Artificial Intelligence-based personal data processing, including automated processing and profiling, as stipulated in Article 39 of the Personal Data Protection Law. This way, the general provisions of the Personal Data Protection Law can be more concretely operationalized to address the challenges of AI utilization.

3) Digital Forensic Technology Advancement.

   The misuse of personal data through cybercrime is becoming increasingly difficult to uncover, especially when it is carried out using Artificial Intelligence technology. AI systems enable the automated processing and distribution of personal data across systems, making the digital footprint of perpetrators increasingly complex to trace. This situation demands enhanced digital forensic technology capabilities in Indonesia so that law enforcement officials can identify, analyze, and prove legal violations related to the misuse of personal data. [14] The automated and anonymous nature of Artificial Intelligence makes it difficult to determine legal liability for personal data breaches. Therefore, improving digital forensics technology is a crucial step to ensure effective law enforcement in the area of personal data protection. Improved digital forensics infrastructure, through the provision of hardware and software capable of detecting, analyzing, and tracing Artificial Intelligence-based personal data processing in cybercrimes, allows for comprehensive disclosure of the flow of personal data use and misuse.

4) Strengthening the Transparency and Accountability Obligations of AI System Organizers.

   Article 35 of the PDP Law grants data subjects the right to obtain information regarding the purpose and use of personal data, which in the context of AI should be interpreted as an obligation for system administrators to provide adequate explanations regarding the logic of data processing and its impact on data subjects. Furthermore, Article 15 of Law Number 11 of 2008 concerning Electronic Information and Transactions requires Electronic System Administrators to operate systems reliably, securely, and responsibly, which normatively includes the use of AI systems that process personal data.[15]

5) Strengthening Supervision and Law Enforcement Mechanisms.

   The existence of a personal data protection supervisory body, as stipulated in the PDP Law, is a crucial instrument in addressing the issue of the effectiveness of personal data protection from AI misuse. An independent and authorized supervisory body is expected to ensure compliance by AI system administrators with legal provisions and provide effective legal protection for affected data subjects.

The development of Artificial Intelligence (AI) to access and process people's personal data has exceeded the capabilities of current positive legal regulations. Although the Personal Data Protection Law provides a normative basis for data subject rights, data controller and processor obligations, and personal data protection mechanisms, these regulations have not been specifically designed to address the complexities of AI-based data processing. Consequently, there is potential legal uncertainty, particularly in determining the limits of legal liability for automated decisions and personal data processing carried out by AI systems.[16]

Indonesia could adopt several key elements of regulations in these countries. First, implementing thorough audits for AI technology before its launch, as the European Union does, could help ensure that the technology in circulation is safe from potential misuse. Second, developing a policy of AI developer liability, similar to that in the United States, would allow for legal sanctions to be imposed on technology manufacturers who fail to anticipate security vulnerabilities or misuse of their products. Finally, China's centralized approach to data protection and digital security could serve as inspiration for developing comprehensive regulations to prevent data exploitation by AI technologies.[17]

Furthermore, Indonesia needs to encourage international cooperation in drafting these regulations, such as the Global Partnership on Artificial Intelligence (GPAI) initiative, which aims to strengthen global collaboration for the ethical and safe regulation and development of AI technology. With appropriate adaptation of international practices, Indonesia can create a legal framework that is more responsive to the risks of AI-based cybercrime.

D. CONCLUSION

Based on the above discussion, it can be concluded that the use of Artificial Intelligence (AI) technology to access and process personal data in Indonesia has not yet been specifically regulated in a comprehensive regulation. However, the use of AI remains subject to the general provisions of Law Number 27 of 2022 concerning Personal Data Protection and Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 concerning Amendments to the ITE Law, which regulates personal data protection obligations, data subject consent, and the responsibilities of electronic system administrators. However, these regulations are still general in nature and do not accommodate the specific characteristics of AI, such as automated processing, adaptive algorithms, and intelligent system-based decision-making, thus creating a legal vacuum (rechtsvacuum). Therefore, legal reform is needed through the establishment of specific AI regulations, strengthening the implementation of the PDP Law, increasing digital forensics capacity, and strengthening the transparency and accountability of AI system administrators to ensure personal data protection and prevent potential misuse of this technology.

E. REFERENCE

[1] D. Z. Abidin, P. Studi, and S. Informasi, “Kejahatan dalam teknologi informasi dan komunikasi,” vol. 10, no. 2, pp. 509–516, 2015.

[2] A. Bener, D. Bhugra, H. F. Moura, J. M. Castaldelli-maia, J. Torales, and A. Ventriglio, “The Humanitarian Emergency in the Gaza Strip : Urgent Actions for Advocacy in Mental Healthcare Management,” vol. XX, no. X, pp. 2–3, 2024, doi: 10.1177/02537176241305681.

[3] B. K. Hassani, “Societal biases reinforcement through machine learning – A credit scoring perspective arXiv : 2006 . 08350v2 [stat . ML] 31 Oct 2020,” pp. 66–72, 2020.

[4] E. Of, C. Of, and N. Of, “F AIRNESS AND B IAS IN A RTIFICIAL I NTELLIGENCE : A B RIEF S URVEY OF S OURCES , I MPACTS , AND M ITIGATION”.

[5] S. Agustin, “Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan

Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber," vol. 1, no. 6, pp. 500–504, 2024.

[6] E. S. Hasibuan and E. A. Putri, "Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya," vol. 10, pp. 70–83, 2024.

[7] Y. Daarul, H. Krueng, D. S. Rahmawati, S. D. Rosadi, and A. Cahyadini, "Implementasi Pelindungan Data Pribadi Berupa Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP) pada Sistem Pemerintahan Berbasis Elektronik Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Media Hukum Indonesia (MHI)," vol. 3, no. 2, pp. 739–749, 2025.

[8] R. D. Pakasi, Y. B. Runtunuwu, W. R. J. Lolong, P. Studi, I. Hukum, and U. Negeri, "Perlindungan Hukum terhadap Korban Tindak Pidana Pencurian Data Pribadi," no. 20, 2025.

[9] M. Gustryan and Z. A. Hoesein, "Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital," vol. 14, 2025.

[10] S. D. Puspasari and U. M. Pasuruan, "PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI TERKAIT PENERAPAN APLIKASI PEDULILINDUNGI DALAM UPAYA PENCEGAHAN COVID-19 DI INDONESIA," vol. 5, no. 1, pp. 30–41, 2023.

[11] P. Teknologi, D. Tantangan, H. Dalam, P. Dan, P. Data, and P. Di, "Indonesian Journal of Law," vol. 1, no. 12, pp. 312–320, 2024.

[12] Y. S. Wulandari, "KECERDASAN BUATAN DAN PERLINDUNGAN DATA : ANALISIS," vol. IX, no. 1, pp. 24–31, 2025.

[13] H. S. Disemadi, F. Hukum, and U. I. Batam, "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia," vol. 5, no. 36, pp. 177–199, 2021, doi: 10.25072/jwy.v5i2.460.

[14] D. Dan, P. Hak, and A. Manusia, "Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan Vol. 12 No 2 Desember 2025," vol. 12, no. 2, pp. 226–238, 2025.

[15] W. Kerta, J. Hukum, and A. Hindu, "No Title," vol. 8, no. November, pp. 98–109, 2025.

[16] A. I. D. I. Indonesia, "Jurnal Legal Reasoning," vol. 7, no. 2, pp. 224–248, 2025.

[17] A. Juliandi, A. R. Desiana, A. U. Hosnah, and N. Latif, "Analisis Perlindungan Data Pribadi dalam Implementasi Undang- Undang Nomor 27 Tahun 2022 di Era Artificial Intelligence," pp. 158–164, 2025.