E-JUSTICE: JOURNAL OF LAW AND TECHNOLOGY

Vol. 1 No. 2, Jan-Jun 2025, pp 31-45

Research Article

Protection of Data Privacy in Artificial Intelligence-Driven World: An Indonesian Perspective

Matthew *Fabio*[1], Sofiah *Lailiyah*[2], Jose *Tjahjono*[3]

Corresponding e-mail: matthewfabio2001@gmail.com

Article Information

Article history
Received: Jan 8th, 2025
Revised: Jul 28th, 2025
Accepted: Jul 29th, 2025

Keywords:
Data Protection; Artificial Intelligence; Personal Data Protection Act; Indonesia

How to Cite:
Fabio, Matthew., Lailiyah, Sofiah., Tjahjono, Jose. "Protection of Data Privacy in Artificial Intelligence-Driven

Abstract

Background: *The increasing influence of AI has penetrated various sectors, including the domain of data privacy. Safeguarding data privacy is a fundamental human right necessitating robust legal protection. However, the advancement and application of AI technologies have prompted significant concerns regarding potential data privacy violations.*

Methodology: *This article employs doctrinal legal research with statutory approach.*

Objectives: *This article seeks to critically assess the extent to which the Indonesian Data Protection Act of 2022 addresses challenges arising from the proliferation of artificial intelligence (AI). This study will explore multiple dimensions: a) an analysis of the risks AI poses to data privacy; b) an examination of the implications of Article 20(2) (a) of the 2022 Data Protection Act in relation to AI development; and c) an evaluation of the existing legislative gaps that hinder effective regulation of AI's impact on data privacy.*

Findings: *The findings reveal notable deficiencies in Indonesia's current data protection laws, which inadequately address the*

[1] Faculty of Law, Universitas Surabaya, Indonesia | https://orcid.org/0009-0008-5779-221X
[2] Faculty of Law, Universitas Surabaya, Indonesia | https://orcid.org/0009-0003-4158-1593
[3] Faculty of Law, University of Waikato, New Zealand | https://orcid.org/0009-0009-6372-3429

World: An Indonesian Perspective." E-Justice: Journal of Law and Technology1, no. 2 (2025): 31-45

challenges posed by AI advancements. Furthermore, the incorporation of responsible AI principles into the legislative framework, particularly under Article 3 of the Data Protection Act 2022, is essential. Developers face significant hurdles due to Article 20(2) (a), which mandates explicit consent from data owners prior to AI development. Incorporating responsible AI concepts could justify exemptions from this strict consent requirement, facilitating regulation that is more balanced.

Originality/Novelty: *The novelty of this study lies in its comprehensive analysis of the Indonesian Data Protection Act 2022 through the lens of artificial intelligence (AI) governance, specifically highlighting the legislative gaps concerning data privacy risks posed by AI technologies. By focusing on Article 20(2) (a) and its implications for AI development, this research provides a novel perspective on how the strict consent requirement could hinder technological advancement. Furthermore, the study proposes a groundbreaking approach by advocating for the integration of responsible AI principles into Indonesia's data protection framework, emphasizing the need for a balanced consent mechanism under PDPA 2022. This innovative contribution addresses both regulatory insufficiencies and practical challenges faced by AI developers, offering a forward-looking perspective on harmonizing data protection with technological progress.*

Introduction

Indonesia has entered the era of Industry 4.0, which is characterized by the integration of automation and improved connectivity for interpersonal communication.[1] The term "Industrial Revolution" denotes a period characterized by swift and profound transformations, with "revolution" signifying a rapid and significant shift and "industry" denoting the activities and processes related to production and execution. According to the aforementioned definition, the Industrial Revolution can be characterized as a swift and profound shift in the adoption and execution of manufacturing methods. Originally, these procedures were executed using manual labour, but they were subsequently substituted by

[1] Paulus Wisnu Yudoprakoso, "KECERDASAN BUATAN (Artificial Intelligence) SEBAGAI ALAT BANTU PROSES PENYUSUNAN UNDANG-UNDANG DALAM UPAYA MENGHADAPI REVOLUSI INDUSTRI 4.0 DI INDONESIA Paulus," *Simposium Hukum Indonesia* 1, no. 1 (2019): 574–86, http://journal.trunojoyo.ac.id/shi.

automated machinery. The resultant output possesses commercial worth. Consequently, the labour-intensive tasks traditionally carried out by individuals have undergone a transformation, transitioning towards automated and digitized processes. The advent of the digitalization and automation eras is evident through the widespread integration of advanced technology across various domains of human existence. The observable progress in various aspects of contemporary society, such as the continuous advancements in information technology and the widespread integration of artificial intelligence into mainstream culture, serves as compelling evidence of major developments.

Artificial Intelligence (AI) refers to a computational system capable of doing activities that typically necessitate human intelligence. Ed Burns defines Artificial Intelligence (AI) as the replication of human intelligence processes through the utilization of machines, particularly computer systems.[2] AI encompasses various specific applications, such as expert systems, natural language processing, speech recognition, and machine vision. Individuals are utilizing artificial intelligence (AI) across Indonesia to fulfil their daily requirements. The utilization of this technology extends to many demographics, including students, those managing household affairs, public and private sector workers, as well as professionals engaged in business activities. The following are instances of artificial intelligence (AI) implementation in daily life within Indonesia: (a) Employment of search engines; (b) Utilization of online video or music streaming platforms or websites; (c) Deployment of tracking devices or the Global Positioning System (GPS); (d) Incorporation of selfie camera functionalities; (e) Utilization of online motorcycle taxi booking services; (f) Engagement with video games; (g) Utilization of internet marketing strategies; (h) Utilization of social media platforms; (i) Utilization of translation tools; (j) Utilization of online shopping platforms.

Artificial Intelligence (AI) is closely connected to the field of "Big Data Analytics" (referred to as BDA henceforth). According to the Gartner IT Glossary, the term "big data" refers to information assets that possess the characteristics of being high-volume, high-velocity, and/or high-variety. These assets require cost-effective and innovative methods of information processing in order to facilitate improved insight, decision-making, and process automation.[3] Artificial intelligence (AI) utilizes a technique known as "Machine Learning" (ML) to acquire knowledge from extensive datasets. Artificial Intelligence (AI) empowers robots to autonomously perform tasks, leading to the development of robotics. Machine Learning (ML) is a field of study that enables computers to acquire knowledge and make predictions based on experience without the need for explicit programming. Machine learning (ML) exhibits a greater emphasis on data analysis in contrast to artificial intelligence (AI). Machine Learning employs algorithms that facilitate the iterative learning process of computers through the analysis and utilization of data. Hence, the utilization of

[2] Ed Burns, "Artificial Intelligence (AI)," n.d., https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence.
[3] Budi Maryanto, "Big Data Dan Pemanfaatannya Dalam Berbagai Sektor," *Media Informatika* 16, no. 2 (2017): 14–19, https://jurnal.likmi.ac.id/Jurnal/7_2017/0717_02_BudiMaryanto.pdf.

artificial intelligence (AI) in the processing of large-scale datasets involves the application of machine learning techniques to acquire knowledge from data, enabling the execution of activities that typically necessitate human cognitive abilities.[4]

According to Article 20 Paragraph (2) Letter a of Law No. 27 of 2022, it is stipulated that the processing of personal data must be based on the explicit consent obtained from the individual whose data is being processed. The Personal Data Controller must obtain this consent prior to the commencement of any data processing activities. Hence, in order to ensure the proprietor of the personal data subject feels secure, it is imperative to obtain consent from the proprietor of the data subject. Obtaining approval from large-scale data owners necessitates a considerable amount of time, while the advancement of AI technology remains imperative. The issue at hand engenders discourse among AI developers and data owners due to the imperative nature of safeguarding personal data, which is seen as a fundamental aspect of human rights.

Artificial Intelligence (AI) not only offers advantages in addressing societal issues but also presents a challenge in the ongoing discourse surrounding the significance of privacy as a fundamental human right. Rapid technological advancements necessitate the handling of increasingly intricate and practical personal data, thereby intensifying the tension between these two concerns. The potential consequences of AI's independent development and its extensive utilization may surpass the detrimental effects already witnessed from the unregulated Internet. Hence, a compelling case can be made, based solely on the observations of Internet usage, the potential capabilities of artificial intelligence (AI), and its anticipated extensive adoption, to advocate for the implementation of a precautionary legal framework. This framework would establish fundamental regulations essential for protecting the public's interest in the advancement and utilization of AI. [5] This article aims to examine the extent to which the existing data protection act adequately addresses and perhaps mitigates the challenges posed by the development of artificial intelligence.

Research Method

This research used a doctrinal legal research by employing a statutory and conceptual approach. In addition to this, a detailed analysis is provided to proof the weak of Article 3 and Article 20 (2) letter a as a barrier for AI developer. The new concept is needed by proposing responsible AI principles as a new concept to address the current debates between AI developer and data owner for a win-win solution.

[4] Surender Reddy Salkuti, "A Survey of Big Data and Machine Learning," *International Journal of Electrical and Computer Engineering* 10, no. 1 (2020): 575–80, https://doi.org/10.11591/ijece.v10i1.pp575-580.
[5] Paul Nemitz, "Constitutional Democracy and Technology in the Age of Artificial Intelligence," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018), https://doi.org/10.1098/rsta.2018.0089.

The Relations between AI and Data Protection Act

The implementation of the Personal Data Protection Act in Indonesia is now taking place due to many factors. To begin with, it is important to acknowledge the prevalence of personal data misuse within the realm of internet usage. Instances of such misuse are observed across several platforms, including social media, internet banking, and public services. The consequences of such misuse can be highly devastating to the individuals who possess the data in question. The primary objective of the Data Protection Law is to achieve a harmonious equilibrium between the fundamental right to privacy of individuals and the imperative necessity of businesses to utilize data. The potential risks associated with artificial intelligence (AI) that jeopardize the security of individuals' personal data necessitate prompt attention and resolution. It is imperative to adopt a proactive approach and ensure the transparent deployment of AI systems in order to effectively manage these difficulties.

The principles and legislation pertaining to the safeguarding of individuals in the context of data processing ought to take into account and uphold the fundamental rights and liberties of individuals, including their entitlement to safeguard their personal data.[6] The principles of data protection encompass several fundamental rights, such as the right to privacy, the right to autonomy, the principle of transparency, and the principle of non-discrimination.[7]

Artificial intelligence (AI) is reliant on two fundamental components, namely programming techniques and extensive datasets. A programming algorithm refers to a systematic and logical technique or formula employed in the context of computer programming to address and resolve a given problem. The process involves executing a predetermined series of activities, wherein these actions delineate the procedural steps for accomplishing a task, ensuring that the computer consistently follows the prescribed instructions. The concept of big data encompasses a vast collection of data that may be subjected to computational analysis in order to uncover patterns, trends, and relationships, particularly in the context of human behaviour and interactions. The utilization of big data has emerged as a fundamental component in the development of artificial intelligence (AI), enabling AI systems to acquire knowledge and enhance their learning capabilities.[8] Companies and organizations frequently define "big data" as information assets that

[6] Russel Butarbutar, "Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia," no. January (2020), https://doi.org/10.2991/aebmr.k.200321.020.
[7] Yvonne McDermott, "Conceptualising the Right to Data Protection in an Era of Big Data," *Big Data and Society* 4, no. 1 (2017): 1–7, https://doi.org/10.1177/2053951716686994.
[8] Humerick and Matthew, "Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence," *Technology Law Journal* 34, no. 4 (2018), https://digitalcommons.law.scu.edu/chtljAvailableat:https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3
.

include distinct attributes, including substantial volume, rapid velocity, and diverse diversity. Consequently, the effective extraction of useful insights and the ability to make well-informed decisions necessitate the utilization of efficient and innovative techniques for processing this information.[9]

The process of data collection encompasses a wide range of information, including personally identifiable information (PII) as well as anonymous data sets derived from Internet of Things (IoT) devices.[10] The inclusion of machine logs and reference data collections from companies is essential in facilitating the machine learning process of artificial intelligence (AI).[11]

According to Article 20, Paragraph (2), Letter A, of Law No. 27 of 2022 on the Protection of Personal Data, it is stipulated that the Personal Data Controller must get valid consent from the data subject before processing their personal data. Hence, in order to safeguard the confidentiality and protection of personal data, it is imperative to obtain the explicit agreement of the data subject. The data subject has significant difficulties exerting control over the processing of their personal data. If the legal framework were not contemporaneous, the utilization of artificial intelligence systems in the processing of personal data would have a restricted influence on augmenting transparency.

The task of ensuring transparency in the handling of personal data by AI entities becomes ever more difficult because legislation and rights are primarily focused on human authorities and frameworks that prioritize human interests. This challenge is further compounded by the rising autonomy of AI entities.[12] The field of Artificial Intelligence exhibits a strong correlation with Big Data and is intricately intertwined with the safeguarding of personal data owners. Nevertheless, it is evident that the current state of the Personal Data Protection Law in Indonesia falls short of effectively addressing the various obstacles presented by the emergence of artificial intelligence (AI) within the country. Consequently, the existing legal framework fails to offer sufficient safeguards to ensure the comprehensive protection of personal data owners. The reason for this is that the efficacy of AI in fulfilling its stated objective of delivering convenience would be compromised if it were required to individually obtain valid authorization from a substantial number of data proprietors.

[9] Svetlana Sicular, "Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three 'V'S," 2013, https://blogs.gartner.com/svetlana-sicular/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/.
[10] Jacob Morgan, "A SIMPLE EXPLANATION OF THE INTERNET OF THINGS," 2018.
[11] Ian Murphy, "Could AI Lead to Breaches of GDPR?," 2017, https://www.enterprisetimes.co.uk/2017/06/21/ai-lead-breaches-gdpr/.
[12] R. van den Hoven van Genderen, "Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics," *European Data Protection Law Review* 3, no. 3 (2017): 338–52, https://doi.org/10.21552/edpl/2017/3/8.

The Barrier for AI Developer

The utilization of artificial intelligence in the present and future may give rise to numerous potential undesirable outcomes if the protection of personal data becomes challenging. The lack of explicit transparency in artificial intelligence (AI) systems instils concern among data owners over potential negative consequences across various domains. The task of individual filtering is a substantial difficulty for artificial intelligence, which in turn has profound implications for the optimal advancement of AI technology. The primary objective of AI is to offer global convenience to humanity. However, if the existing legislation in Indonesia fails to adequately tackle the issues confronting AI, such as the necessity of obtaining consent from those who possess personal data, the efficacy of AI would be compromised while in developing AI, it needs the accuracy, speed, and ease to obtain data as AI technology evolved very advance.[13]

Hence, it is imperative to prioritize clarity and transparency among personal data handlers, including artificial intelligence (AI), in order to provide reassurance and substantiate that the data utilized is legitimately employed for its intended purpose without posing any potential threats to the data subjects. While personal data protection in Indonesia is now robust, it is imperative to ensure transparent practices in the development of artificial intelligence (AI) to eliminate any potential hindrances faced by AI developers.

The integration of Artificial Intelligence (AI) into our future society has the potential to result in infringements on both our physical and informational well-being, irrespective of our awareness or consent. If legal frameworks fail to keep pace with the swift progress of technology, the prevailing regulatory gaps will continue to widen. Law enforcement agencies may encounter challenges in their ability to adequately monitor and control developing technology in a comprehensive fashion.[14] The provision outlined in Article 20, Paragraph (2), Letter of Law No. 27 of 2022 effectively establishes a clear and unambiguous regulation stipulating that prior to the processing of personal data pertaining to individuals, it is imperative to get legal consent from the rightful owner of this data. This implies that the protection of individual rights, as stipulated in Article 28, Paragraph (4) of the Constitution, is of the utmost importance. Nevertheless, a significant challenge arises from the extensive volume of data utilized in social and commercial networks. This renders it exceedingly difficult for individuals to exercise authority over the processing of their own data.

Additionally, obtaining consent from a multitude of entities would prove to be an exceedingly time-consuming task for data controllers. The efficacy and progress of AI in Indonesia will be hindered if the current legislation pertaining to Personal Data Protection fails to accommodate the evolving landscape of AI technology. Hence, it is imperative to

[13] See Fred H. Cate et al., "Expanding the Artificial Intelligence-Data Protection Debate", *International Data Privacy Law* 8, no. 4 (2018): 291.
[14] van den Hoven van Genderen.

implement a revision to the existing regulations in order to address the existing legal loophole pertaining to safeguarding the personal data of individuals who are the rightful owners of such data in the context of AI data processing.

The Debate between Consent with AI Developer

A disagreement ensued between the members of the community and the developer of the artificial intelligence system. This notion is rooted in the prevailing belief among the general populace that one of these programs is geared toward upholding human rights through the prioritization of data privacy protection and preservation. The fundamental requirement for privacy, both at an individual level and throughout society as a whole, is intrinsically linked to the anticipation that our governing bodies will safeguard our privacy against unwelcome intrusions. Nevertheless, in order to ascertain the actions that result in a violation of the right to privacy and the appropriate degree of safeguarding required, it is imperative to elucidate the definition of privacy and differentiate between the notion of privacy and the legal entitlement known as the right to privacy.[15]

The concept of privacy comprises its definition and the degree of significance ascribed to it, while the right to privacy applies to the recognition that privacy ought to be protected through legal means. The interconnection between the idea of privacy and the right to privacy is widely acknowledged, since a precise definition or a concrete comprehension of privacy is essential in order to construct an appropriate legal framework for safeguarding the right to privacy. Article 28G Paragraph (1) of the 1945 Constitution guarantees that privacy is protected under the law. Consequently, the state and everyone living in Indonesia must ensure that privacy is part of fundamental rights that must be preserved.

Privacy can be understood through six overarching categories: (1) the right to solitude and freedom from interference; (2) the ability to defend oneself against unwelcome intrusions; (3) the act of concealing certain information from others; (4) the authority to control personal information; (5) the protection of one's personality, individuality, and dignity; and (6) the ability to regulate access to intimate relationships or aspects of one's life.[16]

Privacy, regarded as an inherent entitlement, has been delineated as the entitlement to solitude.[17] In societies, individuals possess the right to be exempt from any form of interference or intrusion. The concept refers to a range of rights that are inherent in the idea of a well-organized society and are intricately linked to the right to uphold secrecy and restrict the sharing of personal information with others. The fundamental concept of the right to privacy involves the ability to protect a distinct realm of our existence from

[15] Daniel J. Solove, "Conceptualizing Privacy," *The Individual and Privacy: Volume I* 90, no. 4 (2016): 333–401, https://doi.org/10.1145/1929609.1929610.
[16] Daniel Solove, "Understanding Privacy," *Library Review* 59, no. 7 (2010): 562–63, https://doi.org/10.1108/00242531011065163.
[17] Willes J et al., "The Right To Privacy," *Angewandte Chemie International Edition, 6(11), 951–952.* 4, no. Mi (1967): 5–24.

unwarranted interference by the government and others. The concept comprises a broad spectrum of elements, which include the regulation of personal information, safeguarding against surveillance, the entitlement to privacy within one's residence, individual self-governance, physical well-being, and other interconnected entitlements.

The evolution of technology, particularly the internet and artificial intelligence, has led to a paradigm shift in the practices of government and private monitoring. Traditional surveillance and human intelligence gathering have been supplanted by a method known as "data mining." This process involves the intelligent exploration of extensive volumes of pre-existing data in order to uncover novel insights. Moreover, the extensive availability and retrieval of diverse information sources on the Internet, lacking sufficient filtration mechanisms, eventually encroaches upon individuals' privacy. The current issue pertaining to privacy legislation resides in its inadequacy to accommodate technical progressions or conform to social and individual conceptions of privacy, as well as its incapacity to match the rapid developments in the digital realm. This phenomenon elicits concern among individuals due to the capacity of artificial intelligence (AI) to engage in machine learning processes, wherein data is gathered to facilitate the advancement of AI systems, enabling them to emulate human intellect. Importantly, this data collection occurs without the explicit knowledge or consent of the individuals who own the personal data.

However, the requirement of obtaining consent could provide a potential obstacle, as the acquisition of personal data pertaining to the subject would significantly enhance the intelligence of the AI system. The employed approach utilizes a machine learning technique to analyse and process large-scale datasets. Machine learning holds significant prominence within the realm of artificial intelligence. The primary goal of machine learning is to uncover valuable insights and facilitate informed decision-making processes. Machine learning algorithms can be classified into three main categories: supervised, unsupervised, and semi-supervised. [18] In the context of large amounts of data, scaling up machine learning algorithms becomes imperative.

The relation and support between AI and big data is expected to exert a significant impact on the advancement of technology and the generation of innovative solutions. [19] The utilization of big data technologies has significant implications for scientific advancements and the generation of economic value. The field of artificial intelligence has witnessed the emergence of deep machine learning as a prominent area of research. The technique under consideration is a sort of machine learning that leverages multiple layers of information processing stages within hierarchical systems. The computational process involves the generation of hierarchical features or representations of the observational data, with the

[18] C. L. Philip Chen and Chun Yang Zhang, "Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data," 2014, https://www.researchgate.net/publication/262305146_Data-intensive_applications_challenges_techniques_and_technologies_A_survey_on_Big_Data.

[19] Yuri Demchenko et al., "Addressing Big Data Issues in Scientific Data Infrastructure," *Proceedings of the 2013 International Conference on Collaboration Technologies and Systems, CTS 2013*, no. May (2013): 48–55, https://doi.org/10.1109/CTS.2013.6567203.

higher-level features being derived from the lower-level ones. Artificial intelligence (AI), particularly machine learning algorithms trained on large datasets, plays a pivotal role in advancing technological and scientific endeavours. However, the progress of AI might be impeded by the need to obtain agreement from the owners of the data being utilized.

Hence, a contentious issue arises between the public and developers of artificial intelligence (AI) about the issue of obtaining consent for the utilization of personal data in the advancement of AI technology. The ongoing discourse between the community and developers of artificial intelligence (AI) canters on the safeguarding of human rights, particularly with regard to the preservation of data privacy. Privacy is considered an inherent and essential entitlement that spans a multitude of dimensions, encompassing the entitlement to seclusion, authority over personal data, and safeguarding against intrusive monitoring. The advancement of technology, particularly in the fields of artificial intelligence (AI) and the internet, has given rise to apprehensions regarding privacy infringement via unauthorized data mining and the unauthorized collection of personal information.

Based on the aforementioned reasoning, data privacy can be regarded as a tangible expression of the fundamental rights of individuals within a society. Hence, in accordance with the provisions outlined in Article 20, Paragraph 2, Letter a, and Article 3 of the Data Protection Act of 2022, obtaining consent is deemed necessary in relation to matters concerning personal data. On one side of the argument, the concept of consent introduces complexities and obstacles for AI programmers. There exist disparities in perspectives between societal actors and technologists about the development of artificial intelligence (AI). In the end, the developer takes data or does data mining without approval from the black market, and if collecting data is difficult, and then it will be in all ways both legal and illegal. Hence, a conflict arises between legal principles and the objectives of scientific endeavours and technical advancements.

In the end, the debate between consent for personal data and machine learning methods for big data can be addressed through the implementation of responsible AI principles. These principles, such as privacy protection, reliability, transparency, fairness, contestability, accountability, human well-being, and human-cantered values, provide an ethical framework for the use of AI technology. Responsible AI emphasizes human control, technical robustness, and safety measures to prevent harm. It promotes transparency, accountability, and the inclusive benefit of AI for all members of society.

The Responsible AI Principles

The debate between the consent of personal data subjects and machine learning methods for big data can be resolved with the concept of responsible AI Principles. In developing and implementing AI technology, new principles emerge and must be followed by technicians and users including data owner. The new emerging principle for AI

development called as responsible AI principles. There are several principles listed in developing and using AI technology, viz.:

a) human agency and oversight
b) technical robustness and safety
c) privacy
d) transparency
e) diverse and non-discriminatory systems
f) benefit all of society
g) accountability

The principles above reaffirm the passion in the development and use that humans can control from the AI technology itself. Therefore, AI technology is not allowed to be developed and used anonymously. It should be clear who develops and uses, and who exercises control over the technology. In addition, AI technology must be safe from the impact of AI technology. So that if AI technology is created and used that actually has a bad impact, it is actually contrary to the principles of responsible AI. Another principle is privacy, where every developer and user must submit to and respect privacy, including personal data.[20] People need more protection for their privacy and hence more control over their data.[21]

Therefore, in developing and using AI technology, it must not violate the privacy rights of others. Another principle is transparency. This principle provides guidelines that results or products from AI technology must be able to be documented so that the parties involved (stakeholders) can access these documents. Transparency is a fundamental need in both governmental and business uses of decision-making algorithms. This accessible information will help users to understand how algorithms influence which information they see and which information appears most often.[22]

The concept of responsible AI revolves around the ethical framework that governs the use of AI technology, with a focus on promoting the well-being and benefit of individuals. This principle encompasses a set of codes aimed at ensuring the ethical, transparent, and accountable application of AI technologies, including the involvement of human oversight and agency. It emphasizes the importance of human control over AI systems at all times. Additionally, responsible AI entails technical robustness and safety measures to prevent harm.

Privacy is another key principle, emphasizing the security and lawful collection of data. Transparency is also crucial, as it requires the documentation of AI system outcomes and

[20] Rofi Aulia Rahman et al., "Constructing Responsible Artificial Intelligence Principles as Norms : Efforts to Strengthen Democratic Norms in Indonesia and European Union A . Introduction The Cambridge Analytica Scandal Is One of the Striking Cases That Showcased the Influence of Art" 5 (2022): 231–52.
[21] Larry Diamond, "Rebooting Democracy", *Journal of Democracy*, Vol.32, no. 2, 2021: 183
[22] Eileen Donahoe and Megan MacDuffee Metzger, "Artificial Intelligence and Human Rights", Journal of Democracy Vol.30, no. 2, (2019): 124.

making them accessible to stakeholders. This includes the creators of AI being open about the processes, reasons for using AI, and limitations of the systems. It also necessitates that people understand and interpret the behaviours of AI systems.

The principle of AI benefiting all members of society highlights the importance of ensuring that AI technology serves the interests and needs of everyone. Finally, the accountability principle stresses the need for individuals to take responsibility for any errors or mistakes made by AI systems. This accountability helps prevent irresponsible actions and requires human beings to be answerable for the actions of AI systems. These principles provide guidance for regulating AI technology and establishing norms that promote the responsible and ethical use of AI systems.

However, the implementation of ethics principles in practice requires an improved understanding of the practices of designers and developers of AI systems and how they relate to high-level ethics principles. Not only implementing the Responsible AI Principles but also providing an understanding to AI engineers regarding the Responsible AI Principles. This will allow them to understand the high ethical principles applied later on to the latest AI technologies. In addition, this principle must also be applied to Indonesian national law. One of them are Data Protection Act 2022 but putting this responsible AI principles as a norm within that law. By inserting such principles into data protection act 2022, the law is also not only to overcome current problems but can resolve the problem in the future regarding AI technology and data protection.

It is recommended that AI engineers adhere to the Responsible AI Principles while using personal data. If their actions align with these principles, they can proceed with utilizing personal data even without explicit consent. However, it is crucial to ensure that the Responsible AI Principles are strictly followed to safeguard the ethical and responsible use of data in AI development. In addition, the goal of AI technology must be developed in a transparent manner, be beneficial to human civilization and society, and avoid harmfulness. Therefore, inserting responsible AI principle to Article 3 of Data Protection Act 2022 is needed to evolve the principle into norm. Furthermore, the Article 20 Paragraph (2) letter a can be affected as well since in current concept, consent is a strict requirement prior to use their data. However, by implementing the new responsible AI principle, the consent from the data owner can be excused as long as the AI developer implement the responsible AI principle as their ethical guideline in developing AI technology.

Conclusion

The role of big data in supporting the development of AI faces some challenges to data privacy. The debate arises in Article 20 (2) letter a of the Data Protection Act 2022 regarding consent. The AI developer or engineer needs to obtain data with ease since speed and accuracy of data in the AI-driven world plays an important role; however, the sharing of data without strict consent from the data owner is a human rights violation. Therefore, there must be an alternative solution for AI engineers and data owner by amending the

current Data Protection Act 2022 by inserting responsible AI principles as a norm. Then, the AI developer can still develop AI technology for human being. Other than that, the Article 20(2) can be excuses as long as the engineer implement the responsible AI principle in using data from the data owner.

Acknowledgment

None

Conflict of Interest

No conflict of interest

Author(s) Contribution

Author contribution : Author 1: initiated the research ideas, instrument construction, data collection, analysis, and draft writing;
Author 2: revised the research ideas, literature review, data presentation and analysis, and the final draft;
Author 3: contributed to draft the revised article as suggested by the reviewer.

References

Aulia Rahman, Rofi, Valentino Nathanael Prabowo, Aimee Joy David, and József Hajdú. "Constructing Responsible Artificial Intelligence Principles as Norms : Efforts to Strengthen Democratic Norms in Indonesia and European Union A . Introduction The Cambridge Analytica Scandal Is One of the Striking Cases That Showcased the Influence of Art" 5 (2022): 231–52.

Burns, Ed. "Artificial Intelligence (AI)," n.d. https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence.

Butarbutar, Russel. "Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia," no. January (2020). https://doi.org/10.2991/aebmr.k.200321.020.

Demchenko, Yuri, Paola Grosso, Cees De Laat, and Peter Membrey. "Addressing Big Data Issues in Scientific Data Infrastructure." Proceedings of the 2013 International Conference on Collaboration Technologies and Systems, CTS 2013, no. May (2013): 48–55. https://doi.org/10.1109/CTS.2013.6567203.

Eileen Donahoe and Megan MacDuffee Metzger, "Artificial Intelligence and Human Rights", Journal of Democracy Vol.30, no. 2, (2019): 124.

Fred H. Cate et al., "Expanding the Artificial Intelligence-Data Protection Debate", International Data Privacy Law 8, no. 4 (2018)

Hoven van Genderen, R. van den. "Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics." European Data Protection Law Review 3, no. 3 (2017): 338–52. https://doi.org/10.21552/edpl/2017/3/8.

Humerick, and Matthew. "Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence." Technology Law Journal 34, no. 4 (2018). https://digitalcommons.law.scu.edu/chtljAvailableat:https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3.

J. Solove, Daniel. "Conceptualizing Privacy." The Individual and Privacy: Volume I 90, no. 4 (2016): 333–401. https://doi.org/10.1145/1929609.1929610.

J, Willes, In Millar, Taylor, and Burr. "The Right To Privacy." Angewandte Chemie International Edition, 6(11), 951–952. 4, no. Mi (1967): 5–24.

Larry Diamond, "Rebooting Democracy", Journal of Democracy, Vol.32, no. 2, 2021: 183

Maryanto, Budi. "Big Data Dan Pemanfaatannya Dalam Berbagai Sektor." Media Informatika 16, no. 2 (2017): 14–19. https://jurnal.likmi.ac.id/Jurnal/7_2017/0717_02_BudiMaryanto.pdf.

McDermott, Yvonne. "Conceptualising the Right to Data Protection in an Era of Big Data." Big Data and Society 4, no. 1 (2017): 1–7. https://doi.org/10.1177/2053951716686994.

Morgan, Jacob. "A SIMPLE EXPLANATION OF THE INTERNET OF THINGS," 2018.

Murphy, Ian. "Could AI Lead to Breaches of GDPR?," 2017. https://www.enterprisetimes.co.uk/2017/06/21/ai-lead-breaches-gdpr/.

Nemitz, Paul. "Constitutional Democracy and Technology in the Age of Artificial Intelligence." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 376, no. 2133 (2018). https://doi.org/10.1098/rsta.2018.0089.

Philip Chen, C. L., and Chun Yang Zhang. "Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data," 2014. https://www.researchgate.net/publication/262305146_Data-intensive_applications_challenges_techniques_and_technologies_A_survey_on_Big_Dat.

Reddy Salkuti, Surender. "A Survey of Big Data and Machine Learning." International Journal of Electrical and Computer Engineering 10, no. 1 (2020): 575–80. https://doi.org/10.11591/ijece.v10i1.pp575-580.

Sicular, Svetlana. "Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three 'V'S," 2013. https://blogs.gartner.com/svetlana-sicular/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/.

Solove, Daniel. "Understanding Privacy." Library Review 59, no. 7 (2010): 562–63. https://doi.org/10.1108/00242531011065163.

Wisnu Yudoprakoso, Paulus. "KECERDASAN BUATAN (Artificial Intelligence) SEBAGAI ALAT BANTU PROSES PENYUSUNAN UNDANG-UNDANG DALAM UPAYA MENGHADAPI REVOLUSI INDUSTRI 4.0 DI INDONESIA Paulus." Simposium Hukum Indonesia 1, no. 1 (2019): 574–86. http://journal.trunojoyo.ac.id/shi.