**Dewantara: Jurnal Pendidikan Sosial Humaniora**
**Volume 5, Nomor 2, Juni 2026**
e-ISSN: 2962-1127; p-ISSN: 2962-1135, Hal. 448-459
DOI: https://doi.org/10.30640/dewantara.v5i2.6908
Tersedia:https://jurnaluniv45sby.ac.id/index.php/Dewantara

# Tanggung Jawab Hukum atas Kejahatan Siber yang Melibatkan Teknologi *Artificial Intelligence* di Indonesia

**Haris Habibi[1*], Suci Ramadani[2], Rahmayanti[3], Khairuddin Siregar[4], Jhoni Muda Pratama Barus[5]**
[1,4-5]Mahasiswa Magister Hukum, Universitas Pembangunan Panca Budi, Indonesia
[2-3]Dosen Magister Hukum, Universitas Pembangunan Panca Budi, Indonesia
*Email: harishabibi19@gmail.com[1] , jhonibarus1993@gmail.com [3]*
[*]*Penulis Korespondensi: harishabibi19@gmail.com*

***Abstract.*** *The rapid advancement of Artificial Intelligence (AI) technology has fundamentally transformed the landscape of cybercrime in Indonesia by giving rise to various forms of digital offenses that have not been adequately accommodated within the existing legal framework. This study aims to examine the legal regulation of AI-based cybercrime in Indonesia and the legal liability framework applicable to developers, operators, and users when AI systems are utilized to commit criminal acts. This study employs a normative legal research method using statutory, conceptual, and case approaches through the analysis of primary legal materials, including the Law on Electronic Information and Transactions and its amendments, as well as Law No. 27 of 2022 on Personal Data Protection. The findings reveal a significant normative gap, as Indonesia's cybercrime legislation has not been designed to accommodate the autonomous behavior of AI systems. This study concludes that Indonesia requires a dedicated AI governance framework that explicitly regulates the distribution of criminal and civil liability across the AI value chain in order to ensure legal certainty in addressing AI-based cybercrime.*

***Keywords:*** *AI Governance; Artificial Intelligence; Cybercrime; Electronic Information and Transactions Law; Legal Liability.*

**Abstrak.** Perkembangan teknologi *Artificial Intelligence* (AI) yang pesat telah mengubah secara fundamental lanskap kejahatan siber di Indonesia dengan memunculkan berbagai bentuk pelanggaran digital yang belum diakomodasi secara memadai dalam kerangka hukum yang berlaku. Penelitian ini bertujuan mengkaji pengaturan hukum terhadap kejahatan siber berbasis AI di Indonesia serta konstruksi tanggung jawab hukum pengembang, operator, dan pengguna ketika sistem AI dimanfaatkan untuk melakukan kejahatan. Penelitian menggunakan metode hukum normatif dengan pendekatan peraturan perundang-undangan, konseptual, dan kasus melalui analisis bahan hukum primer, termasuk Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Hasil penelitian menunjukkan adanya kesenjangan normatif karena legislasi kejahatan siber di Indonesia belum dirancang untuk mengakomodasi perilaku AI yang bersifat otonom. Penelitian ini menyimpulkan bahwa Indonesia memerlukan kerangka tata kelola AI yang secara khusus mengatur distribusi tanggung jawab pidana dan perdata di sepanjang rantai nilai AI guna menjamin kepastian hukum dalam penanganan kejahatan siber berbasis AI.

**Kata Kunci:** Kejahatan Siber; Kecerdasan Buatan; Tata Kelola AI; Tanggung Jawab Hukum; UU ITE.

## 1. LATAR BELAKANG

Kemajuan teknologi kecerdasan buatan atau *Artificial Intelligence* (AI) dalam satu dekade terakhir bukan sekadar persoalan inovasi teknis, melainkan telah merambah ke hampir seluruh dimensi kehidupan manusia modern termasuk dimensi kejahatan. Ketika AI mulai hadir tidak hanya sebagai alat bantu produktivitas tetapi juga sebagai infrastruktur yang memungkinkan terjadinya penipuan otomatis, pembuatan konten palsu (*deepfake*), peretasan berbasis machine learning, hingga rekayasa sosial yang dipersonalisasi secara presisi, maka pertanyaan hukum yang muncul bukan lagi sekadar tentang "siapa yang melakukan" melainkan

*Naskah Masuk: 25 April 2026; Revisi: 22 Mei 2026; Diterima: 28 Juni 2026; Terbit: 30 Juni 2026*

"siapa yang bertanggung jawab" ketika sebuah sistem otonom yang tidak memiliki kesadaran hukum turut mengambil bagian dalam suatu kejahatan.

Di Indonesia, fenomena ini sudah bukan sekadar proyeksi futuristik. Laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023 mencatat lebih dari 361 juta anomali trafik siber yang terdeteksi sepanjang tahun, meningkat signifikan dibandingkan tahun sebelumnya, dan sebagian insiden tersebut menggunakan metode serangan berkarakter algoritma adaptif, indikator kuat bahwa komponen AI mulai dimanfaatkan dalam ekosistem kejahatan digital (BSSN, 2023). Kasus-kasus nyata telah bermunculan: penipuan berbasis voice cloning yang memanipulasi suara pejabat keuangan perusahaan, penyebaran disinformasi melalui deepfake video yang melibatkan tokoh publik, hingga serangan ransomware yang menggunakan AI untuk mengidentifikasi celah keamanan secara otomatis dan real-time.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diubah melalui UU No. 19 Tahun 2016 dan terakhir UU No. 1 Tahun 2024 dirancang jauh sebelum AI generatif menjadi teknologi yang dapat diakses secara massal. Ketentuan-ketentuan UU ITE dirumuskan dengan asumsi bahwa pelaku kejahatan adalah manusia yang bertindak secara sadar dan disengaja, asumsi yang runtuh ketika berhadapan dengan skenario di mana sebuah sistem otonom secara mandiri menghasilkan konten ilegal atau melaksanakan serangan siber berdasarkan instruksi yang diprogramkan jauh sebelumnya oleh pihak yang mungkin tidak lagi terlibat secara aktif (Zulkarnain & Rahmayanti, 2026). Kondisi ini menciptakan apa yang disebut para ahli hukum teknologi sebagai "*accountability gap*" celah pertanggungjawaban yang berpotensi dimanfaatkan oleh pelaku kejahatan siber.

Sisi empiris permasalahan ini pun tidak kalah mengkhawatirkan. Kasus kebocoran data pribadi di Indonesia meningkat drastis, dari insiden kebocoran data BPJS Kesehatan pada 2021 hingga kebocoran data Pusat Data Nasional Sementara (PDNS) pada 2024 yang melumpuhkan layanan publik selama berminggu-minggu. Berbagai kasus doksing yang difasilitasi oleh agregasi data berbasis AI memperlihatkan betapa seriusnya ancaman ini dan betapa terbatasnya kapasitas hukum Indonesia untuk meresponsnya (Waruwu et al., 2026). Penegakan hukum atas kasus-kasus tersebut seringkali menemui kebuntuan karena ketiadaan norma yang secara eksplisit mengatur skenario di mana AI menjadi aktor intermediat dalam rantai kejahatan (Laia et al., 2025).

Dari perspektif komparatif, respons hukum internasional telah menunjukkan arah yang lebih tegas. Uni Eropa menerbitkan EU Artificial Intelligence Act yang berlaku efektif sejak Agustus 2024, mengklasifikasikan sistem AI berdasarkan tingkat risikonya dan mewajibkan akuntabilitas yang berbeda bagi setiap kategori. Sementara itu Indonesia masih berada pada

tataran kebijakan sektoral yang tersebar tanpa kerangka hukum koheren. Research gap yang ada pun cukup jelas, penelitian sebelumnya banyak yang membahas deepfake Syavica et al. (2025), kejahatan scammer digital Laia et al. (2025), atau kebocoran data Waruwu et al. (2026) secara parsial, namun belum ada yang memetakan secara komprehensif konstruksi pertanggungjawaban hukum atas kejahatan siber berbasis AI dalam satu kerangka analisis terpadu yang mencakup dimensi pidana, perdata, dan administratif sekaligus. Berdasarkan uraian tersebut, penelitian ini merumuskan dua permasalahan:

a. Bagaimana kerangka regulasi hukum yang berlaku di Indonesia dalam mengatur kejahatan siber berbasis AI?
b. Bagaimana konstruksi tanggung jawab hukum terhadap pengembang, operator, dan pengguna teknologi AI yang digunakan untuk kejahatan siber dalam perspektif hukum positif Indonesia?

## 2. KAJIAN TEORITIS

### Teori Pertanggungjawaban Hukum

Pertanggungjawaban hukum merupakan konsep fundamental yang merujuk pada kewajiban seseorang atau entitas tertentu untuk menanggung konsekuensi juridis atas perbuatan atau kelalaian yang telah dilakukannya. Dalam hukum pidana, pertanggungjawaban dibangun di atas dua elemen kumulatif actus reus (perbuatan jahat objektif) dan mens rea (niat jahat subjektif). Pasal 44 KUHP secara eksplisit menegaskan prinsip geen straf zonder schuld, tiada pidana tanpa kesalahan, yang menjadi fondasi bahwa seseorang hanya dapat dipidana apabila perbuatannya dapat dipertanggungjawabkan kepadanya (Moeljatno, 2008).

Persoalan menjadi jauh lebih kompleks ketika teori ini diterapkan pada konteks kejahatan siber berbasis AI. Sebagai entitas non-manusia yang tidak memiliki kesadaran, AI secara definitif tidak dapat memenuhi unsur mens rea. Namun tindakan yang dilakukan AI dapat menghasilkan dampak hukum yang nyata dan serius. Beberapa ahli hukum mengusulkan penerapan teori vicarious liability, pertanggungjawaban tidak langsung, di mana pihak yang menguasai agen bertanggung jawab atas tindakan agen tersebut (Bryson & Winfield, 2017). Konsep ini sebenarnya tidak asing dalam hukum Indonesia, karena Pasal 1365-1367 KUHPerdata sudah lama mengatur tanggung jawab seseorang atas perbuatan pihak yang berada di bawah pengawasannya.

Dalam perkembangan teori hukum kontemporer, muncul konsep distributed liability atau pertanggungjawaban terdistribusi yang lebih relevan untuk konteks AI. Konsep ini mengakui bahwa dalam ekosistem teknologi AI yang kompleks, tanggung jawab perlu

didistribusikan secara proporsional berdasarkan tingkat kontrol, keuntungan yang diperoleh, serta kemampuan untuk mencegah kerugian (Velez et al., 2017). KUHP baru (UU No. 1/2023) yang berlaku efektif 2026 memang memperluas konsep pertanggungjawaban korporasi, namun belum secara eksplisit mengatur pertanggungjawaban pengembang atau operator AI. Teori strict liability juga relevan di sini: jika pengoperasian sistem AI berisiko tinggi menyebabkan kerugian, maka pembuktian kesalahan subjektif seharusnya tidak menjadi satu-satunya syarat pertanggungjawaban, sebuah argumen yang kini mulai diadopsi dalam EU AI Act Pasal 4.

**Teori Kejahatan Siber (*Cybercrime*)**

Kejahatan siber merupakan konsep yang terus mengalami perluasan seiring dengan dinamika teknologi informasi. McQuade (2006) mendefinisikan cybercrime sebagai setiap pelanggaran hukum yang menggunakan komputer atau jaringan komputer sebagai alat, target, atau lokasi kejahatan. Definisi ini kemudian berkembang melampaui komputer fisik, mencakup segala perangkat elektronik yang terhubung ke jaringan termasuk sistem AI yang beroperasi di lingkungan cloud. Secara teoretis, kejahatan siber dapat diklasifikasikan ke dalam tiga kategori: computer as target (peretasan, DDoS), *computer as tool* (penipuan online, pencurian identitas), dan computer as agent, kategori ketiga yang paling relevan dengan AI, di mana algoritma mampu melaksanakan tindakan ilegal tanpa intervensi manusia secara *real-time* (Wall, 2007).

Dalam konteks Indonesia, UU ITE menghadapi keterbatasan struktural fundamental ketika dihadapkan pada kejahatan berbasis AI. Hampir seluruh formulasi tindak pidana dalam UU ITE menggunakan redaksi "setiap orang" yang secara gramatikal menunjuk pada manusia sebagai pelaku, bukan pada sistem atau algoritma otonom. Perkembangan AI generatif telah memunculkan tipologi kejahatan baru yang memerlukan perhatian khusus. Deepfake crime misalnya memanfaatkan model *Generative Adversarial Network* (GAN) untuk membuat konten audio-visual palsu yang sangat meyakinkan. Dalam beberapa kasus di Indonesia, deepfake telah digunakan untuk pembuatan video pornografi non-konsensual maupun manipulasi komunikasi bisnis (CEO fraud) yang mengakibatkan kerugian finansial besar (Syavica et al., 2025).

Fenomena AI-powered phishing juga kian mengkhawatirkan; sistem AI kini mampu menghasilkan pesan phishing yang dipersonalisasi berdasarkan profil digital korban yang dikumpulkan dari berbagai sumber. Dari perspektif kriminologi, kehadiran AI mengubah dinamika kejahatan siber melalui apa yang dikenal sebagai *commoditization of cybercrime*, hampir siapa pun dengan akses ke layanan AI yang tepat kini dapat meluncurkan serangan yang sebelumnya hanya bisa dilakukan oleh aktor negara atau kelompok kriminal terorganisir (Broadhurst et al., 2021). Fenomena ini memperlihatkan perlunya pergeseran pendekatan

penegakan hukum: dari fokus pada individu pelaku menjadi fokus pada ekosistem teknologi yang memungkinkan kejahatan tersebut terjadi (Ramadani, 2024).

**Teori Negara Hukum dan Perlindungan Hak Digital**

Konsep negara hukum (*rechtsstaat*) sebagaimana termaktub dalam Pasal 1 ayat (3) UUD NRI 1945 mengandung empat elemen esensial: kepastian hukum, persamaan di hadapan hukum, jaminan hak-hak dasar warga negara, dan pembatasan kekuasaan negara melalui hukum (Asshiddiqie, 2012). Dalam konteks digital dan AI, prinsip kepastian hukum menjadi tantangan tersendiri. Ketika seseorang menjadi korban kejahatan siber berbasis AI, ia memiliki hak konstitusional untuk mendapatkan kepastian hukum tentang siapa yang bertanggung jawab. Ketiadaan regulasi yang jelas tentang pertanggungjawaban dalam skenario ini secara langsung melanggar prinsip kepastian hukum yang dijamin konstitusi (Waruwu et al., 2026).

Teori perlindungan hukum yang dikembangkan Satjipto Rahardjo membedakan antara perlindungan preventif dan represif. Perlindungan preventif bertujuan mencegah terjadinya pelanggaran melalui regulasi dan standar teknis, sementara perlindungan represif hadir setelah pelanggaran terjadi melalui mekanisme penegakan hukum (Rahardjo, 2000). Dalam konteks AI dan kejahatan siber, kedua dimensi ini harus diimplementasikan secara terintegrasi. Konsep human rights due diligence (HRDD) dalam UN Guiding Principles on Business and Human Rights (UNGPs) juga mulai diterapkan pada perusahaan teknologi AI, mewajibkan mereka untuk secara proaktif mengidentifikasi dan mencegah dampak negatif operasi mereka terhadap hak asasi manusia termasuk hak-hak digital (Ruggie, 2011).

**Teori Tata Kelola AI dan Pertanggungjawaban Berlapis**

Pemikiran tentang tata kelola AI (AI governance) yang berkembang pesat sejak pertengahan dekade 2010-an dapat dipahami sebagai versi kontemporer dari teori kontrak sosial. Platform teknologi AI tidak hanya berperan sebagai fasilitator interaksi sosial, tetapi juga sebagai penentu apa yang dapat dan tidak dapat diungkapkan, bahkan sampai pada tingkat tertentu, apa yang dianggap sebagai kebenaran (Zuboff, 2019). Dalam kerangka tata kelola AI yang baik, beberapa prinsip fundamental telah diidentifikasi: transparansi, akuntabilitas, keadilan, keandalan, keamanan, dan privasi. Relevansinya bagi pertanggungjawaban hukum sangat nyata: ketika sistem AI yang digunakan untuk kejahatan ternyata dikembangkan tanpa prinsip-prinsip ini, kegagalan tata kelola tersebut dapat menjadi dasar hukum untuk membebankan tanggung jawab kepada pengembang (OECD, 2019).

Perdebatan akademik tentang siapa yang seharusnya menjadi primary duty bearer dalam tata kelola AI belum selesai. Satu kubu berpendapat bahwa pengembang AI harus menanggung tanggung jawab utama karena merekalah yang menciptakan kapabilitas sistem.

Kubu lain berargumen bahwa deployer lebih tepat untuk dimintai pertanggungjawaban karena mereka menentukan konteks penggunaan. Perspektif ketiga menekankan tanggung jawab pengguna akhir yang secara aktif menggunakan AI untuk tujuan ilegal (Calo, 2017). EU AI Act merekonsiliasi ketiga perspektif ini dengan membagi tanggung jawab secara berlapis berdasarkan peran masing-masing aktor dalam rantai nilai AI, sebuah model yang sangat relevan untuk diadopsi Indonesia, mengingat struktur industri AI domestik yang banyak mengandalkan model AI buatan pihak asing.

## 3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan penelitian hukum normatif (normative legal research), yang merupakan tradisi metodologi dominan dalam kajian ilmu hukum Indonesia dan sejalan dengan pendekatan yang lazim digunakan dalam penelitian hukum di lingkungan civil law (Marzuki, 2011). Berbeda dari penelitian sosial empiris yang berupaya menjelaskan realitas sosial melalui data lapangan, penelitian hukum normatif menempatkan bahan hukum sebagai objek kajian utama, dengan tujuan untuk mengidentifikasi, menganalisis, dan mengkonstruksi norma hukum yang berlaku maupun yang seharusnya berlaku dalam isu hukum tertentu.

Penelitian ini menggunakan tiga pendekatan secara simultan dan saling melengkapi. Pertama, pendekatan peraturan perundang-undangan (statute approach), yang melakukan analisis sistematis terhadap seluruh regulasi relevan: UU ITE (UU No. 11/2008 jo. UU No. 19/2016 jo. UU No. 1/2024), UU PDP (UU No. 27/2022), KUHP baru (UU No. 1/2023), UU Perlindungan Konsumen (UU No. 8/1999), PP PSTE (PP No. 71/2019), dan secara komparatif terhadap EU AI Act. Kedua, pendekatan konseptual (*conceptual approach*) yang mengandalkan doctrinal analysis terhadap konsep-konsep hukum relevan seperti *mens rea, actus reus, vicarious liability, strict liability*, dan *distributed liability* dalam kaitannya dengan realitas teknologi AI (Marzuki, 2011). Ketiga, pendekatan kasus (*case approach*) yang menganalisis preseden-preseden hukum dari yurisdiksi Indonesia maupun asing yang telah menangani kasus berkaitan dengan kejahatan siber berbasis AI atau teknologi serupa.

Bahan hukum yang digunakan diklasifikasikan ke dalam tiga kategori. Bahan hukum primer mencakup peraturan perundang-undangan yang berlaku, baik nasional maupun instrumen hukum internasional. Bahan hukum sekunder meliputi literatur akademik berupa jurnal *peer-reviewed*, buku-buku hukum, dan laporan lembaga internasional. Bahan hukum tersier mencakup kamus hukum, ensiklopedia hukum, dan glosarium teknis di bidang keamanan siber dan kecerdasan buatan.

Teknik pengumpulan dilakukan melalui penelitian kepustakaan (*library research*) yang sistematis, dengan seleksi sumber menggunakan kriteria relevansi substantif, kredibilitas penerbit, kemutakhiran, dan validitas ilmiah dengan preferensi pada publikasi lima tahun terakhir. Teknik analisis menggunakan metode kualitatif dengan logika deduktif-induktif secara bergiliran: deduktif untuk menerapkan prinsip hukum umum pada skenario spesifik kejahatan berbasis AI, dan induktif untuk merekonstruksi pola dari kasus-kasus konkret menjadi prinsip yang lebih umum. Penafsiran norma dilakukan menggunakan metode gramatikal, sistematis, historis, dan teleologis (Marzuki, 2011).

## 4. HASIL DAN PEMBAHASAN

### Kerangka Regulasi Hukum Indonesia dalam Mengatur Kejahatan Siber Berbasis AI

Kajian terhadap kerangka regulasi hukum Indonesia yang berkaitan dengan kejahatan siber berbasis AI mengungkap gambaran yang bisa disebut sebagai "regulasi tambalan" (*patchwork regulation*), berbagai regulasi yang ada secara parsial menyentuh aspek-aspek tertentu dari fenomena yang dikaji, namun tidak ada satu pun yang menanganinya secara komprehensif dan koheren. Kondisi ini mencerminkan keterlambatan struktural sistem hukum dalam merespons percepatan teknologi yang sesungguhnya sudah sangat mendesak untuk diatasi.

UU ITE sebagai instrumen hukum siber utama Indonesia memang telah mengalami dua kali perubahan, namun perubahan-perubahan tersebut lebih berfokus pada isu-isu kontroversial seperti tindak pidana penghinaan, ketimbang pada tantangan baru yang ditimbulkan AI. Pasal 30 UU ITE mengatur akses ilegal terhadap sistem elektronik, Pasal 31 tentang intersepsi ilegal, dan Pasal 32 tentang perusakan sistem elektronik, ketiganya relevan dengan serangan siber berbasis AI seperti *ransomware* berbasis machine learning. Namun, ketentuan-ketentuan ini dirumuskan dengan asumsi bahwa pelaku adalah individu manusia yang secara aktif melakukan perbuatan ilegal. Ketika serangan dilakukan secara otonom oleh sistem AI, timbul pertanyaan apakah unsur kesengajaan (*opzet*) yang disyaratkan pasal-pasal tersebut masih dapat dibuktikan terhadap manusia yang mungkin hanya memprogram sistem AI tersebut berminggu-minggu sebelumnya (Zulkarnain & Rahmayanti, 2026).

UU ITE perubahan kedua (UU No. 1/2024) memperkenalkan beberapa ketentuan baru yang relevan, termasuk pengaturan lebih tegas mengenai konten ilegal dan penguatan kewenangan pemerintah untuk pemutusan akses. Namun UU ITE 2024 tetap tidak mengatur secara spesifik mengenai AI-generated content, padahal ini merupakan salah satu kategori konten ilegal yang paling cepat berkembang di Indonesia. *Deepfake* video yang memanfaatkan

wajah tokoh publik untuk disinformasi, audio deepfake untuk penipuan finansial, atau teks yang dihasilkan AI untuk menyebarkan narasi kebencian, semuanya adalah bentuk kejahatan AI-generated content yang masih dapat memperdebatkan penerapan UU ITE yang berlaku (Laia et al., 2025).

UU PDP (UU No. 27/2022) memberikan kerangka hukum yang lebih relevan untuk aspek tertentu kejahatan siber berbasis AI, terutama yang berkaitan dengan pelanggaran data pribadi. Pasal 65-70 UU PDP mengatur ketentuan pidana bagi pelanggar perlindungan data dengan ancaman maksimal 6 tahun penjara dan denda hingga Rp 6 miliar. Namun kelemahan utama UU PDP dalam konteks AI adalah tidak adanya ketentuan tentang automated decision making yang menggunakan data pribadi tanpa persetujuan subjek data, serta tidak adanya pengaturan khusus untuk pelanggaran data yang terjadi akibat serangan siber berbasis AI (Waruwu et al., 2026).

KUHP baru (UU No. 1/2023) yang berlaku efektif per 2 Januari 2026 memberikan perkembangan normatif positif melalui pengaturan pertanggungjawaban pidana korporasi dalam Pasal 45-50 yang membuka jalan bagi penuntutan perusahaan teknologi yang produk AI-nya digunakan untuk kejahatan. Analisis komparatif dengan EU AI Act menunjukkan pentingnya pendekatan risk-based yang mengklasifikasikan sistem AI berdasarkan tingkat risikonya, sebuah filosofi regulasi yang sangat tepat untuk diadopsi Indonesia sebagai dasar pembaruan UU ITE dan pengembangan regulasi AI baru (Ramadani & Lase, 2025).

**Konstruksi Tanggung Jawab Hukum Pengembang, Operator, dan Pengguna AI dalam Kejahatan Siber**

Persoalan konstruksi tanggung jawab hukum dalam kejahatan siber berbasis AI pada hakikatnya adalah persoalan tentang cara hukum mengalokasikan risiko dalam ekosistem teknologi yang kompleks. Berbeda dari kejahatan konvensional di mana rantai kausalitas antara pelaku dan kerugian relatif jelas, kejahatan siber berbasis AI menghadirkan rantai kausalitas berlapis dan multi-aktor: ada pengembang model AI dasar (*foundation model developer*), penyedia infrastruktur cloud, pengintegrator aplikasi (*deployer*), dan pengguna akhir yang mungkin memanfaatkannya untuk tujuan ilegal.

Terhadap pengembang sistem AI, konstruksi tanggung jawab hukum dapat dibangun berdasarkan teori negligence atau kelalaian. Jika seorang pengembang AI gagal mengimplementasikan safeguards yang memadai, tidak melakukan red-teaming yang cukup, tidak membangun mekanisme content filtering yang efektif, atau tidak menyediakan mekanisme pelaporan insiden yang transparan, maka mereka dapat dimintai pertanggungjawaban perdata atas kerugian yang timbul dari penyalahgunaan tersebut. Standar

kehati-hatian (*standard of care*) yang diterapkan dalam industri ini terus berkembang, dan pengembang yang tidak mengikuti best practices industri dapat dianggap lalai secara hukum, paralel dengan apa yang dalam hukum produk dikenal sebagai design defect liability (Calo, 2017).

Untuk operator atau deployer AI, pihak yang mengintegrasikan sistem AI ke dalam produk atau layanan bisnis mereka, konstruksi tanggung jawab hukum seharusnya lebih kuat. Berbeda dari pengembang yang mungkin tidak bisa mengantisipasi semua cara penyalahgunaan produknya, operator memiliki pengetahuan langsung tentang konteks penggunaan sistem AI yang mereka deploy dan karenanya lebih mampu mengidentifikasi dan mencegah risiko. PP PSTE Pasal 12 memberikan landasan normatif untuk mewajibkan operator sistem elektronik mengimplementasikan pengamanan yang memadai. Kegagalan memenuhi kewajiban ini berpotensi menjadi dasar gugatan perdata berdasarkan Pasal 1365 KUHPerdata tentang perbuatan melawan hukum (Syahranuddin et al., 2024).

Pertanggungjawaban pengguna (*end users*) yang menggunakan AI untuk kejahatan secara teoretis paling straightforward karena merekalah yang paling proximate dalam kausalitas kejahatan. Pengguna yang secara sadar menggunakan AI untuk melakukan penipuan, pembuatan deepfake ilegal, atau serangan siber dapat dijerat ketentuan UU ITE yang relevan sebagai pelaku utama. Dalam hal ini, sistem AI berfungsi sebagai instrumentum sceleris, alat kejahatan, dan penggunaannya tidak mengurangi apalagi menghapus pertanggungjawaban pidana pengguna (Laia et al., 2025). Namun kompleksitas muncul kembali dalam skenario di mana sistem AI beroperasi secara otonom tanpa intervensi aktif pengguna, sehingga batas antara kesengajaan dan otonomi AI menjadi kabur secara yuridis (Zulkarnain & Rahmayanti, 2026).

Untuk mengisi kekosongan normatif ini, model pertanggungjawaban berlapis (*layered liability framework*) merupakan konstruksi yang paling tepat: pengembang bertanggung jawab secara perdata atas *design defects* dan wajib membangun *safety by design*; operator bertanggung jawab secara administratif dan perdata atas kegagalan pengawasan dan penggunaan yang tidak sesuai tujuan sah; pengguna menanggung pertanggungjawaban pidana penuh atas niat dan tindakan ilegal yang secara aktif mereka arahkan kepada sistem AI. Implementasi model ini memerlukan tidak hanya pembaruan legislasi, tetapi juga penguatan kapasitas aparat penegak hukum, pengembangan standar teknis digital forensics untuk bukti AI, dan penguatan kerjasama internasional dalam penanganan kejahatan siber lintas batas.

## 5. KESIMPULAN DAN SARAN

Berdasarkan analisis yang telah dilakukan, penelitian ini menarik dua simpulan utama yang sekaligus mengandung rekomendasi kebijakan yang mendesak.

Pertama, kerangka regulasi hukum Indonesia dalam mengatur kejahatan siber berbasis AI saat ini berada dalam kondisi yang tidak memadai dan mengandung celah normatif yang signifikan. UU ITE beserta perubahannya, UU PDP, PP PSTE, dan KUHP baru tidak dirancang untuk mengakomodasi kekhasan sistem AI otonom sebagai aktor atau instrumen kejahatan. Ketentuan yang ada masih bertumpu pada asumsi bahwa pelaku kejahatan adalah manusia yang bertindak dengan kesengajaan yang dapat dibuktikan secara langsung, asumsi yang runtuh dalam banyak skenario kejahatan berbasis AI modern. Indonesia mendesak untuk segera menyusun regulasi AI yang komprehensif atau minimal melakukan amandemen terfokus terhadap UU ITE dan UU PDP untuk secara eksplisit mengatur status hukum AI-generated content, kewajiban safeguards bagi pengembang dan operator AI, mekanisme pembuktian dalam kasus kejahatan AI, dan skema pertanggungjawaban yang lebih nuanced untuk skenario AI otonom.

Kedua, konstruksi tanggung jawab hukum atas kejahatan siber berbasis AI di Indonesia memerlukan reformulasi fundamental yang bergerak melampaui model pertanggungjawaban tradisional yang bersifat tunggal dan linear. Model pertanggungjawaban berlapis yang mendistribusikan tanggung jawab secara proporsional kepada pengembang (*strict liability* perdata *atas design defects*), operator (kewajiban pengawasan aktif dengan sanksi administratif dan perdata), dan pengguna (pertanggungjawaban pidana penuh atas niat ilegal yang secara aktif diarahkan kepada sistem AI) merupakan pendekatan yang paling adil, efektif, dan compatible dengan prinsip-prinsip dasar hukum Indonesia. Pembaruan legislasi ini harus disertai penguatan kapasitas aparat penegak hukum dalam digital forensics untuk bukti AI dan penguatan kerjasama internasional dalam penanganan kejahatan siber lintas batas yurisdiksi.

## DAFTAR REFERENSI

Asshiddiqie, J. (2012). *Pengantar ilmu hukum tata negara*. Rajawali Press.

Badan Siber dan Sandi Negara. (2023). *Laporan tahunan keamanan siber Indonesia 2023*. BSSN.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2021). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1–20.

Bryson, J. J., & Winfield, A. F. T. (2017). Standardizing ethical design for artificial intelligence and autonomous systems. *Computer, 50*(5), 116–119. https://doi.org/10.1109/MC.2017.154

Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. *UC Davis Law Review, 51*(2), 399–435. https://doi.org/10.2139/ssrn.3015350

Dharmawan, R. F., & Ramadani, S. (2025). The effectiveness of criminal liability implementation in law enforcement against village fund corruption cases in Indonesia. *Proceedings of International Conference on Islamic Community Studies*, 314–319.

Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., & Wood, A. (2017). *Accountability of AI under the law: The role of explanation* (Berkman Klein Center Working Paper). Harvard University. https://doi.org/10.2139/ssrn.3064761

European Parliament and Council. (2024). *Regulation (EU) 2024/1689 on artificial intelligence (EU AI Act)*. *Official Journal of the European Union*.

Fuady, M. (2010). *Perbuatan melawan hukum: Pendekatan kontemporer*. Citra Aditya Bakti.

https://doi.org/10.53697/jkomitek.v5i2.3155

Kitab Undang-Undang Hukum Perdata (KUHPerdata). *Staatsblad* 1847 Nomor 23.

Laia, Y. R. N., Rahmayanti, R., Tampubolon, S. S., Gea, A. S., & Nasution, S. H. (2025). Implementasi hukum terhadap tindak pidana scammer. *JISPENDIORA: Jurnal Ilmu Sosial Pendidikan dan Humaniora, 4*(1), 603–613.

McQuade, S. C. (2006). *Understanding and managing cybercrime*. Pearson Education.

Moeljatno. (2008). *Asas-asas hukum pidana*. Rineka Cipta.

OECD. (2019). *OECD principles on artificial intelligence*. OECD Legal Instruments.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. *Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185*.

Rahardjo, S. (2000). *Ilmu hukum*. Citra Aditya Bakti.

Rahmadani, S. (2024). Strategi pembelajaran pendidikan agama Islam di era digital: Tinjauan literatur kualitatif. *Jurnal Media Akademik (JMA), 2*(6). https://doi.org/10.61132/jmpai.v2i3.385

Ramadani, S. (2024). The role of government and society in preventing narcotics crime in Indonesia. *International Conference Epicentrum of Economic Global Framework*, 632–637.

Ramadani, S., & Lase, N. A. (2025). Increasing public legal awareness of corruption in Hamparan Perak District Klambir Lima Kebun Village. *Proceedings of International Conference on Islamic Community Studies*, 1821–1828.

Ruggie, J. G. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. United Nations Human Rights Council.

Syahranuddin, S., Ismaidar, I., Ramadani, S., & Aritonang, T. (2024). Implementation of village fund policy and anti-corruption challenges in Pasar Rawa Village, Gebang District. *Proceeding International Seminar and Conference on Islamic Studies (ISCIS), 3*(1).

Syavica, Z., Sahlepi, M. A., & Rahmayanti, R. (2025). The crime of child grooming as digital sexual harassment in the perspective of perpetrator accountability according to laws

and regulations in Indonesia. *Journal of Research in Social Science and Humanities, 5*(3).

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. *Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1*.

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

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58*.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251*.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196*.

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. *Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42*.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Waruwu, P. R., Rahmayanti, R., Suryana, R., & Nurdana, S. A. (2026). Analisis hukum pidana terhadap kebocoran data pribadi dalam sistem elektronik di Indonesia. *YUSTISI, 13*(2).

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Zulkarnain, R., & Rahmayanti, R. (2026). Kedudukan artificial intelligence dalam sistem hukum Indonesia: Analisis normatif antara subjek hukum dan instrumen teknologi. *SIBATIK Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan, 5*(5), 2482–2490.