

Biometric Data Processing Based on Artificial Intelligence and the Principle of Accountability: A Comparative Study of Indonesia and European Union

Sinta Dewi¹⁾, Audena Priscilla Sihombing²⁾ & Tri Andika³⁾

¹⁾Faculty of Law, Universitas Padjadjaran, Indonesia, E-mail: sinta@unpad.ac.id

²⁾Faculty of Law, Universitas Padjadjaran, Indonesia, E-mail: audena21001@mail.unpad.ac.id.

³⁾Faculty of Law, Universitas Bengkulu, Indonesia, E-mail: andikatri@unib.ac.id

Abstract. *Digital advances in Artificial Intelligence (AI) have accelerated the use of biometric data to speed up identification with high accuracy. However, the processing of biometric data raises serious privacy challenges, particularly regarding security and data controllers' accountability. Using normative juridical research methods with descriptive-analytical approaches, laws and regulations, legal doctrines, scientific literature, and practical cases, including World App, Holy Moment, and Clearview AI, this study aims to analyze the application of accountability principles in AI-based biometric data processing through a comparative study between Indonesia and the European Union. The findings indicate that in Indonesia, Law Number 27/2022 on Personal Data Protection (PDP Law) provide a legal basis for biometric data protection; however, its implementation remains constrained by weak supervision, the absence of derivative regulations, and limited understanding of privacy among the public and business actors. In contrast, the European Union, through the General Data Protection Regulation (GDPR) and the EU-AI Act, enforces a robust accountability principle supported by strict oversight and substantial sanctions, resulting in more effective protection of biometric data. The recommendations of this study include strengthening AI regulations and supervisory mechanisms in Indonesia to ensure that AI-based biometric data processing is conducted lawfully, transparently, and responsibly, while simultaneously fostering public trust in digital technologies.*

Keywords: *Artificial; Data; Intelligence Personal.*

1. Introduction

Digital transformation is driven by advances in information technology that facilitate the access to and dissemination of information across various sectors,

supported by technologies such as the Internet of Things (IoT), AI, and robotics (Sinta Dewi, 2016). The increasingly widespread use of digital technologies has given rise to new challenges, particularly concerning data security and privacy. Data has become a highly valuable asset that is vulnerable to misuse, making legal compliance in personal data protection and information security an important aspect of digital transformation.

Sensitive data is particularly vulnerable to cybercrime, thereby requiring that technological development be accompanied by robust security systems and strict compliance with data protection regulations, such as the GDPR. Personal data is information relating to an identifiable individual, while personal data protection encompasses all measures aimed at safeguarding the rights of data subjects. Within the data protection regime, a Personal Data Controller determines the purposes and means of personal data processing, whereas a Personal Data Processor carries out data processing activities on behalf of the controller (Sinta Dewi Rosadi dan Garry Gumelar Pratama, 2018).

Failure to protect personal data gives rise to serious legal consequences as regulated under PDP Law, including notification obligations, administrative sanctions up to monetary fines, as well as criminal liability. Although the accountability of Data Controllers and Data Processors has been explicitly stipulated, law enforcement in Indonesia remains weak, resulting in suboptimal effectiveness of personal data protection in the absence of strong and independent oversight mechanisms.

The GDPR in the EU serves as an international benchmark for personal data protection by emphasizing the principles of security, confidentiality, and accountability of data controllers, including obligations to document and report personal data breaches. By way of illustration, Clearview AI is a facial recognition company that uses automated technology to collect billions of images from the internet and identify individuals. The large-scale collection of images for the processing of personal data by companies requires strict data protection principles (Catherine Jasserand, 2022).

The large-scale collection of images without consent poses serious risks to privacy, data security, and individual rights, thereby necessitating responsibility, ethical standards, and accountability on the part of data controllers. In the Clearview AI case, the French data protection authority imposed a fine of up to EUR 20 million and ordered the cessation of data processing and the erasure of the data, accompanied by daily penalty payments to ensure compliance (EDPB, 2022). In another country, the Netherlands, this company imposed a fine of EUR 30 million on Clearview AI for processing personal data without a lawful legal basis, thereby underscoring the importance of the accountability principle and the obligation of data controllers to comply with, and to be able to demonstrate compliance with, the GDPR (Dutch Data Protection Authority, 2024).

In Indonesia, law enforcement in the protection of personal data are not yet as robust as those in the European Union, both in terms of regulatory frameworks, institutional capacity, and public awareness. Based on a review of prior studies, the author is interested in examining AI-based biometric data processing with a primary focus on the principle of accountability through a comparative analysis between Indonesia and the EU.

Based on the background outlined above, this article attempts to answer the following research questions:

- 1) To what extent do the legal frameworks of Indonesia (PDP Law) and the EU (the GDPR) provide protection for biometric data processed through AI in Indonesia?
- 2) What are the challenges and legal implications in the implementation of the accountability principle in Indonesia when compared to the European Union?

2. Research Methods

The research methodology is designed to analyze legal issues in a systematic and in-depth manner, particularly with regard to personal data protection. This study adopts a normative juridical approach, which emphasizes the examination of secondary legal materials in the form of statutory regulations, legal doctrines, and relevant literature. This approach is selected because the object of the research focuses on positive legal norms governing personal data protection and AI in Indonesia and the EU; therefore, the analysis is conducted through the identification and interpretation of applicable legal provisions. The research specification is descriptive-analytical, aiming to clearly and comprehensively describe existing legal regulations and subsequently analyze them using relevant legal theories. Through this specification, the study not only presents legal rules on personal data protection and artificial intelligence but also systematically and comparatively examines the implementation of legal principles between Indonesia and the EU.

3. Result and Discussion

3.1. Implementation of the Accountability Principle in the Processing of AI-Based Biometric Data in Indonesia and the European Union

In the processing of AI-based biometric data, the principle of accountability becomes crucial due to the high sensitivity of biometric information. Data controllers are obliged to ensure that processing is carried out lawfully, transparently, and in accordance with the applicable data protection legal framework. In addition, data controllers must provide clear information regarding the purpose, legal basis, and operational mechanisms of AI systems to ensure transparency and build public trust.

In May 2025, the public was introduced on World App and Worldcoin. World App

is a digital wallet within the Worldcoin ecosystem, developed by Tools for Humanity to establish globally verified human identities. This application enables the storage of World ID, management of crypto assets, and access to Mini Apps (Raihan Fadilah, 2025). Identity verification is conducted through retinal scanning using the Orb device equipped with the IRIS system, which converts iris images into unique AI-based numerical codes to securely ensure individual uniqueness.

World App users have the opportunity to receive free Worldcoin tokens upon iris verification, which can be converted into Indonesian Rupiah ranging from approximately IDR 300,000 to IDR 800,000. This incentive has encouraged many Indonesians to register and undergo retinal scans without fully understanding the purpose and potential risks associated with the use of their biometric data (Defara Dhanya, 2025).

World App has attracted global attention due to concerns regarding the processing and deletion of biometric data by the Orb device. Tools for Humanity (TFH) claimed that the iris data had been anonymized by converting the Iris Code into a binary code, thereby no longer being considered personal data. However, despite the deletion of the Iris Code, there is no clarity regarding the deletion of derivative data. The fact that the system can still recognize the same iris patterns upon subsequent scans indicates that the data continues to function as a unique identifier. This raises doubts about the effectiveness of anonymization, transparency, and guarantees for the deletion of biometric data within the World App ecosystem.

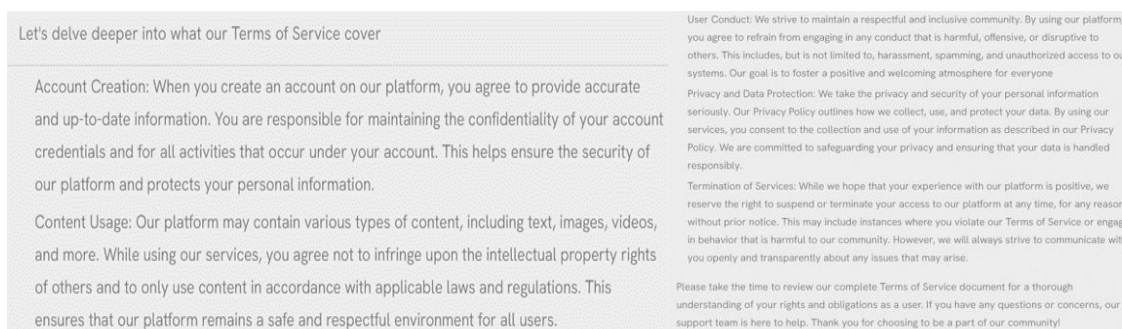
The Ministry of Communication and Digital Information (Kemenkomdigi) temporarily suspended the Worldcoin and WorldID Electronic System Providers (TDPSE) as a preventive measure against alleged violations in the implementation of electronic systems and potential misuse of personal data. The suspension followed the discovery of cooperation with parties that were not registered as Electronic System Providers (PSE) and lacked TDPSE registration. Although no data breaches have been reported, control over biometric data and the accountability of PSEs remain crucial to maintaining public trust.

Beyond World App, AI-based biometric data processing has also been implemented by domestic companies, such as the face recognition feature on the *Holy Moment* platform owned by HW Group, which is used for automatic photo search in event documentation, indicating the expanding adoption of biometric technology in the entertainment sector.

The Terms of Service and Privacy Policy of *Holy Moment* do not provide adequate explanations regarding the AI-based face recognition mechanism, the processing and storage of biometric data, or users' rights over their data. This situation demonstrates a weak implementation of the accountability principle, making *Holy Moment* an important example of the need for transparency and accountability by

service providers in the processing of AI-based biometric data, including in non-technology sectors.

Picture: screenshot of the Holy Moment website terms of service



Clearview AI is a technology company based in the United States that developed a web-based intelligence platform to assist crime investigations by government agencies. The platform employs AI-based facial recognition technology with a database of over 60 billion facial images collected from various online sources, enabling rapid and accurate identity matching (Miriam Kohn, 2022).

Clearview AI has faced legal challenges for using a facial image database collected automatically from the internet without the knowledge or consent of the data owners. This practice has been deemed illegal by various data protection authorities because it involves the processing of sensitive biometric data without a valid legal basis. Consequently, Clearview AI has been subjected to strict sanctions in several European countries, including orders to cease processing and substantial fines in France, Italy, and the Netherlands (Robert Hart, 2024).

Law No. 27 of 2022 on Personal Data Protection serves as the primary legal foundation for data protection in Indonesia, regulating definitions, classifications, processing principles, as well as the obligations of data controllers and processors. The law also guarantees the rights of data subjects and establishes an accountability mechanism through administrative and criminal sanctions, thereby providing a relatively comprehensive legal framework for the protection of personal data.

Despite the existence of the Personal Data Protection Law, the protection of personal data in Indonesia remains constrained by weak implementation and law enforcement due to the absence of an established supervisory authority and the incompleteness of implementing regulations. This situation is further exacerbated by low public and business awareness and literacy, resulting in a persistently high risk of personal data misuse (Anastasya Lavenia Yudi, 2024).

In Indonesia, AI systems are not yet specifically regulated; however, their

implementation can refer to the Information and Electronic Transactions Law (ITE Law), the Government Regulation on the Implementation of Electronic Systems (PP PSTE), and the AI Ethics Circular Letter, which govern the administration of electronic systems. AI can be classified as an electronic agent as stipulated in Article 1(8) of the ITE Law and Article 1(3) of PP PSTE, defining an electronic agent as an electronic system device that operates automatically under human administration. Although the ITE Law does not explicitly define AI, under Indonesian positive law, AI is categorized as part of an electronic system and electronic agent that functions to collect, process, analyze, and transmit electronic information.

Indonesia has issued AI ethical guidelines through the Ministry of Communication and Information Circular Letter No. 9 of 2023; however, these serve merely as ethical reference values and principles for electronic system operators, without any legal sanction mechanisms. Their purpose is limited to encouraging responsible AI use rather than addressing violations.

In contrast, the European Union has implemented the General Data Protection Regulation (GDPR) since 2018 as a comprehensive and binding framework for personal data protection. The GDPR establishes strict data processing principles, obligations for data controllers and processors, supervisory mechanisms, and high fines of up to €20 million or 4% of global revenue. This regulation applies to all organizations processing personal data and is supported by national supervisory authorities empowered to enforce the law consistently through EU coordination.

The GDPR not only enhances the protection of individual rights but also fosters a trustworthy and accountable digital ecosystem and has become a global standard adopted by many countries outside Europe. Although it applies supranationally, GDPR implementation is reinforced by national laws in each EU member state, adapted to domestic legal contexts, ensuring more effective and comprehensive data protection.

The European Union regulates AI specifically through the EU Artificial Intelligence Act (EU AI Act) as the first legal framework governing the development, marketing, and use of AI with a risk-based approach. This regulation prohibits certain hazardous AI practices, including restrictions on the use of remote biometric identification, to ensure security, legal certainty, the protection of fundamental rights, and to promote legitimate and trustworthy AI innovation and investment within the European Union (Tambiana Mediega, 2023).

The EU AI Act regulates AI using a risk-based approach, establishing different obligations according to the risk level of AI systems. This regulation applies to: (1) providers of AI systems operating or marketing AI in the European Union, (2) AI users in the European Union, and (3) providers and users in third countries if the AI output is used within the European Union. However, according to Article 2 of

the EU AI Act, the regulation does not apply to AI used specifically for military purposes, third-country governments, international organizations, or international law enforcement cooperation.

The EU AI Act does not provide a general definition of AI but defines a “AI system” in Article 3(1) as software developed using specific techniques to produce outputs such as content, predictions, recommendations, or decisions that influence its interaction with the environment. This definition refers to OECD standards. AI development includes approaches based on machine learning, logic and knowledge-based systems, and statistical methods.

Article 3 of the EU AI Act also defines the legal subjects related to AI, including providers, small-scale providers, users, authorized representatives, importers, distributors, and operators (covering all these parties collectively).

Based on risk levels, the EU AI Act classifies AI systems into four categories. Minimal-risk AI is not specifically regulated. Limited-risk AI is subject to light transparency obligations, such as for chatbots and deepfake applications. High-risk AI, regulated under Articles 16–49 of the EU AI Act, includes AI that constitutes or affects product safety components and must undergo third-party conformity assessment. This includes AI for remote biometric identification, emergency services, public infrastructure, and the education sector. Meanwhile, unacceptable-risk AI is prohibited under Article 5 of the EU AI Act, such as subliminal manipulative AI, social scoring by public authorities, exploitation of vulnerable groups, and real-time remote biometric identification in public spaces, except under limited circumstances.

3.2. Comparative Legal Analysis of Indonesia and the European Union in the Processing of AI-Based Biometric Data and the Implementation of the Accountability Principle

Law No. 27 of 2022 on Personal Data Protection (PDP Law) aims to safeguard human rights, particularly the rights to security and privacy of personal data, both online and offline. Personal data is considered an essential component of individual identity, necessitating strict regulation to prevent misuse or unauthorized access. The PDP Law provides a legal framework for the processing, storage, and protection of personal data by various parties while granting individuals greater control as data subjects.

This objective is affirmed in Article 3(a) of the PDP Law, which stipulates that the processing of personal data must ensure the security and protection of data subjects from misuse. Furthermore, the explanation of Article 3(g) emphasizes that all parties involved in the processing and oversight of personal data are required to act responsibly to maintain a balance of rights and obligations among stakeholders, including the data subjects. Article 1(4) of the PDP Law defines a

Personal Data Controller as any individual, public body, or international organization that determines the purposes and controls the processing of personal data.

The obligation of accountability for data controllers is also reflected in Article 14(1) of the Government Regulation on the Operation of Electronic Systems (PP PSTE), which mandates that the collection of personal data must be conducted with the knowledge and consent of the data owner. This principle is closely linked to transparency, requiring the provision of clear, accurate, and easily understandable information regarding the processing of personal data to the data subjects.

In the context of biometric data, the PDP Law explicitly classifies it as a specific category of personal data, warranting a higher level of protection. Biometric data such as fingerprints, facial recognition, and iris scans are unique, sensitive, and lifelong, thus requiring explicit consent and strict security standards. Biometric data controllers are also required to implement purpose limitation and Data Protection Impact Assessments (DPIA) and to demonstrate that all stages of processing are conducted safely and lawfully as an embodiment of the principle of accountability.

At the regional level, the European Union implements the General Data Protection Regulation (GDPR), which serves similar objectives as the PDP Law but with a broader scope of protection. The GDPR emphasizes transparency, accountability, and the strengthening of data subject rights, while imposing strict sanctions for violations. The principle of accountability is explicitly stated in Recital 74 of the GDPR, which requires data controllers to implement effective measures and to demonstrate compliance with the GDPR, taking into account the nature, scope, context, purpose of processing, and risks to the rights and freedoms of individuals. Through this principle, the GDPR seeks to build trust between data subjects and data controllers and to ensure that personal data processing is lawful and ethical.

In the EU, biometric data receives the highest level of protection, categorized as “special categories of personal data” under Article 9 of the GDPR. Its processing is only permitted on a lawful basis, such as explicit consent or specific public interest, due to its sensitive, permanent, and high-risk nature. Data controllers are obliged to implement additional safeguards, including DPIA, data minimization, purpose limitation, and robust data security measures.

The development of Artificial Intelligence (AI) poses significant challenges for personal data protection due to the complexity and lack of transparency in AI processes. Hence, regulations emphasizing accountability are crucial to prevent misuse and discrimination. In Indonesia, there is currently no dedicated AI law; however, AI use is subject to the provisions of the Electronic Information and Transactions Law (ITE Law), PP PSTE, and the AI Ethics Circular, which classify AI as a form of electronic agent and mandate accountability for Electronic System

Operators (PSEs).

Conversely, the EU has established a comprehensive AI regulatory framework through the EU AI Act, the world's first specialized legal framework for AI. This regulation employs a risk-based approach, categorizing AI into unacceptable, high, limited, and minimal risk. High-risk AI is subject to stringent requirements, including conformity assessments, human oversight, transparency, and post-deployment monitoring, while limited-risk AI requires transparency to enable informed decision-making by users.

The EU AI Act can serve as a reference for Indonesia in developing comprehensive and accountable AI regulations, especially given the increasing use of AI in biometric data processing. The urgency of regulation is essential to protect citizens' rights, provide legal certainty for industry players, and build a safe and sustainable innovation ecosystem. By drawing on well-established frameworks such as the EU AI Act and Indonesia's PDP Law, which is modeled on the GDPR, Indonesia could more quickly and systematically establish standards, principles, oversight mechanisms, and obligations for AI operators to address the growing complexities of AI risks.

Implementing AI regulations presents challenges for businesses in understanding and applying the principle of accountability, particularly when data processing is conducted automatically by AI systems. The complexity of the technology requires operators to ensure that all stages of data processing remain lawful, transparent, and non-detrimental to data subjects, making accountability a critical issue for in-depth examination.

In Indonesia, advanced biometric AI applications are evident in systems such as World ID within the World App ecosystem, which aim to differentiate human identities from artificial content through iris retina scanning. While this innovation holds significant potential for the digital economy and identity misuse prevention, it also demands high legal clarity regarding the collection, processing, storage, anonymization, and deletion of biometric data. The absence of comprehensive AI regulations complicates the assessment of system security and the accountability of data protection claims.

Challenges of accountability are also reflected in administrative compliance, as illustrated by the temporary suspension of the World App's Electronic System Operator registration (TDPSE) by the Ministry of Communication and Information Technology due to non-compliance. This highlights the importance of regulatory preparedness and oversight before AI technologies are widely deployed. Domestic AI innovations, such as Holy Moment by HW Group, which utilizes face recognition in the entertainment sector to enhance efficiency, convenience, and service personalization, further demonstrate that AI has become integrated across commercial sectors in Indonesia, underscoring the increasing need to strengthen

accountability and regulatory frameworks.

Advancements in AI, particularly face recognition, pose serious challenges for implementing accountability principles in Indonesia, especially concerning transparency and biometric data protection. In the case of Holy Moment, the Terms of Service and Privacy Policy have not provided detailed explanations regarding the technological mechanisms, data processing, storage duration, and user rights over biometric data, potentially violating accountability principles and increasing privacy risks. This indicates that the core issue is not merely the lack of regulation but also the low compliance and practical implementation by business operators.

These challenges are compounded by the absence of the implementing regulation (PP PDP) and the lack of an established Personal Data Protection Authority, resulting in undeveloped operational standards, oversight mechanisms, and enforcement. In the AI sector, Indonesia also lacks specific legislation and supervisory bodies, making it difficult to establish accountability and assess high-risk technologies such as biometrics. In contrast, the EU, through the GDPR and EU AI Act, effectively enforces accountability principles, as evidenced by the sanctions imposed on Clearview AI for violations of Articles 6, 12, 15, 17, and 31 of the GDPR.

The key difference lies in the presence of operational legal frameworks and active supervisory authorities in the EU, whereas in Indonesia, the absence of AI regulations and oversight institutions hampers the realization of accountability principles. Consequently, the risk of biometric data misuse and violations of citizens' privacy is significantly heightened as AI technology proliferates across public and private sectors.

4. Conclusion

The comparative analysis indicates that the protection of AI-based biometric data in Indonesia remains suboptimal due to regulatory and institutional weaknesses. Although the Personal Data Protection Act (Law No. 27 of 2022) classifies biometric data as a specific category of personal data and mandates principles such as accountability, transparency, explicit consent, Data Protection Impact Assessment (DPIA), and purpose limitation, its implementation has been ineffective. This is primarily due to the absence of implementing regulations (PP PDP), the lack of an established Personal Data Protection supervisory authority, and the absence of a specific AI law or oversight body. In contrast, the European Union has established a comprehensive framework through the General Data Protection Regulation (GDPR) and the EU AI Act, which regulate biometric data and AI systems on a risk-based approach, supported by robust supervisory mechanisms and enforcement sanctions. This comparison underscores the urgency for Indonesia to develop derivative regulations under the PDP, establish a supervisory authority, and enact AI legislation to ensure effective protection of biometric data.

5. References

Journals:

- Anastasya Lavenia Yudi. (2024). Lembaga Perlindungan Data Pribadi Belum Dibentuk, Elsam Soroti Risiko Pelanggaran Privasi. *Tempo*. <https://www.tempo.co/politik/lembaga-perlindungan-data-pribadi-belum-dibentuk-elsam-soroti-risiko-pelanggaran-privasi--1180740>
- Brendan F. Klare, Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face Recognition Performance : Role of Demographic Information. *IEEE Transactions on Information Forensics and Security*, 7(6), 4. <https://doi.org/10.1109/TIFS.2012.2214212>
- Imam Alfath Zulkarnain, et. a. (2022). Pengembangan Sistem Biometrik Pengenalan Wajah Menggunakan Convolutional Neural Network (CNN). *Prosiding Seminar Nasional Teknologi Dan Sains*, 1, 132–137.
- Ismi Adnin et.al. (2024). Responsivitas Tenaga Pendidik Terhadap Penyusunan Kebijakan Surat Edaran Pedoman Etika Artificial Intelligence. *PAMARENDA: Public Administration and Government Journal*, 4(2), 296–302.
- Miriam Kohn. (2022). Clearview AI , TikTok , and the Collection of Facial Images in International Law Clearview AI , TikTok , and the Collection of Facial Images in International Law. *Chicago Journal of International Law*, 23(1), 199.
- Mohammad Thoriq Bahri. (2022). Immigration Biometric Data Exchange Among Asean Member States: Opportunities and Challenges In Legislations. *Jurnal Ilmiah Kebijakan Hukum*, 16(3), 433–456.
- Nurhidayati, S. and K. Y. (2021). Pengaturan Perlindungan Data Pribadi dalam Penggunaan Aplikasi PeduliLindungi. *Widya Cipta: Jurnal Sekretari Dan Manajemen*, 5(1), 40. <https://doi.org/10.31294/widyacipta.v5i1.9447>
- Ririen Kusumawati. (2008). Kecerdasan Buatan Manusia (Artificial Intellegence): Teknomogi Impian Masa Depan. *Ulul Albab*, 9(2), 256.
- Salma Mufatikhaturohmah and Zulaikah. (2025). Pengaruh Teknologi Biometrik dan Jaminan Keamanan Cyber Terhadap Minat Transaksi Perbankan Online di Provinsi Lampung dalam Perspektif Islam. *Jurnal Informatika Teknologi Bisnis*, 7(2), 356. <https://doi.org/10.37034/infeb.v7i2.1136>
- Sinta Dewi Rosadi dan Garry Gumelar Pratama. (2018). Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia. *Veritas et Justitia: Jurnal Hukum*, 4(1), 88–110. <https://doi.org/10.25123/vej.2916>
- Sinta Dewi. (2016). Konsep perlindungan hukum atas privasi dan data pribadi dikaitkan dengan penggunaan cloud computing di indonesia. *Yustisia*, 5(1), 22–30.
- Tambiama Mediega. (2023). EU Legislation in Progress Artificial intelligence act. *European Parliamentary Research Service*, June, 3. https://superintelligenz.eu/wp-content/uploads/2023/07/EPRS_BRI2021698792_EN.pdf

- Warren, S. D. and, & Brandeis, L. D. (2007). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220.
- WIPO. (2018). *Inventing the future : an introduction to patents for small and medium-sized enterprises* (Issue 12). Geneva, Switzerland: World Intellectual Property Organization. <https://doi.org/10.34667/tind.29054>

Books:

- Ade Manan Suherman. (2008). *Pengantar Perbandingan Sistem Hukum*. Jakarta: PT. Raja Grafindo Persada.
- Anil K. Jain, Patrick Flynn, and A. A. R. (2007). *Handbook of Biometrics*. New York: Springer Science+Business Media, LLC.
- Barda Nawawi Arief. (2011). *Perbandingan Hukum Pidana, Edisi Revisi*. Jakarta: Rajawali Press.
- Bryan A. Garner. (2014). *Black's Law Dictionary, Deluxe Tenth Edition*. St. Paul: Thomson Reuters.
- Jarot Dian Susatyo. (2021). *Kecerdasan Buatan : Kajian Konsep & Penerapannya*. Semarang: Yayasan Prima Agus Teknik.

Internet:

- Catherine Jasserand. (2022). *Clearview AI: illegally collecting and selling our faces in total impunity? (Part I)*. KU Leuven Centre for IT & IP Law. <https://www.law.kuleuven.be/citip/blog/clearview-ai-illegally-collecting-and-selling-our-faces-in-total-impunity-part-i/>
- Defara Dhanya. (2025). Pemindaian Retina Worldcoin Dinilai Bentuk Kolonialisme Data. *Tempo*. <https://www.tempo.co/digital/pemindaian-retina-worldcoin-dinilai-bentuk-kolonialisme-data-1364565>
- Dhaivat Patel. (2022). *Machine Learning And Continuous Authentication: A Shield Against Cyber Threats*. Rang Technologies. <https://www.rangtech.com/blog/ai-machine-learning/machine-learning-and-continuous-authentication-a-shield-against-cyber-threats>
- Dutch Data Protection Authority. (2024). *Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition*. The Autoriteit Persoonsgegevens. <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition>
- EDPB. (2022). *The French SA fines Clearview AI EUR 20 million*. European Data Protection Board. https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en
- Raihan Fadilah. (2025). Apa itu Worldcoin dari World App, serta apa risikonya? *Antara*. <https://www.antaranews.com/berita/4816901/apa-itu-worldcoin-dari-world-app-serta-apa-risikonya4>
- Robert Hart. (2024). Clearview AI—Controversial Facial Recognition Firm—Fined



\$33 Million For 'Illegal Database.' *Forbes*.
<https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/>