Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 3, 2026
DOI: https://doi.org/10.61104/alz.v4i3.6734

Eksploitasi Teknologi AI dalam Tindak Pidana Siber

(Perspektif Criminal Law Modern)

Yusep Mulyana
Universitas Pasundan, Indonesia
Email Korespondensi: yusep.mulyana@unpas.ac.id

Article received: 02 Mei 2026, Review process: 08 Mei 2026
Article Accepted: 22 Mei 2026, Article published: 01 Juni 2026

ABSTRACT

The rapid development of Artificial Intelligence (AI) has significantly transformed patterns of cybercrime in the modern digital era. AI is no longer merely used as a technological support system but has also been exploited as a tool for committing cybercrimes such as deepfake manipulation, AI-based phishing, intelligent malware distribution, and automated cyber attacks. This study aims to analyze the exploitation of AI technology in cybercrime and examine it from the perspective of modern criminal law. The research employs a normative legal research method using statutory, conceptual, and case approaches. Data were collected through library research by examining legal regulations, scientific journals, books, and relevant legal documents related to cybercrime and artificial intelligence. The findings indicate that AI-based cybercrime creates complex legal challenges, particularly regarding criminal liability, digital evidence, and legal enforcement mechanisms. Existing regulations in Indonesia, especially the Electronic Information and Transactions Law, have not specifically regulated the misuse of AI in cybercrime, resulting in legal gaps in addressing emerging digital threats. Furthermore, AI technology challenges conventional criminal law concepts, especially concerning mens rea and the determination of legal responsibility. Therefore, this study emphasizes the urgency of legal reform, strengthening digital forensic capabilities, and developing adaptive cyber law policies to address the evolution of AI-based cybercrime in the modern era.

Keywords: *Artificial intelligence, cyber crime, criminal law, digital forensics, cyber law*

ABSTRAK

Perkembangan Artificial Intelligence (AI) yang semakin pesat telah membawa perubahan signifikan terhadap pola tindak pidana siber di era digital modern. AI tidak lagi hanya digunakan sebagai sistem pendukung teknologi, tetapi juga telah dieksploitasi sebagai instrumen dalam berbagai bentuk kejahatan siber seperti manipulasi deepfake, phishing berbasis AI, penyebaran malware cerdas, dan otomatisasi serangan siber. Penelitian ini bertujuan untuk menganalisis eksploitasi teknologi AI dalam tindak pidana siber serta mengkajinya dalam perspektif hukum pidana modern. Penelitian menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan pendekatan kasus. Data diperoleh melalui studi kepustakaan dengan menelaah peraturan perundang-undangan, jurnal ilmiah, buku, dan dokumen hukum yang relevan terkait cyber crime dan artificial intelligence. Hasil penelitian menunjukkan bahwa kejahatan siber berbasis AI menimbulkan tantangan hukum yang kompleks, terutama terkait pertanggungjawaban pidana, pembuktian digital, dan mekanisme penegakan hukum. Regulasi yang ada di Indonesia, khususnya UU ITE, belum secara spesifik mengatur penyalahgunaan AI dalam tindak pidana siber sehingga menimbulkan kekosongan hukum

dalam menghadapi ancaman digital modern. Selain itu, teknologi AI juga menantang konsep hukum pidana konvensional, khususnya terkait unsur kesalahan dan penentuan subjek hukum yang bertanggung jawab. Oleh karena itu, diperlukan reformasi hukum, penguatan digital forensic, dan pengembangan kebijakan cyber law yang adaptif untuk menghadapi perkembangan kejahatan siber berbasis AI di era modern.
Kata Kunci: *Artificial Intelligence, Tindak Pidana Siber, Hukum Pidana, Digital Forensik, Cyber Law.*

PENDAHULUAN

Perkembangan teknologi digital dalam beberapa dekade terakhir telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, mulai dari sektor ekonomi, pendidikan, kesehatan, hingga sistem penegakan hukum. Salah satu perkembangan teknologi yang paling signifikan saat ini adalah Artificial Intelligence (AI) atau kecerdasan buatan (Apriadi et al., 2025). Teknologi AI memungkinkan sistem komputer untuk meniru kemampuan kognitif manusia, seperti menganalisis data, mengenali pola, membuat keputusan, hingga menghasilkan konten secara otomatis. Kehadiran AI memberikan berbagai manfaat positif bagi masyarakat modern, terutama dalam meningkatkan efisiensi kerja, mempercepat pengolahan informasi, dan mendukung inovasi di berbagai bidang. Namun, di sisi lain, perkembangan AI juga menghadirkan tantangan baru dalam dunia hukum, khususnya terkait munculnya berbagai bentuk tindak pidana siber yang semakin kompleks dan sulit dideteksi (Wahidi & Zulfa, 2026).

Transformasi digital yang semakin masif telah menciptakan ruang baru bagi pelaku kejahatan untuk melakukan tindakan melawan hukum dengan memanfaatkan teknologi canggih. Jika sebelumnya tindak pidana siber hanya berkaitan dengan peretasan sistem, pencurian data, atau penyebaran malware secara konvensional, maka saat ini AI telah digunakan sebagai instrumen utama dalam melakukan kejahatan digital yang lebih terstruktur dan sistematis (Hutaruk & Sinambela, 2026). Teknologi AI dapat dimanfaatkan untuk membuat deepfake, serangan phishing otomatis, manipulasi identitas digital, penipuan berbasis chatbot, rekayasa sosial berbasis machine learning, hingga otomatisasi serangan siber dalam skala besar. Kondisi ini menunjukkan bahwa AI tidak lagi hanya menjadi alat bantu teknologi, tetapi telah berkembang menjadi medium potensial dalam pelaksanaan cyber crime modern (Guntara et al., 2026).

Fenomena eksploitasi AI dalam tindak pidana siber menjadi perhatian global karena dampaknya yang sangat luas terhadap keamanan data, privasi individu, stabilitas ekonomi, dan keamanan nasional (Aditya & Yudiantara, 2025). Penggunaan AI oleh pelaku kejahatan menyebabkan metode kejahatan menjadi lebih sulit dilacak karena sistem AI mampu bekerja secara otomatis, adaptif, dan anonim. Bahkan, AI dapat digunakan untuk mempelajari kelemahan sistem keamanan digital secara mandiri melalui teknik machine learning. Dalam konteks ini, kejahatan siber mengalami evolusi dari bentuk konvensional menuju intelligent cyber crime yang memiliki tingkat kompleksitas lebih tinggi dibandingkan kejahatan digital sebelumnya (Setiawan, 2024).

Di berbagai negara, peningkatan penyalahgunaan AI dalam kejahatan siber telah memunculkan kekhawatiran mengenai kesiapan sistem hukum pidana dalam menghadapi perkembangan teknologi tersebut. Sistem hukum pidana modern pada dasarnya dibangun berdasarkan konsep pertanggungjawaban manusia sebagai subjek hukum utama. Akan tetapi, penggunaan AI dalam tindak pidana menimbulkan persoalan baru mengenai bentuk pertanggungjawaban pidana, pembuktian unsur kesalahan, serta identifikasi pelaku kejahatan (Budiyanto, 2025). Dalam beberapa kasus, AI berfungsi hanya sebagai alat bantu, tetapi dalam kondisi tertentu AI dapat bertindak secara semi-otonom sehingga mempersulit penentuan pihak yang harus bertanggung jawab secara hukum. Situasi ini menunjukkan adanya kebutuhan untuk melakukan rekonstruksi konsep hukum pidana agar mampu mengakomodasi perkembangan teknologi digital modern (Berlian, 2025).

Di Indonesia, pengaturan mengenai tindak pidana siber saat ini masih berfokus pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) beserta peraturan terkait lainnya. Meskipun regulasi tersebut telah mengatur berbagai bentuk kejahatan digital, namun pengaturan spesifik mengenai eksploitasi AI dalam tindak pidana siber masih relatif terbatas (Aprilianti, 2024) . Perkembangan AI yang sangat cepat menyebabkan hukum sering kali tertinggal dibandingkan realitas teknologi yang berkembang di masyarakat. Akibatnya, muncul kekosongan norma (legal vacuum) terkait batasan penggunaan AI, bentuk pertanggungjawaban hukum, serta mekanisme penegakan hukum terhadap kejahatan berbasis AI. Selain itu, aparat penegak hukum juga menghadapi tantangan teknis dalam proses investigasi dan pembuktian digital karena AI mampu memanipulasi data secara sangat realistis (Setiawan & Arista, 2013).

Dalam perspektif criminal law modern, hukum pidana tidak hanya berfungsi sebagai instrumen represif untuk menghukum pelaku kejahatan, tetapi juga sebagai sarana preventif dalam menjaga ketertiban sosial dan melindungi kepentingan masyarakat. Oleh karena itu, pendekatan hukum pidana modern harus mampu beradaptasi dengan perkembangan teknologi digital, termasuk dalam menghadapi ancaman AI-based cyber crime (M. Yusuf et al., 2025). Pendekatan ini menuntut adanya pembaruan regulasi, penguatan digital forensic, pengembangan cyber law, serta harmonisasi antara hukum nasional dan perkembangan hukum internasional terkait penggunaan AI. Selain itu, konsep pertanggungjawaban pidana modern perlu dikaji ulang untuk menentukan batas tanggung jawab antara pengguna, pengembang, operator, maupun sistem AI itu sendiri dalam suatu tindak pidana siber (Cahyono et al., 2025).

Penelitian terdahulu umumnya lebih banyak membahas AI dari perspektif teknologi, etika, dan keamanan siber secara umum. Beberapa penelitian juga menyoroti peran AI dalam membantu sistem penegakan hukum dan deteksi kejahatan digital. Namun, kajian yang secara khusus membahas eksploitasi teknologi AI sebagai instrumen tindak pidana siber dalam perspektif criminal law modern masih relatif terbatas, terutama dalam konteks sistem hukum di Indonesia. Sebagian besar penelitian sebelumnya belum secara mendalam mengkaji hubungan antara perkembangan AI, problematika pertanggungjawaban pidana, dan kebutuhan reformulasi hukum pidana modern terhadap cyber crime berbasis AI.

Kondisi tersebut menunjukkan adanya research gap yang penting untuk diteliti lebih lanjut.

Berdasarkan research gap tersebut, novelty penelitian ini terletak pada analisis integratif mengenai eksploitasi teknologi AI dalam tindak pidana siber dengan menggunakan pendekatan criminal law modern yang menitikberatkan pada aspek pertanggungjawaban pidana, reformulasi regulasi, dan adaptasi sistem hukum terhadap perkembangan artificial intelligence. Penelitian ini tidak hanya membahas AI sebagai teknologi, tetapi juga mengkaji AI sebagai instrumen kejahatan yang berpotensi mengubah paradigma hukum pidana konvensional. Dengan demikian, penelitian ini diharapkan mampu memberikan kontribusi akademik dalam pengembangan hukum pidana modern sekaligus menjadi referensi bagi pembentukan kebijakan hukum terkait pengaturan AI dan cyber crime di Indonesia.

Penelitian ini bertujuan untuk menganalisis bentuk eksploitasi teknologi AI dalam tindak pidana siber, mengidentifikasi tantangan pertanggungjawaban pidana dalam kejahatan berbasis AI, serta mengkaji relevansi perspektif criminal law modern dalam merumuskan sistem hukum yang adaptif terhadap perkembangan teknologi digital. Dengan adanya penelitian ini, diharapkan dapat tercipta pemahaman yang lebih komprehensif mengenai urgensi reformasi hukum pidana dalam menghadapi ancaman kejahatan siber berbasis artificial intelligence di era digital modern.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan kasus (case approach). Pendekatan perundang-undangan digunakan untuk menelaah berbagai regulasi terkait tindak pidana siber dan pemanfaatan Artificial Intelligence (AI), seperti KUHP, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta regulasi terkait perlindungan data dan keamanan siber. Pendekatan konseptual digunakan untuk mengkaji teori hukum pidana modern, cyber crime, dan pertanggungjawaban pidana dalam penggunaan AI. Sementara itu, pendekatan kasus dilakukan dengan menganalisis fenomena penyalahgunaan AI dalam kejahatan siber, seperti deepfake, phishing berbasis AI, dan manipulasi identitas digital.

Jenis data yang digunakan adalah data sekunder yang terdiri atas bahan hukum primer, sekunder, dan tersier. Data diperoleh melalui studi kepustakaan dengan menelaah peraturan perundang-undangan, jurnal ilmiah, buku, dan dokumen hukum yang relevan dengan penelitian. Selanjutnya, data dianalisis secara kualitatif menggunakan metode deskriptif-analitis untuk memahami bentuk eksploitasi AI dalam tindak pidana siber serta relevansi criminal law modern dalam menghadapi perkembangan kejahatan digital berbasis teknologi artificial intelligence.

HASIL DAN PEMBAHASA

Hasil Penelitian

Hasil penelitian menunjukkan bahwa perkembangan Artificial Intelligence (AI) telah membawa perubahan signifikan terhadap pola tindak pidana siber modern. Berdasarkan studi kepustakaan, analisis regulasi, dan kajian berbagai kasus cyber crime berbasis AI, ditemukan bahwa teknologi AI tidak hanya dimanfaatkan untuk kepentingan produktivitas digital, tetapi juga telah dieksploitasi sebagai instrumen dalam berbagai bentuk kejahatan siber. Bentuk eksploitasi tersebut meliputi penggunaan deepfake untuk penipuan identitas, phishing otomatis berbasis AI, manipulasi data digital, penyebaran malware cerdas, hingga otomatisasi serangan siber menggunakan machine learning (Novrianto, 2025).

Temuan penelitian memperlihatkan bahwa pelaku kejahatan siber memanfaatkan kemampuan AI untuk meningkatkan efektivitas, kecepatan, dan tingkat keberhasilan serangan digital. AI memungkinkan pelaku melakukan analisis terhadap kelemahan sistem keamanan secara otomatis sehingga serangan menjadi lebih adaptif dan sulit dideteksi. Selain itu, penggunaan AI juga menyebabkan peningkatan kualitas manipulasi digital, terutama dalam pembuatan konten palsu yang menyerupai identitas asli seseorang.

Tabel 1. Bentuk Eksploitasi AI dalam Tindak Pidana Siber

No	Bentuk Eksploitasi AI	Dampak yang Ditimbulkan
1	Deepfake dan manipulasi visual	Penipuan identitas dan penyebaran hoaks
2	Phishing berbasis AI	Pencurian data pribadi dan finansial
3	Malware berbasis machine learning	Kerusakan sistem dan pencurian data
4	Bot otomatis untuk cyber attack	Serangan siber massal dan sistematis
5	AI-generated scam content	Penipuan digital yang sulit dideteksi

Berdasarkan tabel tersebut, eksploitasi AI dalam cyber crime menunjukkan pola kejahatan yang semakin kompleks dibandingkan tindak pidana siber konvensional. Kejahatan berbasis AI memiliki karakteristik otomatis, adaptif, dan mampu berkembang sesuai respons sistem keamanan digital yang dihadapinya.

Selain itu, hasil penelitian juga menunjukkan bahwa regulasi hukum di Indonesia masih menghadapi berbagai keterbatasan dalam mengantisipasi perkembangan AI-based cyber crime. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memang telah mengatur beberapa bentuk tindak pidana digital, namun belum secara spesifik mengatur mengenai penggunaan AI sebagai instrumen kejahatan siber. Kekosongan norma tersebut menyebabkan munculnya tantangan

dalam menentukan bentuk pertanggungjawaban pidana terhadap pelaku yang memanfaatkan AI dalam melakukan tindak pidana.

Tabel 2. Tantangan Penegakan Hukum terhadap AI-Based Cyber Crime

No	Tantangan	Penjelasan
1	Identifikasi pelaku	AI memungkinkan anonimitas dan penyamaran identitas
2	Pembuktian digital	Manipulasi data sulit diverifikasi keasliannya
3	Kekosongan regulasi	Belum adanya aturan spesifik mengenai AI
4	Keterbatasan forensik digital	Aparat belum sepenuhnya siap menghadapi AI crime
5	Kompleksitas pertanggungjawaban pidana	Sulit menentukan subjek hukum yang bertanggung jawab

Temuan lainnya menunjukkan bahwa perkembangan AI menyebabkan konsep hukum pidana konvensional menghadapi tantangan serius, terutama terkait unsur kesalahan (mens rea) dan pertanggungjawaban pidana. Dalam beberapa kasus, AI mampu bekerja secara semi-otonom sehingga menimbulkan pertanyaan mengenai batas tanggung jawab antara pengguna, pengembang sistem, dan operator teknologi AI tersebut.

Pembahasan

Eksploitasi Artificial Intelligence dalam Cyber Crime Modern

Perkembangan teknologi AI telah mengubah pola cyber crime dari kejahatan digital sederhana menjadi kejahatan siber yang lebih terorganisasi dan berbasis otomatisasi. Dalam perspektif criminal law modern, perubahan ini menunjukkan bahwa perkembangan teknologi tidak hanya menghasilkan inovasi positif, tetapi juga menciptakan ruang baru bagi pelaku kejahatan untuk melakukan tindakan melawan hukum dengan metode yang lebih canggih (Sihombing & Hermanto, 2026).

Salah satu bentuk eksploitasi AI yang paling banyak ditemukan adalah penggunaan deepfake technology. Teknologi ini memungkinkan pelaku memanipulasi gambar, suara, maupun video sehingga tampak menyerupai individu asli. Dalam praktiknya, deepfake digunakan untuk penipuan finansial, pemerasan digital, penyebaran informasi palsu, hingga pencemaran nama baik. Tingginya tingkat kemiripan hasil manipulasi AI menyebabkan masyarakat sulit membedakan antara konten asli dan konten palsu (Novera, 2024).

Selain deepfake, AI juga dimanfaatkan dalam phishing attack berbasis machine learning. Berbeda dengan phishing konvensional, phishing berbasis AI mampu mempelajari pola komunikasi korban sehingga pesan penipuan terlihat

lebih personal dan meyakinkan. Hal ini meningkatkan kemungkinan korban memberikan data pribadi maupun informasi keuangan kepada pelaku (yanti et al., 2025).

Pemanfaatan AI dalam malware development juga menjadi ancaman serius terhadap keamanan siber modern. Malware berbasis AI memiliki kemampuan adaptif untuk menghindari deteksi sistem keamanan digital. Bahkan, beberapa jenis malware dapat memodifikasi pola serangannya secara otomatis berdasarkan respons sistem target. Kondisi ini menunjukkan bahwa AI telah meningkatkan eskalasi ancaman cyber crime secara signifikan (Santoso et al., 2025).

Perspektif Criminal Law Modern terhadap AI-Based Cyber Crime

Dalam perspektif hukum pidana modern, perkembangan AI-based cyber crime memunculkan kebutuhan akan reformasi hukum yang lebih adaptif terhadap perkembangan teknologi digital. Sistem hukum pidana tradisional pada dasarnya dirancang dengan asumsi bahwa pelaku tindak pidana adalah manusia yang memiliki niat, kesadaran, dan kontrol penuh terhadap perbuatannya. Namun, penggunaan AI dalam tindak pidana menimbulkan kompleksitas baru karena AI dapat bekerja secara otomatis maupun semi-otonom (Ibrahim & Atmanja, 2025).

Konsep mens rea atau unsur kesalahan menjadi salah satu aspek yang paling problematis dalam tindak pidana berbasis AI. Dalam hukum pidana konvensional, pertanggungjawaban pidana didasarkan pada adanya niat jahat atau kesengajaan pelaku. Akan tetapi, ketika AI melakukan tindakan tertentu secara otomatis berdasarkan algoritma machine learning, maka muncul pertanyaan mengenai siapa yang sebenarnya memiliki niat jahat tersebut (Perian et al., 2025).

Permasalahan lain berkaitan dengan penentuan subjek hukum yang bertanggung jawab. Dalam praktiknya, terdapat beberapa pihak yang terlibat dalam penggunaan AI, seperti pengembang sistem, operator, pengguna, maupun pemilik platform digital. Kompleksitas hubungan tersebut menyebabkan penegakan hukum terhadap AI-based cyber crime menjadi lebih sulit dibandingkan tindak pidana konvensional (Nawawi, 2026).

Criminal law modern memandang bahwa hukum pidana harus mampu beradaptasi dengan perkembangan teknologi melalui pembaruan regulasi dan penguatan mekanisme penegakan hukum digital. Reformasi hukum diperlukan agar sistem hukum tidak tertinggal dibandingkan perkembangan teknologi AI yang sangat cepat (Dermawan, 2026).

Urgensi Reformasi Regulasi dan Penguatan Penegakan Hukum

Hasil penelitian menunjukkan bahwa regulasi hukum di Indonesia masih memiliki keterbatasan dalam mengatur eksploitasi AI dalam tindak pidana siber. UU ITE lebih berfokus pada kejahatan digital secara umum dan belum secara spesifik mengatur mengenai penggunaan AI sebagai medium cyber crime. Kondisi tersebut menyebabkan adanya kekosongan norma yang berpotensi menghambat efektivitas penegakan hukum (Prayoga & Tuasikal, 2025).

Dalam konteks criminal law modern, reformasi regulasi menjadi langkah penting untuk memberikan kepastian hukum terhadap tindak pidana berbasis AI.

Pemerintah perlu merumuskan regulasi khusus yang mengatur penggunaan AI, batas tanggung jawab pidana, perlindungan data digital, serta mekanisme pengawasan terhadap teknologi artificial intelligence.

Selain pembaruan regulasi, penguatan kapasitas aparat penegak hukum juga menjadi kebutuhan mendesak. Investigasi terhadap AI-based cyber crime memerlukan kemampuan digital forensic yang lebih maju karena kejahatan berbasis AI memiliki pola yang lebih kompleks dan sulit dilacak. Oleh karena itu, peningkatan kompetensi sumber daya manusia di bidang cyber law dan digital forensic menjadi bagian penting dalam menghadapi perkembangan cyber crime modern (Mecca et al., 2025).

Di samping itu, kerja sama internasional juga diperlukan karena tindak pidana siber berbasis AI sering kali bersifat lintas negara (transnational crime). Harmonisasi regulasi internasional mengenai AI dan cyber crime menjadi langkah strategis untuk memperkuat sistem penegakan hukum global terhadap ancaman kejahatan digital modern (Wahyudi, 2025).

Secara keseluruhan, hasil penelitian menunjukkan bahwa eksploitasi teknologi AI dalam tindak pidana siber telah menciptakan tantangan baru bagi sistem hukum pidana modern. Oleh karena itu, diperlukan reformasi hukum yang adaptif, penguatan penegakan hukum digital, serta pengembangan regulasi khusus terkait artificial intelligence agar sistem hukum mampu menghadapi perkembangan cyber crime di era digital modern.

SIMPULAN

penelitian ini menunjukkan bahwa perkembangan Artificial Intelligence (AI) telah membawa perubahan besar terhadap pola tindak pidana siber modern. Teknologi AI tidak hanya memberikan manfaat dalam berbagai sektor kehidupan, tetapi juga dimanfaatkan sebagai instrumen kejahatan digital melalui deepfake, phishing berbasis AI, malware cerdas, dan otomatisasi serangan siber. Eksploitasi AI dalam cyber crime menyebabkan kejahatan digital menjadi lebih kompleks, adaptif, dan sulit dideteksi dibandingkan tindak pidana siber konvensional. Kondisi tersebut menimbulkan tantangan serius terhadap sistem hukum pidana modern, khususnya terkait pertanggungjawaban pidana, pembuktian digital, dan identifikasi pelaku kejahatan berbasis teknologi artificial intelligence.

Regulasi hukum di Indonesia masih belum sepenuhnya mampu mengakomodasi perkembangan AI-based cyber crime karena belum adanya pengaturan khusus mengenai eksploitasi AI dalam tindak pidana siber. Oleh karena itu, diperlukan reformasi hukum yang adaptif melalui pembaruan regulasi, penguatan kapasitas digital forensic, serta peningkatan kompetensi aparat penegak hukum di bidang cyber law. Selain itu, kerja sama internasional juga diperlukan untuk memperkuat penegakan hukum terhadap kejahatan siber berbasis AI yang bersifat lintas negara. Penelitian ini diharapkan dapat memberikan kontribusi akademik dalam pengembangan criminal law modern sekaligus menjadi referensi dalam pembentukan kebijakan hukum terkait penggunaan artificial intelligence di Indonesia.

UCAPAN TERIMAKASIH

Penulis menyampaikan ucapan terima kasih kepada semua pihak yang telah memberikan dukungan dalam proses penyusunan penelitian ini, baik dalam bentuk masukan akademik, referensi ilmiah, maupun dukungan moral sehingga penelitian dapat diselesaikan dengan baik. Ucapan terima kasih juga disampaikan kepada Al-Zayn: Jurnal Ilmu Sosial & Hukum yang telah memberikan kesempatan bagi penulis untuk mempublikasikan hasil penelitian ini.

DAFTAR RUJUKAN

Aditya, K. M., & Yudiantara, I. G. N. N. K. (2025). ANALISIS KRIMINOLOGI DALAM TINDAK PIDANA PENCURIAN DATA PRIBDADI DI ERA DIGITAL. *Jurnal Media Akademik (JMA)*.

Apriadi, E. A., Julianto, R., Dwiatmoko, F., Kom, S., Kom, M., Bisri, M., & Kom, M. (2025). KECERDASAN BUATAN Teori, Implementasi, dan Aplikasi di Era Digital. Eko Aziz Apriadi.

Aprilianti, A. (2024). Efektivitas dan implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai hukum siber di Indonesia: Tantangan dan solusi. *Begawan Abioso*, *15*(1), 41-50. https://doi.org/10.37893/abioso.v15i1.1002

Berlian, C. (2025). Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan Artificial Intelligence. *Universitas Jambi*.

Budiyanto, S. H. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1), 111-133. https://doi.org/10.64344/djl.v1i1.6

Dermawan, A. (2026). ANALISIS YURIDIS IMPLEMENTASI HAK ASASI MANUSIA DALAM PENANGANAN TINDAK PIDANA SIBER. *Jurnal Ilmu Hukum*, *1*(1), 1-11.

DM, M. Y., Sebayang, B. P. R., Turnip, R. W., & Saputra, H. (2025). PERUBAHAN PIDANA DARI KUHP LAMA KE BARU SALAH SATU ADALAH REFORMASI PENEGAKAN HUKUM. *Collegium Studiosum Journal*, *8*(2), 465-479. https://doi.org/10.56301/csj.v8i2.2008

Guntara, P., Nurdiyanti, E. P., & Valentina, R. W. (2026). DAMPAK TEKNOLOGI AI TERHADAP POLA KEJAHATAN. *Jurnal Riset Multidisiplin Edukasi*, *3*(1), 304-316. https://doi.org/10.71282/jurmie.v3i1.1534

Hutauruk, A., & Sinambela, H. (2026). ANALISIS YURIDIS PENGARUH ESKALASI PENGGUNAAN MEDIA SOSIAL TERHADAP PENINGKATAN KEJAHATAN SIBER DI INDONESIA BERDASARKAN UU NO 1 TAHUN 2024. *Law and Communication Journal*, *2*(1), 26-37.

Ibrahim, M. K., & Atmaja, Z. F. H. (2025). Urgensi Pembaruan Hukum Dalam Menghadapi Kejahatan Yang Melibatkan Teknologi Kecerdasan Buatan

AI. *Journal of Legal, Political, and Humanistic Inquiry*, *1*(2), 106-115. https://doi.org/10.65310/2dk3wh05

Mecca, A. S. P., Hidaya, W. A., & Tuasikal, H. (2025). Pemanfaatan teknologi kecerdasan buatan (artificial intelligence) dalam sistem peradilan pidana di Indonesia. *Jurnal Sosial Teknologi*, *5*(6), 1730-1746. https://doi.org/10.59188/jurnalsostech.v5i6.32207

Nawawi, W. (2026). Kedudukan Hukum Artificial Intelligence dan Konstruksi Pertanggungjawaban Pidana dalam Sistem Hukum Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(2), 7191-7203. https://doi.org/10.61104/alz.v4i2.5450

Novera, O. (2024). Analisis pengaturan hukum pidana terhadap penyalahgunaan teknologi manipulasi gambar (deepfake) dalam penyebaran konten pornografi melalui akun media sosial. *El-Faqih: Jurnal Pemikiran dan Hukum Islam*, *10*(2), 460-474. https://doi.org/10.58401/faqih.v10i2.1539

Novrianto, M. (2025). Kebijakan Hukum Pidana Terhadap Cyber Crime Berbasis Artificial Intelligence di Indonesia. *Jurnal Kepastian Hukum dan Keadilan*, *7*(2), 150-170. https://doi.org/10.32502/khk.v7i2.10615

Perian, A., Atyanta, A., & Syamsudin, M. (2025). Artificial Intelligence Sebagai Pelaku Kejahatan. *Wijayakusuma Law Review*, *7*(2). https://doi.org/10.51921/wlr.25qk5w45

Prayoga, H., & Tuasikal, H. (2025). Penyebaran konten deepfake sebagai tindak pidana: Analisis kritis terhadap penegakan hukum dan perlindungan publik di Indonesia. *Abdurrauf Law and Sharia*, *2*(1), 22-38. https://doi.org/10.70742/arlash.v2i1.194

Santoso, S., Oktarino, A., Tugiman, T., & Wicaksono, A. D. A. (2025). *Buku Ajar Cyber Security*. PT. Sonpedia Publishing Indonesia.

Setiawan, D. A. (2024). Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa. *Masalah-Masalah Hukum*, *53*(1), 78-89. https://doi.org/10.14710/mmh.53.1.2024.78-89

Setiawan, R., & Arista, M. O. (2013). Efektivitas undang-undang informasi dan transaksi elektronik di indonesia dalam aspek hukum pidana. *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *2*(2). https://doi.org/10.20961/recidive.v2i2.32324

Sihombing, G. R. A., & Hermanto, B. (2026). DINAMIKA KEBIJAKAN PENEGAKAN HUKUM TERHADAP PEMANFAATAN KECERDASAN BUATAN DALAM KEJAHATAN SIBER DI INDONESIA. *Jurnal Media Akademik (JMA)*, *4*(1). https://doi.org/10.62281/ekbmtj76

Wahidi, K., & Zulfa, D. A. (2026). Fenomena Kecanduan AI (Artifical Intelligence) di Kalangan Mahasiswa. *Jurnal Pendidikan Agama Islam*, *1*(2), 57-62.

Wahyudi, B. R. (2025). Tantangan penegakan hukum terhadap kejahatan berbasis teknologi AI. *Innovative: Journal Of Social Science Research*, *5*(1), 3436-3450. https://doi.org/10.31004/innovative.v5i1.17519

Yanti, H. A., Aulia, I., Fathiyana, R. Z., Sularso, A. N., Ilmi, N., Muttaqin, W., ... & Zailani, A. U. (2025). *ARTIFICIAL INTELLIGENCE AND CYBERSECURITY:*

FOUNDATIONS, APPLICATIONS, AND FUTURE PERSPECTIVES. Penerbit Widina.

