JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 6, Desember 2025 – Januari 2026
E-ISSN : 3046-4560

# Pengaruh Teknologi Ai Terhadap Evolusi Modus Kejahatan Siber Di Indonesia Tahun 2024–2025 Dan Implikasinya Terhadap Penegakan Hukum

## *The Impact Of Artificial Intelligence Technology On The Evolution Of Cybercrime Modus Operandi In Indonesia (2024–2025) And Its Implications For Law Enforcement*

**Muhamad Nur Ismail**
Fakultas Hukum Universitas Bung Karno
*Email: mni2017cpa@gmail.com*

Article Info

Article history :
Received : 18-12-2025
Revised : 20-12-2025
Accepted : 22-12-2025
Pulished : 24-12-2025

***Abstract***

*The rapid development of Artificial Intelligence (AI) technology during the 2024–2025 period has significantly transformed the patterns and modalities of cybercrime in Indonesia, characterized by increased complexity, automation, and greater challenges in legal proof. This situation poses serious challenges to the national law enforcement system, which was largely designed to address conventional forms of cybercrime. Accordingly, this study aims to examine the impact of AI technology on the evolution of cybercrime modes in Indonesia and its implications for law enforcement, focusing on four main aspects: the identification of new forms of AI-based cybercrime, the readiness and effectiveness of law enforcement institutions, the adequacy and adaptability of the national legal framework, and the development of an adaptive, ethical, and preventive legal policy model. This research employs a qualitative method using a normative juridical approach supported by limited empirical analysis. Data were collected through a literature review of statutory regulations, academic journal articles, official government reports, policy documents, and relevant cybercrime cases occurring in Indonesia during the 2024–2025 period. The data were analyzed descriptively and analytically to examine the relationship between advancements in AI technology, the evolution of cybercrime methods, and the responses of the legal system. The findings indicate that AI has given rise to new forms of cybercrime in Indonesia, including deepfake-based fraud, machine learning–driven adaptive phishing, AI-generated ransomware, and the exploitation of personal data through automated systems. The study also reveals that although law enforcement institutions have demonstrated improved institutional capacity, their effectiveness in responding to AI-based cybercrime remains constrained by limited human resources, insufficient AI-focused forensic capabilities, and suboptimal inter-agency coordination. From a regulatory perspective, the Information and Electronic Transactions Law as amended by Law No. 1 of 2024, together with the Personal Data Protection Law, provides a sufficient legal foundation; however, it has not yet fully adapted to the autonomous and complex characteristics of AI-driven cybercrime. This study concludes that addressing AI-based cybercrime requires a transformation of legal and policy approaches toward more adaptive, preventive, and risk-oriented frameworks, emphasizing regulatory harmonization, the strengthening of AI forensic capacities, and cross-sector collaboration. Future research is recommended to pursue more in-depth empirical studies on law enforcement practices and evidentiary challenges in AI-based cybercrime cases, as well as to formulate a more comprehensive national regulatory framework for AI within the Indonesian legal context.*

***Keywords : Artificial Intelligence (AI), Cybercrime, Law Enforcement***

**Abstrak**

Perkembangan pesat teknologi *Artificial Intelligence* (AI) pada periode 2024–2025 telah membawa perubahan signifikan terhadap pola dan modus kejahatan siber di Indonesia, yang ditandai dengan meningkatnya kompleksitas, otomatisasi, dan kesulitan pembuktian hukum. Kondisi ini menimbulkan tantangan serius bagi sistem penegakan hukum nasional yang pada dasarnya dibangun untuk merespons kejahatan siber konvensional. Oleh karena itu, penelitian ini bertujuan untuk menganalisis pengaruh teknologi AI terhadap evolusi modus kejahatan siber di Indonesia serta implikasinya terhadap penegakan hukum, dengan fokus pada empat aspek utama yaitu identifikasi bentuk-bentuk baru kejahatan siber berbasis AI, kesiapan dan efektivitas lembaga penegak hukum, kecukupan dan adaptabilitas kerangka hukum nasional, serta pengembangan model pendekatan kebijakan hukum yang adaptif, etis, dan preventif. Penelitian ini menggunakan metode kualitatif dengan pendekatan yuridis normatif yang didukung oleh analisis empiris terbatas. Data dikumpulkan melalui studi kepustakaan terhadap peraturan perundang-undangan, artikel jurnal akademik, laporan resmi lembaga negara, serta dokumen kebijakan dan kasus kejahatan siber relevan pada periode 2024–2025. Teknik analisis dilakukan secara deskriptif-analitis untuk mengkaji keterkaitan antara perkembangan teknologi AI, perubahan modus kejahatan siber, dan respons sistem hukum. Hasil penelitian menunjukkan bahwa AI telah melahirkan modus kejahatan siber baru di Indonesia, seperti *deepfake-based fraud*, *phishing adaptif* berbasis *machine learning*, AI-*generated ransomware*, dan eksploitasi data pribadi melalui sistem otomasi cerdas. Temuan juga mengungkap bahwa meskipun lembaga penegak hukum telah menunjukkan peningkatan kapasitas institusional, efektivitas respons terhadap kejahatan siber berbasis AI masih terkendala oleh keterbatasan sumber daya manusia, teknologi forensik AI, dan koordinasi lintas lembaga. Dari sisi regulasi, UU ITE sebagaimana diubah dengan UU Nomor 1 Tahun 2024 dan UU Perlindungan Data Pribadi dinilai cukup sebagai dasar hukum, namun belum sepenuhnya adaptif terhadap karakter kejahatan berbasis AI yang bersifat otonom dan kompleks. Penelitian ini menyimpulkan bahwa penanganan kejahatan siber berbasis AI memerlukan transformasi pendekatan hukum dan kebijakan yang lebih adaptif, preventif, dan berorientasi pada risiko, dengan menekankan harmonisasi regulasi, penguatan forensik AI, serta kolaborasi lintas sektor. Penelitian selanjutnya disarankan untuk mengembangkan kajian empiris yang lebih mendalam mengenai praktik penegakan hukum dan pembuktian kejahatan siber berbasis AI, serta merumuskan kerangka regulasi AI yang lebih komprehensif dalam konteks hukum nasional Indonesia.

***Kata kunci:*** **Kecerdasan Buatan, Kejahatan Siber, Penegakan Hukum**

## PENDAHULUAN

Dalam kurun waktu dua tahun terakhir, yakni periode 2024–2025, Indonesia mengalami peningkatan tajam kejahatan siber yang tidak lagi mengandalkan metode konvensional, melainkan memanfaatkan teknologi *Artificial Intelligence* (AI). Kondisi ini mencerminkan pergeseran struktural dari pola *cybercrime* tradisional menuju *AI-driven cybercrime*, di mana kecerdasan buatan digunakan untuk menjalankan serangan secara otomatis, memanipulasi data secara masif, serta memproduksi deepfake sebagai sarana penipuan digital. Peristiwa peretasan data Badan Pemeriksa Keuangan (BPK) serta kebocoran data pengguna *platform e-commerce* yang melibatkan entitas dengan *machine learning attack* model memperlihatkan bahwa ancaman siber saat ini bersifat adaptif, otonom, dan semakin sulit dideteksi melalui pendekatan forensik konvensional (Syahril dkk, 2025).

Fenomena tersebut tidak dapat dilepaskan dari dinamika sosial yang lebih luas dalam masyarakat digital Indonesia yang sedang bergerak menuju *fase Society* 5.0, yaitu tahap integrasi intensif antara ruang fisik dan ruang digital. Khuan, Paminto, dan Salmon (2025) menjelaskan bahwa perkembangan AI tidak hanya membentuk ulang perilaku sosial masyarakat, tetapi juga melahirkan pola-pola kriminalitas baru yang secara langsung menantang konstruksi hukum klasik

(Khuan, dkk, 2025). Praktik seperti *AI phishing*, *otomasi botnet, serta ransomware* berbasis *generative AI* kini menjadi bagian integral dari ekosistem kejahatan siber di Indonesia.

Implikasi sosial dari perkembangan ini tidak hanya berdampak pada individu sebagai korban, tetapi juga memberikan tekanan signifikan terhadap institusi penegak hukum yang dituntut untuk beradaptasi dengan kompleksitas baru dalam penegakan hukum siber. Satoto dan Santiago (2025) mencatat bahwa meskipun Indonesia telah melakukan pembaruan regulasi melalui UU No. 1 Tahun 2024 Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022), implementasi norma hukum terhadap kejahatan siber berbasis AI masih menghadapi hambatan adaptasi, baik dari sisi teknis maupun konseptual (Satoto dkk, 2025).

Persoalan semakin kompleks ketika ditinjau dari dimensi kebijakan dan kapasitas kelembagaan. Strategi nasional keamanan siber Indonesia belum sepenuhnya memasukkan kerangka analisis risiko AI secara komprehensif (Praditya dkk, 2023). Pola penegakan hukum yang berjalan masih cenderung bersifat reaktif, bukan prediktif, padahal sistem AI dalam konteks kejahatan siber bersifat dinamis, mampu melakukan pembelajaran mandiri, serta beradaptasi terhadap pola intervensi manusia. Kondisi ini menyebabkan aparat penegak hukum kerap tertinggal dari laju inovasi modus kriminal digital.

Temuan Rohimi (2025) semakin menegaskan bahwa regulasi nasional belum menunjukkan tingkat adaptivitas yang memadai dalam merespons potensi pelanggaran hukum pidana berbasis AI. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), misalnya masih berorientasi pada subjek hukum manusia dan belum secara eksplisit mengakomodasi keberadaan entitas otonom seperti AI agents. Kekosongan normatif ini memunculkan problem yuridis baru, khususnya terkait penentuan tanggung jawab hukum ketika tindakan melawan hukum dilakukan oleh sistem AI berdasarkan *autonomous decision*.

Permasalahan penegakan hukum kian rumit ketika dihadapkan pada dimensi etika dan perlindungan hak asasi digital. Penerapan hukum yang bersifat terlalu represif berpotensi menghambat inovasi teknologi, sedangkan pendekatan yang terlalu longgar justru membuka ruang lebih luas bagi berkembangnya kejahatan digital (Rohimi, 2025). Oleh karena itu, diperlukan formulasi kebijakan yang mampu menyeimbangkan kepentingan perlindungan hukum, kebebasan berinovasi, serta kepentingan keamanan siber nasional secara proporsional.

Dari sudut pandang keamanan publik, persoalan ini tidak dapat dipisahkan dari ancaman terhadap stabilitas nasional. Eskalasi kejahatan siber berbasis AI telah berkembang menjadi isu keamanan nasional, terutama karena pelaku kerap memanfaatkan AI *anonymization tools* untuk menyamarkan identitas lintas yurisdiksi negara (Abast dkk, 2025). Dalam kondisi demikian, institusi kepolisian di Indonesia dihadapkan pada tantangan serius untuk meningkatkan kapasitas literasi digital serta kemampuan forensik berbasis big data guna menelusuri pola kejahatan yang semakin kompleks.

Efektivitas penyidikan tindak pidana siber sangat ditentukan oleh tingkat kolaborasi antara masyarakat, sektor swasta, dan aparat penegak hukum (Zulyadi dkk, 2025). Konsep *community policing* digital dipandang sebagai pendekatan yang relatif efektif dalam upaya pencegahan dini dan deteksi kejahatan yang melibatkan teknologi AI. Namun demikian, implementasi sinergi tersebut

masih belum optimal akibat lemahnya koordinasi antar lembaga serta ketiadaan regulasi yang mengatur interoperabilitas data secara memadai.

Di sisi regulasi, Haditama dan Sugianto (2025) mencatat bahwa Indonesia mulai merancang kerangka *AI Law* sebagai upaya untuk menjamin akuntabilitas korporasi atas pemanfaatan AI dalam aktivitas yang berpotensi memicu kejahatan siber. Kendati demikian, jika dibandingkan dengan Uni Eropa yang telah menerapkan *EU AI Act*, pengaturan di Indonesia masih terfragmentasi dan belum terintegrasi dalam satu kerangka hukum pidana siber yang komprehensif (Haditama dkk, 2025).

Sementara itu, gagasan *Prophetic Cyber Law* yang diperkenalkan oleh Setyoningsih dan Farid (2025) menawarkan perspektif alternatif dalam penegakan hukum siber nasional dengan menitikberatkan pada internalisasi nilai-nilai etika, moral, dan spiritual dalam penggunaan teknologi AI (Setyoningsih dkk, 2025). Pendekatan ini menarik untuk dikaji lebih lanjut karena menempatkan aspek humanisasi sebagai fondasi penting dalam ekosistem digital yang semakin terdorong oleh otomasi dan kecerdasan buatan.

Walaupun berbagai kajian telah dilakukan, celah penelitian masih terlihat jelas, khususnya terkait analisis evolusi modus kejahatan siber akibat integrasi AI di Indonesia serta dampaknya terhadap model penegakan hukum yang bersifat adaptif. Sebagian besar penelitian sebelumnya cenderung berfokus pada dimensi regulatif atau teknologis semata, sementara keterkaitan antara perubahan modus kejahatan dan kesiapan kapasitas penegak hukum belum banyak dikaji secara empiris dan kualitatif.

Dengan demikian, penelitian ini memiliki tingkat urgensi yang tinggi baik secara akademik maupun sosial. Dari sisi keilmuan, kajian ini diharapkan dapat memperkaya diskursus hukum pidana dan studi keamanan digital melalui pendekatan sosioteknologis yang menjelaskan peran AI dalam membentuk dinamika baru kejahatan siber. Secara praktis, temuan penelitian ini diharapkan mampu memberikan landasan rekomendasi bagi pembuat kebijakan dan aparat penegak hukum dalam merumuskan strategi yang adaptif dan preventif guna memperkuat keamanan siber nasional Indonesia pada periode 2024–2025 dan masa yang akan datang.

## METODELOGI PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif dengan tujuan utama untuk memahami secara mendalam makna, dinamika, serta kompleksitas fenomena sosial dan hukum yang timbul akibat pengaruh teknologi *Artificial Intelligence* (AI) terhadap kejahatan siber dan praktik penegakan hukum di Indonesia. Pemilihan pendekatan kualitatif didasarkan pada kebutuhan untuk mengeksplorasi realitas sosial secara komprehensif, bukan untuk menguji atau mengukur hubungan numerik antarvariabel, melainkan untuk menelusuri pola, proses interaksi, serta konstruksi makna yang dibangun oleh pelaku kejahatan, korban, dan aparat penegak hukum dalam menghadapi fenomena tersebut.

Sebagaimana dikemukakan oleh Creswell (2018), pendekatan kualitatif relevan digunakan untuk mengkaji fenomena yang belum sepenuhnya terkonseptualisasi, khususnya dalam konteks sosial yang mengalami perubahan cepat akibat kemajuan teknologi. Atas dasar itu, penelitian ini diarahkan untuk membangun pemahaman konseptual yang lebih utuh mengenai bagaimana AI berkontribusi terhadap perubahan modus kejahatan siber sekaligus bagaimana sistem hukum merespons transformasi tersebut.

Secara metodologis, penelitian ini menggunakan pendekatan deskriptif dengan metode studi kasus (*case study descriptive approach*). Pendekatan ini dimaksudkan untuk menyajikan gambaran mendalam atau thick description mengenai pemanfaatan teknologi AI dalam praktik kejahatan siber di Indonesia, serta respons lembaga penegak hukum dalam menanganinya melalui telaah empiris terhadap sejumlah kasus konkret yang terjadi pada periode 2024–2025.

Fokus studi kasus diarahkan pada peristiwa-peristiwa aktual dan representatif yang mencerminkan relasi antara AI dan kejahatan digital, antara lain kasus penipuan berbasis *deepfake* dan pencurian identitas digital, kebocoran data yang melibatkan *algoritma machine learning attack*, serangan *ransomware* yang dihasilkan oleh sistem AI terhadap lembaga keuangan, serta praktik investigasi digital yang dilakukan oleh BSSN dan Polri dengan memanfaatkan sistem analisis forensik berbasis AI. Melalui pemilihan kasus-kasus tersebut, penelitian ini berupaya menelusuri faktor internal dan eksternal yang mendorong evolusi kejahatan siber berbasis AI sekaligus menilai efektivitas respons hukum yang diterapkan.

Metode penelitian yang digunakan merujuk pada studi kasus kualitatif deskriptif. Metode ini dipilih karena memungkinkan peneliti untuk menggali secara mendalam fenomena yang bersifat kompleks dan kontekstual, menganalisis dinamika sosial dan hukum yang tidak dapat direduksi ke dalam ukuran kuantitatif, serta menjelaskan relasi sebab-akibat secara kontekstual, bukan statistik. Dengan demikian, pendekatan ini berpotensi melahirkan teori substantif atau kerangka konseptual baru yang relevan dengan realitas empiris (Yin, 2019).

Sumber data utama dalam penelitian ini diperoleh melalui studi literatur yang mencakup jurnal akademik, peraturan perundang-undangan, laporan resmi BSSN, serta publikasi Kominfo. Selain itu, dilakukan pula analisis terhadap dokumen hukum dan kebijakan seperti UU ITE, UU No. 1 Tahun 2024, UU Perlindungan Data Pribadi, dan Rancangan Undang-Undang AI. Seluruh data yang terkumpul selanjutnya dianalisis dengan menggunakan teknik analisis tematik (*thematic analysis*) dan analisis komparatif kontekstual. Melalui teknik ini, peneliti mengidentifikasi pola, tema, serta relasi yang signifikan dan relevan dengan rumusan masalah serta pertanyaan penelitian yang diajukan.

Pendekatan deskriptif berbasis studi kasus dipilih dengan sejumlah pertimbangan metodologis. Pertama, fenomena kejahatan siber yang melibatkan teknologi *Artificial Intelligence* (AI) bersifat dinamis dan sangat bergantung pada konteks, sehingga tidak mudah disederhanakan ke dalam ukuran kuantitatif. Kedua, orientasi penelitian ini diarahkan untuk menjawab pertanyaan mengenai bagaimana dan mengapa suatu fenomena terjadi, bukan semata-mata menghitung besaran pengaruhnya secara statistik. Ketiga, karakteristik kasus kejahatan siber di Indonesia memiliki dimensi sosial, hukum, dan teknologi yang khas serta tidak selalu sejalan dengan pengalaman negara lain, sehingga diperlukan pendekatan yang mampu menangkap kompleksitas konteks lokal secara mendalam. Keempat, metode studi kasus memberikan ruang untuk menggali makna sosial dan penafsiran hukum dari para aktor yang terlibat dalam penegakan hukum siber, sesuatu yang tidak dapat sepenuhnya diungkap melalui survei kuantitatif.

Penelitian ini memanfaatkan data kualitatif, yaitu data non-numerik yang bersifat deskriptif, naratif, dan kontekstual. Pengumpulan data diarahkan untuk memperoleh pemahaman mendalam mengenai fenomena sosial, hukum, dan teknologi yang diteliti, bukan untuk menguji hubungan statistik antarvariabel, melainkan untuk menjelaskan proses, makna, serta implikasi sosial-hukum

dari pengaruh teknologi AI terhadap kejahatan siber. Jenis data yang digunakan mencakup data primer dan data sekunder. Data primer yang merupakan bahan hukum yang mengikat berupa peraturan perundang-undangan antara lain UU ITE, UU Nomor 1 Tahun 2024 Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan UU Perlindungan Data Pribadi. Sementara itu, data sekunder bersumber yaitu bahan-bahan yang menunjang bahan hukum primer berupa karya-karya ilmiah dan hasil penelitian para ahli hukum, antara lain laporan resmi lembaga pemerintah seperti BSSN dan Kominfo, artikel jurnal akademik, putusan pengadilan terkait perkara siber, dan laporan investigatif dari media yang kredibel.

## PEMBAHASAN

Sebelum memasuki analisis yang lebih mendalam, perlu dikemukakan kerangka teoretis yang relevan sebagai landasan konseptual penelitian ini, salah satunya adalah teori kriminologi teknologi (*Technological Criminology Theory*). Teori yang dikembangkan oleh David Wall (2007, 2020) ini menjelaskan bahwa perkembangan teknologi digital telah melahirkan tipe-tipe kriminalitas baru yang dikenal sebagai *cyber-dependent crimes*, yakni bentuk kejahatan yang keberadaannya sangat bergantung pada teknologi, baik sebagai alat maupun sebagai objek tindak pidana (Wall, 2020).

Wall menegaskan bahwa ketika kecerdasan buatan dimanfaatkan untuk mempermudah atau mengoptimalkan tindakan kriminal, AI berperan sebagai *criminal enabler*. Dalam konteks Indonesia, perspektif ini membantu menjelaskan bahwa pemanfaatan machine learning dan teknologi deepfake dalam praktik penipuan digital merupakan wujud konkret dari teknologi yang memperluas peluang dan skala kejahatan, sementara kapasitas regulasi dan penegakan hukum belum berkembang secara seimbang dengan laju inovasi tersebut (Dharmayanti dkk, 2025).

Kerangka teoritis lain yang relevan adalah *Routine Activity Theory* (RAT) yang diperkenalkan oleh Cohen dan Felson (1979). Teori ini berpijak pada asumsi bahwa kejahatan terjadi ketika tiga unsur utama hadir secara bersamaan, yaitu adanya pelaku yang termotivasi, target yang layak, dan ketiadaan penjaga yang efektif (*absence of capable guardians*). Dalam konteks kejahatan siber berbasis AI, konsep pelaku tidak lagi terbatas pada manusia, melainkan juga mencakup *autonomous agents*, sementara target berwujud data dan sistem digital, serta penjaga direpresentasikan oleh mekanisme keamanan siber dan perangkat regulasi hukum (Cohen dkk, 1979). Kehadiran AI secara signifikan memperluas jangkauan kejahatan melalui otomatisasi tindakan kriminal, seperti *phishing* dan *botnet attacks*.

Selanjutnya, Teori Hukum Responsif yang dikemukakan oleh Nonet dan Selznick (1978) menekankan bahwa sistem hukum idealnya mampu beradaptasi terhadap perubahan sosial dan perkembangan teknologi dengan tetap mengedepankan keadilan substantif (Nonet dkk, 1978). Dalam ekosistem digital, hukum tidak cukup diposisikan sebagai instrumen pengendalian formal semata, melainkan juga berfungsi sebagai *facilitator of innovation* sekaligus *protector of digital justice*. Hukum siber di Indonesia masih cenderung bersifat reaktif dan belum sepenuhnya bergerak menuju karakter hukum yang responsif terhadap tantangan teknologi AI.

Kerangka berikutnya adalah Teori Keamanan Digital Nasional atau *Cybersecurity Governance Theory. Praditya* et al. (2023) memandang bahwa keamanan digital tidak dapat direduksi sebagai persoalan teknis belaka, melainkan mencakup dimensi politik, hukum, dan sosial.

Pendekatan ini menekankan pentingnya koordinasi lintas aktor, termasuk negara, sektor swasta, dan masyarakat, dalam membangun ekosistem hukum yang tangguh dan resilien terhadap ancaman siber yang dipicu oleh pemanfaatan teknologi AI (Praditya dkk, 2023).

**Perkembangan Dan Bentuk-Bentuk Baru Modus Kejahatan Siber Di Indonesia Pada Tahun 2024–2025 Dipengaruhi Oleh Kemajuan Teknologi *Artificial Intelligence* (AI)**

Periode 2024–2025 menandai munculnya perkembangan signifikan sekaligus diversifikasi modus kejahatan siber di Indonesia yang dipengaruhi secara langsung oleh kemajuan teknologi *Artificial Intelligence* (AI). Transformasi ini tercermin dalam berbagai bentuk kejahatan digital yang semakin kompleks, adaptif, dan sulit dideteksi melalui pendekatan konvensional. Salah satu contoh paling menonjol adalah meningkatnya kasus *deepfake-based fraud* dan penipuan identitas digital. Sejak tahun 2024, Indonesia mengalami eskalasi tajam kejahatan digital yang memanfaatkan teknologi *deepfake*, yakni penggunaan algoritma AI untuk memanipulasi wajah, suara, maupun citra individu agar terlihat autentik. Teknologi ini bekerja dengan memanfaatkan *Generative Adversarial Networks* (GANs) yang mampu menghasilkan representasi visual dan audio yang nyaris tidak dapat dibedakan dari materi asli (Goodfellow et al., 2014). Laporan Badan Siber dan Sandi Negara (BSSN) dalam Laporan Keamanan Siber Nasional 2024 menunjukkan bahwa insiden penipuan berbasis AI meningkat hingga 250% dibandingkan tahun sebelumnya.

Menjelang pelaksanaan Pemilu 2024, BSSN bersama Kementerian Komunikasi dan Informatika mendeteksi sedikitnya 42 konten *deepfake* bermuatan politik yang beredar di media social (Kominfo, 2024). Konten tersebut digunakan untuk meniru suara calon presiden dan tokoh publik tertentu, kemudian dimanfaatkan untuk menipu donatur politik dan masyarakat dengan mengarahkan transfer dana ke rekening palsu. Kasus ini menyita perhatian publik karena memperlihatkan potensi serius penyalahgunaan AI dalam manipulasi politik dan ekonomi digital. Selanjutnya, pada Mei 2025, Kepolisian Republik Indonesia berhasil mengungkap dan menangkap sindikat internasional *romance scam* yang menggunakan teknologi *deepfake* wajah dan suara artis Korea untuk menipu korban melalui aplikasi kencan daring. Para pelaku mengaku sebagai aktor ternama dan membangun kepercayaan korban hingga bersedia mengirimkan dana dalam jumlah besar. Hasil penyidikan mengungkap penggunaan perangkat lunak Midjourney dan *DeepFaceLab* yang dikombinasikan dengan teknologi suara berbasis AI *ElevenLabs*, dengan total kerugian korban di Indonesia mencapai Rp 3,2 miliar (Tempo.co 2024).

Selain itu, perkembangan modus kejahatan siber juga terlihat dalam meningkatnya kasus kebocoran data yang melibatkan algoritma *machine learning attack* sepanjang tahun 2024–2025. Indonesia mengalami lonjakan signifikan insiden kebocoran data dan serangan siber berbasis pembelajaran mesin. Laporan Awang Long Law Review (Rumbruren & Watofa, 2025) mencatat lebih dari 30 kasus kebocoran data berskala besar dalam periode tersebut, dengan metode serangan yang berevolusi dari phishing konvensional menuju AI-*driven attacks* dan eksploitasi *adversarial machine learning* (Rumbruren dkk, 2025). Bentuk serangan yang menonjol antara lain data poisoning attack, yaitu manipulasi dataset pelatihan AI untuk menyisipkan bias berbahaya; model inversion attack yang memungkinkan pelaku merekonstruksi data pribadi pengguna melalui model ML *membership inference attack* untuk menebak apakah data individu digunakan dalam pelatihan model serta *deepfake-based social engineering* yang memanfaatkan manipulasi audio dan visual guna mencuri data atau melakukan rekayasa sosial.

Salah satu kasus penting adalah kebocoran data Bank Rakyat Indonesia pada Desember 2024, yang melibatkan serangan *ransomware* generasi baru dengan memanfaatkan *reinforcement learning algorithm* untuk menyesuaikan pola enkripsi secara dinamis. Serangan ini ditandai dengan penggunaan teknik *deep learning adversarial defense bypassing* sehingga mampu menghindari sistem pertahanan keamanan. Peristiwa tersebut melanggar Pasal 30 dan Pasal 32 Undang-Undang ITE mengenai akses tanpa izin dan perusakan sistem elektronik juncto Pasal 46 Undang-Undang Perlindungan Data Pribadi terkait sanksi administratif dan pidana atas kebocoran data pribadi. Selain itu, pada reaktualisasi kasus data BPJS dan eHAC tahun 2025, Haditama dan Sugianto (2025) dalam *Indonesia Law Reform Journal* menemukan kembali indikasi kebocoran historis yang dianalisis menggunakan *AI-based malware forensic tools*. Temuan ini mengindikasikan adanya serangan adaptif berbasis transfer learning dan pelanggaran Pasal 40 ayat (3) UU PDP mengenai kewajiban pengendali data untuk melakukan mitigasi kebocoran (Haditama dkk, 2025).

Modus kejahatan lain yang berkembang pesat adalah serangan *AI-generated ransomware* terhadap lembaga keuangan. Sejak awal 2024, sejumlah institusi finansial di Indonesia, seperti Bank Rakyat Indonesia (BRI), Bank Mandiri, serta berbagai perusahaan *fintech*, menjadi sasaran *ransomware* berbasis AI. Serangan ini memanfaatkan model generatif berbasis *machine learning*, khususnya GANs dan *reinforcement learning agents*, untuk memodifikasi kode *ransomware* secara otomatis agar mampu menghindari deteksi antivirus melalui teknik *adaptive polymorphic encryption*. Selain itu, sistem AI digunakan untuk melakukan *autonomous reconnaissance* dalam mengidentifikasi celah keamanan serta memanfaatkan *natural language generation* (NLG) guna menyusun pesan ancaman yang sangat realistis dan disesuaikan dengan karakteristik lembaga target, seperti bank-*specific phishing note*. Berdasarkan laporan Haditama dan Sugianto (2025), tercatat lebih dari 12 insiden ransomware berbasis AI di sektor keuangan Indonesia antara Januari 2024 hingga Oktober 2025, dengan estimasi kerugian mencapai Rp 900 miliar.

Di sisi penegakan hukum, periode yang sama juga menunjukkan perkembangan penting dalam praktik investigasi digital oleh BSSN dan Polri melalui pemanfaatan sistem analisis forensik berbasis AI. Sejak tahun 2024, kedua institusi tersebut secara intensif mengintegrasikan teknologi AI dalam proses investigasi, terutama untuk menangani kebocoran data nasional seperti kasus PDN dan BPJS, serangan ransomware berbasis *machine learning*, kejahatan digital lintas negara, serta manipulasi konten digital dan *deepfake* pada Pemilu 2024. Upaya ini merupakan bagian dari *Digital Forensic Governance Strategy* 2024–2025 yang dicanangkan BSSN, dengan penekanan pada akreditasi ISO/IEC 17025:2017 bagi laboratorium forensik digital serta penerapan AI-*assisted forensic automation* (Putra dkk, 2025).

Kolaborasi forensik berbasis AI antara BSSN dan Polri juga terlihat dalam penanganan kasus kejahatan kripto dan pendanaan terorisme pada tahun 2025. Densus 88 bersama BSSN menggunakan *AI-powered transaction pattern analysis* dalam konteks *blockchain forensics* untuk mengidentifikasi transaksi kripto mencurigakan. Teknologi yang dimanfaatkan meliputi *graph-based anomaly detection* untuk menelusuri keterkaitan dompet digital serta *natural language processing* (NLP) untuk menganalisis komunikasi terenkripsi di *dark web*. Praktik ini berkaitan dengan pelanggaran Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan Pendanaan Terorisme, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem Elektronik, serta Instruksi Presiden Nomor 3 Tahun 2023 mengenai Keamanan Siber Nasional.

JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 6, Desember 2025 – Januari 2026
E-ISSN : 3046-4560

**Kesiapan Dan Kemampuan Lembaga Penegak Hukum Di Indonesia Dalam Merespons Perubahan Modus Kejahatan Siber Berbasis AI**

Dalam rentang waktu 2024–2025, Indonesia memasuki fase baru perubahan lanskap ancaman siber, di mana teknik-teknik konvensional seperti *phishing, malware*, dan *ransomware* tidak lagi berdiri sendiri, melainkan diperkaya oleh kapabilitas *Artificial Intelligence* (AI). Perkembangan ini terlihat, antara lain, pada otomatisasi kampanye *phishing* yang semakin dipersonalisasi, pemanfaatan *deepfake* untuk penipuan identitas, serta penggunaan modul *malware* yang mengintegrasikan model bahasa berukuran kecil guna mengelabui sistem deteksi heuristik. Konsekuensi langsung dari kondisi tersebut adalah meningkatnya kompleksitas bukti digital, seperti audio dan video yang telah dimanipulasi, log sistem yang direkayasa, serta pola serangan yang berubah dengan sangat cepat. Dalam situasi ini, tantangan utama bagi aparat penegak hukum tidak lagi terbatas pada pendeteksian intrusi, melainkan mencakup kemampuan mengidentifikasi artefak AI, menentukan atribusi sumber serangan, serta menjaga integritas *chain of custody* ketika keluaran AI relatif mudah dimodifikasi atau dikonfigurasi ulang. Keterkaitan tersebut diperkuat oleh laporan teknis dan analogi kasus global, seperti temuan *ransomware* yang mengintegrasikan *large language model* (LLM) local contohnya *PromptLock* yang menunjukkan bagaimana LLM dapat digunakan untuk mengacak perilaku *malware* sehingga semakin menyulitkan mekanisme deteksi otomatis.

Dari sisi regulasi formal, respons hukum Indonesia menunjukkan perkembangan penting melalui pengesahan Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas UU ITE. Regulasi ini memperluas kewajiban penyelenggara sistem elektronik (PSE) sekaligus menegaskan kewenangan negara dalam perlindungan dan penanganan informasi elektronik. Secara normatif, perubahan tersebut memberikan dasar yuridis yang lebih kuat bagi tindakan preventif dan korektif terhadap kejahatan siber. Namun demikian, penguatan tersebut juga memunculkan kebutuhan akan pengaturan teknis lanjutan, seperti perumusan definisi eksplisit mengenai manipulasi AI, *deepfake*, serta perangkat otomatisasi serangan, agar aparat penegak hukum dapat menerapkan ketentuan tersebut secara efektif tanpa melanggar hak privasi maupun kaidah pembuktian forensik. Dengan kata lain, meskipun pijakan normatif telah tersedia, efektivitasnya tetap bergantung pada keberadaan peraturan pelaksana, pedoman teknis, dan protokol forensik AI yang operasional.

Pada aspek kapasitas institusional, periode 2024–2025 memperlihatkan upaya penguatan yang dilakukan oleh BSSN, Polri, dan unit-unit khusus terkait. Langkah tersebut diwujudkan melalui pengembangan laboratorium forensik digital yang terakreditasi, pembentukan forum kolaborasi, serta keterlibatan aktif dalam konferensi internasional di bidang forensik digital dan AI. BSSN menempatkan *forensic readiness* dan *digital trust* sebagai prioritas strategis, sementara Polri memperluas kerja sama internasional, termasuk dengan INTERPOL dan lembaga forensik swasta, guna mendorong alih pengetahuan dan akses terhadap perangkat forensik mutakhir. Meski demikian, praktik di lapangan masih menunjukkan adanya ketimpangan kapasitas antarwilayah, serta kebutuhan besar akan sumber daya manusia yang tidak hanya menguasai forensik digital konvensional, tetapi juga forensik artefak AI, seperti model *extraction, prompt reconstruction*, dan *provenance analysis*. Hal ini menunjukkan bahwa meskipun niat kelembagaan dan kerangka awal telah terbentuk, kapasitas praktis masih berada dalam tahap pengembangan (Badan Siber dan Sandi Negara, 2024).

Perubahan modus kejahatan berbasis AI juga berdampak langsung pada kebutuhan penguatan sumber daya manusia dan pelatihan. Aparat penyidik dituntut memiliki keahlian hibrida, yang tidak terbatas pada pemahaman jaringan dan *malware*, tetapi juga mencakup dasar-dasar *machine learning, interpretabilitas model, analisis dataset*, serta metodologi pembuktian atas keluaran generatif. Sejumlah kajian akademik di Indonesia pada periode 2024–2025 merekomendasikan pembentukan *task force* forensik AI, pengembangan program pendidikan berkelanjutan bagi aparat penegak hukum, serta integrasi kurikulum hukum siber dan teknologi AI pada jenjang sarjana maupun pascasarjana. Tanpa investasi jangka menengah dalam pendidikan, pelatihan, dan sertifikasi seperti sertifikasi forensik AI atau pelatihan analisis dataset bukti—laju evolusi ancaman akan terus melampaui kapasitas deteksi dan analisis aparat.

Dari perspektif infrastruktur, sejumlah laboratorium forensik digital di berbagai lembaga telah mencapai standar sertifikasi tertentu, misalnya ISO/IEC 17025. Namun demikian, kemampuan untuk menganalisis artefak AI seperti model *weights, prompt logs, model fingerprints*, atau *training telemetry* masih relatif terbatas. Perangkat forensik komersial yang tersedia saat ini umumnya lebih unggul dalam imaging file, analisis *timeline log*, dan pemulihan data, dibandingkan dalam pemeriksaan *provenance model generatif* atau pembuktian bahwa suatu video atau audio merupakan *deepfake* yang dihasilkan oleh model tertentu dengan *prompt* tertentu. Oleh karena itu, diperlukan investasi pada perangkat lunak dan alur kerja forensik baru yang mengintegrasikan analisis model, sekaligus pengembangan standar teknis nasional mengenai pengawetan bukti AI agar hasil pemeriksaan dapat dipertahankan secara sah di pengadilan.

Efektivitas respons terhadap kejahatan berbasis AI juga sangat bergantung pada koordinasi antar-lembaga dan kolaborasi publik–swasta. Penanganan yang optimal menuntut keterlibatan ekosistem yang meliputi BSSN sebagai pengampu kebijakan dan intelijen siber, Polri dalam fungsi penyidikan dan penuntutan, Kementerian Kominfo sebagai regulator PSE dan pengelola pelaporan insiden, CSIRT atau sectoral CERT, penyedia layanan cloud dan PSE, serta sektor swasta keamanan siber (CSIRT / BPIP, 2025). Praktik terbaik di tingkat global menunjukkan bahwa berbagi intelijen ancaman, akses cepat terhadap log PSE, serta mekanisme red-teaming proaktif merupakan faktor kunci. Di Indonesia, meskipun telah terdapat inisiatif kolaboratif melalui forum dan konferensi, hambatan hukum-operasional seperti prosedur permintaan data, perlindungan privasi, dan jaminan bagi *whistleblower* kerap memperlambat respons cepat. Oleh sebab itu, penyusunan protokol operasi gabungan (SOP) dan perjanjian teknis antar-pihak perlu diprioritaskan untuk menghadapi serangan berkecepatan tinggi yang dijalankan oleh agen AI.

Dari sudut pandang pembuktian di pengadilan, keterlibatan output AI dalam perkara pidana memunculkan tantangan baru. Persoalan yang mengemuka antara lain penentuan kepemilikan niat ketika hasil perbuatan merupakan sintesis model, penautan antara operator manusia melalui aktivitas prompting dengan akibat hukum yang timbul, serta cara menyajikan bukti model dan hasil analisis forensik AI yang kompleks agar dapat dipahami oleh hakim. Selain itu, perlu keseimbangan antara kebutuhan pembuktian dan perlindungan rahasia dagang, terutama ketika model yang digunakan bersifat proprietari milik perusahaan teknologi. Sejumlah akademisi merekomendasikan penyusunan pedoman pembuktian khusus, serta penguatan kapasitas teknis hakim dan jaksa, agar putusan yang dihasilkan tidak hanya normatif, tetapi juga berbasis bukti teknis yang dapat diverifikasi.

Permasalahan atribusi dan kejahatan lintas yurisdiksi turut memperumit penegakan hukum. Pemanfaatan AI memungkinkan pelaku melakukan serangan secara terdistribusi dan adaptif melalui infrastruktur cloud, botnet, serta layanan *Ransomware-as-a-Service* (RaaS). Mengingat banyak indikator serangan bersumber dari luar negeri, Polri dan lembaga terkait perlu memperkuat jejaring kerja sama internasional, termasuk mekanisme ekstradisi, *mutual legal assistance*, dan akses terhadap data penyedia layanan global. Pengalaman empiris Indonesia dalam beberapa kasus besar pada tahun 2024 yang menimpa instansi publik dan lembaga keuangan menunjukkan bahwa tanpa jalur internasional yang cepat, respons domestik kerap terbatas pada mitigasi sementara. Hal ini menegaskan urgensi perjanjian teknis dan operasional yang memungkinkan akses cepat terhadap log dan artefak yang berada pada infrastruktur asing (Dwiandari, 2025).

Di sisi lain, penguatan respons terhadap ancaman AI tidak boleh mengorbankan perlindungan hak asasi manusia dan kebebasan sipil. Pendekatan represif yang berlebihan berpotensi melanggar hak privasi, kebebasan berekspresi, serta prinsip *due process*. Meskipun UU No. 1 Tahun 2024 mempertegas kewajiban PSE, implementasi teknis seperti pengumpulan metadata secara masif atau pemantauan otomatis berbasis AI harus diimbangi dengan mekanisme pengawasan, audit independen, dan kepastian hukum agar penegakan hukum tidak bertransformasi menjadi praktik pengawasan massal. Oleh karena itu, kebijakan forensik AI perlu mengintegrasikan prinsip proporsionalitas dan perlindungan data pribadi sehingga bukti yang diperoleh sah secara hukum tanpa melanggar HAM.

Dalam perspektif kebijakan jangka menengah, yakni dua hingga lima tahun ke depan, negara perlu menempatkan tiga pilar utama. Pertama, penyusunan regulasi teknis yang mengatur kewajiban mitigasi risiko AI bagi PSE dan penyedia model, termasuk kewajiban transparansi dan pelaporan. Kedua, investasi berkelanjutan pada infrastruktur dan sumber daya manusia di bidang forensik AI, mencakup laboratorium, perangkat analisis, dan pelatihan. Ketiga, penguatan mekanisme operasional lintas lembaga dan lintas negara untuk kepentingan atribusi dan penindakan. Kalangan akademisi Indonesia juga merekomendasikan penerapan skema *white-box audit* terhadap model AI yang digunakan pada layanan publik atau infrastruktur kritikal, sehingga ketika keluaran model menimbulkan kerugian bagi negara atau masyarakat, aparat dapat melakukan audit teknis tanpa harus melanggar rahasia dagang secara tidak proporsional. Tanpa kebijakan terintegrasi tersebut, penegakan hukum berisiko terus bersifat reaktif dan tertinggal dari dinamika modus kejahatan yang terus berevolusi seiring perkembangan AI.

**Kecukupan Dan Adaptabilitas Kerangka Hukum Nasional Khususnya Undang-Undang ITE, Undang-Undang Nomor 1 Tahun 2024 dan Undang-Undang Perlindungan Data Pribadi Dalam Menghadapi Kejahatan Siber Berbasis AI**

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) sepanjang periode 2024–2025 telah memicu perubahan mendasar dalam pola kejahatan siber di Indonesia. Transformasi tersebut tercermin pada munculnya berbagai modus baru, seperti penipuan berbasis *deepfake, phishing adaptif* yang ditopang oleh machine learning, hingga otomatisasi serangan ransomware yang bersifat prediktif. Dinamika ini menempatkan kerangka hukum nasional pada posisi yang sekaligus strategis dan problematis, karena hukum positif dituntut mampu merespons bentuk kejahatan yang terus berubah, bersifat lintas batas, serta tidak selalu dapat diatribusikan secara langsung kepada subjek hukum manusia. Atas dasar itu, penilaian terhadap kecukupan dan

daya adaptasi UU ITE, UU No. 1 Tahun 2024 sebagai hasil revisi terbaru, serta Undang-Undang Perlindungan Data Pribadi menjadi sangat penting untuk mengukur kesiapan hukum nasional dalam menghadapi evolusi kejahatan siber berbasis AI.

Secara konseptual, UU ITE berfungsi sebagai fondasi utama pengaturan kejahatan siber di Indonesia dengan mengusung pendekatan *technology neutral law*. Pendekatan ini pada awalnya memberikan fleksibilitas normatif karena ketentuan hukum tidak dibatasi oleh jenis teknologi tertentu. Namun, ketika dihadapkan pada *AI-driven cybercrime*, pendekatan tersebut menimbulkan persoalan penafsiran, terutama karena kejahatan tidak lagi sepenuhnya bergantung pada tindakan manual pelaku, melainkan dijalankan oleh sistem otonom yang memiliki kemampuan belajar dan beradaptasi. Sejumlah literatur hukum siber menilai bahwa meskipun UU ITE masih dapat menjangkau unsur perbuatan dan akibat hukum di ruang digital, regulasi ini belum secara eksplisit mengantisipasi karakter non-deterministik yang melekat pada sistem AI (Dwiandari, 2024).

Perubahan melalui UU No. 1 Tahun 2024 membawa sejumlah perbaikan penting, khususnya terkait peningkatan kepastian hukum dan proporsionalitas sanksi. Hal tersebut terlihat dari penegasan batasan delik, penyesuaian ancaman pidana, serta penguatan peran negara dalam melindungi sistem elektronik. Meski demikian, ditinjau dari perspektif kejahatan siber berbasis AI, revisi ini masih cenderung merespons persoalan klasik dalam UU ITE dan belum sepenuhnya menjawab tantangan baru, seperti manipulasi konten sintetis (*deepfake*), *automated social engineering*, maupun penggunaan AI untuk menghindari mekanisme deteksi forensik. Kondisi ini menunjukkan bahwa respons normatif hukum masih tertinggal dibandingkan dengan kecepatan inovasi teknologi (Badan Pembinaan Hukum Nasional, 2024).

Salah satu kelemahan mendasar dari UU ITE dan UU No. 1 Tahun 2024 terletak pada ketiadaan definisi hukum yang tegas mengenai AI dan sistem otonom. Kekosongan ini berpotensi menimbulkan problem serius dalam praktik penegakan hukum, khususnya dalam menentukan subjek hukum, bentuk kesalahan (*mens rea*), serta pertanggungjawaban pidana ketika perbuatan melawan hukum dilakukan melalui sistem AI yang beroperasi secara semi-otomatis atau sepenuhnya otomatis. Dalam kajian akademik, situasi tersebut kerap disebut sebagai *responsibility gap*, yakni adanya jarak antara pelaku manusia dan tindakan sistem cerdas yang menimbulkan akibat hukum.

Berbeda dengan dua regulasi sebelumnya, Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) menawarkan perangkat normatif yang relatif lebih progresif dalam menghadapi kejahatan siber berbasis AI, terutama yang berkaitan dengan pemrosesan data, profiling otomatis, dan kebocoran data dalam skala besar. UU PDP secara eksplisit mengatur prinsip keabsahan pemrosesan data, akuntabilitas pengendali data, serta hak subjek data terhadap keputusan yang dihasilkan melalui pemrosesan otomatis. Dalam konteks 2024–2025, ketentuan ini memiliki relevansi tinggi untuk menanggulangi kejahatan berbasis AI yang mengeksploitasi *big data* dan *machine learning*.

Namun demikian, efektivitas UU PDP dalam merespons kejahatan siber berbasis AI sangat bergantung pada mekanisme penegakan hukum dan kapasitas kelembagaan yang tersedia. Sejumlah kajian akademik menunjukkan bahwa tanpa keberadaan otoritas pengawas data yang kuat dan independen, pengaturan mengenai *automated decision-making dan profiling* berpotensi berhenti pada tataran simbolik. Selain itu, orientasi UU PDP yang lebih menitikberatkan pada perlindungan

administratif dan perdata menyebabkan integrasinya dengan rezim pidana dalam UU ITE masih memerlukan proses harmonisasi lebih lanjut, terutama untuk menghadapi kejahatan siber berbasis AI yang terorganisir dan bersifat lintas negara.

Ditinjau dari aspek adaptabilitas, ketiga undang-undang tersebut memperlihatkan tingkat kesiapan yang tidak seragam. UU ITE dan UU No. 1 Tahun 2024 relatif memadai untuk menangani kejahatan siber umum, tetapi kurang spesifik dalam mengantisipasi AI-*enabled cybercrime*. Sebaliknya, UU PDP menunjukkan tingkat adaptivitas yang lebih tinggi karena mengadopsi prinsip-prinsip global seperti *lawfulness, fairness, transparency*, dan *accountability*. Meski demikian, adaptasi normatif yang tidak disertai dukungan teknis dan prosedural berisiko menimbulkan kesenjangan antara ketentuan hukum dan realitas penegakan di lapangan (Wall, 2024).

Dalam ranah pembuktian, kejahatan siber berbasis AI menghadirkan tantangan baru yang belum sepenuhnya terakomodasi dalam ketiga regulasi tersebut. Alat bukti digital berupa output AI, *deepfake*, maupun hasil analisis algoritmik menuntut standar pembuktian khusus yang mempertimbangkan validitas model, integritas data latih, serta potensi manipulasi algoritma. Literatur forensik digital menegaskan bahwa tanpa pedoman pembuktian yang secara khusus dirancang untuk AI, hakim dan jaksa akan mengalami kesulitan dalam menilai reliabilitas dan kekuatan pembuktian alat bukti elektronik.

Implikasi lain yang tidak kalah penting adalah perlunya rekonstruksi konsep kesalahan dan pertanggungjawaban pidana. UU ITE dan KUHP masih bertumpu pada paradigma *human-centric liability*, sementara kejahatan berbasis AI sering melibatkan relasi kompleks antara manusia, sistem cerdas, dan penyedia platform. Oleh karena itu, kajian hukum kontemporer mulai mendorong penerapan pendekatan *extended liability*, di mana pertanggungjawaban dapat diperluas kepada pengembang, operator, atau pengendali sistem AI, sepanjang dapat dibuktikan adanya kelalaian atau kegagalan dalam pengamanan.

Dengan demikian, dapat disimpulkan bahwa kerangka hukum nasional Indonesia dalam menghadapi kejahatan siber berbasis AI secara normatif dasar tergolong memadai, tetapi belum sepenuhnya adaptif terhadap karakteristik teknis dan epistemik teknologi AI. UU ITE dan UU No. 1 Tahun 2024 menyediakan kerangka pidana umum, sedangkan UU PDP berfungsi sebagai instrumen preventif berbasis perlindungan data. Namun, ketiganya belum terintegrasi dalam satu rezim hukum AI-siber yang komprehensif dan berorientasi pada kebutuhan masa depan.

Dalam konteks penelitian mengenai pengaruh teknologi AI terhadap evolusi modus kejahatan siber pada periode 2024–2025, temuan ini menunjukkan bahwa implikasi penegakan hukum tidak semata-mata bergantung pada penambahan norma baru. Lebih dari itu, diperlukan reinterpretasi terhadap norma yang sudah ada, harmonisasi lintas undang-undang, serta penguatan kapasitas aparat penegak hukum. Tanpa langkah-langkah tersebut, hukum berpotensi terus tertinggal dari laju inovasi kejahatan siber yang digerakkan oleh perkembangan AI.

**Model Pendekatan Hukum dan Kebijakan Efektif Untuk Membangun Sistem Penegakan Hukum Yang Adaptif Terhadap Dinamika Kejahatan Siber Berbasis AI di Indonesia**

Pendekatan hibrida dalam regulasi hukum menempatkan prinsip *technology-neutral law* berdampingan dengan ketentuan yang secara khusus mengatur karakteristik *Artificial Intelligence* (AI). Model ini memadukan kekuatan norma umum seperti UU ITE dan ketentuan pidana yang

telah ada yang bersifat fleksibel dalam menghadapi inovasi teknologi, dengan pasal-pasal spesifik yang diarahkan pada ciri khas AI, antara lain manipulasi konten *generatif, automated decision making*, serta penelusuran asal-usul model (*model provenance*). Skema demikian mencegah regulasi menjadi cepat usang akibat ketergantungan pada aturan teknis semata, sekaligus menyediakan dasar hukum yang memadai untuk menjerat aktor yang menyalahgunakan AI bagi kepentingan kriminal. Secara praktis, pendekatan ini dapat diwujudkan melalui penyusunan *addendum AI* dalam bentuk peraturan pelaksana UU ITE atau UU PDP, sehingga hukum tetap adaptif tanpa harus merevisi undang-undang induk setiap kali terjadi pergeseran teknologi.

Arsitektur regulasi yang berbasis risiko (*risk-based regulation*) juga menjadi elemen penting dalam kebijakan yang efektif. Dalam model ini, tingkat risiko suatu sektor misalnya infrastruktur nasional sebagai kategori tinggi, layanan keuangan menengah, platform media sosial rendah, dan aplikasi hiburan paling rendah menentukan intensitas kewajiban mitigasi, audit, serta pelaporan insiden. Penerapannya pada AI berarti adanya keharusan audit keselamatan dan keamanan, penilaian dampak risiko sebelum peluncuran (*AI risk impact assessments*), serta registrasi model untuk sistem yang beroperasi di domain kritikal. Pendekatan ini sejalan dengan rekomendasi internasional, termasuk dari ASEAN dan PBB, yang mendorong pengawasan *generative AI* secara proporsional berbasis tingkat risiko (ASEAN, 2024).

Kerangka hukum adaptif juga perlu mengembangkan mekanisme akuntabilitas dan pertanggungjawaban yang diperluas. Model ini mengakui keberadaan berbagai aktor dalam ekosistem AI, mulai dari pengembang atau pencipta model, penyedia platform, operator atau pengendali sistem, hingga pengguna akhir. Pendekatan *extended liability* atau pertanggungjawaban berjenjang memungkinkan penegakan hukum ketika hubungan kausal tidak mudah dibuktikan hanya pada pelaku terakhir. Namun, penerapannya harus didasarkan pada pembuktian adanya kelalaian, kegagalan mitigasi keamanan, atau pengabaian kewajiban audit, bukan pada prinsip *strict liability* yang berpotensi menghambat inovasi tanpa adanya kesalahan. Oleh karena itu, diperlukan standar keamanan teknis yang jelas sebagai tolok ukur penilaian kelalaian.

Dalam konteks pembuktian, negara perlu membentuk institusi forensik AI yang terpusat dan bersifat multidisipliner. Mengingat bukti AI mencakup aspek teknis seperti model *weights*, *dataset* pelatihan, *prompt logs*, dan metadata provenance, diperlukan unit forensik nasional yang melibatkan BSSN, Polri (unit siber), Kejaksaan, serta kalangan akademisi. Unit ini berfungsi sebagai pusat rujukan untuk perkara kompleks, penyedia opini teknis yang dapat dipertanggungjawabkan di pengadilan, serta perumus pedoman standar pembuktian bukti AI. Sejumlah studi nasional merekomendasikan pembentukan *task force* semacam ini guna meningkatkan reliabilitas investigasi dan menjembatani kesenjangan antara bukti teknis dan kaidah pembuktian hukum.

Pengadilan juga memerlukan mekanisme pembuktian dan pedoman khusus terkait AI. Kebijakan publik harus menyediakan panduan teknis-legal mengenai penilaian bukti yang dihasilkan atau dimediasi oleh AI, termasuk standardisasi metode verifikasi *deepfake*, pengelolaan *chain of custody artefak model*, validasi dataset pelatihan, serta pemanfaatan saksi ahli teknis. Selain itu, perlu diatur kriteria admissibility atau kelayakan alat bukti AI, seperti keberadaan audit trail yang dapat diverifikasi dan kewajiban penyedia teknologi untuk menyimpan metadata relevan

bagi kepentingan hukum dengan tetap menjamin perlindungan privasi. Tanpa pedoman ini, risiko inkonsistensi dan lemahnya putusan pengadilan akan semakin besar.

Kolaborasi publik–swasta dan mekanisme berbagi ancaman (*threat-sharing*) yang memiliki dasar hukum juga menjadi prasyarat penting. Mengingat sebagian besar infrastruktur digital dikelola oleh sektor swasta termasuk penyedia *cloud, platform media,* dan *fintech respons adaptif* harus mengatur kerja sama teknis operasional melalui standar SLA, prosedur *emergency disclosure*, serta mekanisme pertukaran intelijen ancaman yang aman dan dilindungi hukum, misalnya melalui skema safe harbor bagi pelapor. Kebijakan ini idealnya dituangkan dalam peraturan pelaksana yang mewajibkan PSE menyediakan akses terbatas terhadap *log* ketika terdapat perintah pengadilan atau permintaan resmi. Pengalaman kasus-kasus pada periode 2024–2025 menegaskan bahwa akses cepat terhadap *log cloud* sangat krusial untuk keperluan atribusi.

Penguatan kapasitas juga menuntut investasi serius dalam pendidikan hukum teknis dan program sertifikasi. Model adaptif perlu memasukkan pembelajaran berkelanjutan, seperti kurikulum forensik AI bagi penyidik, pelatihan teknis untuk jaksa dan hakim, serta sertifikasi auditor AI independen. Pendekatan ini tidak hanya menekankan penguasaan aspek teknis, tetapi juga kemampuan menilai dimensi etika dan hak asasi manusia dalam penyidikan berbasis AI, termasuk isu privasi dan non-diskriminasi. Rekomendasi akademik menekankan pentingnya integrasi hukum AI dalam program pascasarjana serta pelatihan intensif bagi unit siber kepolisian.

Selain itu, kebijakan adaptif harus dilengkapi dengan mekanisme pengawasan, transparansi, dan perlindungan hak asasi manusia. Keseimbangan antara kebutuhan keamanan dan kebebasan sipil dapat diwujudkan melalui pembentukan lembaga audit independen untuk mengawasi penggunaan AI oleh aparat, penyediaan mekanisme pemulihan bagi korban deepfake atau kerugian akibat keputusan otomatis, serta pembatasan tegas terhadap praktik pengawasan massal berbasis AI. Model ini menempatkan prinsip proporsionalitas dan legalitas sebagai fondasi, sehingga tindakan investigasi tidak bergeser menjadi praktik *surveillance* yang berlebihan. Dokumen kebijakan ASEAN dan rekomendasi PBB juga menegaskan pentingnya tata kelola etis dalam respons kebijakan AI.

Instrumen regulasi eksperimental, seperti *regulatory sandbox* dan *pilot audit*, menjadi pelengkap penting dalam menghadapi percepatan perkembangan AI. Melalui *sandbox*, teknologi baru dapat diuji dalam lingkungan terbatas dan diawasi dengan aturan sementara, monitoring, serta kewajiban pelaporan. Indonesia berpeluang mengadopsi model ini untuk aplikasi AI di sektor kritikal, seperti keuangan dan pemerintahan, agar regulator dan aparat penegak hukum memperoleh pengalaman praktis, pemetaan risiko, dan praktik terbaik sebelum menerapkan kewajiban penuh. Hasil uji coba tersebut juga dapat menjadi dasar empiris dalam merumuskan standar kepatuhan yang realistis.

Harmonisasi hukum nasional dengan mekanisme kerja sama internasional merupakan aspek yang tidak terpisahkan, mengingat kejahatan berbasis AI kerap bersifat lintas yurisdiksi. Model adaptif perlu mengintegrasikan pembaruan perjanjian *mutual legal assistance* (MLAT) yang secara khusus mencakup akses *log cloud* dan artefak model, serta mendorong partisipasi aktif dalam forum multilateral untuk standardisasi metadata forensik AI. Penguatan kapasitas MLA dan perundingan klausul bantuan teknis dengan penyedia layanan global menjadi kunci agar atribusi dan penegakan hukum terhadap aktor asing tidak selalu tertinggal (Wisnubroto, 2025).

Akhirnya, efektivitas model pendekatan adaptif mensyaratkan dukungan pendanaan yang memadai, evaluasi berkala, dan indikator kinerja yang terukur. Alokasi anggaran khusus diperlukan untuk pengembangan infrastruktur forensik AI, riset dan pengembangan *counter-AI*, serta program pelatihan berkelanjutan. Di samping itu, evaluasi tahunan atau dua tahunan perlu dilakukan dengan mengukur indikator seperti waktu respons insiden, tingkat keberhasilan atribusi, kualitas bukti yang diterima pengadilan, dan kepatuhan PSE terhadap kewajiban audit. Mekanisme evaluasi ini menciptakan umpan balik yang krusial agar kebijakan tetap responsif terhadap evolusi modus kejahatan yang digerakkan oleh AI.

## KESIMPULAN

Perkembangan teknologi *Artificial Intelligence* (AI) sepanjang periode 2024–2025 terbukti membawa perubahan mendasar terhadap karakter dan pola kejahatan siber di Indonesia. AI berperan sebagai katalis utama munculnya berbagai modus kejahatan yang semakin canggih, adaptif, dan sulit dideteksi, antara lain penipuan berbasis *deepfake, phishing* yang didukung oleh *machine learning, ransomware* hasil generasi AI, serta eksploitasi data pribadi melalui sistem otomasi cerdas. Temuan ini menegaskan bahwa kejahatan siber berbasis AI tidak lagi dapat dipandang sebagai kelanjutan dari pola konvensional, melainkan sebagai bentuk ancaman baru yang secara substantif memperluas spektrum risiko dan memberikan tekanan serius terhadap sistem penegakan hukum.

Hasil penelitian juga menunjukkan bahwa meskipun lembaga penegak hukum di Indonesia telah mengalami peningkatan kapasitas secara kelembagaan, efektivitas respons terhadap kejahatan siber berbasis AI masih belum optimal. Hambatan utama terletak pada keterbatasan kompetensi forensik AI, minimnya instrumen teknis pembuktian yang memadai, serta lemahnya koordinasi baik antar lembaga domestik maupun dalam kerja sama lintas negara. Kondisi tersebut berdampak pada lambannya proses penanganan dan rendahnya tingkat keberhasilan penegakan hukum terhadap kejahatan siber yang bersifat kompleks dan adaptif.

Dari perspektif normatif, kerangka hukum nasional terutama UU ITE sebagaimana telah diperbarui melalui Undang-Undang Nomor 1 Tahun 2024 dan Undang-Undang Perlindungan Data Pribadi pada dasarnya telah menyediakan landasan hukum yang cukup. Namun demikian, regulasi tersebut belum sepenuhnya responsif terhadap karakter kejahatan siber berbasis AI yang bersifat otonom, dinamis, dan berlapis. Ketiadaan pengaturan yang secara eksplisit mengakomodasi teknologi AI berpotensi menimbulkan persoalan penafsiran hukum sekaligus mengurangi efektivitas implementasi norma dalam praktik penegakan di lapangan.

Berdasarkan temuan tersebut, penelitian ini merekomendasikan perlunya penerapan model pendekatan hukum dan kebijakan yang bersifat adaptif, preventif, dan berlandaskan etika. Langkah-langkah strategis yang disarankan meliputi harmonisasi regulasi, penguatan kapasitas forensik berbasis AI, pengembangan kompetensi aparat penegak hukum, serta peningkatan kolaborasi antara negara dan sektor swasta. Pendekatan komprehensif ini dipandang penting agar sistem penegakan hukum Indonesia mampu merespons secara proaktif perkembangan kejahatan siber berbasis AI, tanpa mengesampingkan prinsip perlindungan hak asasi manusia dan jaminan kepastian hukum.

Berdasarkan temuan penelitian ini, disarankan agar aparat penegak hukum meliputi Polri, Kejaksaan, dan lembaga peradilan melakukan penguatan kapasitas teknis secara berkelanjutan

melalui pengembangan forensik berbasis *Artificial Intelligence*, perumusan pedoman khusus pembuktian digital yang melibatkan AI, serta pembentukan unit-unit khusus yang memiliki kompetensi dalam merespons pola kejahatan siber yang kian adaptif. Upaya tersebut menjadi krusial agar praktik penegakan hukum tidak tertinggal dari percepatan inovasi teknologi yang dimanfaatkan oleh pelaku kejahatan.

Di sisi lain, pembuat kebijakan dan regulator perlu mendorong harmonisasi antara Undang-Undang ITE, Undang-Undang Nomor 1 Tahun 2024, dan Undang-Undang Perlindungan Data Pribadi dengan pengaturan yang lebih tegas dan eksplisit terkait pemanfaatan maupun penyalahgunaan AI. Pengaturan tersebut mencakup, antara lain, kewajiban audit algoritma, kejelasan pembagian tanggung jawab hukum antar aktor dalam ekosistem AI, serta penerapan pendekatan regulasi berbasis risiko guna menjamin keseimbangan antara inovasi dan perlindungan hukum.

Akhirnya, peran akademisi dan masyarakat tidak kalah penting dalam memperkuat ekosistem penegakan hukum siber. Kontribusi tersebut dapat diwujudkan melalui pengembangan riset interdisipliner yang mengintegrasikan kajian hukum dan AI, serta peningkatan literasi digital publik. Sinergi yang berkelanjutan di antara seluruh pemangku kepentingan inilah yang menjadi fondasi utama dalam membangun sistem penegakan hukum siber yang adaptif, preventif, dan berkeadilan di era kecerdasan buatan.

## DAFTAR PUSTAKA

Abast, B. R., Damanik, D. C., & Fahmi, G. J. (2025). *Cybercrime as a Threat to National Security: A Review of the Role and Preparedness of the Indonesian Police.* Proceedings of Police Academy.

ASEAN. (2024). *Expanded ASEAN Guide on AI Governance and Ethics – Generative AI.* Association of Southeast Asian Nations. asean.org

Badan Pembinaan Hukum Nasional. (2024). *Analisis dampak perubahan Undang-Undang ITE terhadap penegakan hukum siber*. Jakarta: BPHN.

Badan Siber dan Sandi Negara (BSSN). (2024). *Lanskap Keamanan Siber Indonesia 2024* [laporan/internal publikasi]. BSSN. Retrieved from BSSN analysis publications.

Badan Siber dan Sandi Negara. (2024). *Laporan Insiden Keamanan Siber Nasional 2024.* Jakarta: BSSN.

Bareskrim Polri. (2025). *Laporan Investigasi Cybercrime Semester I Tahun 2025.* Jakarta: Mabes Polri.

Cohen, L., & Felson, M. (1979). *Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44*(4), 588–608.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th ed.).* Thousand Oaks, CA: SAGE Publications.

CSIRT / BPIP. (2025, Jan 1). *Ancaman Siber 2025: Indonesia Harus Waspada AI Agentik.* CSIRT blog.

Dharmayanti, Y. P., & Soponyono, E. (2025). *Criminal Law Policy in Efforts to Combat Artificial Intelligence (AI) in Cyber Crime. Jurnal Hukum Khaira Ummah.*

Dwiandari, A. S. (2024). Legal challenges of AI-driven cybercrime in Indonesia. *Journal of Indonesian Legal Studies, 9*(2), 145–162. https://doi.org/10.15294/jils.v9i2.XXXX

Dwiandari, A. S. (2025). *Criminal Law Enforcement on Digital Identity Misuse in AI Era.* ICCLE Journal, Universitas Negeri Semarang. Journal UNNES

Haditama, T. K., & Sugianto, F. (2025). *A Comparative Analysis of Corporate Criminal Liability for AI-Based Malware: A Study of Indonesian and EU Law. Indonesia Law Reform Journal.*

Haditama, T.K., & Sugianto, F. (2025). *Corporate Criminal Liability for AI-Based Malware*. Indonesia Law Reform Journal, UMM.

Instruksi Presiden Nomor 3 Tahun 2023 mengenai Keamanan Siber Nasional.

Khuan, H., Paminto, S. R., & Salmon, H. C. J. (2025). *Cybercrime and Law Enforcement Challenges in the Society 5.0 Era. Ipso Jure Journal.*

Kominfo (2024). *Laporan Pengawasan Konten Digital Pemilu 2024.*

Nonet, P., & Selznick, P. (1978). *Law and Society in Transition: Toward Responsive Law.* Harper & Row.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem Elektronik

Praditya, E., Maarif, S., Ali, Y., & Saragih, H. (2023). *National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence. Journal of Human Security.*

Praditya, E., Maarif, S., Ali, Y., & Saragih, H. J. R. (2023). *National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of AI. Journal of Human Security.*

Putra, S.D., & Riyanta, S. (2025). *Digital Forensic Governance Strategy in Indonesia to Realize Accountable Law Enforcement. Journal of Social Research.*

Rohimi, U. E. (2025). *Artificial Intelligence and Cybersecurity Regulation in Indonesia: Towards an Adaptive Legal Framework. Indonesian Cyber Law Review.*

Rumbruren, A., & Watofa, Y. (2025). *Responsibilities of Electronic System Organizers in Data Breach*. Awang Long Law Review.

Satoto, E., & Santiago, F. (2025). *Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention. Global International Journal of Law and Social Science.*

Setyoningsih, A. D. A., & Farid, A. M. (2025). *Prophetic Cyber Law Enforcement: A Holistic Paradigm of Cyber Law Enforcement in Indonesia. ICOSEND Proceedings.*

Syahril, M. A. F., & Karović, S. (2025). *Beware of Cybercrime in Tax Reporting: Threats and How to Protect Yourself. Amsir Accounting & Finance Journal.*

Tempo.co (2024). "Deepfake Politik dan Penipuan Digital Meningkat Jelang Pemilu."

Undang-Undang Nomor 1 Tahun 2024 Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan Pendanaan Terorisme

Wall, D. S. (2020). *Cybercrime: The Transformation of Crime in the Information Age (2nd ed.).* Polity Press.

Wall, D. S. (2024). *Cybercrime and the limits of the law*. Routledge.

Wisnubroto, A. (2025). Preventing AI crime: towards a new legal paradigm. *Journal of Humanitarian and Civil Legal Studies.* jhcls.org

Wisnubroto, A., & Tegnan, H. (2025). *Preventing AI Crime Towards A New Legal Paradigm: Lessons from the United States. Journal of Human Rights, Culture and Legal Studies.*

Yin, R. K. (2019). *Case Study Research and Applications: Design and Methods (6th ed.).* Thousand Oaks, CA: SAGE Publications.

Zulyadi, R., & Frensh, W. (2025). *Cybercrime Investigation on Social Media: Implementation of Community Policing Moderated by Law Enforcement. International Journal of Criminal Justice Sciences.*