OPEN ACCESS

LAW RESEARCH
Review Quarterly

Law Research Review Quarterly is a **Journal for Law, Justice, and Crime in Indonesia and Southeast Asia**. The Journal is a peer-reviewed journal published by Faculty of Law Universitas Negeri Semarang, Indonesia. The Journal published quarterly on February, May, August, and November. ISSN 2716-3415 (Online)
Online at https://journal.unnes.ac.id/journals/snh

Reformulation of Cybercrime Regulations in The Misuse of Artificial Intelligence in Indonesia

Dosni Ana Ragita Pakpahan
Universitas Negeri Semarang, Semarang, Indonesia
ragitapakpahan10@students.unnes.ac.id

Anis Widyawati
Universitas Negeri Semarang, Semarang, Indonesia
anis@mail.unnes.ac.id

Abstract

The rapid development of AI has increased the potential for cybercrime through increasingly sophisticated, automated, and wide-scale abuse methods. In Indonesia, the regulation of cybercrimes related to the abuse of AI is still fragmented and generally relies on general provisions on cybercrimes, so it does not fully accommodate the specific characteristics and risks of AI technology. This study aims to analyze the regulation of cybercrime in the abuse of AI in Indonesia, examine the regulatory approach applied in the European Union, and formulate a reformulation of cybercrime regulations in the misuse of artificial intelligence in Indonesia. This study uses a normative legal research method with a statute approach and a comparative approach conducted through literature studies. Primary legal materials include Indonesian and European Union laws and regulations, as well as other regulations, which are supported by secondary legal materials in the form of academic literature and official documents. The results of the study show that the applicable regulations in Indonesia have not provided adequate legal certainty and accountability mechanisms for AI-based cybercrimes. Instead, the EU implements a more structured

and risk-based regulatory model. This study concludes that Indonesia needs to reformulate the regulation of cybercrime by explicitly integrating the risks of using AI, harmonizing laws and regulations, and strengthening institutional capacity to realize effective law enforcement in the digital era.

KEYWORDS
Regulatory Reformulation, Cybercrime, Artificial Intelligence.

Introduction

The advancement of information and communication technology has brought significant changes to various aspects of people's lives around the world. Along with the rapid flow of digitalization, cybercrime has emerged as one of the serious challenges faced by society, especially in the Southeast Asian region.[1] Cybercrime can be understood as criminal acts committed through the use of information technology, especially computers, computer networks, and the internet, both as a tool and as a target for crime. In this context, digital technology is used to carry out unlawful acts, attack the interests of other parties, or take advantage of security gaps in electronic systems.[2] AI has become one of the most influential technologies; this is evidenced by the increase in AI users in Indonesia by 59 percent in recent years, much higher than the average country in Southeast Asia.[3] AI is a technology that mimics the way humans think through machines that are programmed to learn, reason, understand language, solve problems, and create. In simple terms, AI is a form of intelligence that is embedded in a

[1] Zico Junius Fernando, Anis Widyawati, and Kasmanto Rinaldi, "Cyber Victimology and Legal Gaps in Southeast Asia," *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 2, https://doi.org/10.15294/ildisea.v4i1.20147.
[2] Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Jurnal Hukum & Pembangunan* 2, no. 2 (2023): 302.
[3] Defara Dhanya, "Pengguna AI Di Indonesia Capai 59 Persen, Industri Catat Peningkatan Aktivitas," Tempo.co, accessed February 2, 2026, https://www.tempo.co/digital/pengguna-ai-di-indonesia-capai-59-persen-industri-catat-peningkatan-aktivitas-2081983.

system.[4] The term "artificial intelligence" was first proposed by John McCarthy along with several other scientists in 1956 through a proposal for the Dartmouth Summer Research Project Conference on Artificial Intelligence, which defined artificial intelligence as the science and engineering of creating machines that possess intelligence.[5] Since then, AI has continued to evolve as more and more research has been done on its theories and basic principles.[6] The development of AI then expanded from mere academic research to practical applications in various fields such as education, health, transportation, and others.

In the education sector, AI supports adaptive learning and virtual tutoring, as shown by the Duolingo application that adapts the material to the user's ability. In the health sector, AI contributes to the diagnosis and treatment of patients, for example, through IBM Watson for Oncology, which helps doctors determine cancer treatment plans, while in the field of transportation, the presence of autonomous vehicles is clear evidence of AI innovation in bringing efficiency and safety. [7] The presence of AI presents a new paradigm in various aspects of human life. This technology offers a variety of conveniences and efficiencies that contribute positively to the progress of civilization.

Behind the various benefits offered, the use of AI also brings a number of challenges that cannot be ignored. One is the potential for unfairness in decision-making, especially when AI systems are trained to use data that is biased or does not represent actual conditions, thus risking discrimination.[8] In the healthcare sector, for example, the use of AI to

[4] Kushariyadi et al., *Artificial Intelligence: Dinamika Perkembangan AI Beserta Penerapannya* (Jambi: PT. Sonpedia Publishing Indonesia, 2024).
[5] Ardi Azhar Nampira et al., *Artificial Intelligence: A Guide for Thinking Humans* (Yogyakarta: PT. Green Pustaka Indonesia, 2025).
[6] Hendra Jaya et al., *Kecerdasan Buatan* (Makassar: Fakultas MIPA Universitas Negeri Makassar, 2018).
[7] Rony Sandra Yofa Zebua et al., *Fenomena Artificial Intelligence (AI)* (Jambi: PT. Sonpedia Publishing Indonesia, 2023).
[8] Eric J. Topol, "High-Performance Medicine: The Convergence Of Human And Artificial Intelligence," *Nature Medicine* 25, no. 1 (2019): 51, https://doi.org/10.1038/s41591-018-0300-7.

support the diagnostic process has the potential to cause medical errors if the algorithms used are not closely monitored or have not undergone adequate clinical testing. Meanwhile, in the field of education, the application of AI in automated assessment systems raises various debates, particularly concerning issues of fairness and the accuracy of evaluating students' abilities.[9] In addition, the protection of personal data becomes a very crucial challenge, considering that AI systems rely on processing large amounts of data, including sensitive data such as medical records, financial information, and user preferences, which are at risk of being misused if not regulated and protected by a clear and strict legal framework.[10]

Various cases in Indonesia show how AI can have a serious impact on society. As has happened lately, namely the use of AI to create fake photos or videos *(deepfakes)*. For example, the video of President Prabowo Subianto being falsified as if offering financial assistance through *the WhatsApp* application,[11] shows how technology can be used for fraud, while the manipulation of Finance Minister Sri Mulyani's video with the narrative "teachers are the burden of the state",[12] illustrates how easily public trust is shaken by digital disinformation. In addition, the case of a Universitas Udayana student who edited a female student's personal photo with AI,[13] confirms the emergence of a new form of digital-based sexual violence, where technology is used irresponsibly to the point of injuring the dignity of individuals. In addition, in the financial sector, there are credit card fraud cases that utilize AI applications, where perpetrators use the technology to

[9] Wayne Holmes, Maya Bialik, and Charles Fadel, *Artificial Intelligence in Education. Promise and Implications for Teaching and Learning* (Boston: Center For Curriculum Redesign, 2019).
[10] Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-57959-7.
[11] Shella Octavia and Robertus Belarminus, "Kasus Video 'Deepfake' Prabowo, Semua Bisa Jadi Korban AI," Kompas.com, January 24, 2025.
[12] Rabbani Hidayatullah, "Deepfake Sri Mulyani Dan Kacaunya Publik Indonesia Di Tengah AI," Kompas.com, August 22, 2025.
[13] Tim detikBali, "Siasat Jahat Mahasiswa Unud Edit Foto Teman Wanita Jadi Foto Asusila Dengan AI," detik.com, April 26, 2025, https://www.detik.com/bali/hukum-dan-kriminal/d-7886450/siasat-jahat-mahasiswa-unud-edit-foto-teman-wanita-jadi-foto-asusila-dengan-ai.

manipulate the victim's data and identity to pass the banking verification process. This mode shows that AI can be used as a means to manipulate digital systems that rely on biometric authentication and personal data. The case indicates a serious challenge for the legal system, particularly in the protection of personal data and technology-based crime prevention.[14]

This phenomenon shows that AI not only brings benefits but also opens up new space for the birth of modern forms of crime. This technology-based crime mode is difficult to detect with traditional mechanisms because it takes advantage of the sophistication of algorithms and complex digital networks. This condition poses challenges for the existing legal system, especially in providing legal certainty, community protection, and adaptation to social changes influenced by technological developments.

Along with the wider use of AI, countries around the world have taken concrete steps to draft regulations that are contextual and anticipatory, as the European Union has done. However, until now Indonesia does not have a legal framework that specifically and comprehensively regulates the use of AI. Regulations regarding artificial intelligence (AI) are still generally broad and not yet specifically regulated but are spread across various other laws and regulations, such as the *UU ITE and* the *UU PDP,* and several sectoral regulations, including in the financial sector. The provisions that specifically regulate AI currently are limited to *SE Etika Kecerdasan Artifisial*, which functions as a mere ethical guideline and has no legal consequences in the event of a violation.

The absence of a specific and comprehensive AI regulatory framework in Indonesia raises serious problems from the perspective of the rule of law. In the state of law, law is positioned as the main instrument to direct, limit, and control the use of power and social development, in this case, including technological developments. Article 1, paragraph (3) of the

[14] Ady Anugrahadi, "Polisi Ungkap Modus Baru Penipuan Kartu Kredit Dengan Aplikasi AI, 2 Pelaku Ditangkap," Liputan6.com, accessed February 4, 2026, https://www.liputan6.com/news/read/5913070/polisi-ungkap-modus-baru-penipuan-kartu-kredit-dengan-aplikasi-ai-2-pelaku-ditangkap.

UUD 1945 emphasizes that Indonesia adheres to the principle of a state based on law,[15] so any phenomenon that significantly impacts the rights and obligations of citizens must be regulated within a clear and firm legal framework. Therefore, the formation of laws and regulations needs to consider the protection of human rights as well as social responsibility in community life. On one hand, society is required to have awareness and compliance with the law, while on the other hand, the state is obligated to enforce the law and ensure legal certainty.[16]

Theoretically, the idea of the supremacy of law according to Jimly Asshiddiqie views the supremacy of law, the principle of legality, and the protection of human rights, as well as its role as an instrument to achieve the goals of a welfare state (welfare rechtsstaat), as fundamental elements.[17] In the context of the use of AI, these principles demand that the entire process of developing, deploying, and using AI be under clear and accountable legal control. The rule of law requires that AI technology does not develop freely without normative limits, while the principle of legality requires the existence of a firm legal basis regarding authority, responsibility, and supervisory mechanisms for the use of AI. In addition, the protection of human rights is an integral aspect, considering that AI has the potential to affect the right to privacy.

Furthermore, in the framework of legal theory as a means of community renewal, Mochtar Kusumaatmadja emphasized that changing order is the goal of a developing society, so that if these changes are to be realized in an orderly manner, the law becomes a means that cannot be ignored.[18] In the context of AI development in Indonesia, this view

[15] Undang-Undang Dasar 1945.
[16] Muhtar Hadi Wibowo, Ali Masyhar Mursyid, and Anis Widyawati, "Progressionism Restorative Justice Policies in Achieving Rehabilitative Criminal Justice," *IJCLS (Indonesian Journal of Criminal Law Studies)* 9, no. 1 (2024): 118, https://doi.org/10.15294/ijcls.v9i1.50292.
[17] Jimly Asshiddiqie, "Gagasan Negara Hukum Indonesia," 2011.
[18] Mochtar Kusumaatmadja, *Hukum, Masyarakat Dan Pembinaan Hukum Nasional; Suatu Uraian Tentang Landasan Pikiran, Pola, Dan Mekanisme Pembaharuan Hukum Di Indonesia* (Bandung: Binacipta, 1976).

emphasizes that the rapid technological transformation must be accompanied by regulations capable of guiding these changes to remain within the framework of legal certainty, justice, and benefits. Without law as a controlling instrument, the use of AI has the potential to develop without limits and cause legal and social problems that could disrupt the main objectives of development itself.

This condition reflects that positive law has not yet fully accommodated the reality of technological developments within the national legal system. Therefore, a reformulation of regulations concerning cybercrimes related to AI misuse is needed, which can connect factual and normative aspects so that the law does not lag behind technological advances but rather serves as a preventive, adaptive tool oriented toward protecting public interests and constitutional values. Based on this urgency, this paper focuses on three main points of discussion, namely, examining the regulation of cybercrime in the abuse of AI in Indonesia, the regulation of cybercrime in the abuse of AI in the European Union, and the reformulation of the regulation of cybercrime in the abuse of AI in Indonesia.

Methods

This study applies a normative legal research method with a statutory and comparative law approach conducted through literature review. Primary legal materials include various laws and regulations in force in Indonesia, such as the *KUHP*, the *UU ITE*, and the *UU PDP*, as well as provisions regarding artificial intelligence in the European Union, particularly the EU AI Act, along with other related regulations. Meanwhile, secondary legal materials are sourced from academic literature, scientific journals, books, and official documents that examine AI-based cybercrime.

Research data were collected through document analysis and were analyzed qualitatively using normative juridical methods and legal comparison. This analysis was conducted to interpret norms, compare regulatory frameworks, and identify legal gaps so that it can be used as a basis for drafting recommendations for regulatory reform concerning the misuse of artificial intelligence in the context of cybercrime in Indonesia.

Results and Discussion

1. Regulation of Cybercrime in the Misuse of Artificial Intelligence in Indonesia.

Indonesia does not yet have a comprehensive special regulation regulating AI. The government has so far only relied on a partial legal framework, including the *UU ITE*, a relevant regulation in dealing with cybercrimes. Although the legal instrument has provided a basis for regulating cybercrimes, the scope of the *UU ITE* tends to be general so that it is not able to cover AI-based cybercrimes. There is a fundamental weakness in the law, which does not explain the definition of AI, so it becomes a fundamental obstacle in the formulation and application of criminal law. The existence of the diction "*Agen Elektronik"* in Article 1 number 8, which defines an electronic agent as *"perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh orang,"*[19] this "automatic" characteristic makes AI included in the electronic system according to the Law.[20]

[19] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
[20] Muhammad Tan Abdul Rahman Haris and Tantimin Tantimin, "Analisis Pertanggungjawaban Hukum Pidana terhadap Pemanfaatan Artificial Intelligence di Indonesia," *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (2022): 311, https://doi.org/10.23887/jkh.v8i1.44408.

The provisions of the *UU ITE* basically still focus on conventional forms of cybercrime, such as illegal access, unauthorized interception, data manipulation, and the dissemination of prohibited content. Currently, the existence of AI is not emphasized in any article, so the existing legal formulations are not yet able to explicitly anticipate AI-based cybercrimes. Therefore, the author encourages the establishment of specific regulations regarding AI, considering that the *UU ITE* also does not regulate crucial technical aspects, such as labeling obligations, reporting mechanisms, and oversight of high-risk AI systems, in accordance with the recommendations in the EU AI Act framework from the European Union.[21]

Furthermore, regarding the *UU PDP*, most AI systems operate by collecting, processing, and analyzing personal data on a massive scale,[22] so this law should be able to address issues related to the personal data of AI subjects or users. However, in reality, although the *UU PDP* framework has strengthened the rights of data subjects and requires data controllers to be responsible for the processing of personal data, the regulation is still insufficient to deal with the complexity of risks arising from the use of AI on personal data. The existing arrangements are still general and do not yet detail technical aspects, such as algorithmic audit mechanisms or clarity of legal accountability for decisions generated by AI systems.[23] The use of AI must be regulated in such a way that the state and system operators can ensure legal accountability for every decision made, by upholding the principles of fairness and non-discrimination to prevent harm to individuals or specific groups.

[21] Adnasohn Aqilla Respati, "Reformulasi Undang-Undang ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation," *Jurnal USM Law Review* 7, no. 3 (2024): 1750, https://doi.org/10.26623/julr.v7i3.10578.
[22] Kimmy Baby Kirana and Wilma Silalahi, "Tantangan Regulasi Kecerdasan Buatan (AI) dalam Perspektif Hukum Perlindungan Data Pribadi di Indonesia," *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 6 (2025): 1811.
[23] Mar'atus Solikhah, "Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework," *Indonesian Cyber Law Review* 2, no. 1 (2025): 39–50, https://doi.org/10.59261/iclr.v2i1.14.

Even in personal data protection in general, the *UU PDP* is considered to still have weaknesses in the form of suboptimal implementation and weak enforcement. In practice, the *UU PDP* is considered not optimal because there are no implementing regulations and the establishment of an effective supervisory institution.[24] Articles 58–61 of the *UU PDP* require the establishment of a supervisory institution within two years, but until the transition period is completed, the institution does not exist. This hinders the imposition of administrative sanctions for violators.[25] Thus, strengthening legal infrastructure must be accompanied by massive socialization so that laws are truly able to protect society and answer increasingly complex privacy challenges. Without these concrete steps, regulation will only become a weak formal norm in the face of the risk of misuse of technology.[26]

In addition to the above regulations, a number of sectoral regulations have contained provisions related to the use of digital technology, including AI. In the financial sector, for example, *POJK No. 11/POJK.03/2022* and *POJK No. 21/2023* regulate the governance of information technology and digital services, with an emphasis on the principles of prudence, risk management, and regulatory compliance.[27] OJK has collaborated with several associations, namely AFTECH, AFSI, AFPI, and ALUDI, to issue a code of ethics guideline for the financial technology industry.[28] The guide

[24] Rumadi Ahmad, "Lembaga Perlindungan Data Pribadi," KOMPAS.id, July 22, 2024, https://www.kompas.id/artikel/lembaga-perlindungan-data-pribadi.
[25] Akmal Muhammad Abdullah, "Pelindungan Hak Privasi terhadap Pengumpulan Data Pribadi oleh AI Generatif Berdasarkan Percakapan dengan Pengguna," *Padjadjaran Law Review* 12, no. 2 (2024): 153–54, https://doi.org/10.56895/plr.v12i2.1796.
[26] Asep Mahbub Junaedi, "Urgensi Perlindungan Data Pribadi dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022," *KNOWLEDGE : Jurnal Inovasi Hasil Penelitian dan Pengembangan* 5, no. 2 (2025): 255, https://doi.org/10.51878/knowledge.v5i2.5269.
[27] Theresia Anita Christiani and Chryssantus Kastowo, "Artificial Intelligence in the Banking Sector in Indonesia and Its Challenges from a Legal Perspective," *Liberal Arts and Social Studies International* 1, no. 1 (2025): 48.
[28] "OJK Bersama Asosiasi Fintech Luncurkan Panduan Kode Etik Kecerdasan Buatan (Artificial Intelligence) Di Industri Teknologi Finansial," AFTECH, accessed September 12, 2025, https://fintech.id/id/education-and-literacy/latest-news/ojk-bersama-asosiasi-fintech-luncurkan-panduan-kode-etik-kecerdasan-buatan-(artificial-intelligence)-di-industri-teknologi-finansial.

emphasizes that the use of AI must be in line with the values of Pancasila and ethical principles such as justice, accountability, transparency, and security. Furthermore, the OJK issued a special guidance on banking AI governance that describes the AI lifecycle from initiation to audit while emphasizing the importance of risk mitigation so that the application of AI provides optimal benefits without neglecting the control aspect. All of these steps complement the OJK's authority to supervise artificial intelligence technology innovations that are applied responsibly by banks.[29]

Furthermore, in the health sector, the use of AI in Indonesia is growing quite rapidly as an effort to overcome the limited number of medical personnel and the inequality of distribution.[30] One of the most prominent forms of use of AI is telemedicine services. *UU Kesehatan* has provided a legal basis for telemedicine practice,[31] which was then affirmed through the *Permenkes 20/2019* concerning the Implementation of Telemedicine between Health Service Facilities. [32] This regulation recognizes technology-based remote medical consultation services as part of official health services, including those utilizing AI technology. These services include the exchange of information for the purposes of diagnosis, treatment, disease and injury prevention, research, evaluation, and health education. However, various studies show that there are a number of challenges that accompany the application of AI in the healthcare sector, especially related to the potential for algorithm bias, the protection of patients' personal data, and the risk of malpractice.[33] The dilemma arises

[29] "Tata Kelola Kecerdasan Artifisial Perbankan Indonesia," Portal OJK, accessed September 12, 2025, https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Pages/Tata-Kelola-Kecerdasan-Artifisial-Perbankan-Indonesia.aspx.
[30] Sigit Primasatya, "Perlindungan terhadap Perkembangan Layanan Kesehatan Berbasis Kecerdasan Buatan (Artificial Intelligence) di Indonesia," *Jurnal Globalisasi Hukum* 1, no. 1 (2024): 79, https://doi.org/10.25105/jgh.v1i1.19833.
[31] Undang-Undang Nomor 17 Tahun 2023 Tentang Kesehatan.
[32] Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 Tentang Penyelenggaraan Pelayanan Telemedicine Antar Fasilitas Pelayanan Kesehatan.
[33] Patriot Haryo Trenggono and Adang Bachtiar, "Peran Artificial Intelligence dalam Pelayanan Kesehatan : A Systematic Review," *Jurnal Ners* 7, no. 1 (2023): 449, https://doi.org/10.31004/jn.v7i1.13612.

when there is an error in patient handling that raises the need to determine who must be held legally accountable, given that positive law in Indonesia has not substantively regulated or recognized the concept of artificial intelligence specifically.

Then, the regulation of AI in the transportation sector is evident through the use of unmanned aerial vehicles (drones). As part of the Industrial Revolution 4.0, drones are now widely used for logistics, mapping, disaster management, and military interests.[34] Initially, the government regulated through the *Permenhub 180/2015,* which was updated with the *Permenhub 47/2016,* then updated again with the *Permenhub 37/2020*. This latest regulation confirms the limits of airspace, permit mechanisms, and safety standards in drone operation.[35] However, the existing regulations still emphasize the administrative aspect, while the risks of abuses such as smuggling, privacy violations, and terrorism demand stronger regulations with criminal sanctions to ensure legal protection and public safety.[36]

As a first step in responding to the development of AI, the government, through the Kominfo, issued *SE Nomor 9/2023*. This circular emphasizes the principles of ethics, prudence, safety, and positive impact orientation in the use of AI.[37] While not a legally binding regulation,[38] this policy reflects the government's awareness of the urgency of responsible AI governance. However, because its status is limited to circulars, its effectiveness in providing legal protection is still limited. This raises the need for a stronger legal framework, both in the form of laws and

[34] Mukhlis Al Huda, "Penguatan Pengaturan Pesawat Udara Tanpa Awak (Drone) Melalui Undang-Undang," *IBLAM LAW REVIEW* 1, no. 2 (2021): 103–20.
[35] Peraturan Menteri Perhubungan Nomor 37 Tahun 2020 Tentang Pengoperasian Pesawat Udara Tanpa Awak Di Ruang Udara Yang Dilayani Indonesia.
[36] Al Huda, "Penguatan Pengaturan Pesawat Udara Tanpa Awak (Drone) Melalui Undang-Undang."
[37] Surat Edaran Menteri Komunikasi Dan Informatika Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial.
[38] M. Wildan Mufti et al., "Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence," *Socius: Jurnal Penelitian Ilmu-ilmu Sosial* 1, no. 11 (2024): 139, https://doi.org/10.5281/ZENODO.11422903.

government regulations, so that AI regulation in Indonesia does not stop at the ethical realm but also has clear and enforceable legal certainty. Thus, the *SE 9/2023* can be seen as a temporary normative foundation while waiting for the presence of more comprehensive and binding regulations.[39]

In addition, the regulation on AI has not been specifically regulated in the latest *KUHP*, but provisions on cybercrimes have been formulated as an important instrument in tackling crimes committed through technology and the internet. *KUHP* contains regulations related to various forms of cybercrime, such as illegal access, attacks on state information systems, and violations of the financial and banking systems,[40] with the threat of sanctions that are classified as severe to have a deterrent effect. The formulation of the elements of criminal acts in more detail shows that there is a strengthening of the legal basis compared to previous regulations, as well as providing legal certainty in handling complex and cross-border cybercrimes.[41]

The existence of these regulations is also positioned as a strategic foothold for future legal development, especially in dealing with cybercrime that is increasingly sophisticated due to the development of AI. The rapid advancement of AI technology has driven the emergence of new modus operandi, such as bot-based automated attacks and data manipulation through intelligent algorithms, which demand continuous positive legal updates. Therefore, the *UU ITE* is seen as able to present a more comprehensive and adaptive legal framework in protecting society, as well as creating a safe digital environment in the midst of the dynamics of modern technological developments and crime.

[39] Respati, "Reformulasi Undang-Undang ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation."
[40] Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana.
[41] Yosua Hia, "Analisa Yuridis Pasal-Pasal Khusus terkait Kejahatan Siber dalam KUHP Baru (UU 1/2023)," *Jurnal SELISIK* 10, no. 1 (2024).

2. Regulation of Cybercrime in the Misuse of Artificial Intelligence in the European Union

On August 1, 2024, the European Union became the first region in the world to comprehensively implement Regulation (EU) 2024/1689, or the EU AI Act, to regulate artificial intelligence.[42] This regulation uses a risk-based approach and is based on the seven ethical principles outlined in the 2019 Ethics Guidelines for Trustworthy AI*, namely "human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination, and fairness; societal and environmental well-being and accountability."*[43] The purpose of these principles is to ensure that the development and application of AI take place in a consistent, credible manner and are based on human values, in accordance with the Charter of Human Rights and the fundamental values of the European Union.[44]

Given the potential impact of AI on fundamental rights, safety, and overall societal well-being, the EU adopts a risk-based approach by classifying AI system risks into four categories according to their level of danger.[45] This means that each determines the level of obligations and regulatory requirements that must be met, or the higher the level of risk, the stricter the rules imposed. The four parts are unacceptable, high, limited, and minimal risks.[46] High-risk AI means that it has the potential to have a major impact on individuals or society, under stricter rules and more scrutiny. This condition may require the implementation of adequate transparency mechanisms, clear documentation of data sources and

[42] "Panduan Lengkap Undang-Undang Kecerdasan Buatan Uni Eropa (Undang-Undang AI)," lawandmore.id, accessed September 18, 2025, https://lawandmore.id/blog/Undang-Undang-Kecerdasan-Buatan-Uni-Eropa/.
[43] Regulation (UE) 2024/1689 (Artificial Intelligence Act).
[44] Regulation (UE) 2024/1689 (Artificial Intelligence Act).
[45] Jérôme De Cooman, "Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act," *Market and Competition Law Review*, 2022, 49–88, https://doi.org/10.34632/MCLAWREVIEW.2022.11304.
[46] Martin Ebers, "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act," *European Journal of Risk Regulation* 16, no. 2 (2025): 684–85, https://doi.org/10.1017/err.2024.78.

methods used, and strengthening accountability procedures. In contrast, artificial intelligence systems that are categorized as low-risk may be subject to looser arrangements, thus providing a wider space for flexibility and innovation.[47]

The unacceptable risk category refers to the practice of using AI that is inherently considered to threaten human safety, livelihoods, and individual rights, and is therefore strictly prohibited. The prohibitions, which are explicitly regulated in Article 5 of the EU AI Act, include the use of AI that aims to control human behavior, conduct social assessments, or conduct biometric identification in public spaces.[48]

The EU AI Act also divides artificial intelligence systems into several levels of risk. AI systems that are classified as high-risk are not necessarily banned but must meet strict legal requirements to remain secure and respect fundamental human rights. The provisions regarding this category are set out in Article 6, which highlights AI systems with great potential risks, especially those that serve as safety components in products regulated by EU health and safety regulations. Additionally, this category includes the use of AI in sensitive sectors such as biometric identification, critical infrastructure, education, employment, and law enforcement.[49] On the other hand, AI systems with a limited level of risk are generally only required to be transparent, for example, by letting users know that they are interacting with AI or receiving AI-generated content. Meanwhile, AI systems that are considered at least at risk are not subject to special regulations because they are considered not to have a meaningful impact on society.[50]

[47] Cooman, "Humpty Dumpty and High-Risk AI Systems."
[48] "AI Act," European Commission, accessed January 24, 2026, https://digital-strategy.ec.europa.eu/policies/regulatory-framework-ai.
[49] Lorenzo Ricciardi Celsi, "The Dilemma of Rapid AI Advancements: Striking a Balance between Innovation and Regulation by Pursuing Risk-Aware Value Creation," *Information* 14, no. 12 (2023): 645, https://doi.org/10.3390/info14120645.
[50] Bianca Piachaud-Moustakis, "The EU AI Act," *Pharmaceutical Technology Europe* 35, no. 11 (2023): 8–9.

Parties who can be held accountable under the regulation include *providers* (providers of AI technology), *authorised representatives* (parties appointed in writing by AI manufacturers who are outside the EU to act on their behalf in the EU territory*), deployers* (as entities or persons who use AI systems under their authority for business or professional activities), *importers* (EU-domiciled parties that deploy AI systems from countries outside the EU to the EU market), *distributors* (parties in the supply chain that provide AI systems from *providers* and *importers* in the EU market after the product has entered the market), and *notified bodies* (bodies that carry out conformity assessment procedures).[51]

In line with the division of AI systems based on their level of risk, the EU AI Act also establishes fairly severe administrative sanctions for parties who violate these provisions. Violations of Article 5 of the EU AI Act, which involves the use of AI practices deemed unacceptable risks, can be subject to fines of up to EUR 35,000,000 or 7% of the company's annual global revenue. Non-compliance with other provisions, including obligations for providers, authorized representatives, importers, distributors, users, and notified bodies, as well as transparency obligations, can be subject to fines of up to EUR 15,000,000 or 3% of the company's annual global turnover if the violator is a business entity. Meanwhile, providing false, incomplete, or misleading information to notified bodies or national authorities can be subject to fines of up to EUR 7,500,000 or 1% of the company's annual global turnover.[52] In addition to sanctions in the form of fines, EU member states are also given the authority to impose non-monetary measures, such as warnings, marketing bans, restrictions on use, and withdrawal of products from circulation, as a form of enforcement against violations of the provisions of the EU AI Act.[53]

Within the framework of the EU AI Act, supervisory powers are divided in layers. The AI Office serves as a central authority that oversees AI

[51] Regulation (UE) 2024/1689 (Artificial Intelligence Act).
[52] Regulation (UE) 2024/1689 (Artificial Intelligence Act).
[53] Regulation (UE) 2024/1689 (Artificial Intelligence Act).

models with systemic impacts, while the Market Surveillance Authorities are tasked with enforcing provisions at the national level against AI systems circulating in the market. On the other hand, the European Data Protection Supervisor ensures that the use of AI by EU institutions remains in line with the principles of personal data protection.[54] The EU AI Act is also closely linked to the General Data Protection Regulation (GDPR) as the main personal data protection regime in the European Union.[55] Through the GDPR, individuals are given strong control over their personal data, including the right to access, correct, and delete the data collected.[56] These provisions become very important in the context of AI use, as algorithms often rely on personal data to function optimally, especially in sectors such as education and healthcare that handle large amounts of sensitive data.[57] Therefore, the GDPR sets high standards for personal data protection in the European Union, affirming individuals' rights to maintain control over the use of their data, including in the development and implementation of AI technology.

3. Reformulation of Cybercrime Regulations in The Misuse of Artificial Intelligence in Indonesia

Lessons learned from international practices such as the EU AI Act can provide inspiration to reformulate the regulation of cybercrime in the abuse of AI in Indonesia. Regulations regarding AI in Indonesia have not yet been outlined in a special comprehensive regulation. AI regulations are still regulated indirectly through various other laws and regulations. The issuance of the *SE 9/2023* shows the country's initial recognition of the need

[54] Kasia Söderlund and Stefan Larsson, "Enforcement Design Patterns in EU Law: An Analysis of the AI Act," *Digital Society* 3, no. 41 (2024): 1–21, https://doi.org/10.1007/s44206-024-00129-8.
[55] Regulation (UE) 2016/679 (General Data Protection Regulation).
[56] Voigt and Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)*.
[57] Jonas Tallberg et al., "The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research," pt. 1-23, *International Studies Review* 25, no. 3 (2023), https://doi.org/10.1093/isr/viad040.

to regulate the use of AI. Although non-binding and limited to ethical norms, the policy indicates an open space for the formation of a stronger legal framework. Therefore, the existence of the EU AI Act provides a concrete reference for Indonesia to reformulate the regulation of cybercrime in the abuse of AI.

Based on the previous series of explanations by looking at the legal reality and phenomena that occur in society, it is possible to reformulate the regulation of cybercrimes in the abuse of AI in Indonesia, such as

a. The formation of artificial intelligence laws, such as the EU AI Act, by listing several important aspects, namely:
   - General provisions to define the main concepts of AI-based cybercrime and its scope so that there are no contradictions.
   - The ethical principles of the use of AI to ensure that the use of AI can run in line with the values of Pancasila, the constitution, and the interests of public protection, without hindering the development of technological innovation.
   - Risk-based grouping of AI systems to determine how strict regulation, oversight, and legal accountability should be imposed on an AI system. It can be grouped into four, namely low, medium, high, and unacceptable or prohibited risks.
   - Legal requirements and obligations for the operator, such as periodic algorithm audits, preparation and maintenance of technical documentation and system records, implementation of impact assessments of the use of AI, provision of incident reporting mechanisms, and notification or labeling obligations for the use of AI. This is intended so that AI can be ensured of its safety and does not interfere with the fundamental rights of society.
   - Criminal liability may be imposed on providers, developers, professional users, or other parties who have effective control over the AI system, especially if there is intentional or

negligent conduct in the design, supervision, or use of AI that gives rise to legal consequences. Perpetrators can be criminally threatened in the form of imprisonment, fines, revocation of permits, and other regulatory measures aimed at providing a deterrent effect while encouraging compliance with the provisions stipulated in the regulations.

- The establishment of a special body tasked with auditing algorithms, providing assessments, and conducting certification processes to ensure that the AI is properly implemented in accordance with ethics and legal norms. In addition, the establishment of a special agency plays a role in supervising compliance, taking corrective actions, and evaluating regulations to remain in line with technological advances and community needs.

The process of forming the Artificial Intelligence law needs to be carried out through a participatory and collaborative approach by involving various stakeholders, ranging from the government as a policymaker, academics as providers of theoretical foundations and scientific studies, technology practitioners and industry players as users and developers of AI, to civil society as the directly affected parties. This multi-stakeholder engagement is important to ensure that the regulations formed are not only normative but also applicable and responsive to real needs on the ground. In the formulation stage, experience and best practices from international regulations, such as the EU AI Act, can be selectively referenced, particularly in terms of the principles of prudence, transparency, and risk-based approaches, without disregarding national social, economic, and legal conditions. This process must also be accompanied by harmonization of existing laws and regulations, especially in the field of criminal law, the *UU ITE*, and the *UU PDP*, so that there is no overlap of norms. Thus, the establishment of AI

laws is expected to be able to produce a comprehensive, adaptive, and equitable legal framework, as well as be effective in anticipating the challenges of future technological developments.

b. Improvement of Structural Aspects and Supporting Facilities

In addition to substantial aspects of reform, improving the structure and supporting facilities is also very important to support the effectiveness of law enforcement. Law enforcement officials need to have adequate capacity and competence in the field of digital technology so that legal norms can be applied effectively. On the other hand, the availability of adequate facilities and infrastructure is the main supporting factor in dealing with complex and dynamic crimes so that law enforcement does not only stop at the normative level but can run optimally in practice.

c. International Cooperation

International cooperation is an important element in law enforcement efforts and countermeasures against cybercrimes involving AI, considering the character of cybercrimes that often exceed the boundaries of territory and state jurisdiction. Therefore, handling AI-based cybercrime cannot be done unilaterally but requires collaboration between countries. In this context, Indonesia can pursue various cooperation strategies, including the establishment and strengthening of extradition agreements against perpetrators of cybercrimes and active participation in international forums, such as the Global Forum on Cyber Expertise and the Global Partnership on Artificial Intelligence, as a means of knowledge exchange and joint capacity building.

d. Improving Digital Literacy and Education for the Community

Improving digital literacy and education for the community is a strategic step that needs to be prioritized. The low public understanding of technology, especially artificial intelligence, often makes them vulnerable to becoming victims of cybercrimes. Therefore, efforts to strengthen digital literacy are very important to be carried out through the implementation of a national digital literacy campaign that includes understanding AI, as well as through the preparation and implementation of AI learning modules in a formal education environment to build awareness and understanding of technology from an early age.

Conclusion

This study concludes that the regulation of cybercrimes related to the abuse of Artificial Intelligence (AI) in Indonesia has not been fully able to answer the legal challenges posed by the unique characteristics of AI, especially its autonomous nature, scalability, and cross-border dimensions. Although the existing cybercrime provisions have provided an initial legal basis, these regulations are still inadequate to ensure legal certainty, accountability, effectiveness, and prevention functions against AI-based cybercrimes. By comparison, the European Union has shown that a more structured and risk-based approach to regulation is able to align technological developments with legal protection and the public interest more optimally. Based on these findings, this study suggests that Indonesia reformulate the regulation of cybercrime by explicitly integrating the risks related to the use of AI into the national legal framework. Applicatively, this step can be realized through the establishment of special AI regulations that are harmonized with the *UU ITE* and the *UU PDP*, international cooperation, strengthening the capacity of law enforcement officials and technological infrastructure, as well as increasing digital literacy and

education for the public. This approach is expected to not only be able to respond to existing forms of AI abuse but also anticipate future technological developments so that the effectiveness and sustainability of cyber law enforcement in Indonesia can be guaranteed.

References

Abdullah, Akmal Muhammad. "Pelindungan Hak Privasi terhadap Pengumpulan Data Pribadi oleh AI Generatif Berdasarkan Percakapan dengan Pengguna." *Padjadjaran Law Review* 12, no. 2 (2024): 153–54. https://doi.org/10.56895/plr.v12i2.1796.

AFTECH. "OJK Bersama Asosiasi Fintech Luncurkan Panduan Kode Etik Kecerdasan Buatan (Artificial Intelligence) Di Industri Teknologi Finansial." Accessed September 12, 2025. https://fintech.id/id/education-and-literacy/latest-news/ojk-bersama-asosiasi-fintech-luncurkan-panduan-kode-etik-kecerdasan-buatan-(artificial-intelligence)-di-industri-teknologi-finansial.

Ahmad, Rumadi. "Lembaga Perlindungan Data Pribadi." KOMPAS.id, July 22, 2024. https://www.kompas.id/artikel/lembaga-perlindungan-data-pribadi.

Al Huda, Mukhlis. "Penguatan Pengaturan Pesawat Udara Tanpa Awak (Drone) Melalui Undang-Undang." *IBLAM LAW REVIEW* 1, no. 2 (2021): 103–20.

Anita Christiani, Theresia, and Chryssantus Kastowo. "Artificial Intelligence in the Banking Sector in Indonesia and Its Challenges from a Legal Perspective." *Liberal Arts and Social Studies International* 1, no. 1 (2025): 48.

Anugrahadi, Ady. "Polisi Ungkap Modus Baru Penipuan Kartu Kredit Dengan Aplikasi AI, 2 Pelaku Ditangkap." Liputan6.com. Accessed February 4, 2026. https://www.liputan6.com/news/read/5913070/polisi-ungkap-modus-baru-penipuan-kartu-kredit-dengan-aplikasi-ai-2-pelaku-ditangkap.

Butarbutar, Russel. "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya." *Jurnal Hukum & Pembangunan* 2, no. 2 (2023): 302.

Cooman, Jérôme De. "Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act." *Market and Competition Law Review*, 2022, 49–88. https://doi.org/10.34632/MCLAWREVIEW.2022.11304.

Dhanya, Defara. "Pengguna AI Di Indonesia Capai 59 Persen, Industri Catat Peningkatan Aktivitas." Tempo.co. Accessed February 2, 2026. https://www.tempo.co/digital/pengguna-ai-di-indonesia-capai-59-persen-industri-catat-peningkatan-aktivitas-2081983.

Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act." *European Journal of Risk Regulation* 16, no. 2 (2025): 684–85. https://doi.org/10.1017/err.2024.78.

European Commission. "AI Act." Accessed January 24, 2026. https://digital-strategy.ec.europa.eu/policies/regulatory-framework-ai.

Fernando, Zico Junius, Anis Widyawati, and Kasmanto Rinaldi. "Cyber Victimology and Legal Gaps in Southeast Asia." *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 2. https://doi.org/10.15294/ildisea.v4i1.20147.

Haris, Muhammad Tan Abdul Rahman, and Tantimin Tantimin. "Analisis Pertanggungjawaban Hukum Pidana terhadap Pemanfaatan Artificial Intelligence di Indonesia." *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (2022): 311. https://doi.org/10.23887/jkh.v8i1.44408.

Hia, Yosua. "Analisa Yuridis Pasal-Pasal Khusus terkait Kejahatan Siber dalam KUHP Baru (UU 1/2023)." *Jurnal SELISIK* 10, no. 1 (2024).

Hidayatullah, Rabbani. "Deepfake Sri Mulyani Dan Kacaunya Publik Indonesia Di Tengah AI." Kompas.com, August 22, 2025.

Holmes, Wayne, Maya Bialik, and Charles Fadel. *Artificial Intelligence in Education. Promise and Implications for Teaching and Learning*. Boston: Center For Curriculum Redesign, 2019.

Jaya, Hendra, Sabran, Muh. Ma'ruf Idris, Yasser A Djawad, A Ilham, and Ansari Saleh Ahmar. *Kecerdasan Buatan*. Makassar: Fakultas MIPA Universitas Negeri Makassar, 2018.

Junaedi, Asep Mahbub. "Urgensi Perlindungan Data Pribadi dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022." *KNOWLEDGE : Jurnal Inovasi Hasil Penelitian dan Pengembangan* 5, no. 2 (2025): 255. https://doi.org/10.51878/knowledge.v5i2.5269.

Kirana, Kimmy Baby, and Wilma Silalahi. "Tantangan Regulasi Kecerdasan Buatan (AI) dalam Perspektif Hukum Perlindungan Data Pribadi di Indonesia." *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 6 (2025): 1811.

Kushariyadi, Apriyanto H, Fajar Husain Asy'ari, Loso Judijanto, Yuwanda Purnamasari Pasrun, and Budi Mardikawati. *Artificial Intelligence: Dinamika Perkembangan AI Beserta Penerapannya*. Jambi: PT. Sonpedia Publishing Indonesia, 2024.

Kusumaatmadja, Mochtar. *Hukum, Masyarakat Dan Pembinaan Hukum Nasional; Suatu Uraian Tentang Landasan Pikiran, Pola, Dan Mekanisme Pembaharuan Hukum Di Indonesia*. Bandung: Binacipta, 1976.

lawandmore.id. "Panduan Lengkap Undang-Undang Kecerdasan Buatan Uni Eropa (Undang-Undang AI)." Accessed September 18, 2025.

https://lawandmore.id/blog/Undang-Undang-Kecerdasan-Buatan-Uni-Eropa/.

Nampira, Ardi Azhar, Loso Judijanto, Dia Cahya Wati, Erwin Hermawan, Tri Ari Cahyono, Santi Prayudani, Yuricha, Jarot Budiasto, Sa'dianoor, and Alfina Tiurmida Sitanggang. *Artificial Intelligence: A Guide for Thinking Humans*. Yogyakarta: PT. Green Pustaka Indonesia, 2025.

Octavia, Shella, and Robertus Belarminus. "Kasus Video 'Deepfake' Prabowo, Semua Bisa Jadi Korban AI." Kompas.com, January 24, 2025.

Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 Tentang Penyelenggaraan Pelayanan Telemedicine Antar Fasilitas Pelayanan Kesehatan.

Peraturan Menteri Perhubungan Nomor 37 Tahun 2020 Tentang Pengoperasian Pesawat Udara Tanpa Awak Di Ruang Udara Yang Dilayani Indonesia.

Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum.

Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum.

Piachaud-Moustakis, Bianca. "The EU AI Act." *Pharmaceutical Technology Europe* 35, no. 11 (2023): 8–9.

Portal OJK. "Tata Kelola Kecerdasan Artifisial Perbankan Indonesia." Accessed September 12, 2025. https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Pages/Tata-Kelola-Kecerdasan-Artifisial-Perbankan-Indonesia.aspx.

Primasatya, Sigit. "Perlindungan terhadap Perkembangan Layanan Kesehatan Berbasis Kecerdasan Buatan (Artificial Intelligence) di Indonesia." *Jurnal Globalisasi Hukum* 1, no. 1 (2024): 79. https://doi.org/10.25105/jgh.v1i1.19833.

Regulation (UE) 2016/679 (General Data Protection Regulation).

Regulation (UE) 2024/1689 (Artificial Intelligence Act).

Respati, Adnasohn Aqilla. "Reformulasi Undang-Undang ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation." *Jurnal USM Law Review* 7, no. 3 (2024): 1750. https://doi.org/10.26623/julr.v7i3.10578.

Ricciardi Celsi, Lorenzo. "The Dilemma of Rapid AI Advancements: Striking a Balance between Innovation and Regulation by Pursuing Risk-Aware Value Creation." *Information* 14, no. 12 (2023): 645. https://doi.org/10.3390/info14120645.

Söderlund, Kasia, and Stefan Larsson. "Enforcement Design Patterns in EU Law: An Analysis of the AI Act." *Digital Society* 3, no. 41 (2024): 1–21. https://doi.org/10.1007/s44206-024-00129-8.

Solikhah, Mar'atus. "Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber

Law Framework." *Indonesian Cyber Law Review* 2, no. 1 (2025): 39–50. https://doi.org/10.59261/iclr.v2i1.14.

Surat Edaran Menteri Komunikasi Dan Informatika Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial.

Tallberg, Jonas, Eva Erman, Markus Furendal, Johannes Geith, Mark Klamberg, and Magnus Lundgren. "The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research." Pt. 1-23. *International Studies Review* 25, no. 3 (2023). https://doi.org/10.1093/isr/viad040.

Tim detikBali. "Siasat Jahat Mahasiswa Unud Edit Foto Teman Wanita Jadi Foto Asusila Dengan AI." Detik.com, April 26, 2025. https://www.detik.com/bali/hukum-dan-kriminal/d-7886450/siasat-jahat-mahasiswa-unud-edit-foto-teman-wanita-jadi-foto-asusila-dengan-ai.

Topol, Eric J. "High-Performance Medicine: The Convergence Of Human And Artificial Intelligence." *Nature Medicine* 25, no. 1 (2019): 51. https://doi.org/10.1038/s41591-018-0300-7.

Trenggono, Patriot Haryo, and Adang Bachtiar. "Peran Artificial Intelligence dalam Pelayanan Kesehatan : A Systematic Review." *Jurnal Ners* 7, no. 1 (2023): 449. https://doi.org/10.31004/jn.v7i1.13612.

Undang-Undang Dasar 1945.

Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 17 Tahun 2023 Tentang Kesehatan.

Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Voigt, Paul, and Axel Von Dem Bussche. *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-57959-7.

Wibowo, Muhtar Hadi, Ali Masyhar Mursyid, and Anis Widyawati. "Progressionism Restorative Justice Policies in Achieving Rehabilitative Criminal Justice." *IJCLS (Indonesian Journal of Criminal Law Studies)* 9, no. 1 (2024): 118. https://doi.org/10.15294/ijcls.v9i1.50292.

Wildan Mufti, M., M. Hiroshi Ikhsan, Rafif Sani, and M. Fauzan. "Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence." *Socius: Jurnal Penelitian Ilmu-ilmu Sosial* 1, no. 11 (2024): 139. https://doi.org/10.5281/ZENODO.11422903.

Zebua, Rony Sandra Yofa, Khairunnisa, Hartatik, Pariyadi, Dessy Putri Wahyuningtyas, Ahmad M Thantawi, I Gede Iwan Sudipa, et al. *Fenomena Artificial Intelligence (AI)*. Jambi: PT. Sonpedia Publishing Indonesia, 2023.