Jurnal Daulat Hukum
Volume 8 No. 4, December 2025
ISSN: 2614-560X
SINTA 3 Decree No. 0547/ES/DT.05.00/2024
Dated May 15, 2024

Optimizing AI as an Instrument for Personal Data Protection within the National Legal Framework

Naavi'u Emal Maaliki
Faculty of Law, Universitas Islam Sultan Agung, Indonesia, E-Mail: maaliki@unissula.ac.id

Abstract. *Massive data breaches on electronic platforms indicate a legal enforcement gap caused by technological asymmetry. This study aims to analyze the urgency of optimizing Artificial Intelligence (AI) as an instrument for personal data protection within the national legal framework to overcome the limitations of manual supervision. This study employs normative legal research with a statute approach and a comparative approach toward regulations in the United Kingdom and Malaysia. The results indicate that AI can be positioned as a manifestation of the corporate due diligence principle, capable of transforming data protection from a reactive to a proactive-mitigative paradigm through Privacy by Design mechanisms. Furthermore, the legal comparison emphasizes the need for Indonesia's independent supervisory authority to adopt accountable security algorithm standards. The optimization of AI is not merely a technological adoption but a juridical necessity to fill the technical norm vacuum in the PDP Law, ensuring the fundamental right to privacy and information sovereignty of citizens in the era of digital disruption.*

Keywords: *Artificial; Cyber; Intelligence; Law; Protection.*

1. Introduction

Technological developments have had a profound impact on global life, including Indonesia in the current era of globalization. High mobility, speed of information access, ease of communication, and an instant lifestyle are characteristics of today's societal needs. Indonesia has entered the digital era, marked by automation and easy access to communication between people. (Paulus Wisnu Yudoprakoso, 2019). This technological development is the origin of the creation of artificial intelligence (AI). The escalation of artificial intelligence capabilities has now reached a high level of autonomy, where systems are able to operate autonomously without direct human intervention. This phenomenon creates a new dimension in contemporary legal discourse, given that such autonomous activities, as applied to Tesla's self-driving vehicles, often intersect with areas of legal responsibility. This has sparked debate about the boundaries of criminal and civil liability when autonomous technology is involved in legal events in the public sphere (Eka NAM Sihombing and Muhammad Yusrizal Adi Syaputra, 2020). Human work has shifted from conventional manual methods to integrated digital and automated systems. This momentum is marked by the penetration of cutting-edge technology into various sectors of life,

where the escalation of information technology and the introduction of artificial intelligence (AI) are key pillars that have significantly revolutionized the effectiveness of human activities. (Paulus Wisnu Yudoprakoso, 2019:455).

AI has had a significant positive impact in various fields, such as industry, health, education, government, and so on. The development of AI is very rapid and sophisticated. Artificial intelligence has multifunctional capabilities that include natural language processing, facial biometric recognition, and automation of transportation systems and industrial manufacturing. Although its conceptual embryo was born since 1956, the discourse on AI has only reached its current point of escalation in popularity, driven by the availability of big data, the complexity of algorithms, and the leap in computing performance. Its historical roots in the 1950s actually focused on problem-solving experiments through symbolic methods (SAS Insights,2019). Artificial intelligence (AI) is basically a "machine" that is capable of doing various things that are considered to require intelligence when operated by humans (Febri Jaya and Wilton Goh, 2021). The evolution of AI began as a theoretical object of study in research laboratories before finally transforming into applied technology. The involvement of the United States military sector under the auspices of DARPA in the 1960s became a major catalyst that changed the orientation of AI research. One of the fundamental achievements of this period was the completion of the regional mapping project in the 1970s, which demonstrated the enormous potential of AI in solving complex computational tasks outside the laboratory. The success of AI in moving beyond the laboratory to practical applications—as initiated by the DARPA project—marked a shift in the status of AI from a mere technical instrument to a socio-legal phenomenon.

In Indonesia, this transformation has serious implications for individual information sovereignty. As AI-based systems begin to integrate autonomous data processing capabilities on a massive scale (Pratama, Arya Satya, Suci Maela Sari, et al., 2021). The line between technological efficiency and privacy violations is becoming increasingly blurred. The presence of AI has induced productivity across sectors, shifting conventional work methods toward efficient automation. Beyond its massive economic contribution, the development of information technology has created public dependence on internet-based services, from commercial transactions to electronic public services. This massive digitalization not only facilitates access to information but also creates an urgency for securing cyberspace, considering that every interaction within this virtual ecosystem always involves the exchange of highly sensitive personal data (Adis Nur Hayati, 2021). However, behind this accelerated productivity and ease of access to information, systemic risks related to individual data sovereignty emerge. The integration of AI into public and commercial services has led to massive and automated data harvesting. From a criminal law perspective, this situation creates a new vulnerability where personal data is no longer merely an economic asset but also an object of crime (objectum delicti), highly vulnerable to exploitation, manipulation, and system breaches.

The exploitation of personal data by irresponsible parties underscores the urgency of strengthening the data protection regulatory framework in Indonesia. The government has a constitutional obligation to create a secure digital space through legal regulations that can prevent data misuse in electronic transactions. One strategic instrument that can be optimized

is the adoption of artificial intelligence technology. Through the integration of advanced algorithms capable of detecting cyberattacks pre-emptively. AI becomes a crucial instrument in closing system vulnerabilities and ensuring the integrity of consumers' personal data. (Sinta Dewi, 2016). The urgency of special regulations arises because conventional legal instruments often fail to address the black-box nature of AI (its decision-making process is difficult to trace). Therefore, optimizing AI within the national legal framework is not merely a technical effort, but rather a manifestation of the state's commitment to providing legal protection (rechtsbescherming) for citizens amidst digital disruption. This aligns with the spirit of Law No. 27 of 2022 concerning Personal Data Protection, which requires adaptive and responsive data security mechanisms to technological advancements.

The legal status of AI in Indonesia has not been specifically regulated either in the Criminal Code or in the current laws. AI is still viewed as a tool or machine. Legal regulations regarding AI are not regulated by specific laws, currently AI can be regulated by laws governing matters related to technology. Some laws that may apply to AI are Law No. 1 of 2024 concerning Electronic Transaction Information (ITE) (Law of the Republic of Indonesia Number 1 of 2024 concerning Electronic Information and Transactions). The second, as previously explained, is Law No. 27 of 2022 concerning Personal Data Protection. These two laws provide the legal basis for regulating the use of technology and intellectual property rights (Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection).

From the explanation above, there is no specific law governing AI legal regulations regarding personal data. Therefore, Indonesia requires clearer and more detailed regulations. Therefore, this study discusses optimizing AI as an instrument for personal data protection within the national legal framework

2. Research Methods

The problems in this research include the central issues of penal policy, part of criminal policy. Therefore, the approach cannot be separated from the policy-oriented approach (Barda Nawawi Arief, 1996). The essence of this research is on the problem of legislative policy in determining and formulating criminal provisions which reflect the interconnectedness of the system between general provisions and special provisions in the substantive criminal system, so the main approach in this research is normative research (Maaliki, Naavi'U. Emal, and Eko Soponyono., 2021), and supported and complemented by a comparative juridical approach. The research conducted is normative legal research or library legal research. This normative legal research or library research includes: research on legal principles, research on legal systematics, research on the level of vertical and horizontal synchronization (Soerjono Soekanto, 1985).

3. Results and Discussion

3.1. Personal Data Protection Regulations in Indonesia

Indonesia has passed Law Number 27 of 2022 concerning Personal Data Protection as lex specialis (Bachtiar, Farid Rizki, Wisnu Ardytia, and Demas Brian Wicaksono., 2025). However

legal instruments specifically regulating the integration of artificial intelligence technology into data security are still not comprehensively available. Previously, regulations regarding data privacy were scattered fragmentarily across various regulations, such as the Company Documents Law, the Telecommunications Law, the Population Administration Law, the ITE Law, the Health Law, and the Archives Law. This regulatory fragmentation often only touches on general protection aspects without accommodating the complexity of digital data. Therefore, this study focuses on personal data protection in the electronic realm, in order to evaluate the effectiveness of existing legal norms in facing the challenges of digital automation. The regulatory framework for personal data security in Indonesia also stems from Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and Regulation of the Minister of Communication and Information Technology No. 20 of 2016. Normatively, Article 26 paragraph (1) of the ITE Law emphasizes the principle of data subject consent in every use of electronic information. Although the ITE Law does not explicitly define the terminology of personal data, its explanation constructs such protection as an integral part of the right to privacy. The right to privacy in this context encompasses three fundamental dimensions: the right to a private life free from interference, the confidentiality of communications without surveillance, and the individual's sovereignty to control the accessibility of their personal information. Philosophically, personal protection is an absolute right guaranteed by Article 28G paragraph (1) of the 1945 Constitution, which simultaneously places a legal obligation on the state as the protector of individual sovereignty. Although the constitution has provided clear guidelines, the fact that the regulation of personal data is still partial and sectoral indicates the unpreparedness of the legal system in responding to the urgency of data privacy. This fragmented legislative pattern weakens the bargaining position of citizens as data subjects, considering that the protection provided is still general in nature and has not touched on the core of the human right to personal data in a complex cyber ecosystem (Christoforus Ristianto, 2025).

Referring to Article 1 number 1 of the Minister of Communication and Information Regulation No. 20 of 2016, personal data is constructed as individual information that requires protection standards regarding its accuracy and confidentiality aspects (Junaedi, Asep Mahbub. 2025). Legally the synthesis of these various regulatory definitions confirms that the essence of personal data protection centers on the right to information sovereignty. This grants individuals, as data subjects, full authority to determine the accessibility, purpose, and completeness of their personal data that can be disclosed to other parties. Thus, personal data protection is not merely a technical cybersecurity issue, but a vital instrument in safeguarding the integrity, dignity, and privacy rights of individuals from potential abuse. Several large-scale data breaches, such as those affecting several e-commerce platforms, are empirical indicators that personal data protection in Indonesia remains vulnerable to exploitation by irresponsible parties. Although the government has responded to the urgency of legal certainty by enacting Law Number 27 of 2022 concerning Personal Data Protection, regulatory unification alone is insufficient without strengthening technical security instruments. Repeated leaks emphasize that protection mechanisms must shift from mere administrative compliance to the proactive

implementation of technologies, such as artificial intelligence, to ensure the effectiveness of legal norms in mitigating dynamic cyber risks.

3.2. Optimizing Artificial Intelligence as a Proactive Instrument for Personal Data Protection in the National Legal Ecosystem

Optimizing Artificial Intelligence (AI) within the national legal framework is no longer seen as simply adopting technology, but rather an existential necessity to fill the legal enforcement gap left by conventional methods. Under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), the state has established strict compliance standards for every personal data controller. However, in practice, the complexity of cyberattacks and the speed of large-scale data processing make manual oversight irrelevant. Therefore, positioning AI as a data protection instrument means integrating computational intelligence into the legal defense system to achieve preventative and automated protection.

The term artificial intelligence was first introduced by the British mathematician, Alan Turing in 1950. This term was contained in an article entitled "Computer Machinery and Intelligence." This article became the forerunner of modern thinking related to artificial intelligence, namely the capacity of machines to have human-like abilities in reasoning, learning, planning, and creativity (Qur'ani Dewi Kusumawardani, 2019). Initially artificial intelligence's ability to analyze a problem begins with the input of initial data, algorithms, and computer programs that have been carefully engineered by humans. Then, the artificial intelligence program "learns" from various possibilities and simulations of events collected in large, heterogeneous data sets, enabling it to identify, predict, and even prevent personal data leaks (Kirana Rukmayuninda Ririh et al., 2020). The role of artificial intelligence in society is through its ability to accelerate problem-solving processes quickly and consistently. Substantively, AI's comparative advantage lies in its ability to construct solutions to complex problems that are difficult to reach through conventional approaches. Furthermore, AI functions as an instrument for filtering and interpreting data amidst the information explosion phenomenon. Optimizing these various functions ultimately creates a simplified workflow that linearly contributes to increased productivity and operational efficiency in various sectors of life. The various sophisticated capabilities of artificial intelligence are also utilized to address challenges that are considered quite difficult to overcome, such as natural disasters, climate control, hunger, and the spread of disease outbreaks (Paulus Wisnu Yudoprakoso, 2019: 455).In general, personal data can be defined as data that contains information about a person's identity, which can be in the form of codes, symbols, letters or personal numbers that are only attached to each individual (Rosalinda Elsina Latumahina, 2014).From a criminal law perspective, this AI optimization can be positioned as a manifestation of the principle of due diligence, or the appropriate caution for corporations. AI acts as an independent oversight instrument capable of early detection of suspicious data behavior anomalies before detrimental leaks occur. Technically and legally, the integration of AI equipped with threat scanning algorithms and dynamic antimalware systems functions as a "gatekeeper" that validates every incoming and outgoing data flow in accordance with the principle of purpose limitation. This directly reinforces Article 35 of the PDP Law, which requires data controllers to maintain data security from unauthorized access.

National legal framework, AI optimization must be directed to overcome human error which is often a weak point in cybercrime (Atiyah, Atiyah, Nur Chalesa Fitriani, and Akhmad Zaki Yamani., 2025).AI is capable of automatic encryption, real-time data anonymization, and continuous, non-stop system compliance monitoring. Thus, the presence of AI shifts the paradigm of data protection from a reactive approach, taking action after a crime has occurred, to a proactive, mitigating one. This argument carries significant legal implications: if a corporation optimizes the use of AI for data protection, it has made maximum efforts to prevent criminal acts. Therefore, future specific regulations in Indonesia must not only regulate the limits of human behavior but also regulate standards for data security algorithms. Optimizing AI as a personal data protection instrument bridges the gap between legal norms and technological realities, ensuring that citizens' right to privacy is maintained amidst massive digital disruption.

One of the biggest reasons for the rapid development of technology in Indonesia is since the start of the Covid-19 Pandemic in Indonesia and the government implemented large-scale social restrictions or PSBB as a step to suppress the spread of the Covid-19 Pandemic in Indonesia (Hari Sutra Disemadi and Denis Oxy Handika, 2020).The implementation of Large-Scale Social Restrictions (PSBB) during the COVID-19 pandemic in Indonesia has been a catalyst for accelerating digital transformation across various sectors of life. The escalating use of video conferencing platforms and the massive rise in e-commerce activity have not only changed socio-economic interaction patterns but also expanded the locus and tempo of cybercrime. The public's high dependence on digital infrastructure is directly proportional to increased legal risks, particularly related to the potential for data disputes and the vulnerability of data subjects to various online criminal schemes. (Arfian Setiantoro et al., 2018).

In the context of positive law in Indonesia, the enactment of Law Number 27 of 2022 concerning Personal Data Protection has provided a strong normative foundation, but its effective enforcement faces significant challenges in the form of technological asymmetry. Large-scale data processing by global corporations and e-commerce service providers creates the risk of data breaches that can no longer be mitigated through manual audits or reactive periodic reporting alone. Optimizing AI as a personal data protection instrument within the national legal framework serves as a bridge to address a situation where legal developments consistently lag behind the pace of technological innovation. Through the Privacy by Design and Privacy by Default approaches, AI can be integrated into the legal system as an automated oversight mechanism capable of real-time threat scanning, dynamic data encryption, and detection of unauthorized access without waiting for a breach report.

The use of AI as a legal instrument (Rosyadi, Safriansyah Yanwar, and Zainal Arifin Hoesein., 2025). Provides a new dimension in fulfilling the obligations of personal data controllers as stipulated in Article 35 of the PDP Law. From a criminal law perspective, the failure of data controllers to adopt cutting-edge security technology amid increasingly sophisticated cyber threats can be constructed as a form of negligence that leads to corporate criminal liability. Optimizing AI is a form of legal compliance to minimize the risk of victimization for the public. By integrating artificial intelligence, the state can encourage the creation of a digital ecosystem

that is not only economically efficient but also possesses legal integrity, where protection of citizens' privacy rights is an integral part of the technological system itself.

The urgency of optimizing artificial intelligence (Ramadhan, Muhammad Aziz Tri. 2025), The national data protection system is also closely related to the standardization of more accountable information security audits. Under the PDP Law framework, personal data supervisory authorities demand transparency in data processing, but this transparency is difficult to achieve if the system used remains static and closed. The adoption of explainable AI, a branch of artificial intelligence focused on developing methods and techniques so that the decision-making process and results of AI systems can be understood and explained to humans, overcomes the "black box" problem of traditional AI, thereby increasing trust, accountability, and fairness in its application in various sectors such as health, finance, and law. This can be a legal solution to meet the principle of accountability, where every autonomous decision made by machines in filtering or blocking data access can be traced and legally explained. This is crucial to avoid algorithmic bias that has the potential to violate individual subjective rights, while also facilitating law enforcement in conducting digital forensics in the event of information disputes. Furthermore, the state needs to formulate technical regulations that establish AI not only as an option but also as a minimum standard of security for electronic system providers in high-risk categories. By integrating AI into security protocols (Emmanuel, Rheimanda Devin, et al., 2025), the burden of proof in cyber law cases could shift toward efficiency, with activity logs generated by artificial intelligence becoming strong and valid electronic evidence under Article 5 of the ITE Law. This transformation will ultimately create a balance between the needs of the digital economy and the protection of human rights, so that data sovereignty is no longer merely a normative slogan but is supported by a technological infrastructure that automatically complies with the dictates of the law.

Protection of personal data is a crucial manifestation of legal protection efforts that are based on respect for the dignity and worth of humans as the main legal subject (Pratama, Gede Aditya, and Elfirda Ade Putri.,2022). Theoretically, legal protection in the digital realm is not merely a technical regulatory instrument, but rather a fundamental recognition of absolute human rights that must be upheld based on the principle of equality before the law. Ideal legal protection must be comprehensive and non-discriminatory, with recognition of human rights being the main axis in every norm formation to prevent the dehumanization of technology. In the context of digital sovereignty, legal guarantees for personal data are an absolute requirement for fulfilling the state's responsibility to protect the informational self-determination of its citizens. Therefore, the integrity of this legal protection is no longer sufficient to rely solely on static regulations, but must transform by adopting technological instruments capable of sustainably maintaining individual dignity amidst the increasingly complex dynamics of cyber threats.

In several developed countries, the issue of personal data protection is considered a form of legal protection for human rights, requiring comprehensive regulations to accommodate it. A number of countries have recognized data protection as a constitutional right, in the form of "habeas data," which is the right of individuals to secure their personal data and receive legal protection in the event of misuse of their personal data.Graham Greenleaf, 2012).For example,

in England, to ensure the enforcement of legal regulations, there is a special body, namely the Data Protection Commissioner (Khan, Farha, and Akansha Mer., 2023).The agency's task is to monitor the flow of data related to a person's personal data. Article 14 of the Data Protection Act 2018 explicitly states that if a court finds that the processing of personal data carried out by a data controller is inaccurate, the court can order the data controller to correct, prevent, or delete the data. Any party who feels aggrieved by the inaccurate processing of personal data can seek compensation from the data controller if there are violations of the provisions contained in the Data Protection Act 2018 (Lia Sautunnida, 2018). Apart from the UK, neighboring country Malaysia also has special regulations governing legal protection of personal data. In a comparative perspective in the regional area, Malaysia has pioneered regulatory unification through the ratification of the Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia) (Ismaila, Suharne. 2023). The introduction of this regulation marks a fundamental transformation in the Malaysian legal system, where, for the first time, data privacy protection is specifically and independently regulated through a lex specialis. Substantively, the Malaysian PDPA adopts global standards that bear significant similarities to the European Data Protection Directive, but still prioritizes modifications tailored to the sociological needs and characteristics of local communities. Malaysia's success in integrating international standards into the national context demonstrates that personal data protection must be designed as a specific regulation that adapts to the dynamics of information governance (Zuryati Mohamed Yusoff, 2011). A look at these two countries shows that the effectiveness of data protection is highly dependent on the existence of lex specialis regulations. In Indonesia, a long history of fragmented data regulation has created systemic weaknesses that limit the rights of data subjects. The introduction of the Personal Data Protection Law is a strategic step to end this dualism and legal vacuum. However, the legal certainty offered by this new law still requires supporting instruments in the form of artificial intelligence technology to ensure that existing regulations are not merely administrative in nature. By optimizing AI as a protection instrument, past law enforcement weaknesses can be addressed through an integrated, independent security system.

The Personal Data Protection Law, as a comprehensive regulation, is fundamental in establishing data security standards equivalent to international legal instruments. The essence of the Personal Data Protection Law lies not only in codifying norms but also in strengthening strict sanctions to provide a deterrent effect and enforce compliance by data controllers in maintaining information integrity. In line with best practices in countries such as the United Kingdom through the Data Protection Commissioner under the Data Protection Act 2018, Indonesia has adopted a similar oversight structure through the mandate to establish a Personal Data Protection Authority. The existence of this independent oversight body is crucial as an authority with legal discretion to oversee massive data traffic. In the modern context, the challenge for this oversight body is to integrate artificial intelligence instruments to perform audit and monitoring functions automatically, so that comprehensive data protection can be achieved through synergy between legal authority and technological sovereignty. The establishment of this body with special authority to oversee personal data traffic is to ensure

that personal data controllers have safeguarded citizens' personal data in accordance with standards and ensure the security of personal data. (Antara News, 2021).

4. Conclusion

The urgency of optimizing AI within Indonesia's national legal framework is a logical consequence of the enactment of Law Number 27 of 2022 concerning Personal Data Protection. Although the Personal Data Protection Law has unified previously fragmented regulations, effective law enforcement still faces challenges posed by technological asymmetry and the complexity of cyberattacks that cannot be mitigated through manual oversight. Comparative studies with the United Kingdom (Data Protection Act) and Malaysia (PDPA 2010) show that successful data protection relies heavily on the existence of an independent and competent supervisory authority. The use of AI can position the state as an adaptive protector of citizens' information sovereignty. Moving forward, the government needs to formulate technical regulations that establish AI as a minimums security standard for electronic system administrators, to ensure substantive and technological legal certainty for all Indonesians. The government is also expected to immediately formulate ethical guidelines and accountable AI algorithm standards to complement the implementation of the Personal Data Protection Law, so that the use of artificial intelligence in data security does not create new biases or discrimination against individual subjective rights.

5. References

Journals:

Adis Nur Hayati, "Analisis Tantangan Dan Penegakan Hukum Persaingan Usaha Pada Sektor E-Commerce di Indonesia," *Jurnal Penelitian Hukum De Jure 21*, No. 1 (2021): 109-122, https://doi. org/10.30641/dejure.2021.V21.109-122

Antara News, "Anggota DPR: RUU PDP Perlu Atur Bentuk Badan Pengawas Data Pribadi," 2021, https://www.antaranews.com/berita/2229722/anggota-dpr-ruu-pdp-perlu-atur-bentuk-badanpengawas-data-pribadi.

Arfian Setiantoro et al., "Urgensi Perlindungan Hukum Konsumen Dan Penyelesaian Sengketa E-Commerce Di Era Masyarakat Ekonomi Asean," Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional 7, No. 1 (2018): 1-17, https://doi.org/10.33331/rechtsvinding.v7i1.220.,

Atiyah, Atiyah, Nur Chalesa Fitriani, and Akhmad Zaki Yamani. "Digitalisasi Legal Drafting Melalui Artificial Intelligence: Peluang Dan Tantangan Masa Depan Dokumen Hukum di Indonesia." *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 2 (2025): hlm. 1283-1299. DOI: https://doi.org/10.62976/ijijel.v3i2.1113

Bachtiar, Farid Rizki, Wisnu Ardytia, and Demas Brian Wicaksono. "Analisis Penegakan Hukum Data Pribadi Pada Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Indonesia." *AMAR* 3, no. 2 (2025): DOI: https://doi.org/10.62734/amar.v3i2.762

Christoforus Ristianto, "*DPR Didesak Sahkan RUU Perlindungan Data Pribadi*," 2019, https://pemilu.kompas.com/read/2019/08/02/13450871/dpr-didesak-sahkan-ruu-perlindungan-datapribadi.

Eka N.A.M Sihombing and Muhammad Yusrizal Adi Syaputra, "Implementasi Penggunaan Kecerdasan Buatan Dalam Pembentukan Peraturan Daerah," *Jurnal Ilmiah Kebijakan Hukum* 14, No. 3 (2020): 419-434, https://doi.org/10.30641/kebijakan.2020.V14.419-434.,

Emmanuel, Rheimanda Devin, Ani Anggraini, Agus Condro Wibowo, Kartika Imam Santoso, and Eko Supriyadi. "AI-BAHSI: Metode Hibrid Artificial Intelligence-Behavioral Analysis dan Hybrid Security Intelligence untuk Deteksi dan Mitigasi Ancaman Real-time pada Wireless Access Point." *Julia: Jurnal Ilmu Komputer An Nuur* 5, no. 2 (2025): DOI: https://doi.org/10.35720/julia.v5i2.30

Febri Jaya and Wilton Goh, "Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia," *Supremasi Hukum* 17, No. 2 (2021): 1-11, https://doi.org/https://doi.org/10.33592/jsh.v17i2.1287.,

Hari Sutra Disemadi and Denis Oxy Handika, "Community Compliance with the Covid-19 Protocol Hygiene Policy in Klaten Regency, Indonesia," Legality: Jurnal Ilmiah Hukum 28, No. 2 (2020): https://doi.org/10.22219/ljih.v28i2.12180.,

Ismaila, Suharne. "Personal Data Protection Principles: Ensuring Effective Implementation of Data Privacy Policies in Private Higher Institutions." *Published & distributed by* 2023, no. 3rd (2023):

Junaedi, Asep Mahbub. "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian dan Pengembangan* 5, no. 2 (2025): DOI: https://doi.org/10.51878/knowledge.v5i2.5269

Khan, Farha, and Akansha Mer. "Embracing artificial intelligence technology: Legal implications with special reference to European Union initiatives of data protection." In *Digital transformation, strategic resilience, cyber security and risk management*, Emerald Publishing Limited, 2023.

Kirana Rukmayuninda Ririh et al., "Studi Komparasi Dan Analisis Swot Pada Implementasi Kecerdasan Buatan (Artificial Intelligence) Di Indonesia," *J@ti Undip: Jurnal Teknik Industri* 15, No. 2 (2020): https://doi.org/doi.org/10.14710/jati.15.2.122-133.,

Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia," *Kanun Jurnal Ilmu Hukum* 20, No. 2 (2018): https://doi.org/10.24815/kanun.v20i2.11159.,

Maaliki, Naavi'U. Emal, and Eko Soponyono. "Kebijakan hukum pidana dalam menanggulangi tindak pidana berita bohong." *Jurnal Pembangunan Hukum Indonesia* 3, no. 1 (2021): DOI: https://doi.org/10.14710/jphi.v3i1.59-69

Paulus Wisnu Yudoprakoso, "Kecerdasan Buatan (Artificial Intelligence) Sebagai Alat Bantu Proses Penyusunan Undang-Undang Dalam Upaya Menghadapi Revolusi Industri 4.0 Di Indonesia," *Simposium Hukum Indonesia* 1, No. 1 (2019):

Pratama, Arya Satya, Suci Maela Sari, Maila Faiza Hj, Moh Badwi, and Mochammad Isa Anshori. "Pengaruh Artificial Intelligence, Big data dan otomatisasi terhadap kinerja SDM di Era digital." *Jurnal Publikasi Ilmu Manajemen* 2, no. 4 (2023): DOI: https://doi.org/10.55606/jupiman.v2i4.2739

Pratama, Gede Aditya, and Elfirda Ade Putri. "Edukasi Terkait Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Bagi Masyarakat Desa Lubang Buaya." *Abdi Bhara: Jurnal Pengabdian Kepada Masyarakat* 3, no. 2 (2024): DOI: https://doi.org/10.31599/ya8v0r61

Qur'ani Dewi Kusumawardani, "Hukum Progresif Dan Perkembangan Teknologi Kecerdasan Buatan," *Veritas et Justitia* 5, No. 1 (June 26, 2019): https://doi.org/10.25123/vej.3270.,

Ramadhan, Muhammad Aziz Tri. "Optimalisasi Produktivitas Industri 4.0 Melalui Penerapan Teknologi Kecerdasan Buatan." *Prosiding Sains dan Teknologi* 4, no. 1 (2025):

Rosalinda Elsina Latumahina, "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya," *Jurnal Gema Aktualita* 3, No. 2 (2014): 14-25.,

Rosyadi, Safriansyah Yanwar, and Zainal Arifin Hoesein. "Pembaruan Hukum di Era Digital: Aspek Hukum terhadap Validitas Hasil Analisis Artificial Intelligence Sebagai Alat Bukti Dalam Penegakan Hukum Pidana Pertambangan." *Judge: Jurnal Hukum* 6, no. 03 (2025): https://doi.org/10.54209/judge.v6i03.1569

SAS Insights, "Kecerdasan Buatan/Artificial Intelligence (Apa Itu Dan Mengapa Hal Itu Penting)," 2025, https://www.sas.com/id_id/insights/analytics/what-is-artificial-intelligence.html.

Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia*," Yustisia Jurnal Hukum* 5, No. 1 (April 2016): https://doi.org/10.20961/yustisia.v5i1.8712.

Zuryati Mohamed Yusoff, "The Malaysian Personal Data Protection Act 2010: A Legislation Note," *New Zealand Journal of Public and Internasional Law* 9 No. 1 (2011).

Books:

Barda Nawawi Arief. (1996). *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara*, Semarang: Badan Penerbit Universitas Diponegoro.

Graham Greenleaf. (2012). "*Global Data Privacy Laws: 89 Countries, and Accelerating*," Privacy Laws & Business International Report 115.

Soerjono Soekanto. (1985). *Penelitian Hukum Normatif,* Suatu Tinjauan Singkat, Jakarta: PT Raja Grafindo Persada.

Regulation:

Law of the Republic of Indonesia Number 1 of 2024 concerning Electronic Information and Transactions

Law of the Republic of Indonesia Number 27 of 2022 concerningPersonal Data Protection