Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 304 - 316

DAMPAK TEKNOLOGI AI TERHADAP POLA KEJAHATAN

Peter Guntara[1], Erlinda Putri Nurdiyanti[2], Ratna Wulan Valentina[3]
Universitas Duta Bangsa Surakarta [1,2,3]
Email: peter_guntara@udb.ac.id[1], erlindanurdiyanti688@gmail.com[2], ratnawulan140205@gmail.com[3]

Informasi

Volume : 3
Nomor : 1
Bulan : Januari
Tahun : 2026
E-ISSN : 3062-9624

Abstract

The rapid development of Artificial Intelligence (AI) has significantly transformed the patterns of modern crime, particularly in the realm of cybercrime. This study aims to analyze how AI has changed the modus operandi of cyber offenses and to identify the legal challenges and enforcement strategies in addressing AI-driven crimes. This research employs a normative legal method using statutory and conceptual approaches, examining relevant regulations such as the Electronic Information and Transactions Law, the Personal Data Protection Law, and the National Cybersecurity Strategy. The findings reveal that AI has accelerated, expanded, and personalized cyberattacks through technologies such as deepfake, machine learning-based phishing, and adaptive malware. AI-related crimes complicate legal proceedings since electronic evidence can be easily manipulated and is difficult to authenticate. The main challenges lie in the lack of regulation regarding algorithmic accountability, limited digital forensic capacity, and weak international coordination. Therefore, legal reform is required to incorporate the principle of vicarious liability for AI developers, establish a specialized unit for AI-related crimes, and strengthen technology-based law enforcement capacity.

Keyword: *Artificial Intelligence, Cybercrime, Deepfake, Legal Evidence, Digital Security.*

Abstrak

Perkembangan kecerdasan buatan (Artificial Intelligence /AI) telah memberikan dampak besar terhadap perubahan pola kejahatan, khususnya dalam ranah siber. Penelitian ini bertujuan untuk menganalisis bagaimana AI mengubah modus operandi tindak kejahatan siber serta mengidentifikasi tantangan hukum dan strategi penegakan hukum dalam menghadapinya. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual, yang menelaah regulasi seperti UU ITE, UU Perlindungan Data Pribadi, serta kebijakan keamanan siber nasional. Hasil penelitian menunjukkan bahwa AI telah mempercepat, memperluas, dan mempersonalisasi serangan siber melalui pemanfaatan teknologi seperti deepfake, phishing berbasis pembelajaran mesin, dan malware adaptif. Kejahatan berbasis AI menimbulkan kesulitan dalam pembuktian hukum karena bukti elektronik sering dimanipulasi dan sulit diverifikasi. Tantangan utama terletak pada kekosongan regulasi terkait tanggung jawab algoritma, keterbatasan kemampuan forensik digital aparat, dan lemahnya koordinasi lintas negara. Oleh karena itu, dibutuhkan pembaruan hukum yang mengakomodasi prinsip tanggung jawab pengembang (vicarious liability), pembentukan unit khusus penanganan kejahatan AI, serta penguatan kapasitas penegakan hukum berbasis teknologi.

Kata Kunci: *Kecerdasan Buatan, Kejahatan Siber, Deepfake, Pembuktian Hukum, Keamanan Digital.*

A. PENDAHULUAN

Perkembangan kecerdasan buatan (Artificial Intelligence/AI) yang sangat pesat telah membawa perubahan besar dalam berbagai sektor kehidupan, mulai dari bidang industri, kesehatan, hingga sistem komunikasi. Di balik potensi inovatif dan efisiensi yang ditawarkan, kemajuan AI juga menimbulkan tantangan serius dalam aspek keamanan dan hukum. Kemampuan AI dalam memproses data berskala besar, mengambil keputusan secara otomatis, serta melakukan otomasi tugas tertentu telah membuka peluang baru dalam praktik kejahatan modern. Fenomena ini menunjukkan adanya pergeseran mendasar dalam pola dan modus operandi tindak kejahatan.

Saat ini, pelaku kriminal tidak lagi bergantung pada metode konvensional, melainkan memanfaatkan AI untuk meningkatkan efektivitas, jangkauan, dan kompleksitas aksinya. Penggunaan teknologi deepfake—yakni rekayasa media sintetis berbasis AI yang sangat realistis—telah dimanfaatkan untuk penipuan, pemerasan, dan penyebaran disinformasi. Selain itu, serangan phishing kini dapat diotomatisasi dan dipersonalisasi secara masif, sementara malware berbasis AI mampu beradaptasi untuk menghindari sistem deteksi keamanan. Kondisi ini menunjukkan bahwa AI bersifat ambivalen, karena di satu sisi dapat dimanfaatkan oleh pelaku kejahatan, namun di sisi lain juga menjadi instrumen penting dalam penegakan hukum dan perlindungan keamanan siber.

Ichwan Kurnia (2024) menjelaskan bahwa kejahatan siber memiliki karakter lintas negara, anonim, dan berdampak global karena dapat dilakukan tanpa kehadiran fisik pelaku. Ia mengklasifikasikan kejahatan siber ke dalam tiga kategori, yaitu ketika komputer menjadi sasaran kejahatan, sebagai sarana melakukan kejahatan, atau sebagai unsur pendukung tindak pidana lainnya. Praktik kejahatan tersebut meliputi akses ilegal, manipulasi data, pencurian identitas, hingga distribusi konten yang melanggar hukum dengan memanfaatkan celah sistem digital. Di Indonesia, kepastian hukum diberikan melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019, serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Namun demikian, Kurnia menegaskan bahwa laju perkembangan teknologi sering kali melampaui kecepatan pembaruan regulasi. Akibatnya, aparat penegak hukum dihadapkan pada keterbatasan kemampuan forensik digital, kelemahan prosedur penyidikan, serta minimnya kerja sama internasional. Oleh karena itu, pembaruan regulasi, peningkatan kapasitas sumber daya manusia, dan adaptasi hukum terhadap perkembangan teknologi menjadi kebutuhan yang mendesak.

Dalam konteks sosial, media sosial kini telah menjadi kebutuhan esensial masyarakat untuk mengekspresikan kebebasan berpendapat, berpikir, dan berserikat. Ruang digital menciptakan pola interaksi dan komunikasi baru yang menggantikan ruang konvensional. Pemanfaatan AI dalam media sosial semakin memperkaya bentuk komunikasi, termasuk melalui penciptaan konten sintetis yang mampu menampilkan seolah-olah seseorang berbicara atau bertindak, padahal tidak demikian.

Wibowo (2024) memandang ruang siber sebagai ekosistem digital yang dinamis, tempat terjadinya interaksi antara manusia, perangkat lunak, dan sistem telekomunikasi tanpa batas geografis. Ia menekankan bahwa hukum siber harus mampu mengatur seluruh aktivitas digital, mulai dari perlindungan data pribadi, keamanan jaringan, hingga pertanggungjawaban atas perbuatan di dunia maya. Menurutnya, UU ITE merupakan fondasi utama hukum siber di Indonesia, namun implementasinya masih terkendala keterbatasan sumber daya manusia, belum adanya regulasi khusus keamanan siber yang komprehensif, serta lemahnya koordinasi antar lembaga. Untuk merespons meningkatnya ancaman digital, pemerintah mengembangkan Strategi Keamanan Siber Nasional dan mengadopsi pendekatan Zero Trust, yaitu prinsip keamanan yang tidak memberikan kepercayaan otomatis kepada entitas mana pun dalam jaringan. Wibowo menekankan pentingnya kolaborasi antara pemerintah, sektor swasta, dan masyarakat guna memperkuat literasi digital, kapasitas teknis, dan kerangka keamanan siber nasional.

Perkembangan media sosial dan teknologi digital juga membuka peluang terjadinya perbuatan melawan hukum yang melahirkan bentuk kejahatan baru, yang dikenal sebagai cybercrime. Kejahatan siber memiliki karakteristik yang berbeda dari kejahatan konvensional karena dilakukan di ruang digital dengan memanfaatkan teknologi canggih, termasuk AI. Astuti (2024) menegaskan bahwa cybercrime memiliki tingkat kompleksitas tinggi dan sulit dideteksi, terutama bagi masyarakat yang tidak memiliki literasi teknologi informasi yang memadai.

Keamanan siber kemudian menjadi isu strategis di era transformasi digital. AI menawarkan solusi potensial melalui kemampuannya dalam memproses big data, mengenali pola serangan, dan memprediksi ancaman yang tidak terdeteksi oleh metode tradisional. Teknologi machine learning memungkinkan sistem keamanan untuk belajar secara otomatis dan merespons ancaman secara real-time. Namun, Widalala (2024) menekankan bahwa penerapan AI dalam keamanan siber juga menghadapi berbagai tantangan, mengingat serangan siber terus berkembang dan tidak semua teknik AI efektif untuk setiap jenis ancaman.

Oleh karena itu, diperlukan penelitian lanjutan untuk menentukan metode AI yang paling tepat dalam menghadapi beragam risiko siber.

Santoso (2023) menjelaskan bahwa keamanan siber berfokus pada perlindungan sistem, jaringan, perangkat, dan data melalui prinsip kerahasiaan, integritas, dan ketersediaan informasi. Ia menguraikan berbagai bentuk serangan modern seperti malware, botnet, Advanced Persistent Threat (APT), serangan terhadap perangkat IoT, dan zero-day attack yang menuntut sistem pertahanan adaptif dan otomatis. Santoso mengusulkan penggunaan arsitektur Risk-Centric Detection and Analysis (RCDA) yang mengintegrasikan intelijen ancaman, deteksi otomatis, serta teknologi blockchain pasca-kuantum untuk meningkatkan akuntabilitas. Ia juga menyoroti tingginya kerentanan perangkat IoT yang sering kali tidak memiliki standar keamanan memadai, sehingga memerlukan pendekatan seperti moving target defense dan intrusion detection system berbasis machine learning.

Pemanfaatan AI dalam konteks kejahatan juga melibatkan pengolahan big data, termasuk data pribadi sensitif. Hal ini meningkatkan risiko pelanggaran privasi, pencurian identitas, dan manipulasi informasi. Meskipun Indonesia telah memiliki UU PDP, implementasi perlindungan data dalam penggunaan AI—baik oleh negara maupun oleh pelaku kejahatan—masih memerlukan kajian mendalam. Penelitian ini bertujuan untuk memastikan bahwa pemanfaatan AI dalam penegakan hukum tetap menjunjung tinggi hak asasi manusia, khususnya terkait perlindungan privasi, bias algoritmik, dan potensi pengawasan massal.

Hanafi (2022) mengemukakan bahwa kejahatan siber muncul akibat kombinasi kelemahan sistem digital dan rendahnya literasi keamanan masyarakat. Berbagai bentuk serangan seperti phishing, DDoS, ransomware, botnet, dan spionase digital kerap menargetkan pengguna awam dan sistem yang tidak terlindungi. Dalam konteks forensik digital, penyidik dituntut untuk mampu mengumpulkan, menganalisis, dan mempertahankan bukti elektronik agar dapat diterima di pengadilan. Tanpa kemampuan forensik yang memadai, penegakan hukum akan kesulitan mengungkap kejahatan yang memanfaatkan enkripsi dan teknik penyamaran digital.

Di Indonesia, tindak kejahatan siber memiliki dampak signifikan terhadap individu, korporasi, maupun negara. Beberapa perbuatan tersebut melanggar ketentuan UU ITE Nomor 19 Tahun 2016, khususnya Pasal 28 ayat (1) terkait penyebaran informasi menyesatkan dan penipuan elektronik, serta Pasal 30 dan Pasal 32 mengenai akses dan pengambilan informasi elektronik tanpa izin. Data Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa ancaman siber terus meningkat secara signifikan. Pada periode Januari hingga Agustus 2021

tercatat 888 juta serangan siber, sementara pada Januari hingga Juli 2025 jumlahnya melonjak menjadi 3,64 miliar anomali trafik. Kondisi ini menegaskan bahwa ketahanan siber merupakan fondasi penting bagi keberlangsungan ekonomi digital dan stabilitas nasional.

Rumusan Masalah

1. Bagaimana perkembangan kecerdasan buatan (AI) memengaruhi pola dan modus operandi kejahatan siber di Indonesia?
2. Apa saja tantangan hukum dan penegakan hukum dalam menangani kejahatan siber berbasis AI?

B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (doctrinal research) yang berfokus pada kajian norma hukum terkait pemanfaatan kecerdasan buatan dalam penegakan hukum pidana, khususnya dalam konteks kejahatan siber di Indonesia. Penelitian bersifat deskriptif-analitis dengan tujuan tidak hanya menggambarkan fenomena hukum, tetapi juga menganalisis kesesuaian dan efektivitas regulasi yang berlaku terhadap perkembangan teknologi AI.

Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) dengan menelaah ketentuan hukum seperti UU ITE, UU Perlindungan Data Pribadi, dan regulasi keamanan siber, serta pendekatan konseptual (conceptual approach) untuk memahami prinsip dasar AI, forensik digital, dan perlindungan data pribadi. Bahan hukum yang digunakan terdiri dari bahan hukum primer, sekunder, dan tersier yang diperoleh melalui studi kepustakaan. Analisis dilakukan secara kualitatif dengan metode penalaran deduktif, yaitu menarik kesimpulan dari prinsip hukum dan konsep umum menuju penerapan spesifik dalam konteks kejahatan siber berbasis AI di Indonesia.

C. HASIL DAN PEMBAHASAN

1. Modus Operandi Tindak Kejahatan Siber (Cybercrime) di Indonesia

Pemanfaatan kecerdasan buatan (AI) telah membawa perubahan signifikan terhadap pola kejahatan siber, dari yang semula bersifat manual dan individual menjadi aktivitas yang terotomatisasi, terstruktur, dan berskala besar. Pelaku kejahatan kini menggunakan teknologi pembelajaran mesin untuk mengumpulkan data korban secara sistematis, menyusun skenario penipuan yang disesuaikan dengan bahasa, kebiasaan, serta konteks sosial target, dan melancarkan serangan yang dapat menjangkau ribuan korban dalam waktu singkat. Transformasi ini berdampak pada meningkatnya frekuensi serangan sekaligus besarnya kerugian yang ditimbulkan. Kejahatan siber tidak lagi dilakukan secara acak, melainkan

diarahkan kepada kelompok tertentu yang dinilai rentan, seperti pengguna layanan keuangan digital dan platform perdagangan elektronik, berdasarkan analisis big data terhadap perilaku pengguna (Nanci, 2025).

Di Indonesia, perkembangan tersebut tercermin dalam laporan Badan Siber dan Sandi Negara (BSSN) yang mencatat sebanyak 3,64 miliar serangan siber sepanjang Januari hingga Juli 2025. Sebagian besar serangan tersebut menunjukkan pola otomatisasi yang kuat, termasuk pemindaian sistem secara masif dan manipulasi data korban yang diduga melibatkan penggunaan AI. Hal ini mengindikasikan bahwa teknologi AI telah berkontribusi dalam mempercepat dan memperluas skala serangan siber di tingkat nasional.

Modus penipuan berbasis phishing dan kejahatan finansial juga mengalami evolusi signifikan. Praktik yang sebelumnya dilakukan melalui pengiriman pesan massal kini berkembang menjadi phishing berbasis AI yang bersifat personal, seperti spear-phishing dan skema pig-butchering. Selain itu, muncul pula vishing atau penipuan berbasis suara yang memanfaatkan teknologi sintesis suara dan rekayasa sosial tingkat lanjut. Dengan bantuan AI, pelaku mampu meniru suara figur yang dipercaya korban, merespons percakapan secara real-time, serta membangun skema penipuan jangka panjang yang dirancang untuk menumbuhkan kepercayaan korban secara bertahap. Pola ini terbukti meningkatkan tingkat keberhasilan kejahatan sekaligus memperpanjang durasi keterlibatan korban sebelum kejahatan terdeteksi (Wira, 2025).

Teknologi deepfake turut memperluas variasi modus kejahatan, terutama dalam kasus pencemaran nama baik, pemerasan, dan penipuan administratif. Pelaku menghasilkan konten audio maupun visual palsu yang sangat realistis sehingga sulit dibedakan dari materi asli. Konten tersebut digunakan untuk memanipulasi persepsi publik, menekan korban secara psikologis, atau memalsukan komunikasi resmi, seperti instruksi transfer dana yang seolah-olah berasal dari pejabat atau pimpinan perusahaan. Penyebaran deepfake juga mempercepat laju disinformasi yang berpotensi merusak reputasi individu maupun institusi. Tingginya kualitas konten sintetis ini memaksa penegak hukum dan penyedia platform digital untuk mengembangkan sistem deteksi otomatis, karena metode verifikasi manual tidak lagi memadai (Chiquita, 2024).

Dari perspektif hukum, pembuatan dan penggunaan deepfake yang bertujuan memanipulasi informasi agar tampak sebagai data autentik dapat dikenakan Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ketentuan ini

melarang setiap perbuatan manipulasi, penciptaan, perubahan, atau penghilangan Informasi Elektronik dan/atau Dokumen Elektronik dengan maksud agar dianggap seolah-olah sebagai data yang sah. Dalam konteks ini, deepfake memenuhi unsur perbuatan penciptaan dan manipulasi sebagaimana diatur dalam pasal tersebut.

Selain itu, AI juga memperkuat kemampuan malware dan botnet. Dengan mekanisme otomatisasi dan pembelajaran mandiri, malware modern mampu menyesuaikan diri dengan lingkungan target, menghindari sistem deteksi berbasis tanda tangan, serta menyebar melalui rantai eksploitasi yang adaptif. Pelaku juga memanfaatkan AI untuk mengoptimalkan serangan Distributed Denial of Service (DDoS), mengidentifikasi celah keamanan, dan mengeksploitasi kerentanan zero-day secara otomatis. Situasi ini menuntut penerapan sistem deteksi berbasis perilaku yang didukung machine learning serta percepatan pembaruan keamanan agar respons terhadap insiden dapat dilakukan secara lebih efektif (Fahmi, 2025).

Perubahan modus operandi kejahatan siber berbasis AI turut berdampak pada pembuktian digital dan proses forensik. Bukti elektronik kini bersifat lebih kompleks karena sering kali terenkripsi, tersebar pada berbagai platform dan layanan komputasi awan, serta mengalami modifikasi otomatis oleh sistem AI. Rekonstruksi peristiwa kejahatan memerlukan teknik forensik lanjutan, termasuk analisis terhadap model AI, penelusuran aktivitas agen terdistribusi, dan verifikasi keutuhan rantai data. Kompleksitas ini memperpanjang waktu penyidikan dan menuntut keahlian teknis tinggi untuk membedakan aktivitas AI yang bersifat ilegal dari penggunaan teknologi yang sah. Selain itu, diperlukan penyesuaian standar pembuktian agar bukti elektronik hasil manipulasi AI tetap dapat diterima dalam proses peradilan (Airlangga, 2025).

Lebih lanjut, perkembangan kejahatan berbasis AI menimbulkan tantangan regulatif dan kelembagaan. Sistem hukum pidana yang berlaku saat ini belum sepenuhnya mengakomodasi keberadaan entitas algoritmik, pembagian tanggung jawab antara pengembang, operator sistem, dan pengguna, serta mekanisme penanganan bukti digital yang dihasilkan oleh AI. Kondisi ini menyebabkan kesulitan dalam menentukan subjek hukum yang harus dimintai pertanggungjawaban. Untuk mengatasi kesenjangan tersebut, diperlukan pembaruan regulasi, pembentukan unit khusus penanganan kejahatan berbasis AI yang bersifat lintas disiplin, serta penguatan kerja sama internasional mengingat infrastruktur dan jejak serangan kerap berada di luar wilayah yurisdiksi nasional (Patricia, 2025).

Secara keseluruhan, kemajuan kecerdasan buatan telah mentransformasi kejahatan siber di Indonesia menjadi lebih cepat, kompleks, dan sulit ditelusuri. Pola serangan yang semakin

otomatis dan terpersonalisasi meningkatkan tantangan dalam upaya pencegahan dan penegakan hukum. Oleh karena itu, Indonesia perlu memperkuat literasi digital masyarakat, mengembangkan sistem keamanan berbasis AI, serta melakukan pembaruan regulasi hukum agar mampu mengatur dan menanggulangi kejahatan siber berbasis algoritma secara efektif. Sinergi antara pemerintah, aparat penegak hukum, sektor swasta, dan masyarakat menjadi elemen kunci dalam menjaga ketahanan siber nasional di era digital.

2. Tantangan Hukum dan Penegakan Hukum dalam Mengatasi Kejahatan Berbasis AI

Tantangan paling mendasar dalam penanganan kejahatan berbasis kecerdasan buatan terletak pada persoalan yurisdiksi dan pembuktian hukum. Kejahatan siber yang digerakkan oleh algoritma, seperti phishing terpersonalisasi dan malware adaptif, umumnya bersifat lintas batas negara (borderless crime). Karakter ini menyulitkan penentuan hukum yang berlaku serta mekanisme koordinasi penegakan hukum antarnegara. Pada tingkat nasional, ketiadaan regulasi khusus yang mengatur kecerdasan buatan dan pertanggungjawaban algoritmik menimbulkan hambatan dalam mengkualifikasikan perbuatan pidana yang sepenuhnya dijalankan oleh sistem otonom. Hukum pidana konvensional yang bertumpu pada unsur *mens rea* (niat jahat) dan *actus reus* (perbuatan fisik) menjadi sulit diterapkan ketika tindakan dilakukan oleh kode atau sistem cerdas yang beroperasi tanpa intervensi langsung manusia. Kondisi ini memunculkan problem konseptual mengenai subjek hukum dan bentuk pertanggungjawaban pidana dalam kejahatan berbasis AI.

Selain aspek normatif, tantangan signifikan juga muncul dalam ranah teknis pembuktian di pengadilan. Kejahatan yang melibatkan AI meninggalkan jejak digital yang kompleks, terenkripsi, dan sering kali tersembunyi melalui teknik penghilangan jejak yang canggih. Untuk mengungkapnya, dibutuhkan keahlian forensik digital tingkat lanjut guna melacak asal serangan dan mengidentifikasi aktor di balik sistem otonom. Bukti digital yang dihasilkan atau dimodifikasi oleh AI, seperti video deepfake atau data transaksi yang telah direkayasa, kerap sulit dibedakan dari data autentik. Hal ini menuntut penggunaan teknologi pendeteksi khusus serta pengembangan standar pembuktian baru yang mampu mengakomodasi karakteristik bukti berbasis AI. Keterbatasan sumber daya, baik dari sisi infrastruktur teknologi maupun minimnya aparat penegak hukum—hakim, jaksa, dan penyidik—yang memiliki kompetensi di bidang AI, semakin memperlambat proses penanganan perkara. Akibatnya, tidak sedikit kasus kejahatan berbasis AI yang berakhir tanpa kejelasan pertanggungjawaban hukum.

Permasalahan validitas alat bukti elektronik ini berkaitan erat dengan Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016. Dalam putusan tersebut, Mahkamah

menegaskan bahwa bukti elektronik hanya dapat dinyatakan sah secara hukum apabila diperoleh melalui prosedur yang sah (*lawful interception*) oleh aparat penegak hukum. Ketentuan ini menjadi tantangan tersendiri dalam kejahatan berbasis AI, mengingat bukti sering tersimpan di server publik atau layanan komputasi awan yang berada di luar yurisdiksi nasional. Kesulitan akses prosedural terhadap data lintas negara berpotensi membuat bukti elektronik dianggap tidak memenuhi syarat formil dan dikesampingkan dalam proses peradilan.

Menghadapi kondisi tersebut, diperlukan strategi penegakan hukum pidana yang adaptif melalui reformasi kelembagaan dan prosedural. Strategi ini menekankan pada peningkatan kapasitas aparat penegak hukum guna memperkecil kesenjangan pengetahuan antara pelaku kejahatan dan aparat. Penyidik kepolisian serta jaksa penuntut umum perlu mendapatkan pelatihan intensif mengenai cara kerja sistem AI, khususnya yang berkaitan dengan teknologi deepfake dan malware yang bersifat evasif. Penguasaan terhadap perangkat forensik digital berbasis AI menjadi penting agar aparat mampu mendeteksi manipulasi media dan data yang semakin kompleks. Selain itu, pembentukan unit khusus di lingkungan kepolisian dan kejaksaan yang bersifat multidisiplin—menggabungkan keahlian hukum, data science, dan keamanan siber—menjadi kebutuhan mendesak. Unit ini berperan dalam mengumpulkan, menganalisis, dan menyajikan bukti berbasis AI agar dapat diterima secara sah di pengadilan. Mengingat sifat kejahatan siber yang tidak mengenal batas wilayah, penguatan kapasitas juga harus diiringi dengan kerja sama internasional, termasuk pertukaran *threat intelligence* dan metodologi investigasi terhadap kejahatan berbasis AI.

Koordinasi lintas negara menjadi salah satu tantangan terbesar dalam penegakan hukum terhadap kejahatan siber berbasis AI. Sistem kejahatan yang digerakkan oleh algoritma sering beroperasi secara global, dengan pelaku, infrastruktur, dan server yang tersebar di berbagai yurisdiksi. Ketika penyidikan melibatkan data lintas negara, penegakan hukum kerap terhambat oleh perbedaan regulasi, keterbatasan akses informasi, serta kompleksitas mekanisme ekstradisi. Oleh karena itu, diperlukan integrasi mekanisme berbagi intelijen secara real-time antar lembaga penegak hukum internasional, disertai peningkatan kapasitas analitik berbasis AI untuk mendeteksi pola kejahatan yang berlangsung secara simultan di berbagai wilayah. Kolaborasi internasional ini menjadi instrumen kunci dalam menutup celah hukum yang kerap dimanfaatkan oleh pelaku kejahatan siber transnasional (Interpol, 2025).

Pada tingkat nasional, tantangan lainnya berkaitan dengan kesiapan infrastruktur keamanan digital dan kualitas sumber daya manusia. Masih banyak institusi penegak hukum

yang belum memiliki sistem deteksi dan respons insiden berbasis AI yang terintegrasi. Kondisi ini menyebabkan proses pengumpulan bukti elektronik sering mengalami keterlambatan atau bahkan kehilangan jejak digital akibat keterbatasan teknis. Oleh karena itu, peningkatan kapasitas teknologi penegakan hukum perlu dilakukan melalui penguatan *Security Operation Center* serta pemanfaatan perangkat analitik prediktif. Di samping itu, literasi keamanan digital bagi aparat penegak hukum harus ditingkatkan, tidak hanya sebatas kemampuan menggunakan teknologi, tetapi juga pemahaman mendalam terhadap logika dan cara kerja algoritma yang dimanfaatkan oleh pelaku kejahatan (Taufik, 2024).

Pembaruan hukum nasional menjadi langkah strategis untuk menyesuaikan sistem hukum dengan realitas baru yang dihadirkan oleh kecerdasan buatan. Hukum pidana perlu mengembangkan konsep pertanggungjawaban yang mampu menjangkau entitas algoritmik melalui mekanisme pertanggungjawaban tidak langsung, seperti *vicarious liability* terhadap pengembang, penyedia, atau pengendali sistem AI. Dengan demikian, pihak-pihak yang memiliki kendali atas sistem AI tetap dapat dimintai pertanggungjawaban atas dampak hukum yang ditimbulkan. Pembentukan regulasi yang jelas mengenai batas tanggung jawab, mekanisme pengawasan algoritma, serta standar audit etis AI perlu dilakukan secara terpadu. Selain itu, sinkronisasi antara hukum siber dan hukum pidana umum menjadi penting untuk mencegah terjadinya kekosongan hukum dalam penanganan kejahatan yang melibatkan teknologi kecerdasan buatan (Erry, 2025).

D. KESIMPULAN

Kecerdasan buatan (AI) telah membawa perubahan besar terhadap pola dan modus operandi kejahatan siber di Indonesia. Kejahatan yang sebelumnya dilakukan secara manual kini bertransformasi menjadi otomatis, masif, dan sangat personal. Pelaku memanfaatkan teknologi seperti *deepfake, phishing* berbasis pembelajaran mesin, serta malware adaptif untuk menipu korban dan menghindari deteksi. Pola serangan ini menunjukkan bahwa AI tidak hanya mempercepat dan memperluas jangkauan kejahatan, tetapi juga memperumit proses identifikasi serta pembuktian hukum. Dalam konteks ini, Indonesia perlu memperkuat sistem keamanan digital berbasis AI, meningkatkan literasi digital masyarakat, dan memperbarui regulasi agar mampu mengatur aktivitas kriminal yang melibatkan teknologi cerdas secara efektif dan berkeadilan.

Namun, penanggulangan kejahatan berbasis AI menghadapi tantangan besar, baik dari aspek hukum maupun teknis. Belum adanya aturan spesifik mengenai tanggung jawab algoritma, keterbatasan kemampuan aparat dalam forensik digital, serta lemahnya koordinasi lintas negara menjadi hambatan utama dalam penegakan hukum. Oleh karena itu, strategi yang diperlukan mencakup pembentukan unit khusus penanganan kejahatan AI, peningkatan kapasitas teknis aparat penegak hukum, serta pembaruan kerangka hukum melalui prinsip *vicarious liability* yang menempatkan pengembang dan pengguna AI sebagai pihak bertanggung jawab. Kolaborasi antara pemerintah, lembaga internasional, dan masyarakat menjadi kunci dalam menciptakan sistem hukum yang adaptif, tangguh, dan mampu menghadapi ancaman kejahatan digital di era kecerdasan buatan.

E. DAFTAR PUSTAKA

Astuti, S. A. (2024). Literasi kemanfaatan teknologi terhadap cyber terrorism di era disrupsi dengan artificial intelligence. Indonesian Journal of Criminal Law and Criminology (IJCLC), 5(3).

Banfatin, P. M., Medan, K. K., & Fallo, D. F. N. G. (2025). Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake dalam melakukan tindak pidana cybercrime. Pemuliaan Keadilan, 2(1), 60–73.

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. Jurnal Wawasan Yuridika, 5(2), 177–199.

Djulaeka, & Rahayu, D. (2020). Buku ajar: Metode penelitian hukum. Scopindo Media Pustaka.

Efendi, F. M., Hadi, F., & Pratama, S. (2025). Analisis dan perancangan sistem pendeteksian phishing berbasis AI pada platform WhatsApp dengan pendekatan bahasa lokal Surabaya. Karsa Nusantara, 2, 267–275.

Fitrya, E., Primadhany, F., Rosita, D., Kudus, M., Ahza, & Musthofa, A. (2025). Pengantar hukum siber Indonesia. Banten.

Hanafi. (2022). Dasar cyber security dan forensic. CV Budi Utama.

Husamuddin, M. Z., et al. (2024). Hukum acara pidana dan pidana siber: Buku ajar.

INTERPOL. (2025). INTERPOL Africa cyberthreat assessment report 2025 (4th ed.).

Kurnia, I. (2024). Hukum pidana siber: Aspek teoretis dan praktis dalam era digital di Indonesia. CV Eureka Media Aksara.

Munajat, A. A., & Yusuf, H. (2024). Peran teknologi informasi dalam pencegahan dan

pengungkapan tindak pidana ekonomi khusus: Studi tentang kejahatan keuangan berbasis digital. Jurnal Intelek Insan Cendikia, 1(9), 4853–4865.

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi deepfake di Indonesia sebagai bentuk pelindungan negara. USM Law Review, 7(2), 603–621.

Nurhidayat, T. (2024). Kajian ketahanan siber: Manajemen kerentanan. Politeknik Siber dan Sandi Negara.

Nursiaga, R., et al. (2025). Model jaringan neural untuk deteksi anomali pada sistem keamanan siber: Rancangan, implementasi, dan analisis. JAREKOM: Jurnal Jaringan dan Rekayasa Komputer, 1(1), 1–11.

Putera, A., & Jannah, M. (2025). Rekonstruksi peran digital forensik dalam penyidikan tindak pidana siber: Analisis kritis terhadap konstruksi hukum pidana di Indonesia. Jurnal Tana Mana, 6(2), 289–296.

Putusan Mahkamah Agung Republik Indonesia Nomor 132 K/Pid.Sus/2023 tentang deepfake dan penyebaran konten berbahaya. (2023).

Putusan Pengadilan Negeri Jakarta Pusat Nomor 123/Pid.Sus/2024 tentang phishing berbasis AI pada platform digital. (2024).

Putusan Pengadilan Tinggi Denpasar Nomor 45/Pid.Sus/2024 tentang cyber terrorism dengan elemen artificial intelligence. (2024).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). (2024). Official Journal of the European Union, L 168/1.

Respati, A. A. (2024). Reformulasi UU ITE terhadap artificial intelligence dibandingkan dengan Uni Eropa dan China AI Act regulation. USM Law Review, 7(3), 1737–1758.

Santoso, J. T. (2023). Teknologi keamanan siber. Yayasan Prima Agus Teknik.

Savitri, A. (2019). Revolusi industri 4.0: Mengubah tantangan menjadi peluang di era disrupsi 4.0. Penerbit Genesis.

Simbolon, N. Y. (2025). Ancaman cybercrime di Indonesia: Tinjauan sistematis dan peran cybersecurity pada e-commerce dalam hukum pidana. Inovasi: Jurnal Sosial Humaniora dan Pendidikan, 4(2), 815–825. https://doi.org/10.55606/inovasi.v4i2.4425

Sinaga, N. H., Irmayani, D., & Hasibuan, M. N. S. (2024). Mengoptimalkan keamanan jaringan memanfaatkan kecerdasan buatan untuk meningkatkan deteksi dan respons ancaman. Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), 7(2), 364–369.

Suhaimi. (2018). Problem hukum dan pendekatan dalam penelitian hukum normatif. Jurnal

Yustitia, 19(2).

Taufik, R. (2025). Systematic literature review: Teknik deteksi serangan siber berbasis AI dan data mining. AT-TAKLIM: Jurnal Pendidikan Multidisiplin, 2(2), 158–169.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). Lembaran Negara Republik Indonesia Tahun 2022 Nomor 155.

United States v. Nosal, 676 F.3d 854 (9th Cir.). (2016).

Wahyudi, B. R. (2025). Tantangan penegakan hukum terhadap kejahatan berbasis teknologi AI. INNOVATIVE: Journal of Social Science Research, 5(1), 3436–3450.

Wibowo, A. (2024). Hukum siber dan keamanan informasi.

Widalala, R. R., et al. (2024). Dampak penggunaan artificial intelligence pada keamanan siber: Kajian terhadap potensi keuntungan dan ancaman. Berajah Journal, 4(8), 1541–1550.