ISSN 580-4340 (online)

LEGAL REVIEW OF THE USE OF PERSONAL DATA IN THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE UNDER THE PERSONAL DATA PROTECTION LAW

Habsya Amira Putri[1*]

[1]Sekolah Tinggi Hukum Indonesia Jentera
*Korespondensi: habsyaamira@gmail.com

Abstrak

Penggunaan data pribadi oleh platform media sosial untuk pelatihan kecerdasan buatan (AI) menghadirkan tantangan signifikan dalam melindungi hak privasi pengguna. Praktik semacam itu seringkali dilakukan tanpa transparansi yang memadai, sehingga menimbulkan risiko penyalahgunaan data yang melanggar prinsip-prinsip yang tercantum dalam Undang-Undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi ("Undang-Undang Perlindungan Data Pribadi" atau "UU PDP"). UU PDP menetapkan bahwa pengumpulan dan penggunaan data pribadi harus dilakukan secara sah, adil, transparan, dan berdasarkan persetujuan eksplisit dari subjek data. Namun, berbagai praktik, seperti "persetujuan paksa" dan pemrosesan data untuk tujuan yang tidak disetujui, sering terjadi di platform media sosial. Sistem AI seringkali kompleks dan memiliki algoritma yang menyulitkan pemahaman tentang bagaimana data pengguna dikumpulkan, diproses, dan digunakan. Kurangnya transparansi ini dapat mengakibatkan pelanggaran privasi yang tidak terdeteksi dan mempersulit pengguna untuk meminta pertanggungjawaban pengembang platform media sosial atas pengembangan sistem AI yang menggunakan data pribadi pengguna. Oleh karena itu, perlu ditetapkan suatu klasifikasi perlindungan data pribadi untuk menjaga kepentingan individu pengguna platform media sosial.

Kata Kunci: Data Pribadi, Kecerdasan buatan, Perlindungan Data Pribadi terkait Pengembangan Kecerdasan Buatan di Media Sosial

Abstract

The use of personal data by social media platforms for the training of artificial intelligence (AI) presents significant challenges in safeguarding users' privacy rights. Such practices are often carried out without adequate transparency, creating risks of data misuse that violate the principles set forth in Law No. 27 of 2022 on the Protection of Personal Data ("Personal Data Protection Act" or "PDP Act"). The PDP Act stipulates that the collection and use of personal data must be conducted lawfully, fairly, transparently, and based on the explicit consent of the data subject. However, various practices, such as "forced consent" and the processing of data for unapproved purposes, frequently occur on social media platforms. AI systems are often complex and feature algorithms that make it difficult to understand how users' data is collected, processed, and utilised. This lack of transparency can result in undetected privacy breaches and complicate users' ability to hold the developers of scsial media platforms accountable for the development of AI systems using users' personal data. Therefore, it is necessary to establish a classification of personal data protection to safeguard the interests of individual users of social media platforms.

Keywords: *Personal Data, Artificial Intelligence, Personal Data Protection related to Artificial Intelligence Development in Social Media.*

1. INTRODUCTION

The use of personal data by social media platforms to train artificial intelligence ("**AI**") presents significant challenges in safeguarding users' right to privacy. This practice is often conducted without adequate transparency, creating a risk of data misuse that violates the principles

set out in Law Number 27 of 2022 concerning Personal Data Protection ("**PDP Law**"). The PDP Law stipulates that the collection and use of personal data must be lawful, fair, transparent, and based on the explicit consent of the data subject. However, various practices, such as "coerced consent" and data processing for purposes not agreed upon by users, frequently occur on social media platforms. One such issue arises when social media providers fail to inform users that their personal data will be used for the development of artificial intelligence.

Policies implemented by technology service providers often lack transparency regarding the large-scale extraction of personal data, and users themselves are often unaware of how their personal data is protected. This is partly due to the nature of machine learning algorithms, which operate as a "black box" — meaning the internal logic of the AI system is frequently obscured from both users and, in some cases, even its developers. Social media technology providers have faced criticism for their opaque data processing practices.

The absence of accountability from technology providers gives rise to concerns about the protection of individuals who interact with AI-powered services in their daily lives. As human beings, users require a clear framework to ensure their personal data is adequately protected. Therefore, a more in-depth analysis is necessary to determine how social media platforms can comply with the provisions of the PDP Law and how the PDP Law can be effectively enforced.

2. METHODOLOGY

The research method employed in this legal writing is normative legal research, aimed at examining legal issues at the normative level in accordance with legal principles and doctrines. This study adopts a juridical-normative approach, which is based on the analysis of legislation relevant to the issues under review. Furthermore, the research focuses on literature study to obtain secondary data, allowing for the analysis of the relationship between statutory laws and other related regulations.

Primary legal materials consist of an inventory of statutory instruments as follows:

1. Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems ("**MoCI Reg 20/2016**");
2. Law Number 11 of 2019 concerning the National Science and Technology System ("**Science and Technology Law**");
3. Law Number 27 of 2022 concerning Personal Data Protection ("**PDP Law**");
4. Circular Letter of the Minister of Communication and Informatics Number 9 of 2023 concerning Artificial Intelligence Ethics ("**MoCI AI Circular 2023**");
5. General Data Protection Regulation or Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC ("**GDPR**");
6. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – 2021/0106 ("**AI Act 2021**");

7. European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Belgium, 2014 ("**EDPL Handbook**").

Bahan hukum sekunder adalah berasal dari jurnal-jurnal ilmiah yang dapat diakses melalui Secondary legal materials consist of academic journals accessible via Google Scholar and ResearchGate. Other secondary sources include data reports and information from APJII (Indonesian Internet Service Providers Association), Indonesian survey institutions, and relevant open-source data obtained via Perplexity AI — an AI-based chatbot that utilises large language models and data integration technology to deliver accurate, informative answers, along with a list of relevant references.

The approach used in this study is juridical-normative, which involves an examination of legal theories, concepts, principles, and applicable legislation related to the issues being studied. This method is also referred to as a library-based approach, which is conducted through the study of legal textbooks, statutory instruments, and other relevant legal documents.

3. ANALYSIS

3.1 Regulation of the Use of Personal Data for the Development of Artificial Intelligence

Personal Data Subjects have the right to object to the processing of their personal data. This is enshrined in Article 10 of the Personal Data Protection Law (PDP Law), which states:

"A Personal Data Subject shall have the right to object to decisions made solely on the basis of automated processing, including profiling, which produces legal consequences or significantly affects the Personal Data Subject."

The processing of personal data for the development of artificial intelligence (AI) may fall under the category of automated processing as regulated under Article 10 of the PDP Law. This article governs the processing of personal data carried out through automated means, including decisions that affect the data subject based on such processing.

Artificial intelligence systems, with their capacity to analyse and process vast amounts of data automatically, often make decisions or generate insights based on personal data that has been collected. This aligns with broader concerns that AI technologies are capable of processing data at scale without requiring the explicit consent of individuals, thereby raising issues around privacy and data protection.

The European Union provides specific rules concerning the collection of personal data for statistical purposes in the public interest, as outlined in Article 5(1)(b) of the General Data Protection Regulation (GDPR), which states:

"*Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*"

This can be interpreted as follows:

"*Collected for specific, explicit and legitimate purposes and not further processed in a way that contradicts those purposes; further processing for archiving in the public interest, scientific or historical research, or statistical purposes must comply with Article 89(1) and shall not be regarded as incompatible with the original purpose ('purpose limitation')*."

The GDPR thus requires that the processing of personal data must be based on clearly defined and lawful purposes. Article 5(1)(b) GDPR outlines that if the data is used for purposes beyond its original intent, such use must comply with the provisions under Article 89(1) GDPR, which states:

"*Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner*."

This may be interpreted as:

"*Processing for archiving purposes in the public interest, for scientific or historical research, or for statistical purposes must be accompanied by appropriate safeguards in accordance with this Regulation to protect the rights and freedoms of the data subject. Such safeguards must ensure respect for the principle of data minimisation. These measures may include pseudonymisation, provided that the purposes can still be achieved in that manner. If the intended purpose can be achieved through further processing that does not permit or no longer permits the identification of the data subject, then such processing must be carried out in that way*."

The GDPR thus clearly and specifically regulates the types of data that may be processed and the conditions under which such processing is permitted. Where data processing serves the public interest, scientific research, or historical research purposes, the rights and freedoms of data subjects must still be safeguarded. In this context, personal data originating from social media users may be classified as data used for public interest purposes and must be protected under Article 89(1) GDPR.

By contrast, Indonesia's normative legal framework does not yet explicitly define categories of personal data that require specific forms of protection or their treatment when used for public interest or scientific purposes.

Furthermore, Article 89(2) GDPR states:

"*Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21, subject to the conditions and safeguards referred to in paragraph 1 of this Article, in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*."

3.2 Protection of Personal Data in Relation to the Development of Artificial Intelligence

In the midst of rapid digital transformation, artificial intelligence (AI) has become a fundamental element across various sectors, including the academic sphere. The application of AI is grounded in the technology's capacity to process and analyse vast amounts of data in order to produce algorithm-based decisions tailored to human needs. However, the utilisation of AI also presents significant legal challenges, particularly with respect to the processing of personal data, which is frequently undertaken by social media platforms in their efforts to advance AI technologies.

Given these concerns, there is a pressing need for a clear regulatory framework governing the protection of personal data in the context of AI development. The following section provides a comparative legal analysis based on primary legal sources from Indonesia — namely the Personal Data Protection Law ("**PDP Law**"), Ministry of Communication and Informatics Regulation No. 20 of 2016 ("**MoCI Reg 20/2016**"), and the Ministerial Circular on AI Ethics ("**MoCI AI Circular**") — as well as legal instruments from the European Union, particularly the General Data Protection Regulation ("**GDPR**"). This comparative analysis is presented in tabular form below:

Table.3.2.1

Table of Analysis of PDP Law, MoCI Reg 20/2016, and GDPR.

Scope	PDP Law	MoCI Reg 20/2016	GDPR
Definition of Personal Data	Information about an individual who can be identified directly or indirectly.[1]	Personal data must be protected in terms of confidentiality.[2]	Information relating to an identified or identifiable individual.[3]
Legal Basis for Data Processing	Must be based on explicit consent or other lawful grounds.[4]	Consent must be given explicitly and be aligned with the purpose of personal data protection.[5]	Must have a lawful basis that is clearly specified, such as consent, legal obligation, or public interest.[6]

[1] Article 1 point 1 of the Personal Data Protection Law (PDP Law)

[2] Article 1 point 1 of the Regulation of the Minister of Communication and Informatics No. 20 of 2016 on the Protection of Personal Data in Electronic Systems

[3] Article 4(1) of the General Data Protection Regulation (GDPR)

[4] Article 20(2) of the PDP Law

[5] Pasal 2 ayat (2) Permenkominfo 20/2016

[6] Article 2(2) of MoCI Regulation No. 20/2016.

Data Subject Rights	Right to clarity of information[7], renewal[8], access[9],deletion[10], restriction of processing[11], correction and objection.[12]	Data subjects have the right to access, correct, update, and delete their data. They also have a right to privacy.[13]	Right to recctification[14], dihapus ("*right to be forgotten*"), data portability [15], and to processing in certain cases.[16]
Automated Decision-Making and Profiling	Data subjects have the right to object to automated decision-making.[17]	No specific provisions discussing AI and automated data processing for particular purposes	Strict restrictions on profiling and automated decision-making. [18]; Must have a clear legal basis and human intervention in some cases..
Data Security	Data controllers and processors must implement protective measures to prevent data breaches.[19]	Electronic systems processing personal data must have security certifications..[20]	Must apply "*privacy by design*" and "*privacy by default*" principles; obliged to report breaches within 72 hours.[21]

[7] Article 5 of the PDP Law.
[8] Article 6 of the PDP Law.
[9] Article 7 of PDP Law.
[10] Article 8 of the PDP Law
[11] Article 11 of the PDP Law
[12] Article 9 of the PDP Law
[13] Article 8(2) of MoCI Regulation No. 20/2016
[14] Article 16 of the GDPR – Right to Rectification
[15] Article 17 of the GDPR – Right to Erasure ("Right to be Forgotten")
[16] Article 20 of the GDPR – Right to Data Portability
[17] Article 10(1) of the PDP Law
[18] Article 22(1) of the GDPR – Automated Individual Decision-Making, Including Profiling
[19] Articles 35 to 37 of the PDP Law.
[20] Article 4(1) and (2) of the Regulation of the Minister of Communication and Informatics No. 20 of 2016 on the Protection of Personal Data in Electronic Systems
[21] Article 33 of the General Data Protection Regulation (GDPR) – Notification of a Personal Data Breach to the Supervisory Authority

International Data Transfers	Must be carried out with sufficient data protection safeguards or under regulatory compliance.[22]	Not explicitly regulated regarding cross-border data transfers.	Transfers allowed only to countries with adequate and appropriate data protection standards..[23]
Sanctions for Violations	Fines up to IDR 6 billion and/or imprisonment..[24]	Individuals who disseminate data without consent may face sanctions such as temporary suspension.[25]	Fines up to €10 million or 2% of global annual turnover.[26]
Principles of Data Protection	Emphasises legal certainty, public interest, usefulness, prudence, balance, accountability, and confidentiality.[27]	Data must be obtained lawfully, managed properly, and guaranteed to be secure.[28]	Emphasises transparency, accountability, data minimisation, and purpose limitation.[29]

It can be concluded that Law Number 27 of 2022 on Personal Data Protection (PDP Law) represents a progressive step within the Indonesian legal system, providing legal certainty regarding individuals' rights over their personal data.

Prior to the enactment of the PDP Law, regulations concerning personal data protection were fragmented across various sectoral regulations, such as the Regulation of the Minister of Communication and Informatics Number 20 of 2016 on the Protection of Personal Data in Electronic Systems, as well as the Law on Electronic Information and Transactions. The enactment of the PDP Law introduces several key advantages, including the explicit recognition of data subject rights, stricter obligations for data controllers and processors, and a clearer legal enforcement mechanism compared to previous regulatory frameworks.Meskipun demikian, jika dibandingkan dengan *General Data Protection Regulation* (GDPR)

[22] Articles 56 to 58 of the PDP Law
[23] Articles 44 to 50 of the GDPR – Transfers on the Basis of an Adequacy Decision
[24] Articles 67 to 73 of the PDP Law
[25] Article 36(1) of MoCI Regulation No. 20/2016.
[26] Article 83(4) of the GDPR – General Conditions for Imposing Administrative Fines
[27] Article 3 of the PDP Law.
[28] Article 2(2) of MoCI Regulation No. 20/2016
[29] Article 5 of the GDPR – Principles Relating to the Processing of Personal Data.

The European Union and Indonesia's PDP Law still diverge on several fundamental points, which may hinder the effectiveness of Indonesia's framework in safeguarding personal data in the digital age. One of the most significant differences between the two lies in the regulation of profiling and automated decision-making based on artificial intelligence.

Under the GDPR, profiling that may have legal effects or significantly impact individuals is strictly limited, and human intervention is required in automated decision-making processes.[30]. In contrast, Indonesia's PDP Law merely provides data subjects the right to object to automated processing, without offering any specific mechanism or safeguards[31] or safeguards limiting the use of AI in decisions that may affect individuals. This demonstrates that the PDP Law remains insufficient in addressing the potential risks posed by the misuse of artificial intelligence in personal data processing.

Moreover, in terms of sanctions, the GDPR imposes stricter administrative fines, with penalties reaching up to €20 million or 4% of a company's global annual turnover.[32] In contrast, the PDP Law provides for a maximum fine of IDR 6 billion (approx. €350,000)—a relatively small amount, especially in the context of potential violations by large technology companies. This disparity may result in lower levels of compliance in Indonesia compared to the European Union. In the context of cross-border data transfers, the GDPR allows data transfers only to countries with adequate levels of data protection or under strict safeguard mechanisms. Conversely, the PDP Law provides more flexibility in international data transfers, but lacks a stringent supervisory mechanism over the receiving countries. This flexibility opens the door for potential exploitation of Indonesian citizens' personal data by foreign entities, without adequate protection..[33]

Conversely, the Personal Data Protection Law (PDP Law) affords broader flexibility in the international transfer of personal data[34], without establishing a robust supervisory mechanism over the recipient country. This flexibility may create loopholes for the exploitation of personal data by foreign entities, leaving Indonesian citizens without adequate protection.

Another challenge in the implementation of the Personal Data Protection Law (PDP Law) lies in the institutional weakness of its supervisory framework. The GDPR establishes the European Data Protection Board [35](”**EDPB**”) as an independent authority responsible for ensuring compliance with the regulation. In contrast, Indonesia has yet to establish an independent supervisory body with strong enforcement powers to uphold the PDP Law. Moreover, public awareness regarding the importance of personal data protection remains relatively low, which creates a risk that the rights granted under the PDP Law may not be effectively exercised or enforced.

[30] Article 22 of the GDPR
[31] Article 10(1) of the Personal Data Protection Law (PDP Law)
[32] *Artikel* 83, GDPR. Article 83 of the GDPR.
[33] Articles 44 to 50 of the GDPR
[34] Articles 56 to 58 of the Personal Data Protection Law (PDP Law)
[35] *Artikel* 68, *European Data Protection Board.* GDPR.

Overall, while Indonesia has established a more structured legal framework for personal data protection through the enactment of the Personal Data Protection Law (PDP Law), several aspects still require improvement in order to enhance its effectiveness and bring it into closer alignment with global standards such as the GDPR. In the context of AI deployment, stricter regulations are necessary to ensure that technological advancement does not come at the expense of individuals' right to privacy. By pursuing more progressive regulatory reforms and developing a robust supervisory system, Indonesia can ensure that personal data protection remains a top priority in an increasingly complex digital era.

In 2021, the European Union introduced the Artificial Intelligence Act (AI Act), which was formally adopted on 13 March 2024 and will enter into force on 2 August 2026, with phased implementation beginning on 2 February 2025. According to the European Commission, the AI Act establishes a comprehensive risk-based methodology for identifying high-risk AI systems, which are deemed to pose significant threats to individuals' health, safety, or fundamental rights. These AI systems must comply with a set of mandatory horizontal requirements to ensure that AI remains trustworthy, and they must undergo conformity assessments prior to being placed on the EU market.

The risk-based approach is classified into: unacceptable risk (prohibited artificial intelligence practices), high risk (regulated high-risk artificial intelligence), limited risk which requires transparency, and minimal or low risk. The regulation stipulates that high-risk artificial intelligence systems processing special categories of personal data are subject to adequate safeguards for fundamental rights and individual freedoms, in other words, such artificial intelligence systems are subject to the EU GDPR. The following is an analysis of Circular Letter of the Minister of Communication and Informatics No. 9 of 2023 ("**CL of MoCI No. 9/2023**") and the Artificial Intelligence Act (Regulation (EU) 2024/1689), ("**AI ACT**"):

Table.3.2.2
Table of Analysis of CL of MoCI No. 9/2023 and AI ACT.

Scope	CL of MoCI No. 9/2023	AI ACT
Legal Basis	- Law No. 27 of 2022 concerning Personal Data Protection; - Law No. 11 of 2008 concerning Electronic Information and Transactions; - Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions;	- GDPR (General Data Protection Regulation - Regulation (EU) 2016/679) - Artificial Intelligence Act (Regulation (EU) 2024/1689)

Definition of Artificial Intelligence	Artificial intelligence is a form of programming on a computer device that performs processing and/or data management accurately.[36]	Artificial intelligence is a system based on machines that operates automatically at various levels of adaptability, prediction, recommendations, and decision-making.[37]
Regulatory Approach	Ethics of artificial intelligence serve as a guideline for the implementation of AI. The focus is on responsible and inclusive governance.	A risk-based and function-oriented approach focusing on risk, transparency, and accountability.
Transparency Principle	Artificial intelligence must be transparent in its use so it is not misused.[38]	The type and degree of transparency for high-risk AI systems must be determined based on purpose.[39]
Accountability Principle	Information produced by artificial intelligence must be accurate and accountable when disclosed to the public.[40]	AI system providers must notify the European Commission if the system meets the criteria for high risk within 2 weeks of fulfilling the requirements.[41]
Ethics and Safety	The ethical principle of artificial intelligence upholds the value of inclusivity[42] humanity[43], safety[44], accessibility[45], transparancy[46], credibility and accountability[47], protection of personal data[48],	Artificial intelligence is prohibited from engaging in: psychological manipulation and automated decision-making that may harm human rights.[51]

[36] Section on Definitions, paragraph (a), Circular Letter No. 9/2023 (MoCI)
[37] Article 3, paragraph (1), Definitions, AI Act
[38] Main Content of the Circular, paragraph 5, Circular Letter No. 9/2023 (MoCI)
[39] Article 13, paragraph 13, Transparency and provision of information to developers, AI ACT.
[40] Main Content of the Circular, paragraph 6, Circular Letter No. 9/2023 (MoCI)
[41] Article 52, Procedures, AI Act
[42] Main Content of the Circular, letter (b), point 1, Circular Letter No. 9/2023 (MoCI).
[43] Main Content of the Circular, letter (b), point 2, Circular Letter No. 9/2023 (MoCI)
[44] Main Content of the Circular, letter (b), point 3, Circular Letter No. 9/2023 (MoCI)
[45] Main Content of the Circular, letter (b), point 4, Circular Letter No. 9/2023 (MoCI)
[46] Main Content of the Circular, letter (b), point 5, Circular Letter No. 9/2023 (MoCI)
[47] Main Content of the Circular, letter (b), point 6, Circular Letter No. 9/2023 (MoCI)
[48]Main Content of the Circular, letter (b), point 7, Circular Letter No. 9/2023 (MoCI)
[51] Article 5, Prohibited AI Practices, AI Act

	sustanaibility[49], and intellectual property.[50]	
Biometric Identification and Social Scoring	AI must ensure the protection of personal data in accordance with applicable laws and regulations.[52]	Artificial intelligence is prohibited from using social scoring and biometric identification in public spaces without special permission.[53]
Use of AI in Automated Decision-Making in Public Services	Not regulated in the Circular, but relevant regulations can refer to the Electronic Information and Transactions Law (ITE Law).	High-risk artificial intelligence in public service decision-making (e.g., recruitment, education, social benefits) must be regulated by law.[54]
AI Classification	Use of AI technology includes subsets such as machine learning, natural language processing, expert systems, deep learning, robotics, neural networks, and others.[55]	The classification of artificial intelligence includes: Unaccaptable Risk AI (prohibited) [56] High Risk AI (regulated)[57] and General-purpose AI models with Systemic Risk and Limited Risk AI.[58]
Sanctions for Violations	Does not specify sanctions, but encourages compliance with existing regulations.	Provides for distinct sanctions for violations of AI prohibitions[59], breaches of obligations related to high-risk AI systems, and failures to meet transparency and reporting requirements.[60], breach of

[49] Main Content of the Circular, letter (b), point 8, Circular Letter No. 9/2023 (MoCI)
[50] Main Content of the Circular, letter (b), point 9, Circular Letter No. 9/2023 (MoCI)
[52] Main Content of the Circular, paragraph 7, Circular Letter No. 9/2023 (MoCI)
[53] Article 5, Prohibited AI Practices, AI ACT.
[54] Article 17, Quality Management System, AI ACT.
[55] Main Content of the Circular, letter (a), Circular Letter No. 9/2023 (MoCI)
[56] Article 5, Prohibited AI Practices, AI ACT.
[57] Article 6, Classification for high-risk AI System, AI ACT.
[58] Article 51, Classification of general-purpose AI Models as general-purpose AI models with Systemic Risk, AI ACT.
[59] Article 5, AI ACT.
[60] Article 6-17, AI ACT.

		transparency and reporting obligations[61].

According to Article 99 of the AI Act, sanctions for violations of artificial intelligence regulations must be effective, proportionate, and dissuasive. One of the most serious violations subject to the heaviest penalties is the use of prohibited AI, such as social scoring, psychological manipulation, and mass biometric identification, which may result in fines of up to €35 million or 7% of the total worldwide annual turnover, whichever is higher. In addition, high-risk AI systems—such as those used in recruitment, healthcare, and financial services—are required to meet strict standards regarding transparency, auditability, and human oversight. Failure to comply with these obligations may result in fines of up to €15 million or 3% of the total worldwide annual turnover.

The Circular Letter of the Minister of Communication and Informatics No. 9 of 2023 (CL No. 9/2023 – MoCI) reveals several weaknesses in the regulation of artificial intelligence, particularly in areas of risk classification, prohibition of harmful AI, enforcement mechanisms, transparency, and sector-specific regulation. One key shortcoming is the absence of AI risk classification, meaning all types of artificial intelligence are treated equally, without distinguishing between different levels of harm or societal impact. This differs from the EU AI Act, which categorises AI systems based on their level of risk, from minimal risk to high risk, with corresponding regulatory obligations proportional to the threat posed. Without a clear classification system, the Circular risks allowing high-risk AI to develop without adequate oversight.

Moreover, the Circular does not explicitly prohibit the use of harmful AI, such as social scoring, mass biometric surveillance, or psychological manipulation. The absence of these prohibitions opens the door to potential misuse of AI in mass surveillance and algorithmic discrimination, posing a serious threat to human rights. In contrast, the EU AI Act clearly prohibits AI used for social scoring and unauthorised biometric surveillance. Another major shortcoming of the Circular is the lack of enforcement mechanisms. The regulation only provides ethical guidelines, without any legal sanctions or binding consequences for companies that violate AI principles. Without auditing, monitoring, or penalty mechanisms, companies have little incentive to comply. This stands in stark contrast to the EU AI Act, which imposes fines of up to 7% of global turnover for serious breaches.

The lack of mandatory transparency is another weakness of the Circular. The regulation does not require AI companies to prepare technical documentation, undergo audits, or provide transparent information to users about how their AI systems function. This absence of transparency standards leaves AI systems in Indonesia vulnerable to bias, data misuse, and a lack of

[61] Article 52, AI ACT.

accountability. By comparison, the AI Act requires regular audits, technical documentation, and human oversight for high-risk AI systems. Additionally, Indonesian regulations fail to specify requirements for critical sectors such as finance, healthcare, law, and transportation, all of which are designated as high-risk under the AI Act and therefore subject to strict regulation.

From a normative legal perspective, the Personal Data Protection Law (PDP Law) only provides a basic option, namely the right to request the erasure of personal data by data subjects who feel harmed. However, if in practice it is found that the processing of personal data by a data controller carries a high potential risk to the data subject, the controller is required to conduct a Personal Data Protection Impact Assessment (DPIA). The term high potential risk refers to certain automated decisions that have legal effects or significantly affect the data subject.[62]

The processing of personal data carries a high potential risk when it involves automated decision-making that has legal effects or significant impacts on the data subject, particularly when the processing involves specific categories of personal data. One of the high-risk factors referred to in Article 10(2)(f) is the "use of new technologies in the processing of personal data."It can therefore be concluded that artificial intelligence, which operates based on the processing of personal data, constitutes a newly developed technology. Accordingly, under the PDP Law, it is recommended that a Personal Data Protection Impact Assessment ("**DPIA**") be carried out to safeguard the rights and interests of the relevant data subjects.

One of the key tools for assessing the impact of personal data protection is the Data Protection Impact Assessment ("**DPIA**"). A DPIA is carried out to evaluate the potential risks arising from the processing of personal data, as well as the measures or steps that must be taken to mitigate such risks. A DPIA is only required when the processing of personal data presents a high potential risk to the data subject. High-risk situations typically involve certain automated decisions. It can therefore be concluded that automated decision-making that has legal effects or causes significant impacts on the data subject falls within the scope of processing activities that require a DPIA.[63]

However, conducting a DPIA (Data Protection Impact Assessment) is not mandatory under the PDP Law. In fact, a DPIA should be mandatory for products or technologies that carry a high level of risk, one of which—new technology—is expressly mentioned in the PDP Law. Moreover, the Government Regulation that is supposed to govern the implementation of Personal Data Protection Impact Assessments has not yet been enacted. As a result, the only available DPIA indicators currently applicable in Indonesia are those partially regulated within Law No. 27 of 2022 itself.[64]

---

[62] Hukumonline, "*Memahami Data Protection Impact Assessments Dalam Perlindungan Data*." *Pribadi*.https://www.hukumonline.com/berita/a/memahami-data-protection-impact-assessments-dalam-perlindungan-data-pribadi-lt667615ca09b2e/ accessed 24 November 2024.

[63] *Ibid.*

[64] Tegar et al, 'Data Protection Impact Assessment Indicators in Protecting Consumer Personal Data on E-Commerce Platforms' (2024) 6(1) The Indonesian Journal of International Clinical Legal Education 111–150, 128.

Measures have also been proposed to support innovation, particularly through the establishment of an AI regulatory sandbox..[65] The use of personal data in certain artificial intelligence systems is permitted, provided that all stipulated requirements are met—for example, for the development of AI in crime prevention, maintaining public security, or improving environmental quality. However, such personal data must be erased once the agreed participation period has ended or the data retention period has reached its limit.[66]

4. CONCLUSION

Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) represents a significant step forward in regulating personal data protection in Indonesia. However, compared to the European Union's General Data Protection Regulation (GDPR), the Indonesian regulation still presents several weaknesses—particularly in its treatment of profiling and automated decision-making based on artificial intelligence, its lighter sanctions, and its less stringent mechanisms for international data transfers. Moreover, Indonesia has yet to establish a strong, independent supervisory authority comparable to the European Data Protection Board under the GDPR. To improve its effectiveness, there is a pressing need to strengthen AI-related regulation, increase penalties, and implement the principles of "privacy by design" and "privacy by default" in electronic systems.

The Circular Letter of the Minister of Communication and Informatics No. 9 of 2023 (CL No. 9/2023) also contains significant shortcomings in its regulation of artificial intelligence. Chief among these are the lack of risk classification, the absence of explicit prohibitions on harmful AI, the lack of legal enforcement mechanisms, insufficient transparency requirements, and the absence of sector-specific regulations. In contrast, the EU AI Act adopts a risk-based approach, imposing strict regulatory obligations on high-risk AI systems, whereas the Circular only provides ethical guidance with no clear sanctions. To enhance personal data protection and prevent the misuse of artificial intelligence, Indonesia should adopt a risk-based AI classification system, establish explicit bans on harmful AI practices, and introduce stronger audit and sanction mechanisms. This would ensure that AI regulation in Indonesia not only supports innovation but also safeguards human rights and public security.

Technology service providers are often criticised for their lack of transparency in data collection and processing practices. However, demanding full transparency from AI algorithms also carries risks. If an AI model is fully disclosed, it could be misused by malicious actors—for instance, through hacking or exploitation for illegal purposes. Therefore, it is crucial to have independent audit mechanisms and clear regulatory frameworks established by legislative authorities within the country. Measures such as Data Protection Impact Assessments (DPIA) are vital for evaluating and mitigating risks in personal data processing, particularly when using emerging technologies like artificial intelligence. Although not yet explicitly mandatory, conducting DPIAs is a necessary step to ensure stronger personal data protection. By implementing

[65] AI ACT, *Ibid.*

[66] Detiknews, *Ibid.*

transparent, secure, and accountable data management, the development of artificial intelligence can promote technological innovation without compromising the rights and privacy of data subjects. Consistent enforcement of the principles enshrined in the PDP Law is key to achieving a balance between technological advancement and personal data protection in the digital era.

REFERENCES

Circular Letter of the Minister of Communication and Informatics Number 9 of 2023 concerning Artificial Intelligence Ethics ("**MoCI AI Circular 2023**");

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Belgium, 2014 ("**EDPL Handbook**").

General Data Protection Regulation or Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC ("**GDPR**");

Hukumonline, "*Memahami Data Protection Impact Assessments Dalam Perlindungan Data.*" *Pribadi*.https://www.hukumonline.com/berita/a/memahami-data-protection-impact-assessments-dalam-perlindungan-data-pribadi-lt667615ca09b2e/ accessed 24 November 2024.

Law Number 11 of 2019 concerning the National Science and Technology System ("**Science and Technology Law**");

Law Number 27 of 2022 concerning Personal Data Protection ("**PDP Law**");

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – 2021/0106 ("**AI Act 2021**");

Regulation of the Minister of Communication and Informatics No. 20 of 2016 on the Protection of Personal Data in Electronic Systems

Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems ("**MoCI Reg 20/2016**");

Tegar et al, 'Data Protection Impact Assessment Indicators in Protecting Consumer Personal Data on E-Commerce Platforms' (2024) 6(1) The Indonesian Journal of International Clinical Legal Education 111–150, 128.