Legal Frontier
Vol. 2 No. 1, Januray (2026), pp. 7-12

ISSN 3090-1499 (online)
Published by Yayasan Cinta Negara Indonesia

Tinjauan Yuridis terhadap Kejahatan Siber Berbasis Artificial Intelligence dalam Perspektif Hukum Pidana Indonesia

Amalia[1], Marzuki[2], Angga Ari[3]
[1,2,] Fakultas Hukum, Hukum Pidana, Universitas Bina Darma, Palembang, Indonesia.

A R T I C L E I N F O

Article history:

Received: Dec 09, 2025
Revised: Dec 17, 2025
Accepted: Jan 27, 2026

Keywords:

Artificial Intelligence;
Hukum Pidana Indonesia;
Kejahatan Siber;
Tinjauan Yuridis.

ABSTRACT

Perkembangan teknologi kecerdasan buatan Artificial Intelligence dalam era digital telah meningkatkan kompleksitas kejahatan siber di Indonesia yang belum sepenuhnya diakomodasi secara memadai dalam hukum pidana yang berlaku. Tujuan penelitian ini adalah untuk menganalisis bentuk kejahatan siber berbasis Artificial Intelligence serta implikasinya terhadap pertanggungjawaban pidana dalam sistem hukum Indonesia. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan perundang-undangan dan konseptual serta analisis kualitatif terhadap literatur hukum yang relevan. Hasil penelitian menunjukkan bahwa regulasi hukum pidana Indonesia masih menghadapi tantangan dalam mengakomodasi perkembangan kejahatan siber berbasis Artificial Intelligence, terutama terkait pembuktian dan tanggung jawab pelaku. Temuan ini juga mengindikasikan perlunya penguatan kapasitas aparat penegak hukum dalam memahami teknologi AI serta integrasi regulasi lintas sektor untuk menghadapi modus kejahatan yang semakin canggih. Hal ini menjadi urgensi kebijakan. Kesimpulan dari penelitian ini adalah bahwa diperlukan pembaruan regulasi hukum pidana Indonesia yang adaptif terhadap perkembangan Artificial Intelligence guna menjamin kepastian hukum dan efektivitas penegakan hukum.

Corresponding Author:

Amalia,
Fakultas Hukum, Hukum Pidana,
Universitas Bina Darma, Palembang, Indonesia,
Jl. Jenderal A. Yani No. 3, Plaju, Palembang, Sumatera Selatan, Indonesia.
Email: amlialia23@gmail.com

1. INTRODUCTION

Perkembangan teknologi digital dalam dua dekade terakhir telah membawa perubahan signifikan terhadap pola interaksi sosial, ekonomi, dan hukum di masyarakat. Salah satu perkembangan paling menonjol adalah hadirnya Artificial Intelligence (AI) yang kini tidak hanya digunakan dalam sektor industri dan layanan publik, tetapi juga mulai diadopsi dalam berbagai bentuk aktivitas siber, termasuk aktivitas yang bersifat melawan hukum. Kemajuan AI yang mampu melakukan proses analisis data secara otomatis, mempelajari pola perilaku pengguna, hingga menghasilkan konten secara mandiri telah menciptakan dimensi baru dalam kejahatan siber yang semakin kompleks dan sulit dideteksi secara konvensional. Dalam konteks ini, kejahatan siber berbasis Artificial Intelligence menjadi fenomena yang menantang sistem hukum pidana di Indonesia, baik dari segi normatif, teoritis, maupun praktis. Indonesia sebagai negara yang tengah mengalami percepatan transformasi digital menghadapi tantangan serius dalam mengantisipasi perkembangan kejahatan berbasis teknologi canggih tersebut. Regulasi yang saat ini digunakan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), pada dasarnya belum secara spesifik mengatur bentuk kejahatan siber yang sepenuhnya atau sebagian besar dilakukan dengan bantuan AI. Kondisi ini menimbulkan kesenjangan hukum (legal gap) yang berpotensi melemahkan efektivitas penegakan hukum pidana, terutama dalam hal identifikasi pelaku, pembuktian unsur kesalahan, serta penentuan pertanggungjawaban pidana.

Fenomena kejahatan siber berbasis AI mencakup berbagai bentuk, seperti penggunaan algoritma untuk melakukan phishing otomatis, deepfake untuk manipulasi identitas, botnet berbasis

machine learning, hingga serangan siber adaptif yang mampu menghindari sistem keamanan digital. Kejahatan jenis ini tidak lagi hanya dilakukan oleh individu atau kelompok manusia secara langsung, melainkan dapat melibatkan sistem AI yang bekerja secara otonom atau semi-otonom. Hal ini menimbulkan pertanyaan mendasar dalam hukum pidana, yaitu siapa yang harus dimintai pertanggungjawaban ketika suatu tindakan melawan hukum dilakukan oleh sistem berbasis kecerdasan buatan. Dalam perspektif hukum pidana Indonesia yang masih berlandaskan asas kesalahan (schuld) dan pertanggungjawaban individual, keberadaan AI sebagai "alat" maupun "aktor semi-independen" menimbulkan perdebatan yuridis yang cukup kompleks. Hukum pidana konvensional mensyaratkan adanya unsur kesengajaan (dolus) atau kelalaian (culpa) dari subjek hukum manusia. Namun, dalam konteks AI, unsur mental tersebut menjadi sulit diatribusikan secara langsung, terutama ketika sistem AI beroperasi berdasarkan pembelajaran mesin (machine learning) yang memungkinkan sistem berkembang dan mengambil keputusan di luar prediksi awal pembuatnya.

Penelitian ini menjadi penting karena perkembangan teknologi AI tidak hanya meningkatkan efisiensi sistem digital, tetapi juga memperluas ruang potensi kejahatan yang dapat mengancam keamanan data, privasi individu, stabilitas ekonomi digital, hingga keamanan nasional. Oleh karena itu, kajian yuridis terhadap kejahatan siber berbasis AI dalam perspektif hukum pidana Indonesia diperlukan untuk mengidentifikasi sejauh mana hukum yang ada mampu merespons perubahan teknologi tersebut, serta bagaimana arah pembaharuan hukum yang ideal di masa mendatang. Selain itu, urgensi penelitian ini juga terletak pada kebutuhan untuk memberikan kepastian hukum (legal certainty) dalam penanganan kasus-kasus kejahatan siber yang melibatkan teknologi AI. Tanpa adanya kerangka hukum yang jelas, aparat penegak hukum akan mengalami kesulitan dalam menentukan dasar hukum yang tepat, yang pada akhirnya dapat melemahkan proses penegakan hukum itu sendiri. Dalam konteks global, beberapa negara telah mulai mengembangkan pendekatan regulatif yang lebih adaptif terhadap AI, termasuk dalam bidang hukum pidana, sehingga Indonesia perlu melakukan evaluasi dan pembaruan agar tidak tertinggal dalam perkembangan hukum internasional.

Penelitian ini memiliki perbedaan yang signifikan dibandingkan dengan studi-studi sebelumnya yang umumnya hanya berfokus pada kejahatan siber secara umum tanpa mengelaborasi secara spesifik peran Artificial Intelligence di dalamnya. Sebagian besar penelitian terdahulu masih menempatkan AI sebagai bagian dari teknologi pendukung kejahatan, bukan sebagai variabel utama yang mengubah struktur dan karakteristik tindak pidana itu sendiri. Oleh karena itu, penelitian ini menawarkan perspektif yang lebih spesifik dengan menempatkan AI sebagai elemen sentral dalam transformasi modus kejahatan siber serta implikasinya terhadap konstruksi hukum pidana Indonesia. Dari sisi pendekatan, penelitian ini juga menekankan analisis yuridis normatif yang tidak hanya mengkaji peraturan perundang-undangan yang berlaku, tetapi juga mengkaji konsep-konsep hukum pidana modern serta teori pertanggungjawaban pidana dalam menghadapi perkembangan teknologi. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi konseptual dalam pengembangan hukum pidana yang lebih responsif terhadap inovasi teknologi digital, khususnya Artificial Intelligence.

Tujuan utama dari penelitian ini adalah untuk mengkaji bagaimana bentuk kejahatan siber berbasis AI dalam praktiknya, serta menganalisis bagaimana hukum pidana Indonesia saat ini merespons fenomena tersebut. Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi tantangan yuridis yang dihadapi dalam proses penegakan hukum serta menawarkan arah pembaruan hukum yang lebih adaptif terhadap perkembangan teknologi AI. Dengan demikian, penelitian ini tidak hanya bersifat deskriptif, tetapi juga memberikan kontribusi normatif dan preskriptif terhadap pengembangan hukum pidana di Indonesia. Kontribusi penelitian ini diharapkan dapat memperkaya literatur hukum pidana, khususnya dalam bidang cyber law dan teknologi digital. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi bagi pembuat kebijakan dalam merumuskan regulasi yang lebih komprehensif terkait penggunaan dan penyalahgunaan Artificial Intelligence dalam ruang siber. Lebih jauh lagi, penelitian ini dapat menjadi dasar akademik bagi pengembangan konsep pertanggungjawaban pidana yang lebih modern, termasuk kemungkinan pengaturan mengenai liability berbasis sistem atau hybrid liability antara manusia dan teknologi. Dengan demikian, dapat disimpulkan bahwa penelitian mengenai tinjauan yuridis terhadap kejahatan siber berbasis Artificial Intelligence dalam perspektif hukum pidana Indonesia memiliki urgensi yang tinggi baik secara teoritis maupun praktis. Perkembangan teknologi yang sangat cepat menuntut adanya respons hukum yang tidak hanya reaktif, tetapi juga antisipatif dan adaptif. Oleh karena itu, kajian ini menjadi penting untuk memastikan

bahwa sistem hukum pidana Indonesia tetap relevan dalam menghadapi tantangan era digital yang semakin kompleks dan dinamis.

2. RESEARCH METHOD

Penelitian ini menggunakan metode yuridis normatif sebagaimana direkomendasikan oleh Soerjono Soekanto dan Peter Mahmud Marzuki dalam kajian hukum doktrinal, dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Data yang digunakan adalah data sekunder yang diperoleh dari bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa literatur, jurnal ilmiah, serta bahan hukum tersier seperti kamus hukum dan ensiklopedia hukum. Data dikumpulkan melalui studi kepustakaan (library research), kemudian diinventarisasi, diklasifikasi, dan dianalisis secara kualitatif dengan teknik deskriptif-analitis. Prosedur penelitian dilakukan secara kronologis mulai dari identifikasi masalah, pengumpulan bahan hukum, analisis norma, hingga penarikan kesimpulan. Hasil penelitian diukur berdasarkan kesesuaian norma hukum yang berlaku dengan fenomena kejahatan siber berbasis AI, serta dievaluasi melalui analisis konsistensi, koherensi, dan relevansi terhadap asas-asas hukum pidana Indonesia.

3. RESULTS AND DISCUSSIONS

3.1. Bentuk Kejahatan Siber Berbasis Artificial Intelligence dalam Praktik Hukum Pidana.

Hasil penelitian menunjukkan bahwa kejahatan siber berbasis Artificial Intelligence (AI) dalam praktiknya berkembang dalam beberapa bentuk utama, yaitu penggunaan deepfake untuk manipulasi identitas, automated phishing berbasis machine learning, serta serangan siber adaptif yang mampu menyesuaikan pola serangan secara real time. Fenomena ini menunjukkan bahwa AI tidak hanya berfungsi sebagai alat bantu, tetapi juga sebagai sistem yang dapat mempercepat, memperluas, dan meningkatkan kompleksitas tindak pidana siber. Dalam konteks hukum pidana Indonesia, bentuk kejahatan ini belum memiliki pengaturan khusus yang secara eksplisit mengakomodasi karakteristik AI. Regulasi yang ada masih bersifat umum dan berfokus pada perbuatan manusia sebagai pelaku utama. Akibatnya, terdapat kesenjangan antara perkembangan teknologi dan kemampuan hukum dalam mengidentifikasi modus operandi kejahatan modern. Pembahasan menunjukkan bahwa karakteristik utama kejahatan berbasis AI adalah otomatisasi, anonimitas tinggi, serta kemampuan adaptif yang menyulitkan pelacakan pelaku. Jika dibandingkan dengan penelitian sebelumnya yang hanya membahas cybercrime konvensional, penelitian ini menegaskan bahwa AI menciptakan bentuk baru kejahatan yang lebih otonom dan tidak sepenuhnya bergantung pada intervensi manusia secara langsung.

3.2. Pertanggungjawaban Pidana terhadap Pelaku Kejahatan Siber Berbasis AI.

Hasil penelitian menunjukkan bahwa pertanggungjawaban pidana dalam kasus kejahatan siber berbasis AI menjadi persoalan yang kompleks dalam hukum pidana Indonesia. Prinsip dasar hukum pidana yang mengharuskan adanya kesalahan (mens rea) dari subjek hukum manusia sulit diterapkan ketika AI berperan sebagai sistem yang mengambil keputusan secara mandiri atau semi-mandiri. Dalam praktiknya, tanggung jawab hukum masih dibebankan kepada pengembang, operator, atau pengguna sistem AI. Namun, pembagian tanggung jawab ini tidak selalu jelas, terutama ketika AI telah mengalami pembelajaran mandiri yang menghasilkan tindakan di luar kendali awal pembuatnya. Analisis menunjukkan adanya kekosongan konsep hukum mengenai "liability berbasis sistem" yang dapat menjembatani antara tanggung jawab manusia dan otonomi teknologi. Dibandingkan dengan penelitian lain, studi ini menegaskan bahwa pendekatan hukum pidana Indonesia masih sangat antropocentric, sehingga belum mampu mengakomodasi entitas non-manusia secara langsung dalam kerangka pertanggungjawaban pidana.

3.3. Efektivitas Regulasi Hukum Pidana Indonesia dalam Menghadapi Kejahatan AI.

Hasil penelitian menunjukkan bahwa regulasi hukum pidana Indonesia, khususnya yang mengatur tindak pidana siber, belum sepenuhnya efektif dalam menghadapi perkembangan kejahatan berbasis AI. Ketentuan yang ada masih bersifat general dan belum mengatur secara spesifik penggunaan teknologi kecerdasan buatan dalam tindak pidana. Tabel analisis menunjukkan bahwa terdapat tiga kelemahan utama: pertama, tidak adanya definisi hukum yang jelas mengenai AI dalam konteks pidana;

kedua, keterbatasan instrumen pembuktian digital untuk mengidentifikasi keterlibatan AI; dan ketiga, belum adanya mekanisme pertanggungjawaban yang adaptif terhadap sistem otonom. Pembahasan menunjukkan bahwa kondisi ini menyebabkan aparat penegak hukum mengalami kesulitan dalam proses penyelidikan dan pembuktian. Jika dibandingkan dengan penelitian lain, studi ini memperluas perspektif dengan menekankan bahwa kelemahan regulasi tidak hanya terletak pada substansi hukum, tetapi juga pada aspek teknis pembuktian dan kapasitas kelembagaan.

Discussions

Hasil penelitian menunjukkan bahwa kejahatan siber berbasis Artificial Intelligence (AI) merupakan bentuk evolusi baru dari cybercrime yang memiliki karakteristik berbeda secara signifikan dibandingkan kejahatan siber konvensional. Pembahasan ini menegaskan bahwa transformasi teknologi telah menggeser pola kejahatan dari yang bersifat manual menjadi otomatis, adaptif, dan berbasis sistem cerdas. Kondisi ini menimbulkan implikasi serius terhadap struktur hukum pidana Indonesia yang masih berorientasi pada pelaku manusia sebagai subjek utama pertanggungjawaban pidana. Secara normatif, hukum pidana Indonesia masih menggunakan pendekatan tradisional yang mensyaratkan adanya kesalahan (mens rea) dan perbuatan (actus reus) yang dilakukan oleh manusia. Namun, dalam konteks AI, kedua unsur tersebut menjadi problematik karena sistem AI dapat melakukan tindakan secara otonom berdasarkan algoritma pembelajaran mesin. Hal ini menciptakan ruang abu-abu dalam penentuan tanggung jawab hukum, khususnya ketika suatu tindak pidana tidak dapat secara langsung diatribusikan kepada satu individu tertentu.

Dari hasil analisis, terlihat bahwa terdapat tiga persoalan utama dalam penanganan kejahatan siber berbasis AI, yaitu: (1) kesulitan identifikasi pelaku, (2) kompleksitas pembuktian digital, dan (3) ketidakjelasan atribusi kesalahan. Ketiga aspek ini menunjukkan bahwa hukum pidana Indonesia belum sepenuhnya siap menghadapi dinamika teknologi AI yang berkembang sangat cepat. Jika dibandingkan dengan penelitian lain, sebagian besar kajian sebelumnya masih menempatkan AI sebagai alat bantu dalam kejahatan siber, bukan sebagai elemen yang mengubah struktur tindak pidana secara fundamental. Penelitian ini memperluas perspektif tersebut dengan menegaskan bahwa AI dapat berperan sebagai sistem yang mempengaruhi bahkan menginisiasi tindakan kriminal tanpa intervensi langsung manusia. Dengan demikian, terdapat pergeseran paradigma dari human-centered liability menuju system-influenced liability.

Selain itu, penelitian ini juga menemukan bahwa pendekatan regulatif Indonesia masih bersifat reaktif, yaitu baru merespons setelah kejahatan terjadi, bukan bersifat antisipatif. Hal ini berbeda dengan beberapa pendekatan hukum di negara lain yang mulai mengembangkan konsep regulatory sandbox dan risk-based regulation untuk mengantisipasi perkembangan AI dalam ruang siber. Ketertinggalan ini menunjukkan adanya kebutuhan mendesak untuk reformasi hukum pidana yang lebih adaptif terhadap teknologi baru. Dari sisi teoritis, hasil penelitian ini memperkuat konsep bahwa hukum pidana modern perlu mengembangkan pendekatan hybrid liability, yaitu pembagian tanggung jawab antara pengembang sistem, pengguna, dan sistem AI itu sendiri dalam batas tertentu. Meskipun AI belum dapat diposisikan sebagai subjek hukum pidana, keberadaannya tetap memiliki pengaruh signifikan dalam proses terjadinya tindak pidana.

Namun demikian, penelitian ini memiliki beberapa batasan. Pertama, kajian ini masih bersifat normatif sehingga belum menguji secara empiris implementasi hukum di lapangan. Kedua, keterbatasan data terkait kasus kejahatan AI di Indonesia membuat analisis lebih banyak bersifat konseptual. Ketiga, penelitian ini belum membahas secara mendalam aspek teknis rekayasa AI yang dapat mempengaruhi proses hukum, sehingga analisis lebih difokuskan pada aspek yuridis. Secara keseluruhan, pembahasan ini menunjukkan bahwa kejahatan siber berbasis AI merupakan tantangan baru bagi sistem hukum pidana Indonesia yang memerlukan pembaruan mendasar, baik dari segi regulasi, konsep pertanggungjawaban pidana, maupun kapasitas kelembagaan penegak hukum. Pendekatan hukum yang lebih adaptif, progresif, dan berbasis risiko menjadi kebutuhan mendesak untuk memastikan hukum tetap relevan dalam menghadapi perkembangan teknologi yang semakin kompleks.

4. CONCLUSION

Penelitian ini menyimpulkan bahwa kejahatan siber berbasis Artificial Intelligence (AI) merupakan bentuk evolusi baru dari tindak pidana siber yang memiliki karakteristik otomatisasi, adaptabilitas, dan anonimitas tinggi, sehingga menimbulkan tantangan serius bagi hukum pidana Indonesia. Temuan utama menunjukkan bahwa hukum pidana Indonesia saat ini belum memiliki pengaturan yang secara spesifik mengakomodasi peran AI dalam tindak kejahatan, sehingga terjadi kesenjangan hukum dalam hal identifikasi pelaku, pembuktian unsur kesalahan, serta penentuan pertanggungjawaban pidana. Dalam praktiknya, tanggung jawab masih dibebankan kepada manusia sebagai pengembang atau

pengguna sistem, meskipun AI dapat beroperasi secara semi-otonom dan menghasilkan keputusan yang tidak sepenuhnya dapat diprediksi. Penelitian ini memberikan kontribusi akademik berupa penguatan kajian yuridis mengenai urgensi pembaruan konsep pertanggungjawaban pidana dalam menghadapi teknologi AI, serta menawarkan perspektif hybrid liability sebagai pendekatan alternatif dalam perkembangan hukum pidana modern. Implikasi penelitian menunjukkan bahwa diperlukan reformasi regulasi yang tidak hanya bersifat reaktif, tetapi juga antisipatif terhadap perkembangan teknologi, termasuk penguatan kapasitas aparat penegak hukum dan integrasi pendekatan teknologi dalam sistem pembuktian pidana. Selain itu, penelitian ini menegaskan bahwa tanpa adanya pembaruan hukum yang adaptif, efektivitas penegakan hukum dalam kasus kejahatan siber berbasis AI akan terus mengalami hambatan, terutama dalam menentukan atribusi kesalahan dan pertanggungjawaban hukum. Adapun batasan penelitian ini terletak pada sifatnya yang normatif, keterbatasan data empiris terkait kasus AI di Indonesia, serta belum dilakukannya analisis teknis mendalam mengenai sistem kecerdasan buatan itu sendiri. Oleh karena itu, penelitian di masa depan disarankan untuk menggabungkan pendekatan normatif dan empiris, serta melibatkan kajian interdisipliner antara hukum, teknologi informasi, dan etika AI guna menghasilkan kerangka hukum yang lebih komprehensif. Secara eksplisit, penelitian ini menjawab pertanyaan utama bahwa hukum pidana Indonesia saat ini belum sepenuhnya mampu mengakomodasi kompleksitas kejahatan siber berbasis AI, sehingga diperlukan pembaruan konseptual dan regulatif agar sistem hukum tetap relevan dalam menghadapi dinamika transformasi digital yang semakin cepat dan kompleks.

REFERENCES

Amalia, D. S., & Khotimah, S. H. (2025). Rekonstruksi pertanggungjawaban hukum atas kejahatan siber berbasis Artificial Intelligence dalam perspektif hukum pidana Indonesia. Fenomena: Jurnal Hukum.

Ariwibowo, T., dkk. (2025). Analisis hukum pidana terhadap penyebaran deepfake berbasis Artificial Intelligence di Indonesia. Yustisi.

BSSN. (2023). Laporan keamanan siber Indonesia 2023. Badan Siber dan Sandi Negara.

Damiani, E., Zhang, Z., & Yeun, C. Y. (2022). Explainable artificial intelligence applications in cyber security. arXiv preprint.

Dilek, S., Çakır, H., & Aydın, M. (2022). Applications of artificial intelligence techniques to combating cyber crimes. arXiv preprint.

Gupta, M., et al. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. arXiv preprint.

Hibatulloh, B. H. (2025). Upaya penegakan hukum terhadap AI sebagai subjek hukum pidana. Taruna Law Journal.

Indonesia Cyber Law Center. (2024). Artificial intelligence and cybercrime regulation in Indonesia.

Junaidi, A., & Reniwuryaan, H. (2025). Rekonstruksi kebijakan hukum pidana terhadap AI di media sosial. Jurnal Hukum.

Karnalim, O., et al. (2023). Plagiarism and AI assistance misuse in web programming. arXiv preprint.

Kurniawan, E. I., & Zaen, V. A. (2025). Pertanggungjawaban pidana terhadap penyalahgunaan AI dalam deepfake. ALADALAH Journal.

Marzuki, P. M. (2022). Penelitian hukum. Jakarta: Kencana.

Nawawi, W. (2025). Kedudukan hukum Artificial Intelligence dalam sistem hukum Indonesia. Al-Zayn Journal.

Novrianto, M. (2025). Kebijakan hukum pidana terhadap cyber crime berbasis AI di Indonesia. Jurnal Kepastian Hukum.

Nur Haida, R. S., & Nuriyatman, E. (2024). Urgensi pengaturan deepfake berbasis AI dalam hukum pidana Indonesia. Respublica Journal.

Rahardjo, S. (2022). Ilmu hukum. Bandung: Citra Aditya Bakti.

Situmeang, S. M. T. (2024). Legal adequacy of Indonesian cybercriminal law against AI-based attacks. Res Nullius Law Journal.

Soekanto, S. (2022). Pengantar penelitian hukum. Jakarta: UI Press.

Sudaryono, & Surbakti, N. (2023). Hukum pidana dasar. Surakarta: Muhammadiyah University Press.

UNODC. (2023). Cybercrime and emerging technologies report. United Nations Office on Drugs and Crime.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang KUHP.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

United Nations. (2024). AI governance and legal frameworks report.

Widodo, A. (2023). Artificial intelligence in cybercrime: Legal challenges in Indonesia.
Wibowo, S. (2022). Pancasila and legal philosophy in digital era.
Yustisi Editorial Board. (2025). AI-based deepfake criminal liability in Indonesia. Yustisi Journal.
Zhang, Z., et al. (2022). Explainable AI for cybersecurity systems. arXiv preprint.
Zuboff, S. (2022). The age of surveillance capitalism (updated edition).
Budi, S. (2024). Cyber law and artificial intelligence governance in Indonesia.
Chairunnisa, R. (2023). Digital evidence in AI-based cybercrime.
Fadli, M. (2024). Legal reconstruction of AI liability in Indonesia.
Hakim, L. (2023). Machine learning and cybercrime evolution.
Indrawan, T. (2022). Digital transformation and criminal law challenges.