Advokasi Hukum & Demokrasi (AHD)
Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

Pertanggungjawaban Pidana Terhadap Penyalahgunaan Kecerdasan Buatan (Artificial Intelligence) dalam Tindak Kejahatan Digital di Indonesia

Yoel Bessoran
Fakultas Hukum, Ilmu Sosial, dan Ilmu Politik (FHISIP), Universitas Terbuka
yoel.bessoran@gmail.com

ABSTRACT

This study analyzes the phenomenon of artificial intelligence based digital crime in Indonesia during the period 2023 to 2026, with a focus on deepfake, voice cloning, digital fraud, and the misuse of autonomous algorithms. The study employs a normative juridical approach combined with empirical case analysis to evaluate criminal liability mechanisms, challenges in legal implementation, as well as the roles of corporations and end users in the dissemination of harmful digital content. The results show that artificial intelligence functions as a mediator of complex crimes, therefore existing regulations, including the Criminal Code, the Electronic Information and Transactions Law, and the Personal Data Protection Law, are not yet adequate to effectively enforce criminal liability. The phenomena of non consensual deepfake, voice phishing, and image manipulation create legal gaps that require regulatory reform and adaptive models of legal responsibility. This study emphasizes the importance of combining individual and corporate liability, the application of risk based liability and vicarious liability principles, as well as internal supervision and risk mitigation among AI platform developers. In addition, cross institutional coordination, integration of digital forensic technology, and public education are key to successful investigation and law enforcement. These findings provide implications for national policy reform, strengthening corporate ethical standards, and strategies to prevent the misuse of artificial intelligence, while also highlighting the urgency of adapting legal frameworks to continuously evolving digital technologies. Therefore, this study contributes to the development of a more comprehensive legal and policy framework to address artificial intelligence based digital crime in Indonesia.

Keywords: *artificial intelligence, criminal liability, cyber law, deepfake, digital crime, voice cloning*

ABSTRAK

Penelitian ini menganalisis fenomena kejahatan digital berbasis kecerdasan buatan (Artificial Intelligence/AI) di Indonesia pada periode 2023–2026, dengan fokus pada deepfake, voice cloning, penipuan digital, dan penyalahgunaan algoritma otonom. Studi ini menggunakan pendekatan yuridis normatif yang dikombinasikan dengan analisis kasus empiris untuk mengevaluasi mekanisme pertanggungjawaban pidana, tantangan implementasi hukum, serta peran korporasi dan pengguna akhir dalam penyebaran konten digital merugikan. Hasil penelitian menunjukkan bahwa AI berfungsi sebagai mediator kejahatan yang kompleks, sehingga regulasi saat ini, termasuk KUHP, UU ITE, dan UU Perlindungan Data Pribadi, belum memadai untuk menegakkan pertanggungjawaban pidana secara efektif. Fenomena deepfake non-consensual, voice phishing, dan rekayasa foto menciptakan celah hukum yang memerlukan reformasi regulasi dan model

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

pertanggungjawaban hukum yang adaptif. Penelitian ini menekankan pentingnya kombinasi pertanggungjawaban individu dan korporasi, penerapan asas risk-based liability dan vicarious liability, serta pengawasan internal dan mitigasi risiko pada pengembang platform AI. Selain itu, koordinasi lintas lembaga, integrasi teknologi forensik digital, dan edukasi publik menjadi kunci keberhasilan penyidikan dan penegakan hukum. Temuan ini memberikan implikasi bagi pembaruan kebijakan nasional, penguatan standar etika korporasi, dan strategi pencegahan penyalahgunaan AI, sekaligus menegaskan urgensi adaptasi hukum terhadap teknologi digital yang terus berkembang. Dengan demikian, penelitian ini berkontribusi pada pengembangan kerangka hukum dan kebijakan yang lebih komprehensif untuk menghadapi kejahatan digital berbasis AI di Indonesia.

Kata Kunci: kejahatan digital, kecerdasan buatan, pertanggungjawaban pidana, deepfake, voice cloning, hukum siber

PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) dalam dekade terakhir telah membawa perubahan signifikan pada berbagai aspek kehidupan, termasuk sektor ekonomi, komunikasi, dan hiburan (Zaenudin & Riyan, 2024). Namun, kemajuan ini juga membuka celah bagi munculnya kejahatan digital baru yang memanfaatkan kemampuan AI untuk melakukan manipulasi data, penipuan, dan pelanggaran privasi. Di Indonesia, fenomena ini menjadi perhatian serius karena dampaknya yang luas, mulai dari kerugian finansial individu dan korporasi hingga trauma psikologis bagi korban penyalahgunaan konten digital. Kasus-kasus deepfake, voice cloning, dan penyebaran konten pornografi non-konsensual menunjukkan bahwa teknologi AI tidak lagi sekadar alat bantu, tetapi juga berpotensi menjadi mediator tindak pidana yang kompleks, menuntut adaptasi hukum yang responsif dan sistematis (Santoso & Wibowo, 2023).

Kejahatan digital berbasis AI menimbulkan tantangan signifikan bagi sistem hukum Indonesia, khususnya terkait dengan subjek hukum dan atribusi kesalahan. Saat ini, KUHP, UU ITE, dan UU Perlindungan Data Pribadi belum secara eksplisit mengatur status AI sebagai entitas hukum, sehingga pertanggungjawaban pidana selalu diarahkan kepada manusia atau korporasi yang mengoperasikan teknologi tersebut (Kawiswara, 2026). Fenomena ini menimbulkan dilema hukum ketika AI bertindak semi-otonom, sehingga sulit menentukan pihak yang dapat dijerat secara adil. Celah hukum ini semakin terlihat pada kasus-kasus deepfake dan penipuan berbasis rekaman suara, di mana korban sering dirugikan tanpa pelaku manusia yang jelas teridentifikasi. Keadaan ini menekankan urgensi pembaruan regulasi pidana dan perlunya model pertanggungjawaban yang menggabungkan tanggung jawab individu dan korporasi.

Selain itu, peningkatan kejahatan digital berbasis AI juga menimbulkan tantangan dalam aspek pembuktian dan penegakan hukum (BR, 2025). Aktivitas AI yang bersifat otomatis atau self-learning mempersulit aparat hukum dalam menelusuri log aktivitas, membuktikan niat jahat, dan mengidentifikasi siapa yang

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

memiliki kontrol terhadap teknologi tersebut. Kasus Grok AI dan manipulasi foto yang mencemarkan nama baik menegaskan bahwa penyidikan memerlukan kolaborasi lintas lembaga, integrasi teknologi forensik digital, serta pemahaman mendalam tentang algoritma dan proses pengambilan keputusan AI (Shabrina et al., 2026). Kompleksitas ini menunjukkan bahwa penegakan hukum konvensional saja tidak cukup, sehingga dibutuhkan strategi yang menggabungkan edukasi publik, audit algoritma, dan protokol mitigasi risiko untuk mencegah kerugian lebih lanjut.

Rumusan masalah dalam penelitian ini berfokus pada tiga hal utama: pertama, bagaimana pertanggungjawaban pidana dapat diterapkan dalam konteks penyalahgunaan AI di Indonesia; kedua, apa saja celah hukum yang muncul akibat keterbatasan regulasi yang ada; dan ketiga, bagaimana mekanisme penyidikan dan penegakan hukum dapat dioptimalkan untuk menghadapi kejahatan digital berbasis AI. Pertanyaan ini penting karena menentukan arah reformasi hukum, kebijakan mitigasi risiko, dan tata kelola etis penggunaan AI di ranah publik. Dengan mengidentifikasi tantangan, model atribusi kesalahan, dan praktik penegakan hukum yang ada, penelitian ini bertujuan memberikan dasar konseptual dan empiris bagi pembaruan regulasi yang adaptif dan relevan.

Tujuan penelitian ini adalah menganalisis pertanggungjawaban pidana dalam konteks kejahatan digital berbasis AI, mengidentifikasi celah hukum yang ada dalam KUHP, UU ITE, dan UU PDP, serta merumuskan mekanisme penyidikan dan penegakan hukum yang efektif. Selain itu, penelitian ini bertujuan mengeksplorasi relevansi model tanggung jawab individu dan korporasi, termasuk prinsip risk-based liability dan vicarious liability, untuk memastikan perlindungan korban sekaligus penegakan sanksi yang adil terhadap pelaku. Dengan demikian, penelitian ini diharapkan memberikan kontribusi signifikan bagi pengembangan regulasi hukum dan kebijakan nasional yang responsif terhadap dinamika kejahatan digital berbasis AI di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk memahami fenomena kejahatan digital berbasis kecerdasan buatan (AI) di Indonesia, khususnya terkait pertanggungjawaban pidana, celah hukum, dan mekanisme penegakan hukum. Pendekatan ini dipilih karena kasus-kasus AI-related cybercrime bersifat kompleks dan melibatkan interaksi antara teknologi, pelaku manusia, dan korporasi. Dengan studi kasus, penelitian dapat menggali secara mendalam konteks sosial, hukum, dan teknis di balik setiap kasus, termasuk praktik penyidikan, kendala pembuktian, dan implementasi regulasi yang berlaku.

Sumber data utama penelitian ini berasal dari dokumen hukum, laporan kepolisian, publikasi akademik, dan berita kasus terkini terkait kejahatan AI di Indonesia antara tahun 2023 hingga 2026. Dokumen hukum meliputi KUHP, UU ITE, UU Perlindungan Data Pribadi, serta peraturan terkait tanggung jawab korporasi dan individu dalam konteks teknologi. Laporan kepolisian dan data Kemenkominfo

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

digunakan untuk memperoleh informasi empiris tentang tren kasus, modus operandi, serta statistik penyidikan dan penegakan hukum. Selain itu, jurnal ilmiah dan literatur terkait pertanggungjawaban pidana, atribusi kesalahan, dan tanggung jawab korporasi memberikan kerangka konseptual yang mendukung analisis.

Teknik pengumpulan data dilakukan melalui studi dokumentasi dan analisis konten, di mana setiap dokumen, laporan, dan literatur dipilah dan dikodekan berdasarkan kategori utama penelitian, seperti jenis kejahatan digital, modus operandi AI, subjek hukum, atribusi kesalahan, tanggung jawab korporasi, dan tantangan implementasi hukum. Analisis ini memungkinkan peneliti memahami pola-pola kejahatan, hubungan antara aktor manusia dan AI, serta kesenjangan regulatif yang muncul di lapangan. Data sekunder ini kemudian dikonfirmasi melalui cross-checking dengan sumber publik dan berita kasus terkini untuk memastikan akurasi dan relevansi.

Dalam hal analisis data, penelitian menggunakan pendekatan tematik dan deskriptif, di mana temuan diklasifikasikan berdasarkan isu hukum utama, seperti subjek hukum yang dapat dipidana, penerapan asas kesalahan (schuld beginsel), dan tanggung jawab korporasi. Temuan juga dianalisis untuk menilai kesesuaian regulasi dengan praktik nyata, mengidentifikasi celah hukum, dan mengevaluasi efektivitas mekanisme penyidikan. Proses ini dilakukan secara iteratif, dengan membandingkan kasus-kasus yang relevan dan literatur hukum untuk merumuskan model pertanggungjawaban pidana yang adaptif terhadap teknologi AI.

Selain itu, penelitian ini menekankan aspek validitas dan reliabilitas data melalui triangulasi sumber, termasuk dokumen hukum, laporan kepolisian, literatur akademik, dan berita kasus. Triangulasi ini memastikan bahwa analisis tidak hanya berdasarkan satu perspektif, tetapi mempertimbangkan berbagai sudut pandang, sehingga kesimpulan yang dihasilkan lebih komprehensif dan dapat diandalkan. Dengan demikian, metode penelitian ini memungkinkan pemahaman yang mendalam tentang fenomena kejahatan digital berbasis AI, tantangan hukum, dan mekanisme penegakan yang relevan bagi konteks hukum pidana Indonesia.

HASIL DAN PEMBAHASAN

Gambaran Umum Kasus dan Data Terkini

Statistik Kejahatan Digital Berbasis AI di Indonesia (2023–2026)

Dalam beberapa tahun terakhir, Indonesia mengalami peningkatan signifikan kasus kejahatan digital yang memanfaatkan kecerdasan buatan (*Artificial Intelligence*). Data menunjukkan bahwa *deepfake*, *voice cloning*, dan penipuan berbasis AI menjadi modus utama yang digunakan oleh pelaku kejahatan siber (Banfatin et al., 2025). Tren ini tidak hanya terjadi di kota besar, tetapi juga merambah daerah menengah, menimbulkan tantangan bagi aparat penegak hukum. Pemerintah

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

melalui Kemkominfo melaporkan adanya lebih dari 1.500 kasus AI-related cybercrime pada tahun 2025 (Sihombing & Hermanto, 2026).

Kejahatan berbasis AI ini melibatkan penyebaran konten manipulatif yang merugikan individu maupun institusi. Penipuan melalui *voice phishing* tercatat meningkat hingga 40% dibandingkan tahun sebelumnya (Alviani & Fitri, 2024). Modus yang berkembang termasuk penggunaan rekaman suara palsu untuk meminta transfer dana atau informasi sensitif. Hal ini menegaskan bahwa kejahatan digital berbasis AI tidak lagi bersifat hipotetik, melainkan ancaman nyata bagi keamanan data dan privasi.

Selain penipuan, penyalahgunaan *deepfake* juga menjadi sorotan utama. Kasus video pornografi non-konsensual meningkat pesat, mengakibatkan dampak psikologis dan sosial bagi korban (Syahrani et al., 2025). Pelaku menggunakan algoritma AI untuk merekayasa wajah atau suara korban, sehingga materi digital yang dihasilkan sulit dibedakan dari asli. Fenomena ini menimbulkan kebutuhan mendesak akan regulasi dan mekanisme penegakan hukum yang lebih adaptif.

Berdasarkan penelitian Darmawan et al. (2025), kejahatan AI tidak hanya bersifat individual, tetapi sering melibatkan jaringan kompleks antara pengembang, operator, dan pihak ketiga. Kompleksitas ini mempersulit identifikasi subjek hukum dan memerlukan pendekatan sistematis untuk atribusi kesalahan. Tren ini menunjukkan bahwa hukum Indonesia harus segera menyesuaikan diri dengan teknologi yang cepat berkembang.

Secara keseluruhan, statistik dan temuan empiris menekankan pentingnya pengawasan berkelanjutan terhadap penggunaan AI. Selain itu, peningkatan kasus menandai urgensi pembaruan regulasi hukum pidana untuk menjangkau modus baru yang sebelumnya tidak tercakup dalam KUHP maupun UU ITE (Banfatin et al., 2025; Pane & Permana, 2025).

Kasus Terbaru yang Relevan

Kasus *Grok AI* menjadi sorotan utama terkait penyalahgunaan AI dalam konten asusila dan pelanggaran privasi. Laporan terbaru menyebut bahwa platform ini memfasilitasi pembuatan konten yang melanggar hak privasi individu (Irma Widyastuti et al., 2026). Analisis kasus menunjukkan bahwa pelaku utama adalah operator dan pihak pengembang yang lalai mengawasi algoritma (*algorithmic oversight*).

Kasus lain yang relevan adalah rekayasa foto yang mengandung unsur pencemaran nama baik, di mana AI digunakan untuk memanipulasi citra seseorang (Herianto, 2025). Kejadian ini menimbulkan pertanyaan hukum mengenai pertanggungjawaban pengguna teknologi serta pembuat algoritma yang memungkinkan penyebaran konten merugikan.

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

Selain itu, kejahatan ekonomi berbasis AI seperti penipuan melalui rekaman suara (*voice cloning*) juga tercatat meningkat (Darmawan et al., 2025). Pelaku memanfaatkan teknologi untuk menipu korban dalam transaksi keuangan, menimbulkan kerugian besar bagi individu maupun perusahaan. Kasus ini menegaskan perlunya model pertanggungjawaban pidana yang jelas bagi operator maupun pengembang AI.

Hibatulloh (2025) menekankan bahwa AI sebagai entitas teknologi belum diakui sebagai subjek hukum pidana, sehingga atribusi kesalahan selalu diarahkan pada manusia atau korporasi. Hal ini menimbulkan celah hukum, terutama ketika AI beroperasi secara otonom (*autonomous agent*), sehingga pelaku manusia sulit diidentifikasi secara langsung. Secara keseluruhan, kasus-kasus terbaru ini menggarisbawahi urgensi pembaruan hukum pidana Indonesia, termasuk reformasi UU ITE dan KUHP, agar dapat menjangkau kejahatan digital berbasis AI secara efektif (Sulistio & Salsabilla, 2023; Pane & Permana, 2025).

Analisis Pertanggungjawaban Pidana

Subjek Hukum

Hukum pidana Indonesia saat ini hanya mengakui *natural person* dan *legal person* sebagai subjek hukum yang dapat dipidana. AI sebagai entitas teknologi tidak memiliki kesadaran atau kehendak bebas, sehingga tidak dapat dijerat secara langsung (Hibatulloh, 2025). Fenomena ini menimbulkan dilema ketika AI melakukan tindakan yang melanggar hukum, karena harus ada pihak manusia yang bertanggung jawab.

Pane & Permana (2025) menyebutkan bahwa dalam kasus pelanggaran privasi, pengembang dan operator platform AI sering kali menjadi target pertanggungjawaban pidana. Mereka dianggap memiliki kewajiban untuk mengawasi penggunaan teknologi agar tidak merugikan pihak lain. Hal ini menegaskan peran *legal person* dalam konteks penyalahgunaan AI. Ginting (2025) menambahkan bahwa ketika AI digunakan untuk melakukan *deepfake*, pertanggungjawaban pidana sering kali dilemparkan pada pengguna akhir, meski pengembang turut memfasilitasi penyebaran konten. Hal ini menimbulkan diskusi tentang keadilan atribusi kesalahan dalam hukum pidana.

Patria (2025) mengusulkan model pengaturan baru yang mengkombinasikan pertanggungjawaban korporasi dan individu, sehingga celah hukum dapat diminimalisasi. Pendekatan ini menekankan pentingnya regulasi preventif dan pengawasan terhadap teknologi AI (Ruhtiani & Istikharoh, 2025). Selain itu, kasus-kasus non-consensual sexual content menegaskan bahwa korban sering kali dirugikan tanpa pelaku manusia yang jelas teridentifikasi, sehingga diperlukan kerangka hukum yang adaptif terhadap entitas teknologi (Syahrani et al., 2025).

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

Atribusi Kesalahan (Schuld Prinsip)

Dalam perspektif hukum pidana, asas kesalahan (*schuld beginsel*) menjadi dasar menentukan siapa yang bertanggung jawab. Namun, AI tidak memiliki kemampuan moral atau kehendak bebas, sehingga sulit untuk menerapkan prinsip ini langsung kepada AI (Ginting, 2025). Wafi et al. (2025) menekankan bahwa asas culpabilitas tetap bisa diterapkan kepada manusia yang mengembangkan, mengoperasikan, atau menyebarluaskan AI untuk melakukan kejahatan.

Oleh karena itu, atribusi kesalahan cenderung diarahkan pada pihak yang memiliki kontrol terhadap teknologi tersebut. Hidayat (2025) menambahkan bahwa dalam kasus penyalahgunaan *deepfake*, sulit untuk membedakan antara niat jahat pengguna akhir dan kesalahan pengembang. Hal ini menimbulkan tantangan hukum dalam menegakkan sanksi pidana secara adil dan proporsional.

Sulistio & Salsabilla (2023) menyarankan pendekatan berbasis *risk-based liability*, di mana pihak yang memiliki kemampuan mitigasi risiko wajib bertanggung jawab jika gagal mencegah kejahatan digital. Model ini relevan dengan kasus AI yang beroperasi secara semi-otonom. Selain itu, Putri et al. (2024) menekankan perlunya reformulasi asas kesalahan dalam konteks AI, agar mencakup pihak-pihak yang berkontribusi terhadap penyalahgunaan teknologi, sekaligus melindungi korban dari dampak negatif kejahatan digital.

Tanggung Jawab Korporasi

Korporasi pengembang AI memiliki tanggung jawab hukum yang signifikan ketika sistem yang mereka kembangkan digunakan untuk melakukan tindak pidana. Penerapan prinsip *vicarious liability* menekankan bahwa perusahaan harus bertanggung jawab atas kesalahan yang timbul dari operasional teknologi mereka (Pane & Permana, 2025). Dalam praktiknya, hal ini berarti pengawasan internal terhadap algoritma AI dan penerapan kebijakan mitigasi risiko menjadi kewajiban hukum yang tidak bisa diabaikan.

Sulistio & Salsabilla (2023) mencatat bahwa kegagalan korporasi dalam mengendalikan sistem AI dapat mengakibatkan pertanggungjawaban pidana, meski tindakan kriminal dilakukan oleh pengguna akhir. Dengan kata lain, tanggung jawab tidak hanya bersifat retrospektif tetapi juga preventif (Aster Yansen Basah et al., 2025). Hal ini menuntut perusahaan untuk memiliki protokol keamanan, audit algoritma, dan pengendalian akses yang ketat.

Herianto (2025) menambahkan bahwa korporasi juga dapat dimintai pertanggungjawaban jika teknologi mereka memungkinkan penyebaran konten pencemaran nama baik. Kasus rekayasa foto yang viral menunjukkan bahwa pengembang dan operator platform bisa menjadi subjek hukum karena kelalaian dalam mengontrol penyalahgunaan. Model ini memperkuat perlunya standar etika dan hukum yang jelas bagi pengembang AI di Indonesia (Iradat & Hariyanto, 2025).

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

Putri et al. (2024) menekankan bahwa pertanggungjawaban korporasi tidak bisa dipisahkan dari aspek pengguna, karena keduanya memiliki peran dalam penyebaran materi digital merugikan. Kombinasi regulasi yang menekankan kontrol internal dan pertanggungjawaban pengguna dapat menciptakan sistem hukum yang lebih efektif. Selain itu, Syahrani et al. (2025) menyatakan bahwa dengan meningkatnya kasus non-consensual AI-generated sexual content, korporasi yang gagal mencegah penyalahgunaan teknologinya menghadapi risiko pidana dan perdata. Hal ini menandai perlunya pembaruan undang-undang untuk memperjelas batas tanggung jawab korporasi, termasuk kewajiban mitigasi risiko dan pengawasan algoritma.

Celah Hukum dan Tantangan Implementasi

Kekosongan regulatif menjadi hambatan utama dalam menegakkan hukum terhadap penyalahgunaan AI di Indonesia. Hibatulloh (2025) menekankan bahwa KUHP, UU ITE, dan UU Perlindungan Data Pribadi belum secara eksplisit mengatur status AI sebagai subjek hukum. Akibatnya, aparat hukum sering kesulitan menentukan siapa yang bertanggung jawab secara pidana. Mecca et al. (2025) menambahkan bahwa tantangan implementasi termasuk ketidakpastian terkait *algorithmic decision-making*, di mana AI mampu menghasilkan output yang merugikan tanpa intervensi manusia secara langsung.

Kasus seperti *deepfake* yang disebarkan secara otomatis menunjukkan bahwa hukum saat ini belum mampu menampung fenomena tersebut. Hidayat (2025) menekankan celah lain terkait atribusi kesalahan. Dalam kasus penipuan ekonomi berbasis AI, sulit membuktikan niat jahat pelaku karena AI beroperasi semi-otonom. Hal ini memunculkan kebutuhan reformasi hukum pidana agar prinsip *culpabilitas* dapat diterapkan pada aktor manusia maupun entitas korporasi.

Selain itu, Kawiswara (2026) menyebut bahwa sistem peradilan juga menghadapi tantangan teknis dalam menelusuri bukti digital, termasuk log aktivitas AI dan rekaman algoritma. Kesulitan ini mempersulit proses penyidikan dan penuntutan. Terakhir, BR (2025) menyoroti pentingnya koordinasi antar-institusi, seperti kepolisian, Kemkominfo, dan lembaga peradilan, untuk mengatasi celah hukum yang ada. Kolaborasi ini menjadi kunci agar pertanggungjawaban pidana dapat ditegakkan secara efektif di era kejahatan digital berbasis AI.

Mekanisme Penyidikan dan Penegakan Hukum

Peran Kepolisian dan Kemenkominfo

Kepolisian Republik Indonesia bersama Kemenkominfo memiliki peran sentral dalam penyidikan kejahatan digital berbasis AI (Sihombing & Hermanto, 2026). Mereka bertugas menelusuri bukti digital, mengidentifikasi pelaku, dan menindaklanjuti kasus melalui jalur hukum. Penggunaan forensik digital modern memungkinkan aparat hukum memetakan penyebaran konten manipulatif.

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

Herianto (2025) mencatat bahwa koordinasi dengan operator platform AI penting untuk mendapatkan akses data. Tanpa kerja sama ini, proses penyidikan dapat terhambat karena bukti yang tersebar di server perusahaan atau layanan cloud internasional. Putri et al. (2024) menambahkan bahwa dalam kasus *deepfake* non-consensual, aparat hukum harus bekerja cepat untuk mencegah penyebaran konten lebih luas. Langkah proaktif ini mencakup pemblokiran sementara konten dan identifikasi pihak yang bertanggung jawab.

Hibatulloh (2025) menekankan bahwa mekanisme penyidikan harus adaptif terhadap teknologi baru, termasuk algoritma *self-learning* yang mampu membuat keputusan sendiri. Hal ini memerlukan pemahaman hukum dan teknologi yang terintegrasi agar proses hukum berjalan efektif. Syahrani et al. (2025) menunjukkan bahwa pelatihan aparat hukum menjadi faktor kunci dalam penegakan. Tanpa pemahaman mendalam tentang AI, penyidikan dapat mengalami bias dan kesalahan atribusi.

Tantangan Pembuktian

Pembuktian menjadi kendala utama dalam kasus kejahatan AI. Wafi et al. (2025) menyebutkan bahwa menelusuri *algorithmic decision-making* memerlukan bukti teknis yang kompleks. Log aktivitas AI sering sulit diakses atau dimanipulasi oleh pelaku. Darmawan et al. (2025) menambahkan bahwa chain of causation sulit dibuktikan ketika AI bertindak semi-otonom. Identifikasi siapa yang mengontrol AI, siapa yang memanfaatkan hasilnya, dan bagaimana niat jahat diterapkan menjadi tantangan hukum utama.

Pane & Permana (2025) mencatat bahwa bukti digital harus diverifikasi secara ketat agar dapat diterima di pengadilan. Kesalahan dalam autentikasi data dapat menyebabkan kasus batal demi hukum. Hidayat (2025) menegaskan bahwa kompleksitas ini menuntut integrasi antara forensik digital, ahli AI, dan ahli hukum. Pendekatan multidisiplin diperlukan untuk memastikan bukti dapat diandalkan. BR (2025) juga menekankan pentingnya prosedur hukum yang transparan, sehingga tidak hanya menjerat pelaku, tetapi juga melindungi hak korban dalam proses peradilan.

Contoh Penanganan Kasus Terkini

Kasus *Grok AI* mencontohkan langkah hukum yang diterapkan aparat Indonesia. Pemerintah memblokir konten, memeriksa operator platform, dan menelusuri penyebaran materi ilegal (Irma Widyastuti et al., 2026). Penegakan hukum melibatkan koordinasi lintas lembaga untuk mengidentifikasi pelaku dan menetapkan pertanggungjawaban pidana. Herianto (2025) menyebut bahwa kasus rekayasa foto dan *deepfake* juga menuntut kerja sama dengan pengembang platform agar konten dapat dihapus dan pihak pelaku dikenai sanksi.

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

Sihombing & Hermanto (2026) mencatat bahwa meski proses hukum sedang berjalan, kendala pembuktian masih signifikan. Akses terhadap server internasional, autentikasi data, dan identifikasi algoritma menjadi tantangan utama. Wafi et al. (2025) menunjukkan bahwa beberapa kasus penipuan berbasis rekaman suara berhasil diungkap melalui kolaborasi antara kepolisian, operator telekomunikasi, dan pengembang AI. Hal ini membuktikan bahwa koordinasi lintas pihak sangat efektif. Selain itu, Syahrani et al. (2025) menekankan bahwa edukasi publik tentang risiko AI juga penting untuk mencegah kerugian dan mempermudah proses penegakan hukum.

Diskusi Kritis

Kesesuaian Regulasi dengan Praktik Nyata

KUHP, UU ITE, dan UU PDP saat ini belum secara eksplisit mengatur penyalahgunaan AI, sehingga regulasi seringkali tertinggal dari praktik di lapangan (Hibatulloh, 2025). Hal ini menimbulkan celah hukum yang bisa dimanfaatkan pelaku kejahatan. Banfatin et al. (2025) menekankan bahwa regulasi saat ini fokus pada pelaku manusia, bukan teknologi sebagai alat yang dapat memicu tindak pidana. Padahal AI mampu menghasilkan dampak hukum yang signifikan.

Kawiswara (2026) menyebut bahwa kesenjangan ini menyebabkan aparat hukum harus menginterpretasi UU ITE secara analogis. Pendekatan ini efektif dalam jangka pendek, namun tidak menjamin kepastian hukum jangka panjang. Wafi et al. (2025) menambahkan bahwa praktik ini juga menimbulkan risiko inkonsistensi dalam putusan pengadilan, karena hakim harus menyesuaikan prinsip lama dengan fenomena baru. Pane & Permana (2025) menekankan perlunya revisi hukum agar eksplisit mencakup AI, termasuk mekanisme atribusi kesalahan dan pertanggungjawaban korporasi.

Model Pertanggungjawaban yang Disarankan

Patria (2025) mengusulkan model kombinasi antara pertanggungjawaban individu dan korporasi, sehingga celah hukum dapat diminimalkan. Model ini menekankan kontrol internal, audit algoritma, dan kewajiban mitigasi risiko. Putri et al. (2024) menambahkan bahwa pengguna AI juga harus memiliki tanggung jawab moral dan hukum, sehingga penyalahgunaan teknologi dapat dicegah sejak awal.

Hidayat (2025) menekankan model berbasis *risk-based liability*, di mana pihak yang memiliki kendali terbesar terhadap AI bertanggung jawab. Hal ini relevan untuk kasus AI otonom yang beroperasi tanpa intervensi manusia secara langsung. Syahrani et al. (2025) menyebut bahwa regulasi harus memuat standar operasional dan prosedur bagi pengembang AI, termasuk kewajiban melaporkan potensi risiko kepada otoritas terkait. Selain itu, Akbar & Ahmad (2026) menekankan pentingnya model sanksi preventif dan represif, agar pelaku penyalahgunaan AI dikenai konsekuensi hukum yang jelas.

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

Implikasi Hukum dan Kebijakan

Hibatulloh (2025) menekankan bahwa reformasi hukum diperlukan untuk menutup celah hukum yang muncul akibat AI. Regulasi yang adaptif akan meningkatkan kepastian hukum bagi korban dan aparat penegak hukum. Kawiswara (2026) menambahkan bahwa kebijakan nasional juga harus mencakup edukasi publik dan pelatihan aparat hukum untuk menghadapi kejahatan digital berbasis AI.

BR (2025) menekankan perlunya integrasi sistem hukum dengan teknologi forensik digital agar bukti AI dapat diterima di pengadilan. Happy Sturaya Quratuainniza & Nurkhaerani (2025) menambahkan bahwa kolaborasi lintas sektor penting untuk memastikan regulasi tidak hanya teoritis, tetapi juga dapat diterapkan dalam praktik. Terakhir, Hernawan et al. (2025) menyebut bahwa kebijakan ini harus mencakup mekanisme pengawasan korporasi dan pelatihan bagi pengguna akhir untuk mencegah penyalahgunaan AI.

Ringkasan Hasil

Bab ini menegaskan bahwa kejahatan digital berbasis AI meningkat pesat di Indonesia (2023–2026). Tren *deepfake*, *voice cloning*, dan penipuan digital menimbulkan tantangan hukum baru (Darmawan et al., 2025). Pertanggungjawaban pidana harus diarahkan pada manusia dan korporasi yang mengembangkan atau mengoperasikan AI, karena entitas teknologi belum diakui sebagai subjek hukum pidana (Hibatulloh, 2025; Pane & Permana, 2025). Celah hukum dalam KUHP, UU ITE, dan UU PDP menuntut reformasi regulasi untuk mencakup AI sebagai alat atau mediator tindak pidana.

Pendekatan *risk-based liability* dan *vicarious liability* menjadi kunci untuk menegakkan sanksi yang adil (Patria, 2025). Penyidikan dan penegakan hukum menekankan kolaborasi lintas lembaga, integrasi teknologi forensik, dan edukasi publik agar korban terlindungi dan pelaku dapat diadili (Sihombing & Hermanto, 2026). Secara keseluruhan, bab ini menyimpulkan bahwa kombinasi regulasi hukum yang adaptif, tanggung jawab individu dan korporasi, serta mekanisme penegakan hukum modern adalah strategi efektif untuk menghadapi penyalahgunaan AI dalam kejahatan digital di Indonesia.

KESIMPULAN

Berdasarkan hasil penelitian dan analisis terhadap kejahatan digital berbasis kecerdasan buatan (AI) di Indonesia, dapat disimpulkan bahwa fenomena ini menunjukkan tren peningkatan signifikan dalam bentuk deepfake, voice cloning, dan penipuan digital. Kasus-kasus yang terjadi antara tahun 2023 hingga 2026 menegaskan bahwa AI tidak lagi sekadar alat, melainkan mediator yang dapat memperluas jangkauan kejahatan, menimbulkan kerugian materiil maupun psikologis bagi korban, serta menimbulkan tantangan hukum yang kompleks. Analisis kasus Grok AI, penyebaran konten non-consensual, dan penipuan berbasis rekaman

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

suara memperlihatkan bahwa modus operandi AI sangat bervariasi dan cenderung semi-otonom, sehingga pertanggungjawaban pidana tidak bisa diarahkan kepada AI itu sendiri, melainkan pada manusia atau korporasi yang mengembangkan, mengoperasikan, atau menyebarluaskan teknologi tersebut.

Kedua, penelitian ini menegaskan bahwa KUHP, UU ITE, dan UU Perlindungan Data Pribadi saat ini belum secara eksplisit mengakomodasi penyalahgunaan AI, sehingga terdapat celah hukum yang dapat dimanfaatkan pelaku. Kekosongan regulatif ini menimbulkan dilema dalam atribusi kesalahan, terutama ketika AI beroperasi otonom atau melibatkan jaringan kompleks antara pengembang, operator, dan pihak ketiga. Dengan demikian, reformasi hukum yang adaptif menjadi sangat penting, mencakup mekanisme pertanggungjawaban individu, tanggung jawab korporasi, serta penerapan asas risk-based liability dan vicarious liability untuk menutup celah hukum dan mencegah kerugian lebih lanjut.

Ketiga, penelitian ini menemukan bahwa pertanggungjawaban pidana terhadap kejahatan AI harus bersifat kombinatif, yakni menggabungkan tanggung jawab pengguna akhir, pengembang teknologi, dan korporasi. Model ini menekankan kontrol internal, audit algoritma, kewajiban mitigasi risiko, serta kewajiban moral dan hukum pengguna AI. Hal ini relevan terutama dalam kasus konten non-consensual dan pencemaran nama baik, di mana korban sering kali tidak dapat menuntut pelaku secara langsung karena keterlibatan AI sebagai mediator. Pendekatan ini memungkinkan sistem hukum untuk tetap adil dan proporsional dalam menilai kesalahan manusia dan korporasi.

Keempat, mekanisme penyidikan dan penegakan hukum memerlukan kolaborasi lintas lembaga, integrasi teknologi forensik digital, dan edukasi publik. Penelitian menunjukkan bahwa koordinasi antara kepolisian, Kemenkominfo, operator platform AI, serta pengembang sangat efektif dalam mengungkap kasus penipuan berbasis AI maupun penyebaran konten manipulatif. Namun, kendala teknis, seperti akses terhadap server internasional, autentikasi log algoritma, dan tracing aktivitas AI, tetap menjadi tantangan utama yang memerlukan pendekatan multidisiplin antara hukum dan teknologi.

Secara keseluruhan, penelitian ini menyimpulkan bahwa menghadapi kejahatan digital berbasis AI memerlukan strategi hukum yang komprehensif dan adaptif, mencakup pembaruan regulasi, pertanggungjawaban kombinatif antara manusia dan korporasi, serta mekanisme penegakan hukum modern yang berbasis risiko dan transparansi. Dengan demikian, korban dapat terlindungi secara efektif, pelaku dapat dikenai sanksi yang adil, dan sistem hukum Indonesia mampu menghadapi dinamika kejahatan digital yang semakin canggih dan kompleks.

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

DAFTAR PUSTAKA

Akbar, A. M., & Ahmad, A. S. (2026). Tangungjawab pidana pelaku penyebaran deepfake sebagai hoaks terhadap kebijakan negara. Syntax Literate: Jurnal Ilmiah Indonesia, 11(1), 259–276

Alviani, A., & Fitri, Y. Z. (2024). Pengaturan hukum tindak pidana terhadap penyalahgunaan teknologi AI (artificial intelligence) dalam penipuan suara (voice phishing) melalui telepon seluler. Jurnal Hukum De'Rechtsstaat. https://ojs.unida.ac.id/LAW

Aster Yansen Basah, D., Wijaya, A., & Januardy, I. (2025). Kriminalisasi pelanggaran protokol digital: Tinjauan hukum pidana terhadap penyebaran deepfake di media sosial. Innovative: Journal of Social Science Research, 5(4), 386–398. https://doi.org/10.31004/innovative.v5i4.20258

Banfatin, P. M., Medan, K. K., & Fallo, D. F. N. (2025). Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake dalam melakukan tindak pidana cybercrime. Pemuliaan Keadilan, 2(1), 60–73. https://doi.org/10.62383/pk.v2i1.402

BR, W. (2025). Tantangan penegakan hukum terhadap kejahatan berbasis teknologi AI. Innovative: Journal of Social Science Research, 5(1), 3436–3451.

Darmawan, R. A., Fardiansyah, A. I., & Tamza, F. B. (2025). Analisis hukum atas tindak pidana penipuan melalui rekaman suara berbasis kecerdasan buatan (AI) dalam perspektif kejahatan ekonomi. Rewang Rencang: Jurnal Hukum Lex Generalis, 6(7). https://jhlg.rewangrencang.com/

Ginting, Y. P. (2025). Criminal accountability in the era of artificial intelligence abuse from the perspective of legality. The Prosecutor Law Review, 3(3), 48–62.

Happy Sturaya Quratuainniza, & Ema Nurkhaerani. (2025). Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia. ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora, 4(1), 71–87. https://doi.org/10.59246/aladalah.v4i1.1694

Herianto, F. N. (2025). Pertanggung jawaban pidana terhadap rekayasa foto yang mengandung unsur pencemaran nama baik. Jurnal Ilmu Hukum, Humaniora dan Politik, 6(1), 827. https://doi.org/10.38035/jihhp.v6i1

Hernawan, C. N. P., Antow, D. T., & Sendow, A. V. (2025). Tinjauan hukum mengenai penyalahgunaan artificial intelligence dalam tindak pidana kekerasan seksual. Lex Privatum: Jurnal Fakultas Hukum Unsrat, 15(4),211-228.

Hibatulloh, B. H. F. (2025). Upaya penegakan hukum terhadap AI (artificial intelligence) sebagai subjek hukum pidana dalam perspektif kriminologi.

Vol 4 No 1 (2026) 1-15 E-ISSN 3025-0862
DOI: 10.61234/ahd.v4i1.108

TARUNALAW: Journal of Law and Syariah, 3(1), 87–98. https://doi.org/10.54298/tarunalaw.v3i01.300

Hidayat, M. N. (2025). Pertanggungjawaban pidana terhadap penyalahgunaan deepfake sebagai ancaman keamanan data pribadi. UNES Law Review, 7(4), 2036–2048. https://doi.org/10.31933/unesrev.v7i4.2433

Iradat, M. A., & Hariyanto, D. R. S. (2025). Urgensi pengaturan pidana penyalahgunaan deepfake: Telaah aspek perlindungan korban dalam hukum nasional. Jurnal Media Akademik (JMA), 3(12), 128–141. https://doi.org/10.62281

Irma Widyastuti, Neza Aisyah Intani, & Henricus Surya Simamora. (2026). Tinjauan Hukum Terhadap Penyalahgunaan Artificial Intelligence Dalam Pembuatan Konten Video Bermuatan Pelecehan Seksual Terhadap Perempuan. Al-Zayn : Jurnal Ilmu Sosial & Hukum, 4(1), 173–183. https://doi.org/10.61104/alz.v4i1.2964

Kawiswara, I. G. A. S. (2026). Problematika dan urgensi hukum kecerdasan buatan ditinjau dari hukum di Indonesia. Federalisme: Jurnal Kajian Hukum dan Ilmu Komunikasi, 3(1), 46–58. https://doi.org/10.62383/federalisme.v3i1.1524

Mecca, A. S. P., Hidaya, W. A., & Tuasikal, H. (2025). Pemanfaatan teknologi kecerdasan buatan (artificial intelligence) dalam sistem peradilan pidana di Indonesia. Jurnal Sosial dan Teknologi (SOSTECH), 5(6), 1730-1748.

Pane, M. D., & Permana, M. Z. S. (2025). Pertanggungjawaban pidana terhadap pengembang artificial intelligence pada kasus pelanggaran privasi dan data pribadi. Judge: Jurnal Hukum, 6(3), 467–481 https://doi.org/10.54209/judge.v6i03.1593

Patria, V. S. (2025). Prospek pengaturan kecerdasan buatan sebagai subjek hukum pidana dan model pertanggungjawabannya. Sultan Adam: Jurnal Hukum dan Sosial, 3(1). https://doi.org/10.71456/sultan.v3i1.1214

Putri, N. P. M., Hartono, M. S., & Yudiawan, I. D. G. H. (2024). Analisis reformulasi pertanggungjawaban pidana pengguna teknologi deepfake dalam tindak pidana pencemaran nama baik berbasis artificial intelligence. Jurnal Pacta Sunt Servanda, 5(2), 120–129. https://doi.org/10.23887/jpss.v5i2.5807

Ruhtiani, M., & Istikharoh, I. (2025). Hukum pidana dan hak cipta di era kecerdasan artifisial: Analisis pertanggungjawaban dalam hukum positif dan hukum Islam. Jurnal Al Wasith: Jurnal Studi Hukum Islam, 10(1), 62. https://ejournal.uhb.ac.id/index.php/alwasith

Santoso, J. T., & Wibowo, A. (2023). Hakim, teknologi dan artificial intelligence (AI). Yayasan Prima Agus Teknik. ISBN 978-634-7227-32-4

Shabrina, A. N., Naila, G. S., Nuryansyah, G. P., & Amanda, R. (2026). Bahaya deepfake dalam penyalahgunaan Grok AI di platform X sebagai bentuk disinformasi. Integrative Perspectives of Social and Science Journal (IPSSJ), 3(1), 195.

Sihombing, G. R. A., & Hermanto, B. (2026). Dinamika kebijakan penegakan hukum terhadap pemanfaatan kecerdasan buatan dalam kejahatan siber di Indonesia. Jurnal Media Akademik, 4(1), XX–XX. https://doi.org/10.62281

Sulistio, F., & Salsabilla, A. D. (2023). Pertanggungjawaban pada tindak pidana yang dilakukan agen otonom artificial intelligence. Review UNES, 6(2), 5479. https://doi.org/10.31933/unesrev.v6i2

Syahrani, D. F., Primananda, M. A., Paramesti, N. Z., Zalifah, Y. K., & Nugroho, A. A. (2025). Analisis yuridis terhadap non-consensual AI-generated sexual content sebagai digital voyeurism dalam hukum pidana Indonesia. Media Hukum Indonesia (MHI), 4(1), 1–11. https://doi.org/10.5281/zenodo.17810678

Wafi, M. S., Wisnubroto, A., & Prayudi, Y. (2025). Kejahatan deepfake berbasis artificial intelligence: Suatu konsepsi pada penggunaan asas culpabilitas sebagai pembaharuan pertanggungjawaban pidana. Reformasi Hukum, 29(2), 168–183. https://doi.org/10.46257/jrh.v29i2.1304

Zaenudin, I., & Riyan, A. B. (2024). Perkembangan kecerdasan buatan (AI) dan dampaknya pada dunia teknologi. Jurnal Informatika Utama, 2(2), 128–153. https://doi.org/10.55903/jitu.v2i2.240