Injuruty: Interdiciplinary Journal and Humanity
Volume 4, Number 7, July 2025
e-ISSN: 2963-4113 and p-ISSN: 2963-3397

Optimization of Personal Data Rights Protection in Artificial Intelligence Era Under Indonesia's Cybersecurity Law

Dwi Nugroho Masudianto[1], Megawati Barthos[2]
[1, 2]Universitas Borobudur, Indonesia
Email: dwi_shinchan@yahoo.com[1], megawati_barthos@borobudur.ac.id[2]

Abstract

The absence of clear regulations on Artificial Intelligence (AI) in Indonesia's Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) creates significant challenges in safeguarding personal data, particularly in automatic data processing, algorithm transparency, and accountability for AI-based decisions. This study aims to highlight the importance of strengthening personal data protection regulations in Indonesia, specifically focusing on the use of AI, and to propose improvements based on global best practices to ensure a balance between technological innovation and the protection of individual rights. The research uses a qualitative approach, examining the gaps in Indonesia's PDP Law regarding AI through comparative analysis with international standards, particularly the EU's General Data Protection Regulation (GDPR). The study identifies several risks associated with the lack of regulation, including unauthorized data exploitation, algorithmic bias, and the black-box problem in AI-based decision-making. The absence of mechanisms for legal recourse in AI decisions further exacerbates these issues. In contrast, the GDPR provides guidelines for transparency and accountability in AI systems, which the Indonesian PDP Law lacks. Strengthening the regulation of AI within the personal data protection framework is crucial to ensuring fairness, transparency, and accountability. Adopting concepts such as Explainable AI (XAI) will help address the challenges posed by the rapid advancement of AI technologies. The findings suggest that Indonesia must revise the PDP Law to include provisions that regulate AI's use of personal data, ensuring a more ethical and transparent approach to AI-based decision-making.

Keywords: Cybersecurity, Personal Data Protection, Artificial Intelligence

INTRODUCTION

Artificial intelligence (AI) has developed rapidly and is applied in various sectors, including business, health, government, and security (Arnoldy & Rachman, 2023; Hastini et al., 2020; Najwa Fathiro Cahyono et al., 2023; Pratama & Safrilah, 2021; Rahardja, 2022). In the business world, AI is used to analyze market trends, automate customer service, and improve operational efficiency (Amira, 2023). In the health sector, AI plays a role in disease diagnosis, medical data management, and drug development with big data-based analysis (Kushariyadi, 2024). The government also utilizes AI in public services, cybersecurity, and surveillance and law enforcement systems (Pakina, 2024). However, this development brings new legal challenges, especially in terms of privacy and protection of personal data, which is increasingly vulnerable to exploitation by irresponsible parties.

AI relies heavily on processing large amounts of data to support automated decision-making. This technology collects, analyzes, and predicts individual behavioral patterns based on data from myriad sources, including social media, financial transactions, and medical records (Sugiana, 2023). Although it can increase efficiency and accuracy in various fields, data processing by AI also poses risks to privacy violations, algorithmic bias, and misuse of information (Masrichah, 2023). The lack of transparency in how AI processes data often raises concerns about accountability and fairness in the decisions made by AI systems. The urgency of legal regulation in regulating the use of AI is becoming increasingly important to prevent violations of individual rights. Without adequate regulation, AI can be used to conduct mass surveillance, algorithm-based discrimination, or even information manipulation (Richard, 2025). Therefore, a clear policy is needed regarding transparency in data processing, user consent mechanisms, and accountability in automated decision-making. In cyber law in Indonesia, more specific regulations related to AI and personal data protection must be developed immediately to ensure that the use of this technology remains based on the principles of justice, security, and respect for human rights (Sugeng, 2024).

In the digital era, the amount of personal data collected by companies, government agencies, and digital platforms has increased significantly (Prayuti, 2024). Personal data such as identity information, location, search history, and user preferences are valuable assets for various entities, including businesses and governments. Companies use this data to improve services, personalize user experiences, and develop more effective marketing strategies. Meanwhile, government agencies use it for population administration, national security, and public policy (Situmeang, 2021). However, without adequate protection, this large-scale data collection risks threatening individuals' privacy rights.

As the use of personal data increases, the risk of data leakage and misuse of information also increases (Kehista, 2023). Data leakage incidents have occurred in various sectors, like private companies and government agencies, causing sensitive information to fall into the hands of irresponsible parties. In addition, automated decision-making by non-transparent AI systems can lead to discrimination or injustice for individuals whose data is used. For example, credit or insurance decisions based on algorithms without human supervision can disadvantage certain groups due to the bias of the data used in the process (Mahendra, 2024). This shows that personal data protection is not only about technical security but also about ensuring fairness and the rights of every individual in the digital environment.

Therefore, comprehensive regulation is needed in cyber law to protect personal data from the threat of exploitation and misuse (Anugerah, 2022). Strong regulation should include transparency in data processing, users' rights to control their personal information, and sanctions for parties who violate data protection principles. In Indonesia, the Personal Data Protection Law has been the first step in building a legal framework that protects individual privacy (Suari, 2023). However, with the rapid development of AI technology, more specific regulations are needed to ensure that automated systems that use personal data remain within clear ethical and legal boundaries.

Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law) is the main legal basis for regulating personal data protection in Indonesia. Article 2 of the PDP Law emphasizes that this provision applies to every person, public body, and international organization that processes personal data, both within and outside the territory of Indonesia, as long as it has a legal impact on Indonesian citizens (Alfitri, 2024). This regulation aims to provide legal certainty in the protection of personal data, as emphasized in Article 3, which prioritizes the principles of public interest, benefit, and balance. However, in managing the development of AI, the PDP Law still has limitations, especially in terms of algorithm transparency, automated decision-making, and cross-border data flows (Zein, 2024). One of the main challenges that has not been specifically regulated in the PDP Law is transparency in the use of AI algorithms to process personal data. Articles 65 and 66 have regulated the prohibition on misuse of personal data, including the collection, disclosure, and falsification of data without permission. However, this regulation does not yet accommodate oversight of how AI uses this data in automated systems that can directly impact individuals, such as credit, recruitment, or healthcare systems. This ambiguity risks creating algorithmic bias, where decisions made by AI can be discriminatory due to a lack of accountability in data processing.

The sanction aspect in the PDP Law as regulated in Article 67 focuses more on explicit violations, such as theft or misuse of personal data unlawfully (Rosadi, 2023). However, there are challenges that arise in the development of AI technology not only related to illegal access to data but also the use of data that is legitimate but has a negative impact on individuals, such as automated decision-making without an appeal mechanism or openness in the logic of the system (Cahya, 2024). Therefore, it is necessary to strengthen more specific regulations regarding the use of AI in processing personal data, including algorithm transparency standards, ethical audits of AI systems, and stricter control mechanisms for cross-border data management to ensure a balance between technological innovation and the protection of individual privacy rights.

Regulation plays a crucial role in balancing the advancement of AI technology with the protection of individual privacy rights, especially in cyber law in Indonesia. The impact of AI on personal data protection raises new challenges, such as massive data collection, automated decision-making, and the risk of information leakage and misuse that can harm individuals (Sudira, 2025). Although the Personal Data Protection Law (UU PDP) has regulated various aspects of data protection, challenges such as algorithm transparency, AI accountability, and cross-border data flows are still not fully accommodated in existing regulations. Therefore, legal updates are needed that not only strengthen privacy protection but also provide space for technological innovation to develop responsibly. Learning from AI regulations in other countries, such as the European Union with GDPR or the ethical approach to AI development in the United States, can be a reference in designing policies more adaptive to AI challenges in Indonesian cyber law. Thus, strengthening regulations based on a balance between innovation and personal data protection is the main solution in optimizing data security in the AI era. Previous research has focused on personal data protection and the integration of AI in various sectors, but there are gaps regarding the specific legal challenges of AI implementation in the Indonesian context. For instance, Kahf and Hadiz (2023) discuss AI's role in data processing and the associated risks, such as algorithmic bias and privacy violations. However, their research lacks an in-depth exploration of how Indonesian laws, such as the Personal Data Protection Law (PDP Law), address AI-related issues like algorithm transparency and accountability. In a similar vein, Suharto and Aziz (2024) have analyzed the effectiveness of Indonesia's PDP Law, but their study does not sufficiently focus on AI-specific challenges like automated decision-making and cross-border data flows, leaving a significant gap.

This study aims to evaluate the adequacy of Indonesia's PDP Law in regulating the use of AI in personal data processing, focusing on algorithm transparency, automated decision-making, and cross-border data management. The findings of this research are crucial in providing recommendations for improving the existing regulatory framework to ensure a balance between technological innovation and the protection of individual privacy rights. Strengthening these regulations will not only protect citizens from AI-related risks but also foster responsible AI development in Indonesia.

METHOD

This study uses a normative legal method with a legal analysis approach to examine the impact of artificial intelligence (AI) on personal data protection in *cyber law* in Indonesia. This approach is conducted by examining the *Personal Data Protection Law* (PDP Law) and related regulations to identify the extent to which existing regulations can accommodate the challenges posed by AI. In addition, this study also applies case studies to explore the concrete implications of AI in managing personal data, including the potential for misuse and the risk of data leakage. As a comparison, this study examines data protection regulations in other countries, such as the *General Data Protection Regulation* (GDPR) in the *European Union* and AI policies in the *United States*, to gain a broader perspective on legal strategies that can be adopted in Indonesian law. Analysis of policy documents related to AI and personal data protection is conducted to identify opportunities and challenges in strengthening statutes in Indonesia to balance technological innovation with the protection of individual privacy rights.

RESULT AND DISCUSSION

The Impact of Artificial Intelligence on Personal Data Protection in Cybersecurity Law in Indonesia

The unclear provisions related to Artificial Intelligence (AI) in the PDP Law are one of the challenges in data protection regulations in Indonesia. The current PDP Law focuses more on general personal data protection without explicitly regulating how personal data can be processed by AI-based systems (Rahman, 2021). It creates legal loopholes in automated data processing, algorithm transparency, and accountability for AI-based decisions. Globally, regulations such as the European Union's General Data Protection Regulation (GDPR) have established provisions on transparency and accountability of AI systems, including the right of individuals to understand how automated decisions are made, something that is still not specifically regulated in the PDP Law. Article 4 of the PDP Law defines personal data into two main categories, namely specific personal data and general personal data. However, this regulation does not further regulate how AI can use, process, or combine this data in automated decision-making. The main risk of this ambiguity is the possibility of non-transparent data utilization, where AI systems can collect and process personal data without the consent or adequate understanding of the data subject. In addition, the lack of clarity regarding the limitations of AI in processing biometric data or other sensitive information can open up opportunities for misuse by irresponsible parties.

Articles 65 to 67 of the PDP Law regulate the prohibition of obtaining, disclosing, or using personal data unlawfully with a criminal penalty of up to five years in prison and a maximum fine of five billion rupiah. However, this regulation does not explicitly discuss how AI systems that process data automatically can be held accountable if a violation occurs. This ambiguity may cause problems in legal sanctions, especially in cases where AI-based decisions harm individuals, but there is no obvious mechanism to hold the AI system or its developer accountable.

Artificial Intelligence (AI) based data processing requires the use of large volumes of data to function optimally. In the process, AI relies on an individual's confidential data to improve the accuracy and effectiveness of the models used, both in predictive analysis, pattern recognition, and automated decision-making. However, AI's dependence on personal data poses a major risk to the protection of individual privacy. Without strict regulations, certain companies or entities can easily collect, store, and utilize personal data without the clear consent of the data owner, which has the potential to violate privacy rights. In addition, the lack of control mechanisms for data used by AI can open up loopholes for unethical data exploitation, such as personal data for commercial purposes without transparency.

AI systems are also vulnerable to the threat of data leakage and data scraping. Data leakage occurs when an AI system that stores personal information does not have adequate security protection, allowing irresponsible parties to access and exploit the data. Meanwhile, data scraping by AI where the system automatically collects information from various sources without permission can cause personal data to be spread without the owner's knowledge. This risk is increasing with the development of AI which can process and analyze data on a large scale, including data from social media, health records, and financial transactions. Without clear boundaries on how AI can access and use personal data, individuals are increasingly losing control over their information.

AI can also lead to discrimination or detrimental algorithmic bias to certain individuals or groups. AI systems qualified using imbalanced or biased data can produce discriminatory decisions, especially in the public service sector, workforce recruitment, and financial systems. For example, in an AI-based credit scoring system, bias in the training data can cause certain groups to be treated worse in loan or insurance approvals. Likewise, in facial recognition systems used for public safety, AI has the potential to be more accurate in recognizing certain races than others. Without regulations that ensure transparency in data processing by AI, the risk of discrimination can become more entrenched and lead to injustice in various aspects of social and economic life.

One of the main challenges in the application of AI in cyber law is the black box problem phenomenon, where the automated decision-making system by AI cannot be explained or clearly understood by humans. In many cases, AI algorithms operate in complex and difficult-to-trace ways, making the resulting decisions difficult to analyze or account for. This poses a serious legal and human rights issue, especially when AI decisions directly impact individuals' lives, such as in the justice system, job selection, or public service delivery. The lack of clarity based on decision-making risks creating injustice, as affected individuals do not have access to understand or object to AI decisions that are considered detrimental to them.

Currently, regulations in Indonesia, including the Personal Data Protection Law (UU PDP), do not specifically regulate transparency in AI-based decision-making. The absence of provisions requiring AI to explain the basis for its decisions weakens the accountability of AI systems. In some cases, companies or institutions that use AI can hide behind the complexity of the technology to avoid responsibility for the negative impacts of their systems. Without a clear legal mechanism to control and supervise automated decision-making, the public is vulnerable to discriminatory treatment or unfair decisions without having effective legal means to sue or request an explanation. Several countries have addressed this issue by implementing the concept of Explainable AI (XAI), an approach that ensures that decisions made by AI systems can be understood by humans. The European Union, for example, in its General Data Protection Regulation (GDPR), has regulated the individual's right to obtain an explanation regarding decisions made by automated systems. This concept requires companies or institutions to provide transparency in the algorithms used and ensures that individuals have the right to reject decisions made entirely by AI without human intervention. This case study of the implementation of XAI can be a critical reference for Indonesia in drafting stricter regulations regarding the transparency and accountability of AI so that it can create a balance between technological innovation and the protection of individual rights.

Weaknesses of Law Number 27 of 2022 concerning Personal Data Protection in Facing the Challenges of Artificial Intelligence

The PDP Law in Indonesia does not explicitly regulate data processing by AI-based systems, especially in terms of transparency, accountability, and risk mitigation. This ambiguity creates a legal loophole that allows companies or institutions that use AI to process personal data without clear regulations regarding limitations, consent, and protection for data subjects. The absence of a specific definition of AI in the PDP Law may also create legal uncertainty in enforcing privacy rights. Unlike the General Data Protection Regulation (GDPR) in the European Union, which has regulated the principles of AI transparency, the right of data subjects not to be the object of automated decisions that have significant impacts, and the obligation of data managers to ensure the ethical and accountable use of AI, the Indonesian PDP Law still does not provide similar protection. It indicates the need for revision or supplementation of regulations so that AI in the processing of personal data can be regulated more comprehensively.

The consent mechanism in the Personal Data Protection Law (PDP Law) requires the processing of personal data based on the consent of the data subject. Article 5 of the PDP Law emphasizes that every individual has the right to obtain information about the identity, legal basis, purpose of use, and accountability of the party processing their data. However, in Artificial Intelligence (AI) technology, transparency regarding how data is processed is usually challenging. Many AI systems that use machine learning perform complex data processing, making it difficult for users to understand how their data is used. As a result, the consent given is often a formality without adequate understanding from the data subject regarding the risks and purposes of data processing by AI.

Articles 7 and 9 of the PDP Law provide the right for data subjects to access, obtain a copy of, and withdraw consent to process their data. However, in AI systems that use big data, personal data is often collected from various sources without direct notification to the data subject, making it difficult to ensure whether the data is processed with valid consent. The absence of explicit regulations governing how AI must provide clear and easy-to-understand information exacerbates the inequality between individuals and companies or entities that utilize AI in processing personal data. It creates the risk of unauthorized data use without an effective mechanism to control it.

Article 8 of the PDP Law states that data subjects have the right to terminate processing, delete, or destroy their data by legal provisions. However, in practice, machine learning-based AI systems find it difficult to completely delete data that has been used, especially if the data has been included in an AI model that develops automatically. The challenge is further complicated when AI combines data from various sources so that data subjects lose full control over their personal information. Therefore, additional regulations are needed that align the AI consent and transparency mechanisms with the principles in the PDP Law so that personal data protection can be implemented effectively in the digital era. The gap between existing regulations and Artificial Intelligence (AI) usage in Indonesia is a major challenge in defending personal data. Currently, AI has developed rapidly in various sectors like finance, health, cybersecurity, and public services. However, existing regulations, including the Personal Data Protection Law (PDP Law), are not fully aligned with legal requirements in AI-based data management. There are no rules that specifically regulate how AI should operate in the processing of personal data, including aspects of transparency, accountability, and risk mitigation. As a result, individuals whose data is used by AI systems are often unaware of how their information is processed and used.

The absence of technical guidelines or compliance standards for companies and institutions using personal data-based AI makes enforcement difficult. The PDP Law regulates the rights of data subjects, including the right to transparency and consent, but in practice, the mechanisms for ensuring companies comply with these principles remain unclear. Many companies rely on internal policies to manage AI data without strict oversight from regulators. Without binding operational standards, there is potential for data misuse, such as the exploitation of consumer data for commercial purposes without clear consent.

Regulatory delays in anticipating AI developments risk generating innovation technology developed without adequate supervision, which can increase the violation of individual privacy rights. In other countries, such as the European Union, the Explainable AI (XAI) principle in the GDPR has been implemented to ensure that decisions made by AI can be understood and audited. However, in Indonesia, no regulation regulates the obligation of AI to explain the basis for the decisions it makes, especially in critical sectors such as banking and public services. Therefore, harmonization between legal needs and AI practices is necessary so that regulations can protect individual interests without hindering technological innovation.

Efforts That Can Be Implemented to Optimize Personal Data Protection in the Era of Artificial Intelligence

The current PDP Law does not explicitly regulate the processing of personal data carried out by artificial intelligence (AI) systems. AI has unique characteristics in data processing, such as collecting large amounts of data, automatic processing, and self-learning that can update its algorithms without direct human intervention. Without specific regulations governing how AI should manage personal data, there is a risk that this system will operate without clear boundaries, increasing the potential for privacy violations and data misuse.

The absence of specific regulations regarding AI in the PDP Law also has significant legal implications, especially regarding transparency and accountability. Without provisions requiring data controllers or companies to explain how AI processes personal data, data subjects lose control over their information. In addition, AI systems used in automated decision-making are at risk of producing algorithmic bias that can harm certain individuals or groups. It is contrary to the principles of fair, transparent, and accountable data protection as mandated in various international regulations, such as the General Data Protection Regulation (GDPR) in the European Union.

To overcome these problems, there needs to be an insertion of special provisions in the PDP Law that regulate the use of AI in processing personal data. The regulation must include a clear definition of AI and its use in data processing, limitations on the use of AI regarding the protection of personal data, and obligations for data controllers to ensure that the use of AI remains by the principles of transparency and accountability. In addition, this regulation must also provide the right for data subjects to know how AI makes decisions regarding their data, and provide a mechanism to challenge decisions made automatically by AI. Thus, this special regulation can be a legal instrument that can balance technological innovation and individual privacy rights protection. The integration of the principle of transparency in AI regulations is crucial to ensure that artificial intelligence systems can be understood and audited by humans. The Explainable AI (XAI) notion allows every decision made by AI to be explained rationally and easily understood, both by regulators and data subjects. Without transparency, users and data owners cannot know how the AI system processes information, increasing the risk of misuse and injustice in automated decision-making. Therefore, AI regulation needs to require every data controller that uses AI to provide a noticeable explanation mechanism regarding the data processing process and the factors that influence AI decisions.

Besides transparency, accountability must also be a key principle in AI regulation. Every entity that uses AI in processing personal data must be legally responsible for any consequences caused by the technology. Data controllers are required to ensure that the AI they use does not violate individual privacy rights and continues to operate within ethical and legal boundaries. Regulations must include accountability mechanisms, including regular audits, independent monitoring systems, and the imposition of sanctions for parties who commit violations, either in administrative fines or more severe legal action in the event of misuse of personal data.

Ethical principles in AI must also be enforced to prevent the negative impacts of algorithmic bias and discrimination against certain groups. AI used in public services, banking, health, or workforce recruitment systems must operate based on the principles of fairness and non-discrimination so as not to harm individuals based on race, gender, or other social backgrounds. Regulations must ensure that AI systems are designed with data diversity in mind and are rigorously tested to avoid biases that can create injustice. By implementing the principles of transparency, accountability, and ethics in AI regulations, this technology usage can develop while esteeming individual rights and upholding the values of justice in society.

Improving law enforcement mechanisms and supervision of AI-based data processing is urgent in ensuring company or institution compliance with personal data protection regulations. Currently, existing supervision mechanisms still focus on general personal data protection, without a specific approach to AI technology that has unique characteristics, such as automated decision-making machine learning. Evaluation of the effectiveness of this mechanism needs to be carried out to assess the extent to which existing regulations can control data misuse by AI, including the application of sanctions for violators and the effectiveness of enforcing data subject rights in the face of detrimental AI decisions.

The role of supervisory authorities, such as the Ministry of Communication and Information (Kominfo) and independent institutions responsible for personal data protection, must be strengthened in enforcing AI compliance with data protection standards. These authorities must have broader authority in supervising AI systems that process personal data, including through technology audits, compliance inspections, and reporting obligations from companies that use AI. In addition, coordination with other sectors, such as the Financial Services Authority (OJK) and the Ministry of Health, is also needed so that AI supervision in various sectors can run effectively and in line with the needs of personal data protection in each industry.

To strengthen supervision, legal instruments need to be developed such as regular audits of AI systems that process personal data to ensure that the AI decision-making process does not violate the principles of transparency and fairness. In addition, AI certification can be applied as a standard that must be met by companies before adopting AI in processing personal data, to ensure compliance with applicable regulations. On the other hand, the public complaint mechanism must also be expanded so that the public has easier access to report cases of data abuse by AI and obtain fast and effective protection from regulators. With a combination of strict supervision and more comprehensive legal instruments, the risk of data abuse by AI can be minimized, while increasing public trust in AI technology based on personal data.

Comparative studies of AI regulations in various countries can be a recommendation for Indonesia in designing policies that balance personal data protection and technological innovation. The European Union's General Data Protection Regulation (GDPR) has set high standards with the principles of transparency and the right of individuals not to be subject to automated decisions that have significant impacts, which can be used as a reference in strengthening data subject rights in Indonesia. In the United States, AI regulations are applied sectorally, such as in the financial and health sectors, which shows flexibility in the regulatory approach according to industry characteristics. Meanwhile, Singapore and Japan have adopted AI ethics standards and stricter law enforcement mechanisms, including transparency guidelines and AI system audits that can increase accountability. Based on this study, Indonesia needs to design AI regulations that are not only oriented towards protecting personal data but can support the development of innovative AI while still considering ethical, transparency, and accountability aspects in its use.

CONCLUSION

The unclear regulation of *Artificial Intelligence* (AI) in Indonesia's *Law Number 27 of 2022 concerning Personal Data Protection* creates challenges in data protection, particularly in transparency, accountability, and automated data processing. This gap poses risks such as data exploitation, leakage, algorithmic bias, and the *black box* problem in AI decision-making, which can reduce accountability and increase injustice, especially in essential public services. Compared to global practices like the *EU's General Data Protection Regulation* (GDPR) and the concept of *Explainable AI* (XAI), Indonesia needs stricter policies to ensure transparency, control over AI usage, and protection of individual rights. The current *PDP Law* has legal loopholes, especially in regulating AI's processing of personal data, and lacks binding technical guidelines, increasing the risk of data misuse. To address these issues, revisions or additional regulations are necessary, specifically targeting AI's use in data processing, prioritizing transparency, accountability, and ethics. Stronger enforcement mechanisms, including technology audits and AI certification, are crucial for compliance. Comparative studies of AI regulations globally highlight the need for Indonesia to balance technological innovation with privacy protection, ensuring AI develops responsibly while upholding fairness and transparency.

REFERENCES

Adha, L. A. (2020). Digitalisasi Industri dan Pengaruhnya Terhadap Ketenagakerjaan dan Hubungan Kerja. *Jurnal Ekonomi Digital*, 5(2), 88–95.

Alfitri, N. A. (2024). Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Journal Social Society*, 92–111.

Amira, B. (2023). Pemanfaatan kecerdasan buatan (AI) dalam meningkatkan efisiensi dan pengembangan usaha mikro, kecil dan menengah (UMKM). *Jurnal Riset Manajemen*, 362–371.

Anugerah, F. (2022). Pencurian data pribadi di internet dalam perspektif kriminologi. *Jurnal Komunikasi Hukum (JKH)*, 419–435.

Arnoldy, V. E. S., & Rachman, L. O. A. (2023). Penerapan kecerdasan buatan (Artificial Intelligence) dalam praktik keperawatan: Sebuah tinjauan literatur. *Jurnal Inovasi Kesehatan Adaptif, 5*(5).

Cahya, A. N. (2024). Transformasi budaya hukum dalam era digital (Implikasi penggunaan AI dalam perkembangan hukum di Indonesia). *IKRA-ITH Humaniora: Jurnal Sosial dan Humaniora*, 361–373.

Fathiro Cahyono, N., ’Uyun, K., & Mukaromah, S. (2023). Etika penggunaan kecerdasan buatan pada teknologi informasi. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi, 3*(1). https://doi.org/10.33005/sitasi.v3i1.334

Hastini, L. Y., Fahmi, R., & Lukito, H. (2020). Sistem informasi pertanian berbasis kecerdasan buatan. *Jurnal Manajemen Informatika (JAMIKA), 10*(April).

Kehista, A. P. (2023). Analisis keamanan data pribadi pada pengguna e-commerce: Ancaman, risiko, strategi kemanan (literature review). *Jurnal Ilmu Manajemen Terapan (JIMT)*.

Kushariyadi. (2024). *Artificial Intelligence: Dinamika perkembangan AI beserta penerapannya*. Jambi: Sonpedia Publishing Indonesia.

Mahendra, G. S. (2024). *Teknologi AI: Pengantar, teori, dan contoh penerapan artificial intelligence di berbagai bidang*. Jambi: Sonpedia Publishing Indonesia.

Masrichah, S. (2023). Ancaman dan peluang artificial intelligence (AI). *Khatulistiwa: Jurnal Pendidikan dan Sosial Humaniora*, 83–101.

Pakina, R. (2024). Pengaruh teknologi informasi terhadap hukum privasi dan pengawasan di Indonesia: Keseimbangan antara keamanan dan hak asasi manusia. *Journal of Scientech Research and Development*, 273–286.

Pratama, J. C. P., & Safrilah. (2021). Tinjauan literatur tentang kecerdasan buatan sebagai pendekatan dalam pengendalian sistem lalu lintas. *Jurnal Infrastruktur, 7*(1).

Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum*, 903–913.

Rahardja, U. (2022). Masalah etis dalam penerapan sistem kecerdasan buatan. *Technomedia Journal, 7*(2). https://doi.org/10.33050/tmj.v7i2.1895

Rahman, F. (2021). Kerangka hukum perlindungan data pribadi dalam penerapan sistem pemerintahan berbasis elektronik di Indonesia. *Jurnal Legislasi Indonesia*, 81–102.

Richard. (2025). Peran transformasi hukum pidana dalam mengatasi kejahatan siber berbasis AI dan geopolitik. *Jurnal Retentum*, 434–449.

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta: Sinar Grafika.

Situmeang, S. M. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *Sasi*, 38–52.

Suari, K. R. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 132–142.

Sudira, I. W. (2025). Keadilan digital: Tantangan hukum dalam era disrupsi teknologi. *Kertha Widya*, 35–59.

Sugeng. (2024). *Hukum Telematika Indonesia: Edisi Revisi*. Jakarta: Prenada Media.

Sugiana, N. S. (2023). Analisis data sistem informasi monitoring marketing; Tools pengambilan keputusan strategic. *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, 696–708.

Zein, H. M. (2024). *Digitalisasi pemerintahan daerah: Katalis untuk integrasi dan optimasi good governance*. Banten: Sada Kurnia Pustaka.