SUBJEK HUKUM DAN PERTANGGUNGJAWABAN PIDANA DALAM KEJAHATAN SIBER BERBASIS KECERDASAN BUATAN: SINTESIS FILOSOFIS DAN MODEL ATRIBUSI BERTINGKAT DALAM SISTEM HUKUM INDONESIA

Pebrin Putra Yasa[1], Muhammad Aminuddin Shofi[2], I Gede Widhiana Suarda[3], Fendi Setyawan[4]
[1]Universitas Jember
[2]Institut Agama Islam Miftahul Ulum Lumajang
[3]Universitas Jember
[4]Universitas Jember
Email: ppebrin@gmail.com[1], shofihasan85@gmail.com[2], igedewidhiana.suarda@unej.ac.id[3] fendisetyawan.fh@unej.ac.id[4]

Abstract: The increasing autonomy of artificial intelligence (AI) challenges the doctrines of legal subjects and criminal liability in Indonesia, particularly in cybercrime. This article combines two studies of the same issue: the first emphasizes the reconstruction of legal personality and shared responsibility, while the second urges caution so that the operational autonomy of AI is not directly treated as a basis for criminal subjecthood. The aim is to analyze the nature of AI through ontology, epistemology, and axiology, and then to formulate a framework for attributing criminal liability grounded in the principles of legality and culpability. This normative legal research is a literature study using conceptual, statutory, and philosophical approaches, with qualitative analysis through thematic synthesis. The findings are: (1) AI is a dual-natured socio-technical system that has not been shown to possess consciousness or moral agency, so it is not appropriate to treat it as a criminal subject; (2) the accountability gap is addressed by attributing liability to humans and corporations based on their acts, control, foreseeability of risk, and fault; (3) transparency and audit trails serve as prerequisites for proof, not as substitutes for the elements of an offense. The article proposes a tiered attribution model that places shared responsibility, strict liability, and vicarious liability in a measured way.
Keywords: Artificial intelligence; Legal subject; Cybercrime; Legal personality; Criminal liability
Abstrak: Perkembangan kecerdasan buatan (*artificial intelligence*/AI) dengan tingkat otonomi yang semakin tinggi menantang doktrin subjek hukum dan pertanggungjawaban pidana dalam sistem hukum Indonesia, khususnya pada kejahatan siber. Artikel ini memadukan dua kajian atas isu yang sama dengan

penekanan berbeda: kajian pertama menekankan rekonstruksi personalitas hukum dan skema tanggung jawab bersama, sedangkan kajian kedua menekankan kehati-hatian agar otonomi operasional AI tidak serta-merta dianggap sebagai dasar subjek pidana. Tujuan penulisan ini adalah menganalisis hakikat AI melalui ontologi, epistemologi, dan aksiologi, lalu merumuskan kerangka atribusi pertanggungjawaban pidana yang tetap berpegang pada asas legalitas dan asas kesalahan. Penelitian ini merupakan penelitian hukum normatif berbentuk studi pustaka dengan pendekatan konseptual, perundang-undangan, dan filosofis; kedua kajian diperlakukan sebagai bahan hukum sekunder dan dianalisis secara kualitatif melalui sintesis tematik. Hasil analisis menunjukkan bahwa (1) AI merupakan sistem sosio-teknis berwujud ganda yang belum terbukti memiliki kesadaran dan agensi moral, sehingga tidak tepat diperlakukan sebagai subjek pidana; (2) kesenjangan pertanggungjawaban lebih tepat dijawab dengan atribusi kepada manusia dan korporasi berdasarkan perbuatan, kendali, keterdugaan risiko, dan kesalahan; dan (3) transparansi, dokumentasi, serta jejak audit berfungsi sebagai prasyarat pembuktian dan tata kelola, bukan pengganti unsur delik. Artikel ini menawarkan model atribusi bertingkat yang menempatkan konsep *shared responsibility*, *strict liability*, dan *vicarious liability* secara terukur sesuai asas kesalahan.
Kata Kunci: Kecerdasan buatan; Subjek hukum; Kejahatan siber; Personalitas hukum; Pertanggungjawaban pidana.

PENDAHULUAN

Perkembangan kecerdasan buatan (*artificial intelligence*/AI) memperluas kapasitas manusia untuk menghasilkan, mengolah, dan menyebarkan informasi, tetapi pada saat yang sama membuka ruang penyalahgunaan sebagai sarana kejahatan siber. Di Indonesia, ancaman tersebut tidak lagi sekadar potensi. Laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023 mencatat lebih dari 361 juta anomali trafik siber, yang menunjukkan meningkatnya kompleksitas ancaman digital, termasuk pemanfaatan teknologi algoritma adaptif. Ancaman itu tercermin dalam berbagai modus, seperti penipuan melalui peniruan suara (*voice cloning*), penyebaran disinformasi menggunakan *deepfake*, serta serangan *ransomware* yang memanfaatkan AI untuk mengidentifikasi celah keamanan secara otomatis dan real-time (Habibi et al., 2026).

Kompleksitas ancaman tersebut mempersulit deteksi dan penanggulangan. Mekanisme keamanan konvensional belum mampu mengimbangi karakteristik dan pola serangan berbasis AI, harmonisasi regulasi global belum terbentuk sehingga penyalahgunaan AI dapat melintasi batas yurisdiksi, dan perkembangan teknologi berlangsung lebih cepat daripada penyesuaian protokol keamanan. Ketergantungan AI pada data berskala besar

juga menimbulkan persoalan privasi, sebab data yang telah dianonimkan masih berpotensi diidentifikasi kembali melalui serangan inferensi (*inference attacks*) (Knecht et al., 2025). Bagi penegakan hukum, konsekuensinya konkret: identifikasi pelaku, penentuan atribusi perbuatan, dan pertanggungjawaban pidana menjadi semakin sulit.

Kesulitan itu berakar pada struktur hukum pidana yang berorientasi pada manusia. Kasus DABUS di Australia dan *Random Darknet Shopper* kerap dirujuk untuk menunjukkan bahwa AI dapat menghasilkan tindakan secara otonom yang berpotensi menimbulkan akibat hukum. Dalam hukum Indonesia, subjek tindak pidana pada dasarnya masih manusia, sedangkan korporasi baru diakui secara terbatas dalam peraturan tertentu (Mahardhika et al., 2023). Kondisi ini memunculkan tiga persoalan: belum jelasnya kedudukan AI dalam sistem hukum, sulitnya menerapkan asas kesalahan (*mens rea*) pada sistem yang tidak memiliki kesadaran dan kehendak bebas, serta terbatasnya sanksi pidana konvensional terhadap entitas nonmanusia. Bentuk sanksi alternatif seperti penonaktifan, pembatasan fungsi, penghapusan data, atau modifikasi sistem telah diusulkan, dengan syarat tetap berlandaskan asas legalitas, kepastian hukum, keadilan, dan proporsionalitas (Fransisco, 2025).

Kecerdasan buatan (AI) memperluas kapasitas manusia untuk menghasilkan, mengolah, dan menyebarkan informasi, tetapi juga dapat disalahgunakan sebagai sarana penipuan, manipulasi konten, atau serangan siber. Analisis hukum perlu membedakan setidaknya dua keadaan. Pertama, seseorang dengan sengaja menggunakan AI sebagai alat untuk melakukan tindak pidana; dalam keadaan ini, fokus utama tetap pada perbuatan dan kesalahan manusia. Kedua, sistem yang beradaptasi atau beroperasi dengan otonomi tertentu menghasilkan keluaran yang menimbulkan akibat pidana, sementara kendali dan keterdugaan oleh para pihak tidak sederhana. Persoalan kedua dapat menimbulkan kesenjangan atribusi, tetapi tidak membuktikan bahwa AI telah menjadi pelaku pidana. Kajian hukum Indonesia yang membahas AI dan pertanggungjawaban juga menempatkan atribusi kesalahan serta hubungan antara norma pidana yang ada dan penggunaan AI sebagai persoalan sentral. (Fitriya et al., 2026).

Debat tentang "kesenjangan pertanggungjawaban" tidak boleh langsung berujung pada kesimpulan bahwa hukum harus menciptakan subjek pidana baru. Literatur filsafat teknologi menunjukkan bahwa kesenjangan tersebut bukan satu masalah tunggal: ia dapat menyangkut kesalahan moral, akuntabilitas publik, kewajiban bertindak, dan penyebab teknis maupun organisasi. Dengan demikian, respons yang hanya menambah sanksi atau

teknologi audit belum tentu menyelesaikan seluruh masalah. (de Sio & Mecacci, 2021).

Masalah filosofisnya terletak pada kecenderungan menyamakan kapasitas fungsional dengan agensi moral. AI dapat memproses informasi dan menghasilkan keluaran yang kompleks; tetapi dari kemampuan itu tidak otomatis mengikuti bahwa sistem memiliki pengalaman subjektif, kehendak bebas, kepentingan, atau kemampuan memahami alasan normatif. Pertanyaan mengenai "apa" AI secara ontologis harus dipisahkan dari pertanyaan epistemologis tentang bagaimana pengetahuan dan keluaran sistem dihasilkan, serta dari pertanyaan aksiologis tentang nilai dan kepentingan yang harus dilindungi oleh hukum. Pemisahan itu membantu menghindari dua lompatan: menganggap AI sekadar benda pasif dalam semua keadaan, atau sebaliknya menganggap keluaran yang otonom sebagai bukti kepribadian dan kesalahan pidana.

Di Indonesia, hukum pidana perlu dianalisis berdasarkan hukum yang berlaku sekarang, bukan hanya naskah awal KUHP. Undang-Undang Nomor 1 Tahun 2023 tentang KUHP mulai berlaku pada 2 Januari 2026, sementara Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana juga berlaku sejak tanggal tersebut dan melakukan penyesuaian terhadap ketentuan pidana. Karena itu, setiap kesimpulan tentang kekosongan norma, pasal yang relevan, atau status pertanggungjawaban korporasi harus diuji terhadap naskah konsolidasi dan peraturan sektoral terkini. (Republik Indonesia, 2023, 2026). UU Nomor 1 Tahun 2024 tentang perubahan kedua UU ITE tercatat berlaku, sehingga analisis kejahatan siber juga perlu menggunakan versi perubahan yang mutakhir dan memperhatikan perkembangan putusan pengujian undang-undang. (Republik Indonesia, 2024).

Berdasarkan persoalan tersebut, artikel ini menjawab dua pertanyaan: (1) bagaimana kedudukan AI sebagai entitas dan agen teknis jika ditelaah melalui ontologi, epistemologi, dan aksiologi, serta apa implikasinya bagi konsep subjek hukum pidana; dan (2) bagaimana model atribusi pertanggungjawaban pidana yang dapat diterapkan terhadap kejahatan siber yang menggunakan atau melibatkan AI tanpa mengorbankan asas legalitas dan kesalahan?

Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, filosofis, dan perbandingan terbatas. Pendekatan perundang-undangan digunakan untuk menelaah KUHP nasional, perubahan ketentuan pidana yang berlaku, UU ITE beserta perubahannya, serta peraturan lain yang relevan dengan tindak pidana siber dan pertanggungjawaban korporasi. Pendekatan konseptual digunakan untuk

menguji pengertian subjek hukum, personalitas, agensi, kesalahan, kendali, dan kausalitas. Pendekatan filosofis mengorganisasi analisis ke dalam dimensi ontologi, epistemologi, dan aksiologi. Perbandingan terbatas dipakai untuk menguji argumen doktrinal dalam literatur internasional; bukan untuk menganggap aturan yurisdiksi lain otomatis berlaku di Indonesia. Bahan hukum dan literatur dianalisis secara kualitatif melalui penafsiran, sistematisasi, dan evaluasi normatif.

Masalah filosofisnya terletak pada kecenderungan menyamakan kapasitas fungsional dengan agensi moral. AI dapat memproses informasi dan menghasilkan keluaran yang kompleks, tetapi dari kemampuan itu tidak otomatis mengikuti bahwa sistem memiliki pengalaman subjektif, kehendak bebas, kepentingan, atau kemampuan memahami alasan normatif. Karena itu, pertanyaan ontologis tentang apa AI itu perlu dipisahkan dari pertanyaan epistemologis tentang bagaimana pengetahuan dan keluaran sistem dihasilkan, serta dari pertanyaan aksiologis tentang nilai dan kepentingan yang harus dilindungi hukum. Pemisahan ini membantu menghindari dua lompatan: menganggap AI sekadar benda pasif dalam semua keadaan, atau sebaliknya menganggap keluaran yang otonom sebagai bukti kepribadian dan kesalahan pidana.

Persoalan ini juga harus dibaca dalam hukum positif yang berlaku sekarang. Undang-Undang Nomor 1 Tahun 2023 tentang KUHP mulai berlaku pada 2 Januari 2026, dan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana berlaku sejak tanggal yang sama. Analisis kejahatan siber juga harus memakai Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024. Setiap kesimpulan tentang kekosongan norma atau status pertanggungjawaban korporasi karena itu harus diuji terhadap naskah konsolidasi dan peraturan sektoral terkini (Republik Indonesia, 2023, 2024, 2026).

Berdasarkan uraian tersebut, artikel ini menjawab dua rumusan masalah. Pertama, bagaimana hakikat dan kedudukan AI sebagai entitas dalam perspektif ontologi, epistemologi, dan aksiologi filsafat ilmu, serta apa implikasinya bagi konsep subjek hukum dan personalitas dalam kejahatan siber? Kedua, bagaimana rekonstruksi konsep subjek hukum dan pertanggungjawaban pidana dalam kejahatan siber berbasis AI yang mewujudkan sistem hukum pidana Indonesia yang berkeadilan dan berkepastian hukum tanpa mengorbankan asas legalitas dan asas kesalahan? Tujuan penulisan adalah memadukan temuan kedua kajian menjadi satu

kerangka analisis yang konsisten, menguji titik temu dan titik beda keduanya, serta menawarkan model atribusi pertanggungjawaban yang dapat diuji dalam pembaruan hukum pidana Indonesia.

METODE

Penelitian ini merupakan penelitian hukum normatif (doktrinal) yang dilaksanakan melalui studi pustaka (Marzuki, 2010). Objek kajiannya adalah konsep, doktrin, dan norma tentang kedudukan AI sebagai subjek hukum serta pertanggungjawaban pidana atas kejahatan siber yang melibatkan AI. Karena penelitian ini memadukan dua naskah kajian yang sudah ada, kedua naskah tersebut diperlakukan sebagai bahan hukum sekunder yang dibaca secara kritis, bukan sebagai data lapangan. Artikel ini tidak melakukan wawancara, survei, atau pengumpulan data empiris baru.

Penelitian ini memakai empat pendekatan yang bersumber dari kedua kajian. Pendekatan konseptual menguji pengertian subjek hukum, personalitas hukum, agensi, kesalahan, kendali, dan kausalitas. Pendekatan filosofis mengorganisasi analisis ke dalam tiga dimensi filsafat ilmu, yaitu ontologi (hakikat keberadaan AI), epistemologi (bagaimana pengetahuan dan keluaran AI dihasilkan serta dibuktikan), dan aksiologi (nilai yang hendak dilindungi hukum). Pendekatan perundang-undangan menelaah KUHP nasional, ketentuan penyesuaian pidana, UU ITE beserta perubahannya, dan peraturan yang berkaitan dengan pertanggungjawaban korporasi serta pelindungan data pribadi. Pendekatan perbandingan terbatas dipakai untuk menguji argumen doktrinal dalam literatur internasional; pendekatan ini tidak dimaksudkan untuk menyatakan bahwa aturan yurisdiksi lain otomatis berlaku di Indonesia.

Bahan hukum primer adalah peraturan perundang-undangan yang dirujuk kedua kajian: Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana, serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Bahan hukum sekunder terdiri atas Kajian I, Kajian II, dan literatur yang dikutip keduanya, yaitu buku, artikel jurnal, laporan lembaga, dan rilis resmi pemerintah. Rincian sumber tercantum dalam daftar pustaka.

Bahan dianalisis secara kualitatif melalui sintesis tematik yang berlangsung dalam empat langkah. *Pertama*, pembacaan dan pengodean. Setiap argumen, istilah, dan rujukan dalam kedua kajian dikodekan menurut tema: hakikat AI, personalitas hukum, kesenjangan pertanggungjawaban, doktrin kesalahan, pembuktian, pertanggungjawaban korporasi, dan pembaruan

hukum. *Kedua*, pemetaan dan perbandingan. Posisi kedua kajian pada setiap tema dibandingkan untuk menemukan konvergensi (titik temu), divergensi (titik beda), dan hal yang hanya dibahas oleh salah satu kajian. *Ketiga*, penafsiran dan sistematisasi. Titik beda diuji dengan penafsiran terhadap asas legalitas dan asas kesalahan sebagai batas normatif; argumen yang tidak sejalan dengan asas tersebut tidak dijadikan dasar rekonstruksi. *Keempat*, rekonstruksi. Hasil pengujian dirumuskan menjadi satu model atribusi pertanggungjawaban yang dapat diuji, beserta implikasinya bagi pembaruan hukum.

HASIL DAN PEMBAHASAN

Pembahasan disusun mengikuti dua rumusan masalah. Rumusan pertama dijawab melalui tiga dimensi filsafat ilmu, yaitu ontologi, epistemologi, dan aksiologi. Rumusan kedua dijawab melalui analisis kesenjangan pertanggungjawaban, perbandingan posisi kedua kajian, perumusan model atribusi bertingkat, pembuktian dan tata kelola korporasi, serta implikasi bagi pembaruan hukum Indonesia.

Ontologi AI: entitas komputasional bukan otomatis pribadi hukum

Secara ontologis, AI paling tepat dipahami sebagai sistem sosio-teknis: model komputasional berjalan melalui perangkat keras, perangkat lunak, data, infrastruktur, organisasi, dan keputusan manusia. Menggambarkannya hanya sebagai "algoritma" mengabaikan kondisi material dan institusional yang memungkinkan sistem bekerja. Sebaliknya, menyebut AI sebagai "entitas" tidak dengan sendirinya memberinya status sebagai orang atau subjek hukum.

Pembedaan Descartes antara *res extensa* dan *res cogitans* dapat dipakai secara terbatas untuk menandai perbedaan antara infrastruktur material dan proses komputasional. Namun, algoritma atau representasi informasi tidak dapat begitu saja disamakan dengan substansi berpikir atau kesadaran. Kerangka dualisme itu bukan bukti empiris tentang ada atau tidaknya kesadaran mesin; ia hanya membantu memperjelas bahwa keberadaan perangkat komputasi dan keberadaan pengalaman subjektif merupakan klaim yang berbeda. Dengan demikian, naskah ini tidak menyatakan secara metafisik bahwa kesadaran mesin mustahil, melainkan bahwa kemampuan yang teramati saat ini tidak cukup untuk membuktikan agensi moral yang diperlukan bagi celaan pidana.

Personalitas hukum juga bukan sekadar label ontologis. Hukum dapat memberikan kapasitas terbatas kepada entitas nonmanusia untuk tujuan tertentu, tetapi pengakuan tersebut tidak serta-merta menjawab apakah entitas itu layak dicela atau dipidana. Bryson, Diamantis, dan Grant memperingatkan

bahwa penciptaan personalitas hukum bagi entitas sintetis dapat mempersulit akuntabilitas dan berisiko menjadi sarana pengalihan tanggung jawab manusia. (Bryson et al., 2017). Perdebatan dalam filsafat hukum pidana tetap terbuka: Simmler dan Markwalder menunjukkan bahwa konsep kesalahan dan kelayakan menjadi agen pertanggungjawaban memiliki dimensi sosial, sehingga argumen tentang ketidakmungkinan personalitas pidana AI tidak seharusnya diperlakukan sebagai aksioma tanpa pembahasan. (Simmler & Markwalder, 2018).

Untuk hukum pidana, pertanyaan yang lebih terarah bukan "apakah AI hidup atau berpikir seperti manusia", melainkan apakah sistem dapat memenuhi fungsi normatif yang menjadi dasar subjek pidana: memahami larangan, merespons alasan, memiliki kapasitas untuk dicela, dan menerima sanksi dengan cara yang sesuai tujuan pidana. Literatur kriminalitas robot menekankan bahwa sistem AI saat ini tidak memahami tanggung jawab moral atau makna pidana retributif sebagaimana manusia. (Gless et al., 2016). Oleh karena itu, status AI sebagai subjek pidana tidak dapat diturunkan hanya dari otonomi operasional atau kemampuan menghasilkan tindakan yang tidak diperintahkan secara langsung.

Epistemologi: Luaran AI, Keterjelasan, dan Pembuktian

Dimensi epistemologis menanyakan bagaimana suatu klaim tentang AI diketahui dan dibuktikan. Keluaran sistem bukan pengetahuan netral yang berdiri sendiri: hasilnya dipengaruhi data, tujuan optimasi, desain model, konteks penerapan, serta interpretasi pengguna. Karena itu, keluaran yang tampak meyakinkan tidak boleh diterima sebagai bukti niat, pengetahuan, atau kesalahan tanpa pemeriksaan atas proses dan konteksnya.

Kompleksitas sistem dapat mempersulit identifikasi kontribusi tiap aktor dan rekonstruksi sebab-akibat. Namun, istilah "kotak hitam" tidak boleh digunakan sebagai jalan pintas untuk menyimpulkan bahwa sistem sama sekali tidak dapat dipahami atau bahwa tidak ada manusia yang bertanggung jawab. De Sio dan Mecacci menekankan bahwa masalah pertanggungjawaban muncul dari sumber teknis, organisasi, hukum, etika, dan sosial yang berbeda; rancangan sistem yang mempertahankan kendali manusia yang bermakna merupakan salah satu respons, tetapi bukan solusi tunggal. (de Sio & Mecacci, 2021).

Dari sini, transparansi, dokumentasi, pencatatan versi model, dan jejak audit memiliki fungsi epistemik dan prosedural: membantu penyidik dan pengadilan menilai apa yang dilakukan sistem, siapa yang menetapkan tujuan dan parameter, risiko apa yang diketahui, serta langkah pengawasan yang

tersedia. Kewajiban tersebut tidak boleh membalik beban pembuktian pidana atau menggantikan pembuktian unsur tindak pidana dan kesalahan. Pembagian tanggung jawab di antara pengembang, penyedia, operator, dan pengguna lebih tepat dinilai melalui bukti konkret mengenai kendali, kontribusi, kewajiban, pengetahuan, serta kemampuan mencegah akibat.

Aksiologi: Asas kesalahan, Martabat manusia, dan Perlindungan masyarakat

Dimensi aksiologis menguji nilai yang hendak diwujudkan oleh pengaturan. Dalam hukum pidana, perlindungan masyarakat dan korban harus diseimbangkan dengan legalitas, kesalahan personal, proporsionalitas, dan perlindungan dari pemidanaan tanpa dasar kesalahan. Menyebut sistem AI sebagai penyebab teknis tidak cukup untuk menentukan siapa yang patut dipidana; sebaliknya, kompleksitas teknologi juga tidak boleh menjadi alasan otomatis untuk membebaskan seluruh aktor manusia dan korporasi.

Karena pidana menyatakan celaan publik, penerapannya terhadap entitas yang tidak terbukti mampu memahami norma menimbulkan persoalan legitimasi. Namun, penolakan terhadap pemidanaan AI tidak berarti menolak pertanggungjawaban manusia. Gless, Silverman, dan Weigend berpendapat bahwa pengguna yang dengan sengaja memakai robot untuk mencelakakan orang dapat dipertanggungjawabkan, dan kelalaian operator dapat relevan ketika risiko kehilangan kendali dapat diperkirakan serta langkah pencegahan yang wajar diabaikan. (Gless et al., 2016).

Aksiologi juga mengingatkan agar "efisiensi penegakan hukum" tidak menjadi alasan untuk menerapkan *strict liability* pidana secara luas. Tanggung jawab mutlak dapat dipertimbangkan dalam ranah regulasi atau kompensasi sesuai dasar hukum yang jelas, tetapi pertanggungjawaban pidana tetap mensyaratkan dasar normatif dan pembuktian yang konsisten dengan asas kesalahan. Pembedaan antara pertanggungjawaban pidana, administratif, perdata, dan kewajiban tata kelola harus dinyatakan secara eksplisit.

Model Atribusi Pertanggungjawaban Pidana yang Bertingkat

Artikel ini mengusulkan model atribusi bertingkat berbasis perbuatan, kendali, keterdugaan, dan kesalahan, bukan pengakuan AI sebagai subjek pidana. Model ini memiliki empat tahap analitis:

1. Klasifikasi peran AI. Tentukan apakah AI hanya alat yang digunakan dengan sengaja, sistem pendukung keputusan, atau sistem yang menghasilkan tindakan adaptif dengan intervensi langsung terbatas. Klasifikasi ini menjelaskan konteks faktual, tetapi tidak menentukan kesalahan dengan sendirinya.

2. Identifikasi aktor dan kontribusi. Petakan pengembang, penyedia, pemilik, operator, pengguna, serta korporasi; tentukan perbuatan atau pembiaran spesifik masing-masing, bukan membebankan tanggung jawab berdasarkan jabatan atau kedekatan dengan teknologi semata.
3. Uji kesalahan dan atribusi. Untuk setiap aktor, periksa kesengajaan atau kealpaan yang relevan menurut norma pidana, kewajiban kehati-hatian yang berlaku, tingkat kendali, pengetahuan atau keterdugaan risiko, kemampuan mencegah akibat, serta hubungan kausal. Jika AI dipakai secara sadar sebagai sarana tindak pidana, analisis diarahkan pada pelaku manusia dan/atau korporasi sesuai unsur delik. Jika akibat timbul tanpa maksud langsung, pertanggungjawaban hanya layak dibebankan jika unsur kealpaan atau bentuk kesalahan lain dapat dibuktikan berdasarkan hukum positif.
4. Pilih respons hukum yang tepat. Pisahkan pidana dari tindakan pencegahan dan pemulihan. Pengamanan, penghentian sementara, audit, atau perbaikan sistem dapat menjadi kewajiban tata kelola atau konsekuensi administratif apabila ada dasar hukumnya; tindakan tersebut bukan pengganti pembuktian kesalahan pidana.

Model ini berangkat dari kenyataan bahwa siklus pengembangan, penerapan, dan penggunaan teknologi kompleks saling beririsan; beberapa aktor mungkin memiliki pengaruh tanpa seorang pun menguasai keseluruhan sistem. Custers, Lahmann, dan Scott mengusulkan agar analisis tanggung jawab memperhatikan kontribusi bersama, pencegahan, dan pengaruh para pihak, sekaligus mengingatkan bahwa pembagian tanggung jawab yang terlalu luas dapat menimbulkan efek menghambat inovasi. (Custers et al., 2025). Gagasan tersebut berguna sebagai lensa tata kelola dan atribusi, tetapi tidak boleh disalin begitu saja menjadi dasar pemidanaan karena artikel tersebut terutama membahas tanggung jawab hukum privat, bukan unsur pertanggungjawaban pidana.

Model ini menolak dua ekstrem. Pertama, *strict liability* tidak dijadikan jawaban umum atas semua akibat yang melibatkan AI. Kedua, *shared responsibility* tidak dipahami sebagai tanggung jawab pidana kolektif tanpa pemetaan kesalahan individual atau korporasi. Untuk pelanggaran yang secara sengaja dilakukan dengan AI, hukum pidana yang sudah mengatur perbuatan tersebut tetap dianalisis terlebih dahulu. Untuk risiko yang lahir dari kegagalan tata kelola, kewajiban audit, pengujian, pencatatan, keamanan, dan pengawasan dapat memperjelas standar kehati-hatian—namun pelanggaran standar itu baru

menjadi dasar pidana apabila peraturan yang berlaku mengkriminalisasikannya dan seluruh unsur delik terbukti.

Rekonstruksi Konsep Subjek Hukum dan Pertanggungjawaban Pidana dalam Kejahatan Siber Berbasis Kecerdasan Buatan untuk Mewujudkan Sistem Hukum Pidana Indonesia yang Berkeadilan dan Berkepastian Hukum

Perkembangan kecerdasan buatan menimbulkan tantangan terhadap teori pertanggungjawaban pidana konvensional. AI merupakan kemampuan sistem komputasi untuk menjalankan tugas yang umumnya membutuhkan kecerdasan manusia, seperti belajar, bernalar, mengenali pola, memprediksi, dan mengambil keputusan. Berbeda dengan perangkat lunak konvensional yang bekerja berdasarkan instruksi tetap, AI modern mampu meningkatkan kinerjanya melalui pengalaman (Nazhir & Utama, 2025).

Perkembangan tersebut didorong oleh *machine learning*, yaitu metode komputasi yang memungkinkan sistem mempelajari pola dari kumpulan data dan menghasilkan prediksi tanpa harus diprogram untuk setiap kemungkinan situasi. *Deep learning* sebagai bagian dari *machine learning* memanfaatkan jaringan saraf tiruan berlapis untuk mengolah informasi kompleks, seperti gambar, bahasa, dan data perilaku. Meskipun telah diterapkan dalam berbagai bidang, termasuk kendaraan otonom, pengenalan wajah, dan diagnosis medis, kompleksitas proses pengambilan keputusan AI sering kali menyulitkan penelusuran dasar suatu keputusan (Hassan Raza, 2026). Karakteristik tersebut menimbulkan persoalan hukum dalam menentukan hubungan kausalitas, memperkirakan akibat suatu tindakan, serta mengidentifikasi pihak yang harus memikul pertanggungjawaban pidana.

Karakteristik pengambilan keputusan otonom semakin memperumit persoalan pertanggungjawaban pidana karena sistem AI mampu mengumpulkan informasi, mengevaluasi berbagai alternatif, dan melaksanakan tindakan tanpa intervensi langsung manusia. Meskipun manusia tetap berperan dalam perancangan, penerapan, dan pengawasan sistem, meningkatnya otonomi AI dapat memperlemah hubungan kausal antara kehendak manusia dan tindakan yang dihasilkan teknologi tersebut. Kondisi ini memunculkan *accountability gap*, yaitu kesenjangan pertanggungjawaban ketika suatu tindakan AI menimbulkan kerugian, tetapi doktrin hukum yang berlaku belum mampu mengidentifikasi pihak yang secara memadai dapat dimintai pertanggungjawaban karena akibat tersebut tidak sepenuhnya dikehendaki atau diperkirakan oleh pihak-pihak yang terlibat (Romadlon Adi Ali Fikri, 2026).

Doktrin hukum pidana Indonesia secara konvensional mensyaratkan adanya kesalahan (*schuld*) sebagai dasar pertanggungjawaban pidana, baik dalam bentuk kesengajaan (*dolus*) maupun kealpaan (*culpa*), sebagaimana tercermin dalam asas geen straf zonder schuld. Prinsip tersebut ditegaskan dalam Pasal 37 huruf a Undang-Undang Nomor 1 Tahun 2023 tentang KUHP yang mensyaratkan adanya kesalahan pada diri pelaku untuk menjatuhkan pidana. Namun, penerapannya menjadi kompleks ketika perbuatan yang menimbulkan akibat pidana dihasilkan oleh sistem machine learning yang bersifat otonom atau semiotonom, karena keluaran algoritmanya dapat berkembang melalui proses komputasi probabilistik dan adaptif tanpa intervensi langsung manusia.

Persoalan tersebut berkaitan dengan dua kendala utama, *yakni human control problem*, berupa terbatasnya kendali manusia atas tindakan AI, dan *explainability problem*, yaitu sulitnya memahami serta menelusuri proses pengambilan keputusan internal AI. Kedua persoalan ini menunjukkan keterbatasan doktrin pertanggungjawaban pidana konvensional dalam mengatribusikan kesalahan dan menegaskan perlunya pembaruan konseptual agar otonomi teknologi tetap dapat dipertanggungjawabkan berdasarkan prinsip legalitas, kepastian hukum, dan keadilan (Sihombing & Nuraeni, 2026).

Salah satu pendekatan untuk mengatasi kesenjangan pertanggungjawaban (*accountability gap*) akibat penggunaan AI adalah melalui pengaturan terhadap tahap perancangan, pengembangan, penerapan, dan pemanfaatannya. Teknologi yang berpotensi menimbulkan dampak berbahaya dan sulit diprediksi memerlukan pembatasan serta pengawasan yang ketat, sebagaimana penerapan regulasi terhadap teknologi nuklir untuk meminimalkan risiko kecelakaan. Pendekatan serupa perlu diterapkan terhadap AI melalui dua aspek, yaitu peningkatan tanggung jawab pengembang berdasarkan kemampuan mereka dalam memahami dan memprediksi risiko sistem yang dikembangkan, serta penguatan peran masyarakat dan lembaga regulator dalam mengawasi pemanfaatan dan mencegah penyalahgunaan AI. Seiring meningkatnya pemahaman terhadap karakteristik dan risiko AI, kemampuan untuk mengantisipasi dampak penggunaannya juga semakin berkembang sehingga pembentukan regulasi yang mengatur pengembangan dan penerapan sistem AI berisiko tinggi menjadi kebutuhan penting untuk menjamin kepastian hukum dan mencegah timbulnya kerugian (Stamatiou, 2026).

Persoalan pertanggungjawaban pidana semakin kompleks ketika AI secara tidak sengaja menimbulkan kerugian serius, seperti kerusakan harta benda atau hilangnya nyawa manusia, sementara akibat tersebut tidak diperkirakan maupun dikehendaki oleh pihak yang terlibat. Dalam kondisi

demikian, doktrin pertanggungjawaban pidana, termasuk *constructive liability*, perlu dikaji dan dikembangkan agar dapat mengakomodasi tindak pidana yang melibatkan AI. Salah satu alternatifnya ialah membentuk pengaturan khusus mengenai kejahatan berbasis AI (*AI Crime Act*) yang mengatur pertanggungjawaban atas penggunaan AI secara sengaja maupun lalai oleh pengembang, pengguna, pemilik, pengelola, dan pelatih sistem. Namun, pendekatan tersebut menghadapi keterbatasan ketika AI memiliki tingkat otonomi yang semakin tinggi, sehingga tidak lagi dapat dipandang semata-mata sebagai alat yang sepenuhnya berada di bawah kendali manusia. Situasi ini menimbulkan dilema hukum dalam menentukan pihak yang patut dipidana, sebab pembebanan tanggung jawab secara otomatis kepada pengembang atau pengguna berpotensi mengabaikan unsur kesalahan sekaligus menghambat inovasi teknologi.

Mekanisme pertanggungjawaban hukum dapat diterapkan melalui empat pendekatan, yaitu pertanggungjawaban berbasis kausalitas (*causation-based liability*) dengan mengidentifikasi pihak yang secara langsung menyebabkan kerugian; pertanggungjawaban berbasis kendali (*control-based liability*) dengan membebankan tanggung jawab kepada pihak yang memiliki kendali signifikan atas AI; tanggung jawab mutlak (*strict liability*) terhadap aktivitas AI berisiko tinggi tanpa mensyaratkan pembuktian unsur kelalaian; serta tanggung jawab pengganti (*vicarious liability*) yang membebankan pertanggungjawaban kepada pemilik atau korporasi atas tindakan AI yang berada dalam lingkup pengelolaannya. Penerapan keempat pendekatan tersebut diharapkan dapat membangun mekanisme pertanggungjawaban yang komprehensif sekaligus mencegah kekosongan hukum yang memungkinkan pihak-pihak terkait menghindari tanggung jawab atas kerugian yang ditimbulkan AI.

Manusia tetap menjadi subjek utama pertanggungjawaban hukum, baik dalam kapasitasnya sebagai pengembang, pengguna, pemilik, maupun korporasi, mengingat AI belum memiliki kesadaran, kehendak, dan kemampuan penilaian moral sebagaimana manusia. Meskipun demikian, tindakan AI dapat menimbulkan kewajiban hukum bagi pihak yang memiliki kendali atas pengoperasiannya. Pengembang bertanggung jawab atas cacat desain atau algoritma, penyedia platform atas pengawasan, pemeliharaan, dan pembaruan sistem, sedangkan pengguna bertanggung jawab atas penyalahgunaan atau pengoperasian yang lalai. Pendekatan ini mencerminkan karakteristik ekosistem AI yang melibatkan banyak pihak sekaligus mencegah terjadinya kekosongan pertanggungjawaban hukum (Custers, et al. 2025).

Pembagian pertanggungjawaban antara pengembang, penyedia platform, pengguna, dan korporasi mencerminkan pergeseran paradigma hukum dari pendekatan yang berpusat pada pelaku tunggal menuju konstruksi pertanggungjawaban yang bersifat kolektif dan proporsional. Secara ontologis, AI dipahami sebagai entitas teknologi yang memiliki kemampuan operasional dan otonomi tertentu, tetapi belum dapat disamakan dengan manusia sebagai subjek hukum yang memiliki kesadaran, kehendak, dan pertimbangan moral. Secara epistemologis, penentuan pertanggungjawaban tidak cukup didasarkan pada hubungan kausal antara tindakan dan akibat, tetapi harus mempertimbangkan kontribusi, tingkat kendali, kemampuan mengantisipasi risiko, serta kewajiban masing-masing pihak dalam siklus pengembangan dan penggunaan AI. Sementara itu, secara aksiologis, pembebanan tanggung jawab harus berorientasi pada keadilan, kepastian hukum, dan perlindungan kepentingan masyarakat agar tidak terjadi pengalihan tanggung jawab maupun kekosongan hukum. Konsep *shared responsibility* menjadi landasan rekonstruksi pertanggungjawaban hukum yang lebih adaptif terhadap karakteristik teknologi AI tanpa mengabaikan prinsip fundamental hukum pidana dan nilai-nilai keadilan.

Rekonstruksi normatif pertanggungjawaban pidana dalam kejahatan siber berbasis AI memerlukan perluasan doktrin kesalahan (*schuld*) agar mencakup kegagalan dalam mengawasi, mengendalikan, dan memitigasi risiko yang ditimbulkan oleh sistem AI. Dalam doktrin hukum pidana klasik, asas *geen straf zonder schuld* menempatkan kesalahan, baik berupa kesengajaan (dolus) maupun kealpaan (culpa), sebagai dasar penjatuhan pidana. Namun, dalam kejahatan siber berbasis AI, kesalahan tidak hanya dapat diwujudkan melalui kehendak langsung manusia, tetapi juga melalui kelalaian dalam merancang sistem, lemahnya perlindungan keamanan siber, tidak memadainya pengawasan algoritma, serta kegagalan mengantisipasi risiko teknologi yang dapat diperkirakan (Andreas Matthias, 2004).

Meskipun KUHP Indonesia telah mengakui pertanggungjawaban berdasarkan kealpaan dan pertanggungjawaban pidana korporasi, pengaturannya belum secara khusus mengakomodasi kewajiban pengawasan algoritmik, tata kelola risiko AI, dan tanggung jawab pengawasan terhadap sistem komputasi otonom. Padahal, kompleksitas AI menuntut adanya kewajiban penilaian risiko, mekanisme audit, pengawasan manusia, dan jaminan keamanan sistem, khususnya pada penerapan AI berisiko tinggi. Pengembangan konsep *algorithmic negligence* merupakan bentuk perluasan kealpaan yang memungkinkan pertanggungjawaban pidana dibebankan kepada

pengembang, operator, atau pihak yang menerapkan AI apabila kegagalan pengawasan maupun penerapan teknologi secara ceroboh menimbulkan akibat yang seharusnya dapat diperkirakan dan dicegah (Ryan Abbot, 2020). Pendekatan ini dapat menjadi dasar rekonstruksi hukum pidana Indonesia yang lebih adaptif terhadap perkembangan teknologi tanpa mengesampingkan asas kesalahan dan kepastian hukum.

Rekonstruksi hukum pembuktian dalam kejahatan siber berbasis AI perlu mengakomodasi kewajiban transparansi algoritma, dokumentasi sistem, dan rekam jejak audit (*audit trails*) sebagai bagian integral dari mekanisme pembuktian pidana. Pasal 5 dan Pasal 6 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 telah mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah. Namun, ketentuan tersebut belum secara khusus mengatur kewajiban pembuktian yang berkaitan dengan sistem AI, seperti penyimpanan log algoritma, kumpulan data pelatihan (*training datasets*), rekaman proses pengambilan keputusan, serta dokumentasi yang menjelaskan keluaran sistem.

Akibatnya, belum terdapat standar yang memadai bagi penyidik, penuntut umum, dan hakim dalam memverifikasi, mengautentikasi, serta menilai bukti yang dihasilkan atau diproses oleh sistem komputasi otonom. Persoalan ini semakin kompleks karena karakteristik black box pada AI menyebabkan proses pengambilan keputusan sulit ditelusuri, bahkan oleh pengembangnya sendiri. Transparansi dan keterlacakan algoritma perlu ditempatkan sebagai prasyarat akuntabilitas hukum agar hubungan kausal antara proses algoritmik dan akibat yang ditimbulkan dapat dibuktikan secara objektif serta menjamin kepastian dan keadilan dalam proses peradilan pidana.

Rekonstruksi normatif pertanggungjawaban pidana korporasi perlu diarahkan pada penguatan kewajiban tata kelola risiko AI dan keamanan siber sebagai dasar penilaian kesalahan korporasi. Persoalan mendasarnya terletak pada doktrin kesalahan hukum pidana Indonesia yang masih berorientasi pada kesalahan individual, sedangkan kejahatan siber berbasis AI dapat bersumber dari kelalaian organisasi secara sistemik, seperti lemahnya pengawasan algoritma, pengendalian internal, tata kelola data, serta tidak tersedianya audit risiko secara memadai. Meskipun Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, Undang-Undang Informasi dan Transaksi Elektronik, dan Undang-Undang Pelindungan Data Pribadi telah mengakui korporasi sebagai subjek hukum, pengaturannya belum secara khusus merumuskan konsep *organizational fault* dalam penerapan AI dan sistem pengambilan keputusan

otomatis. Diperlukan pengembangan doktrin pertanggungjawaban pidana korporasi yang tidak hanya didasarkan pada kesengajaan individu, tetapi juga mempertimbangkan kegagalan sistem kepatuhan dan tata kelola teknologi, terutama ketika korporasi menerapkan AI berisiko tinggi tanpa mekanisme pengamanan, pengawasan, dan mitigasi risiko yang memadai. Kegagalan organisasi dalam mencegah risiko teknologi yang dapat diperkirakan perlu dipertimbangkan sebagai dasar atribusi kesalahan korporasi, sepanjang unsur-unsur pertanggungjawaban pidana dapat dibuktikan (Haditama & Sugianto, 2025).

Perkembangan kecerdasan buatan dalam kejahatan siber menuntut rekonstruksi konsep subjek hukum dan pertanggungjawaban pidana yang tidak lagi semata-mata bertumpu pada pendekatan konvensional, tetapi mampu mengakomodasi karakteristik otonomi, kompleksitas algoritma, dan keterlibatan berbagai aktor dalam ekosistem AI. Rekonstruksi tersebut perlu diarahkan pada penegasan kedudukan AI dalam sistem hukum, pembagian pertanggungjawaban secara proporsional berdasarkan kontribusi, tingkat kendali, dan kesalahan pengembang, operator, pengguna, serta korporasi, disertai penguatan tata kelola risiko dan mekanisme pembuktian digital. Pembaruan hukum pidana Indonesia diharapkan mampu mengatasi kesenjangan pertanggungjawaban (*accountability gap*), mencegah impunitas, serta memastikan bahwa setiap kerugian akibat kejahatan siber berbasis AI dapat ditangani melalui mekanisme hukum yang menjunjung tinggi asas legalitas, kesalahan, keadilan, dan kepastian hukum.

KESIMPULAN

Pertama, jawaban atas rumusan masalah pertama: secara ontologis, AI adalah sistem sosio-teknis berwujud ganda yang memadukan infrastruktur fisik dengan struktur informasional dan komputasional, dan keberadaannya tidak membuktikan adanya kesadaran atau agensi moral. Secara epistemologis, keluaran AI dipengaruhi bias data, algoritma, dan interpretasi sehingga tidak dapat dibaca sebagai bukti niat atau kesalahan tanpa pemeriksaan atas proses dan konteksnya; transparansi, dokumentasi, dan jejak audit diperlukan agar kontribusi dan keterdugaan risiko dapat dibuktikan. Secara aksiologis, perlindungan masyarakat harus berjalan bersama legalitas, asas kesalahan, dan proporsionalitas. Atas dasar itu AI belum layak diperlakukan sebagai subjek pidana, dan pengakuan subjek hukum elektronik tidak diperlukan untuk menjawab persoalan yang ada saat ini.

Kedua, jawaban atas rumusan masalah kedua: pertanggungjawaban pidana dalam kejahatan siber yang melibatkan AI perlu direkonstruksi melalui model atribusi bertingkat. Tingkat pertama mencakup penggunaan AI secara sengaja sebagai sarana tindak pidana, yang dianalisis berdasarkan delik yang sudah ada terhadap pelaku manusia atau korporasi. Tingkat kedua mencakup kelalaian yang dapat diperkirakan, yang dapat dijangkau melalui pengembangan doktrin *algorithmic negligence* dan *organizational fault* sepanjang dikriminalisasi dan unsurnya terbukti. Tingkat ketiga mencakup kejadian yang tidak dapat secara wajar diantisipasi, yang tidak menimbulkan pidana tetapi tetap dapat memicu tindakan pencegahan, perbaikan sistem, dan pemulihan sesuai dasar hukum. Dalam model ini, *shared responsibility* berfungsi sebagai lensa untuk memetakan kontribusi dan kesalahan setiap aktor, sedangkan *strict liability* dan *vicarious liability* ditempatkan secara terukur dan tidak menjadi jawaban umum.

Sebagai saran, penelitian lanjutan perlu menguji ketentuan KUHP yang berlaku sejak 2026, UU Penyesuaian Pidana 2026, UU ITE beserta perubahan dan putusan pengujiannya, serta aturan sektoral melalui pembacaan pasal demi pasal, agar klaim tentang kekosongan norma dapat dipastikan. Penelitian lanjutan juga dapat memperkaya model dengan telaah putusan pengadilan, perbandingan yurisdiksi lain secara lebih mendalam, dan pengujian empiris terhadap kemampuan penyidik dalam memeriksa bukti yang dihasilkan sistem AI. Keterbatasan artikel ini, yakni bertumpu pada dua kajian dan literatur yang dikutipnya, perlu diperhatikan dalam membaca kesimpulan di atas.

DAFTAR PUSTAKA

Abbott, R. (2020). *The reasonable robot: Artificial intelligence and the law*. Cambridge University Press.

Bayer, S., & Weber, I. (2026). *Human-in-command governance for multi-agent scientific workflows* (hal-05466131).

Bostrom, N. (n.d.). *Nick Bostrom on artificial intelligence*. Oxford Martin School, University of Oxford. https://www.oxfordmartin.ox.ac.uk/blog/nick-bostrom-on-artificial-intelligence (diakses 4 November 2026).

Bryson, Joanna J., Mihailis E. Diamantis, dan Thomas D. Grant. "Of, for, and by the People: The Legal Lacuna of Synthetic Persons." *Artificial Intelligence and Law* 25 (2017). https://doi.org/10.1007/s10506-017-9214-9.

Custers, Bart, Henning Lahmann, dan Benjamyn I. Scott. "From Liability Gaps to Liability Overlaps: Shared Responsibilities and Fiduciary Duties

in AI and Other Complex Technologies." *AI & Society* (2025). https://doi.org/10.1007/s00146-024-02137-1.

de Sio, Filippo Santoni, dan Giulio Mecacci. "Four Responsibility Gaps with Artificial Intelligence: Why They Matter and How to Address Them." *Philosophy & Technology* 34 (2021). https://doi.org/10.1007/s13347-021-00450-x.

Fikri, R. A. A., dkk. (2026). Pertanggungjawaban hukum agentic artificial intelligence dalam pelaksanaan tindakan pada sistem elektronik. *Jurnal Review Pendidikan dan Pengajaran, 9*(4), 2120.

Fransisco, W. (2025). Drafting laws for the lifeless: A legal framework for criminal liability and punishment for artificial intelligence. *Jurnal Hukum dan Peradilan, 14*(3), 702–703, 725–726.

Gless, Sabine, Emily Silverman, dan Thomas Weigend. "If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability." *New Criminal Law Review* 19, no. 3 (2016). https://doi.org/10.1525/nclr.2016.19.3.412.

Habibi, H., dkk. (2026). Tanggung jawab hukum atas kejahatan siber yang melibatkan teknologi artificial intelligence di Indonesia. *Dewantara, 5*, 449. [nomor terbitan perlu dilengkapi]

Haditama, T. K., & Sugianto, F. (2025). A comparative analysis of corporate criminal liability for AI-based malware: A study of Indonesian and European Union law. *Indonesia Law Reform Journal, 5*(2), 308–322.

Hawkins, D. J. B. (1954). *Being and becoming: An essay towards a critical metaphysic.*

Johnson, D. (2026). *When AI hurts people, who's to blame? Global experts grapple with accountability*. United Nations. https://news.un.org/en/story/2026/07/1167886 (diakses 5 November 2026).

Kemkomdigi. (n.d.). *Siaran pers: Kemkomdigi ingatkan ancaman AI, penipuan kini bisa meniru suara dan identitas*. https://www.komdigi.go.id/berita/siaran-pers/detail/kemkomdigi-ingatkan-ancaman-ai-penipuan-kini-bisa-meniru-suara-dan-identitas (diakses 5 November 2026).

Knecht, L., dkk. (2025). *AI and cybercrime: A policy framework for organizational defense*. University of Applied Sciences and Arts Northwestern Switzerland FHNW, School of Business, Institute for Information Systems. https://www.fhnw.ch/plattformen/digitrust/wp-content/uploads/sites/340/ac2025_ai_and_cybercrime_a_framework_submission_code_60.pdf (diakses 30 Oktober 2026).

Mahardhika, V., dkk. (2023). Could artificial intelligence be the subject of criminal law? *Yustisia, 12*(1), 3.

Maia, J. S. V. D. M. (2023). Res cogitans dan res extensa sebagai substansi pembentuk ruang dan waktu dalam terang rasionalisme Descartes. *Jurnal Borneo Humaniora*, 56–64.

Marzuki, P. M. (2010). *Penelitian hukum*. Kencana Prenada Media Group.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology, 6*, 175–183.

Nazhir, S. A. M., & Utama, A. S. (2025). Artificial intelligence and criminal liability: Reassessing mens rea in the age of autonomous systems. *Indonesian Journal of Digital Crime and Criminal Justice, 1*(1), 9.

Prayogi, A., & Nasrullah, R. (2024). Artificial intelligence dan filsafat ilmu: Bagaimana filsafat memandang kecerdasan buatan sebagai ilmu pengetahuan. *LogicLink: Journal of Artificial Intelligence and Multimedia in Informatics, 1*(2), 144–155.

Raza, H., dkk. (2026). Machine learning driven decision making in the modern data era. *Perfect, 3*(1), 11.

Republik Indonesia. (2023). *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*.

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2026). *Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana*.

Sihombing, L. A., & Nuraeni, Y. (2026). Reconstructing criminal liability for AI-enabled cybercrime in Indonesia: Toward a normative framework of responsibility. *Al-Risalah, 26*(2), 49.

Simmler, Monika, dan Nora Markwalder. "Guilty Robots? Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence." *Criminal Law Forum* 29 (2018). https://doi.org/10.1007/s10609-018-9363-3.

Stark, F. (2023). Deconstructing constructive liability. *Criminal Law Review*, 1–2.