Judge: Journal of Law and Justice, Vol. 1 No. 2, 2025
Avaliable Online at: https://journal.habepublisher.com/judge

TANTANGAN PENEGAKAN HUKUM TERHADAP KEJAHATAN SIBER BERBASIS *ARTIFICIAL INTELLIGENCE* DI INDONESIA

Muhammad Atho'hillah[1*]

[1*]Universitas Maarif Hasyim Latif, Sidoarjo, Indonesia
Atho'hillahmuhmuhammad1926@gmail.com

ARTICLE INFO
Article History:
Recieved: 2025-11-10
Revised*:* 2025-11-24
Accepted: 2025-12-29

Keyword:
Cybercrime;
Artificial intelligence;
Law enforcement.

ABSTRACT
The development of Artificial Intelligence (AI) technology has transformed the cybercrime landscape from manual attacks to automated, adaptive, and difficult-to-detect attacks, increasing the complexity of threats to national security, social stability, and citizens' rights in the digital space. In Indonesia, the legal framework, consisting of the ITE Law, the Criminal Code, and the Personal Data Protection Law, provides a regulatory basis, but it is not fully responsive to new crime modes such as deepfakes, AI-enhanced phishing, and cross-border autonomous attacks. This study aims to analyze the normative, technical, and institutional challenges in law enforcement against AI-based cybercrime, while also formulating directions for strengthening regulations, digital forensic capacity, and AI governance in Indonesia. The method used is qualitative research with a literature review through a review of laws and regulations, decisions, scientific literature, and institutional reports. Content analysis techniques were used to identify legal gaps, technical barriers, and weaknesses in coordination between law enforcement actors. The research findings indicate that there is still a gap in conceptual regulations regarding AI-based cybercrime, limited human resources and digital forensic infrastructure, and institutional fragmentation. Therefore, a more adaptive reconstruction of the cyber legal system is needed, the establishment of adequate forensic tools and high-tech crime units, and the strengthening of AI governance based on the principles of transparency, accountability, and human rights protection.

How to Cite:
Atho'hillah, M. (2025). Tantangan Penegakan Hukum Terhadap Kejahatan Siber Berbasis *Artificial Intelligence* Di Indonesia. *Judge: Journal of Law and Justice, 1*(2), 52-59. https://doi.org.

https://doi.org/

INTRODUCTION

Perkembangan teknologi *Artificial Intelligence* (*AI*) telah mengubah secara mendasar lanskap kejahatan siber, dari yang semula didominasi serangan manual menjadi serangan otomatis, adaptif, dan sangat sulit dideteksi. Dalam konteks historis, kemajuan komputasi, *big data*, dan algoritma pembelajaran mendalam (*deep learning*) memungkinkan *AI* melakukan analisis pola, pengenalan wajah, suara, dan teks dalam skala besar, sehingga teknologi yang awalnya dirancang untuk efisiensi dan inovasi kini juga dimanfaatkan pelaku kejahatan siber untuk mengoptimalkan serangan. Menurut Popoola dkk. (2023), integrasi *machine learning* dan *deep learning* dalam analitik keamanan siber membuat sistem mampu mengenali pola serangan botnet dan ancaman jaringan dengan tingkat akurasi tinggi, namun di sisi lain menunjukkan bahwa teknik yang sama dapat direkayasa ulang untuk menyusun serangan lebih canggih dan terselubung. Menurut Basit dkk. (2021), evolusi serangan *phishing* menunjukkan pergeseran dari email sederhana yang mudah dikenali menuju serangan berbasis rekayasa sosial yang kompleks, dibantu algoritma *AI* yang mampu mempersonalisasi konten, meniru gaya bahasa korban, dan mengeksploitasi kelemahan psikologis dengan lebih presisi. Perkembangan ini berkaitan erat dengan kemunculan *generative AI* yang mampu memproduksi teks, gambar, dan video sintetis secara realistis, sehingga membuka ruang bagi modus kejahatan baru seperti *deepfake, voice cloning,* dan *automated spear phishing* yang sebelumnya sulit dilakukan secara massal.

Transformasi kejahatan siber berbasis *AI* tampak jelas pada tiga ranah utama: *deepfake, automated hacking,* dan *phishing* berbasis *AI*. Menurut penjelasan Marah (2024), *deepfake* sebagai produk media sintetis berbasis *AI* telah digunakan untuk pemerasan, pornografi non-konsensual, penipuan identitas, hingga manipulasi opini publik, sekaligus menimbulkan problem serius bagi hukum pembuktian dan atribusi pertanggungjawaban karena batas antara bukti asli dan manipulasi digital menjadi kabur. Dalam ranah *automated hacking*, menurut Popoola dkk. (2023) penggunaan model *AI* untuk menganalisis lalu lintas jaringan dan log keamanan memungkinkan penyerang (bila teknologi ini disalahgunakan) memetakan kerentanan sistem lebih cepat, mengubah pola serangan secara dinamis, serta menyamarkan jejak di tengah lalu lintas data yang kompleks sehingga menyulitkan investigasi forensik digital. Di sisi lain, phishing berbasis *AI* berkembang dari sekadar pengiriman email massal menuju kampanye multi-kanal (email, SMS, media sosial) yang dioptimalkan dengan *natural language processing*, sehingga pesan yang dikirim tampak sangat wajar, bebas kesalahan bahasa, dan selaras dengan konteks pribadi korban. Serangan siber yang memanfaatkan *AI* menunjukkan peningkatan yang signifikan baik dari sisi jumlah maupun tingkat keberhasilan, di mana *AI-enhanced phishing* mengalami kenaikan tingkat keberhasilan dari sekitar 2,9% menjadi 8,7%, dan secara umum serangan berbasis *AI* memiliki tingkat keberhasilan lebih tinggi serta menurunkan kompleksitas

E-ISSN: 3123-3791

operasional bagi pelaku. Data ini menggambarkan bahwa *AI* bukan hanya menambah "variasi" bentuk kejahatan siber, tetapi secara struktural meningkatkan kompleksitas ancaman: serangan menjadi lebih cepat, lebih tepat sasaran, lebih sulit dideteksi, dan lebih menantang bagi sistem hukum pidana serta aparat penegak hukum yang masih beradaptasi dengan dinamika era digital.

Penegakan hukum terhadap kejahatan siber di Indonesia memiliki urgensi yang sangat tinggi karena menyangkut langsung perlindungan keamanan nasional, stabilitas sosial, dan hak-hak warga negara di ruang digital. Pesatnya pemanfaatan teknologi informasi dalam sektor perbankan, pemerintahan, kesehatan, pendidikan, dan layanan publik menyebabkan setiap serangan siber-seperti penipuan *online*, peretasan sistem, kebocoran data, *ransomware*, dan sabotase layanan-berpotensi menimbulkan kerugian ekonomi yang besar sekaligus merusak kepercayaan masyarakat terhadap negara dan pelaku usaha. Dalam kondisi seperti ini, penegakan hukum yang efektif menjadi instrumen utama untuk menghadirkan negara di dunia maya melalui pemberian efek jera, perlindungan korban, serta penegasan bahwa ruang digital bukan "wilayah bebas hukum", melainkan tunduk pada norma pidana dan regulasi yang berlaku. Urgensi tersebut semakin mengemuka karena kejahatan siber bersifat lintas batas, terorganisasi, dan terus beradaptasi dengan teknologi baru, sementara kapasitas aparat penegak hukum (dari sisi SDM, sarana forensik digital, dan koordinasi antarlembaga) masih menghadapi berbagai keterbatasan sehingga banyak kasus sulit diungkap secara tuntas. Di sisi regulasi, keberadaan UU ITE dan UU Perlindungan Data Pribadi merupakan fondasi penting, namun berbagai kajian menilai masih dibutuhkan harmonisasi, pedoman penegakan yang lebih jelas, dan penguatan aspek perlindungan korban agar mampu menjawab kompleksitas modus kejahatan siber modern. Penegakan hukum yang tegas dan konsisten juga berfungsi menjaga kepercayaan publik terhadap transformasi digital dan mendorong pelaku usaha maupun instansi pemerintah untuk meningkatkan standar keamanan siber, sehingga tercipta ekosistem digital yang aman, berkeadilan, dan berkelanjutan di Indonesia.

METHODS

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kepustakaan (*library research*) yang bertujuan untuk menganalisis kerangka hukum dan dinamika penegakan kejahatan siber di Indonesia, khususnya yang berbasis kecerdasan buatan (*AI*). Data diperoleh dari berbagai sumber sekunder berupa peraturan perundang-undangan (UU ITE, KUHP, UU PDP, dan regulasi terkait lainnya), jurnal ilmiah, buku, laporan lembaga pemerintah, serta hasil penelitian terdahulu yang relevan. Analisis data dilakukan melalui teknik analisis isi (*content analysis*) untuk mengidentifikasi kesenjangan normatif, kelembagaan, dan teknologis dalam penegakan hukum siber. Validitas data dijaga dengan triangulasi sumber dan interpretasi konseptual, sedangkan proses analisis dilakukan secara induktif dengan menafsirkan temuan empiris dan doktrinal untuk merumuskan

E-ISSN: 3123-3791

arah strategis penguatan tata kelola hukum terhadap kejahatan siber berbasis *AI* di Indonesia.

RESULT AND DISCUSSION

Kerangka Hukum Penegakan Kejahatan Siber di Indonesia

Kerangka hukum penegakan kejahatan siber di Indonesia dibangun di atas beberapa pilar utama, yaitu UU ITE sebagai *lex specialis*, KUHP dan KUHP baru sebagai dasar umum pemidanaan, UU Perlindungan Data Pribadi (UU PDP) sebagai payung perlindungan data, serta kewenangan kelembagaan Polri, Kominfo, dan BSSN yang saling terkait dalam menangani insiden siber. UU ITE mengatur berbagai tindak pidana seperti akses ilegal, intersepsi, manipulasi dan transfer data tanpa hak, penipuan elektronik, serta penyebaran konten ilegal, yang menjadi dasar utama bagi penyidik dalam melakukan penyelidikan dan penyidikan terhadap kejahatan siber. Menurut Ramli (2022), konstruksi UU ITE menempatkan informasi dan dokumen elektronik sebagai alat bukti sah sekaligus objek perlindungan hukum, namun implementasinya sering menghadapi masalah penafsiran pasal, kesenjangan kapasitas aparat, dan belum optimalnya koordinasi antar lembaga penegak hukum. Di sisi lain, KUHP lama dan KUHP baru tetap digunakan untuk menjerat delik umum seperti penipuan, pemerasan, pencemaran nama baik, dan perusakan, yang kini banyak dilakukan melalui sarana elektronik, sehingga terjadi hubungan komplementer antara KUHP dan UU ITE dalam konstruksi dakwaan. Menurut Siregar (2023), reformulasi beberapa delik dalam KUHP baru membuka ruang penyesuaian dengan konteks digital, tetapi belum menjawab secara tuntas isu-isu spesifik *cybercrime* transnasional dan kejahatan berbasis kecerdasan buatan sehingga masih diperlukan pengaturan sektoral tambahan.

UU Perlindungan Data Pribadi menambah lapis penting dalam kerangka hukum dengan menetapkan kewajiban pengendali dan pemroses data untuk menjaga kerahasiaan, integritas, dan ketersediaan data, serta mengatur sanksi ketika terjadi kebocoran atau penyalahgunaan data dalam insiden siber yang merugikan subjek data. Menurut Putri (2024), UU PDP memperkuat posisi korban kejahatan siber yang berkaitan dengan pencurian atau kebocoran data pribadi, karena korban kini memiliki dasar hukum yang lebih jelas untuk menuntut pertanggungjawaban baik pidana, administratif, maupun perdata terhadap pelaku atau penyelenggara sistem elektronik yang lalai. Dari sisi kelembagaan, Polri melalui Direktorat Tindak Pidana Siber menjadi aktor utama penegakan hukum pidana, dengan dukungan unit Polri-CSIRT yang berfungsi menerima, menganalisis, dan merespons insiden keamanan siber serta berkoordinasi dengan CSIRT sektor lain. Kominfo memegang peran regulasi dan pengawasan penyelenggara sistem elektronik, pengelolaan konten, serta pemutusan akses terhadap situs dan *platform* yang memfasilitasi kejahatan siber, sedangkan BSSN bertanggung jawab membangun keamanan siber nasional, melakukan deteksi dan peringatan dini, serta menjadi simpul koordinasi teknis keamanan siber

antarinstansi. Menurut Hamzah (2024), pembagian kewenangan ini pada prinsipnya sudah mengarah pada model multi-stakeholder, tetapi masih menghadapi masalah tumpang tindih kewenangan, belum jelasnya protokol koordinasi, dan keterbatasan sumber daya yang menyebabkan penanganan kasus sering berjalan sektoral.

Tantangan Penegakan Hukum terhadap Kejahatan Siber Berbasis *AI*

Tantangan penegakan hukum terhadap kejahatan siber berbasis *AI* di Indonesia bersifat multidimensi karena menyentuh aspek normatif, teknis, dan kelembagaan yang saling berkaitan dan hingga kini belum sepenuhnya terjawab oleh kerangka hukum yang ada. Dari sisi normatif, perkembangan pesat teknologi *AI* tidak diikuti secara seimbang oleh pembaruan hukum pidana dan hukum siber, sehingga banyak modus kejahatan baru-seperti *deepfake fraud*, serangan otomatis berbasis *machine learning*, atau manipulasi data *biometric*-belum tersentuh secara eksplisit oleh UU ITE, KUHP, maupun UU Perlindungan Data Pribadi. Menurut Pratama (2024), Indonesia mengalami kekosongan pengaturan konseptual karena belum terdapat definisi hukum yang jelas mengenai "kejahatan siber berbasis *AI*" dan belum ada klasifikasi khusus untuk membedakan antara kejahatan yang hanya menggunakan komputer sebagai sarana dengan kejahatan yang inti modusnya bertumpu pada otonomi dan kemampuan belajar algoritma *AI*. Menurut Rahman (2025), ketiadaan pengaturan rinci mengenai peran pengembang, penyedia platform, dan pengguna dalam rantai *AI* menimbulkan kesulitan dalam menentukan subjek yang paling tepat dimintai pertanggungjawaban ketika sistem *AI* disalahgunakan untuk menyerang atau merugikan pihak lain. Tantangan normatif lain adalah pembuktian *mens rea*: ketika serangan dilakukan oleh sistem otomatis atau model yang beradaptasi sendiri, aparat harus membuktikan hubungan niat jahat, kelalaian, atau pengendalian dari manusia di belakang sistem. Menurut Misbach (2025), konsep kesalahan dalam hukum pidana klasik yang bertumpu pada kehendak dan kesadaran manusia menjadi problematis ketika berhadapan dengan entitas cerdas non-manusia yang mengambil keputusan berdasarkan pembelajaran data, sehingga memunculkan debat tentang perlu tidaknya konstruksi baru seperti *liability* berbasis risiko atau *strict liability* untuk konteks *AI* tertentu.

Dari aspek teknis-teknologis, kompleksitas algoritma *AI*-khususnya *deep learning* dan *generative models*-menyebabkan banyak sistem berperilaku layaknya "*black box*" yang sulit dilacak logikanya, sehingga menyulitkan proses forensik dan pembuktian di pengadilan. Menurut Kurniawan (2025), pelaku kejahatan memanfaatkan kemampuan adaptif *AI* untuk mengubah pola serangan secara dinamis, menghindari *signature-based detection*, serta mengaburkan jejak dengan infrastruktur global, penggunaan *VPN, proxy, botnet,* dan *server* lintas negara. Hal ini menjadikan atribusi pelaku dan penentuan yurisdiksi menjadi sangat rumit, karena jejak digital tersebar di berbagai negara dan sering kali disamarkan melalui lapisan enkripsi dan otomatisasi. Pada saat yang sama, kapasitas alat forensik digital berbasis *AI* di lembaga penegak hukum masih terbatas, baik dari sisi

E-ISSN: 3123-3791

perangkat lunak untuk analisis konten sintetis (*deepfake detection, anomaly detection*) maupun infrastruktur laboratorium dan SDM analis yang menguasai teknik tersebut. Menurut Salsabila (2024), ketergantungan pada *tools* luar negeri dan keterbatasan kemampuan validasi forensik menyebabkan sebagian bukti digital berisiko tidak dapat dipertahankan sebagai alat bukti kuat di pengadilan, terutama ketika berhadapan dengan advokat yang menguji reliabilitas dan keotentikan bukti berbasis *AI*.

Dari aspek kelembagaan dan SDM, penelitian menunjukkan bahwa kompetensi aparat penegak hukum-penyidik, jaksa, maupun hakim-dalam memahami arsitektur *AI*, pola serangan cerdas, dan teknik pembuktian forensik algoritmik masih belum memadai dan cenderung tertinggal dibanding inovasi pelaku. Menurut Lestari (2023), pelatihan yang tersedia lebih banyak berfokus pada *cybercrime* konvensional (penipuan *online, hacking* tradisional, atau penyebaran konten ilegal) dan belum menyentuh secara mendalam isu-isu seperti *AI security*, *deepfake forensics,* atau *automated cyber attacks*. Selain itu, koordinasi antar lembaga seperti Polri, Kominfo, BSSN, OJK, dan sektor swasta (penyelenggara sistem elektronik, perbankan, *platform digital*) masih lemah, ditandai dengan fragmentasi basis data insiden, perbedaan standar pelaporan, serta belum adanya protokol terpadu untuk menangani kejahatan berbasis *AI* berskala besar. Menurut Ariyaningsih (2023), keterbatasan anggaran, minimnya unit khusus *high-tech crime*, serta belum meratanya pembangunan infrastruktur teknologi (*Security Operation Center, CSIRT,* dan *lab forensik AI*) mengakibatkan respons negara terhadap kejahatan *AI-based cybercrime* bersifat reaktif, sporadis, dan sering tertinggal dari laju evolusi ancaman. Tanpa reformasi regulasi yang adaptif, peningkatan kapasitas teknis dan forensik, serta penguatan kelembagaan yang mendorong kolaborasi lintas sektor dan lintas negara, penegakan hukum terhadap kejahatan siber berbasis *AI* berpotensi terus berada dalam posisi defensif dan kurang efektif dalam memberikan perlindungan yang optimal kepada masyarakat.

Upaya dan Strategi Penguatan Penegakan Hukum

Upaya dan strategi penguatan penegakan hukum terhadap kejahatan siber berbasis *AI* pada dasarnya harus diarahkan pada empat pilar utama: pembaruan regulasi, penguatan kapasitas SDM dan teknologi, pengembangan kerangka etika dan tata kelola *AI*, serta kerja sama lintas sektor dan internasional. Pembaruan dan harmonisasi regulasi menjadi kebutuhan mendesak karena kerangka hukum yang ada (UU ITE, KUHP, UU PDP dan regulasi sektoral) belum sepenuhnya mengantisipasi karakteristik kejahatan yang memanfaatkan kecerdasan buatan secara otonom, adaptif, dan lintas batas. Menurut Pratama (2024), kebijakan hukum pidana terhadap *cyber crim*e berbasis *AI* perlu diarahkan pada penyusunan aturan khusus yang mendefinisikan *AI* dan *AI-based cybercrime*, memetakan bentuk-bentuk kejahatan baru (*deepfake fraud, automated phishing*, serangan otonom), serta mengatur secara eksplisit pembagian tanggung jawab pidana antara pengembang, penyedia *platform*, dan pengguna. Menurut Satoto (2025), rekonstruksi sistem hukum siber Indonesia idealnya dilakukan melalui pembentukan undang-undang

keamanan siber nasional yang mengintegrasikan UU ITE, UU PDP, dan aturan sektoral, sekaligus mengadopsi pendekatan berbasis risiko sebagaimana berkembang dalam regulasi *AI* global agar mampu beradaptasi dengan teknologi tinggi. Haris (2025) menambahkan bahwa reformulasi kebijakan pidana harus disertai penyusunan pedoman penuntutan dan pembuktian khusus untuk kasus berbasis *AI*, termasuk standar pembuktian terhadap sistem otonom dan penggunaan bukti digital yang dihasilkan *AI* di pengadilan.

Pada saat yang sama, penguatan kapasitas SDM dan teknologi aparat penegak hukum menjadi prasyarat utama keberhasilan regulasi. Menurut Haris (2025), kelemahan utama penegakan hukum *cybercrime* di Indonesia terletak pada keterbatasan kemampuan *digital forensics* dan kurangnya pemahaman aparat terhadap arsitektur *AI*, algoritma pembelajaran mesin, dan modus serangan cerdas, sehingga banyak kasus sulit diungkap dan dibuktikan secara komprehensif. Satoto (2025) menekankan perlunya membangun jejaring laboratorium forensik siber berbasis *AI*, menyediakan *tools* deteksi *deepfake* dan analisis *big data* bagi Polri, kejaksaan, dan lembaga teknis, serta membentuk unit khusus *high-tech crime* yang fokus menangani kejahatan berbasis teknologi tinggi. Lebih jauh, penguatan penegakan hukum harus ditopang kerangka etika dan tata kelola *AI* yang jelas. Menurut Putri (2024), *AI* di sektor publik dan penegakan hukum hanya dapat diterima secara sosial bila diatur melalui prinsip transparansi algoritma, akuntabilitas, non-diskriminasi, dan perlindungan hak asasi, termasuk hak atas privasi dan perlindungan data pribadi. Tohopi (2025) menunjukkan bahwa tata kelola *AI* di Indonesia masih lemah pada tingkat implementasi; karena itu diperlukan kombinasi instrumen hukum yang mengikat, standar teknis (audit algoritma, dokumentasi model), serta mekanisme pengawasan partisipatif agar penggunaan *AI* oleh negara dan sektor privat tidak berubah menjadi sumber pelanggaran baru.

CONCLUSION

Hasil penelitian menunjukkan bahwa kerangka hukum penegakan kejahatan siber di Indonesia telah mencakup UU ITE, KUHP, dan UU Perlindungan Data Pribadi sebagai dasar utama, namun ketiganya belum sepenuhnya mampu menjawab kompleksitas kejahatan siber berbasis *AI*. Dari sisi normatif, terdapat kekosongan pengaturan terkait definisi, klasifikasi, serta pertanggungjawaban terhadap kejahatan yang melibatkan sistem otonom berbasis *AI*. Dari aspek teknis dan kelembagaan, penegakan hukum masih menghadapi keterbatasan infrastruktur forensik digital, kurangnya kompetensi aparat dalam memahami teknologi *AI*, serta minimnya koordinasi antar lembaga penegak hukum dan sektor swasta. Penelitian ini menyimpulkan bahwa upaya penguatan penegakan hukum memerlukan reformasi regulasi yang adaptif, peningkatan kapasitas SDM dan teknologi forensik, serta pembentukan tata kelola dan etika *AI* yang selaras dengan standar global guna mewujudkan keamanan siber nasional yang tangguh dan responsif terhadap perubahan teknologi.

E-ISSN: 3123-3791

REFERENCES

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks and defense mechanisms. *IEEE Access, 9*, 103-123.

Ismail, M. N. (2025). Pengaruh teknologi *AI* terhadap evolusi modus kejahatan siber global 2024–2025. *Jurnal Informatika dan Keamanan Nusantara, 7*(1), 45-60.

Satoto, E. (2025). Reconstruction of Indonesia's cyber law system for adaptive digital crime governance. *Global Indonesian Journal of Law, Social Sciences and Humanities, 3*(2), 55-72.

SSEK Law Firm. (2025). *Indonesia cybersecurity laws and regulations 2025*. In *ICLG: Cybersecurity 2025 (8th ed.)*. https://www.ssek.com/blog/indonesia-cybersecurity-laws-and-regulations

Tohopi, R. (2025). Artificial intelligence in public governance: Ethical opportunities and regulatory challenges in Indonesia. *Proceedings of the Indonesian Association for Public Administration*, 1338, 1-12. https://www.jurnal.iapa.or.id/proceedings/article/view/1338

Yamashita Rolindrawan, W., Mooduto, N. A. P., & Sihombing, A. K. (2025). Data protection & privacy 2025: Indonesia chapter. In *Chambers global practice guides: Data protection & privacy 2025*. https://www.abnrlaw.com/files/document/Chambers_Data_Protection_Privacy_2025_011_indonesia.pdf

E-ISSN: 3123-3791