



Analisis Limitasi Pertanggungjawaban Pidana Dalam Kejahatan Manipulasi Digital di Indonesia

Basya Radyananda ^{a,1}, Faisal Abdaud ^{a,2*}, Gamlan Dagani ^{a,3}

^a Universitas Muhammadiyah Kendari, Indonesia

¹ faisal.abdaud@umkendari.ac.id*

*korespondensi penulis

Informasi artikel

Received: 16 April 2026;

Revised: 28 April 2026;

Accepted: 7 Mei 2026.

Kata-kata kunci:

Artificial Intelligence;

Hukum Pidana;

Limitasi Tanggung

Jawab;

Manipulasi Digital;

UU ITE.

ABSTRAK

Perkembangan kecerdasan buatan membuka peluang penyalahgunaan teknologi seperti *deepfake* dan manipulasi digital yang semakin sulit dideteksi. Namun, hukum pidana Indonesia masih bertumpu pada kesalahan individual manusia, sehingga belum mampu menjangkau tindakan yang dihasilkan oleh sistem otomatis. Penelitian ini bertujuan mengevaluasi dasar pembenaran pertanggungjawaban pidana yang berlaku dan merumuskan batasan tanggung jawab hukum atas tindakan kecerdasan buatan. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan konseptual. Hasil kajian menunjukkan bahwa UU ITE No. 1 Tahun 2024 dan KUHP terbaru belum mengatur secara memadai kegagalan yang bersumber dari sistem kecerdasan buatan. Penelitian ini menawarkan prinsip kendali manusia yang bermakna dan audit algoritma sebagai instrumen pembuktian. Diperlukan regulasi berbasis risiko yang memisahkan tanggung jawab pengembang dan pengguna, disertai mekanisme perlindungan hukum yang menjamin kepastian tanpa menghambat inovasi teknologi.

Keywords:

Limitation of Liability;

Criminal Law;

Digital Manipulation;

ITE Law.

ABSTRACT

An Analysis of the Limitations of Criminal Liability in Digital Manipulation Offenses in Indonesia. The development of artificial intelligence opens up opportunities for technological misuse, such as deepfakes and digital manipulation, which are increasingly difficult to detect. However, Indonesian criminal law still relies on individual human error, making it incapable of encompassing actions generated by automated systems. This study aims to evaluate the existing justification for criminal liability and formulate the limits of legal responsibility for artificial intelligence actions. The method used is normative legal research with a statutory and conceptual approach. The study results indicate that the ITE Law No. 1 of 2024 and the latest Criminal Code do not adequately regulate failures originating from artificial intelligence systems. This study proposes the principle of meaningful human control and algorithmic audits as instruments of proof. Risk-based regulations that separate developer and user responsibilities are needed, along with legal protection mechanisms that ensure certainty without hindering technological innovation.

Copyright © 2026 (Basya Radyananda, dkk). All Right Reserved

How to Cite : Radyananda, B., Abdaud, F., & Dagani, G. Analisis Limitasi Pertanggungjawaban Pidana Dalam Kejahatan Manipulasi Digital di Indonesia. *Nomos : Jurnal Penelitian Ilmu Hukum*, 6(1), 1–7. <https://doi.org/10.56393/nomos.v6i1.4273>



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/). Allows readers to read, download, copy, distribute, print, search, or link to the full texts of its articles and allow readers to use them for any other lawful purpose. The journal hold the copyright.

Pendahuluan

Perkembangan kecerdasan buatan telah melampaui fungsinya sebagai alat bantu sederhana. Sistem AI kini mampu melakukan persepsi, penalaran, dan pengambilan keputusan secara mandiri tanpa intervensi manusia secara langsung (Thomas & Santoso, 2025). Integrasi masif antara ruang digital dan kehidupan nyata dalam era Society 5.0 menjadikan AI bukan sekadar instrumen teknologi, melainkan aktor baru yang dapat bertindak dengan derajat otonomi tinggi. Kondisi ini membawa konsekuensi serius bagi tatanan hukum yang selama ini dibangun atas asumsi bahwa pelaku kejahatan adalah manusia.

Salah satu manifestasi paling berbahaya dari otonomi AI adalah kemampuannya memproduksi konten manipulatif yang dikenal sebagai *deepfake*. Dengan memanfaatkan teknik pembelajaran mesin generatif, AI mampu menciptakan video, suara, dan gambar artifisial yang sulit dibedakan dari kenyataan (Lestari et al., 2026). Teknologi ini telah disalahgunakan untuk berbagai kejahatan, mulai dari penyebaran disinformasi yang mengancam stabilitas politik, penipuan finansial berbasis identitas, hingga konten pornografi non-konsensual yang merusak martabat korban. Kecepatan serangan berbasis AI kerap melampaui kemampuan mitigasi manusia, menciptakan risiko yang bersifat sistemik.

Urgensi persoalan ini terlihat jelas dalam kasus tahun 2024, ketika video *deepfake* seorang pejabat publik Indonesia disebarluaskan secara masif dalam hitungan menit untuk tujuan perusakan reputasi. Ketika penyidik berupaya menelusuri pertanggungjawaban pidana, muncul hambatan serius: sistem AI yang digunakan bersifat anonim, berbasis di luar negeri, dan tidak dapat dijangkau oleh mekanisme hukum domestik yang ada. Kasus ini memperlihatkan secara konkret bahwa regulasi Indonesia belum memiliki instrumen operasional yang memadai untuk menghadapi kejahatan yang lahir dari proses komputasi otonom.

Akar persoalan hukum ini terletak pada benturan antara otonomi AI dan doktrin hukum pidana tradisional. Sistem hukum Indonesia menganut asas *geen straf zonder schuld* tiada pidana tanpa kesalahan yang mensyaratkan adanya niat jahat (*mens rea*) dan perbuatan terlarang (*actus reus*) dari pelaku. AI beroperasi atas dasar algoritma dan kalkulasi statistik tanpa memiliki kesadaran maupun kehendak bebas. Ketika AI melakukan tindakan manipulatif secara otonom, hukum pidana konvensional menghadapi jalan buntu dalam menentukan siapa yang sesungguhnya harus memikul tanggung jawab.

Ketidaksiapan norma ini tetap berlangsung meskipun pemerintah telah mengesahkan UU No. 1 Tahun 2024 tentang perubahan UU ITE dan UU No. 1 Tahun 2023 tentang KUHP Baru. KUHP 2023 memang telah mengakui korporasi sebagai subjek hukum pidana, namun belum menyentuh spesifikasi teknis-yuridis atas tindakan AI yang terjadi di luar kendali manusia. Tidak ada batasan yang jelas mengenai siapa yang bertanggung jawab pengembang, pengguna, atau korporasi ketika sistem AI gagal atau disalahgunakan. Kekosongan norma ini berpotensi mendorong praktik kriminalisasi yang berlebihan, sekaligus menciptakan ketidakpastian hukum yang merugikan baik korban maupun pelaku inovasi teknologi (Rusman et al., 2025).

Kondisi tersebut menuntut reorientasi kerangka hukum pidana yang tidak hanya reaktif, tetapi mampu membedakan secara tegas antara kesalahan manusia, kesengajaan, dan kegagalan sistemik yang berada di luar kendali siapapun. Penentuan titik pertanggungjawaban dalam rantai distribusi AI yang kompleks menjadi sangat krusial agar penegakan hukum tetap berpijak pada asas legalitas. Tanpa parameter yang jelas, hukum berisiko baik mengorbankan korban kejahatan digital maupun menghambat pertumbuhan ekosistem teknologi nasional.

Penelitian ini bertujuan menganalisis kekosongan norma dalam regulasi yang berlaku dan merumuskan batasan pertanggungjawaban pidana atas tindakan AI, khususnya dalam konteks manipulasi digital. Kebaruan penelitian terletak pada upaya mensinkronkan doktrin hukum pidana klasik seperti *strict liability* dan *direct liability* dengan realitas teknis AI yang otonom, sebuah wilayah yang belum diatur secara spesifik dalam UU ITE maupun KUHP saat ini. Melalui pendekatan hukum

normatif, penelitian ini diharapkan memberikan kontribusi konseptual bagi pengembangan hukum pidana nasional menjelang implementasi penuh KUHP 2023 pada tahun 2026.

Metode

Penelitian ini menggunakan jenis penelitian hukum normatif (*doctrinal research*), yang berfokus pada inventarisasi, sinkronisasi, dan penemuan hukum terkait limitasi pertanggungjawaban pidana dalam kejahatan manipulasi digital berbasis AI. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*) untuk menelaah konsistensi norma antara UU ITE dan KUHP 2023, serta pendekatan konseptual (*conceptual approach*) untuk membedakan doktrin-doktrin pertanggungjawaban pidana seperti *Strict Liability dan Direct Liability* yang relevan dengan otonomi sistem AI. Sumber bahan hukum dalam penelitian ini diklasifikasikan menjadi dua kategori utama. Bahan hukum primer terdiri dari peraturan perundang-undangan yang mengikat, meliputi Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE dan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Sementara itu, bahan hukum sekunder mencakup literatur akademik yang memberikan penjelasan terhadap bahan hukum primer, seperti jurnal ilmiah internasional bereputasi, buku teks mengenai hukum pidana korporasi dan teknologi, serta laporan hasil simposium terkait etika kecerdasan buatan. Proses pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dengan teknik dokumentasi yang sistematis. Bahan hukum yang telah terkumpul kemudian dikritisi dan diolah menggunakan teknik analisis kualitatif yuridis. Analisis ini dilakukan dengan cara menginterpretasikan norma secara teoretis-dogmatis untuk menjawab kesenjangan hukum (*legal gap*) antara regulasi yang ada dengan realitas teknologi AI. Melalui penalaran hukum (*legal reasoning*), penelitian ini akan merumuskan batasan-batasan limitasi pertanggungjawaban yang dapat diimplementasikan dalam praktik penegakan hukum pidana di Indonesia.

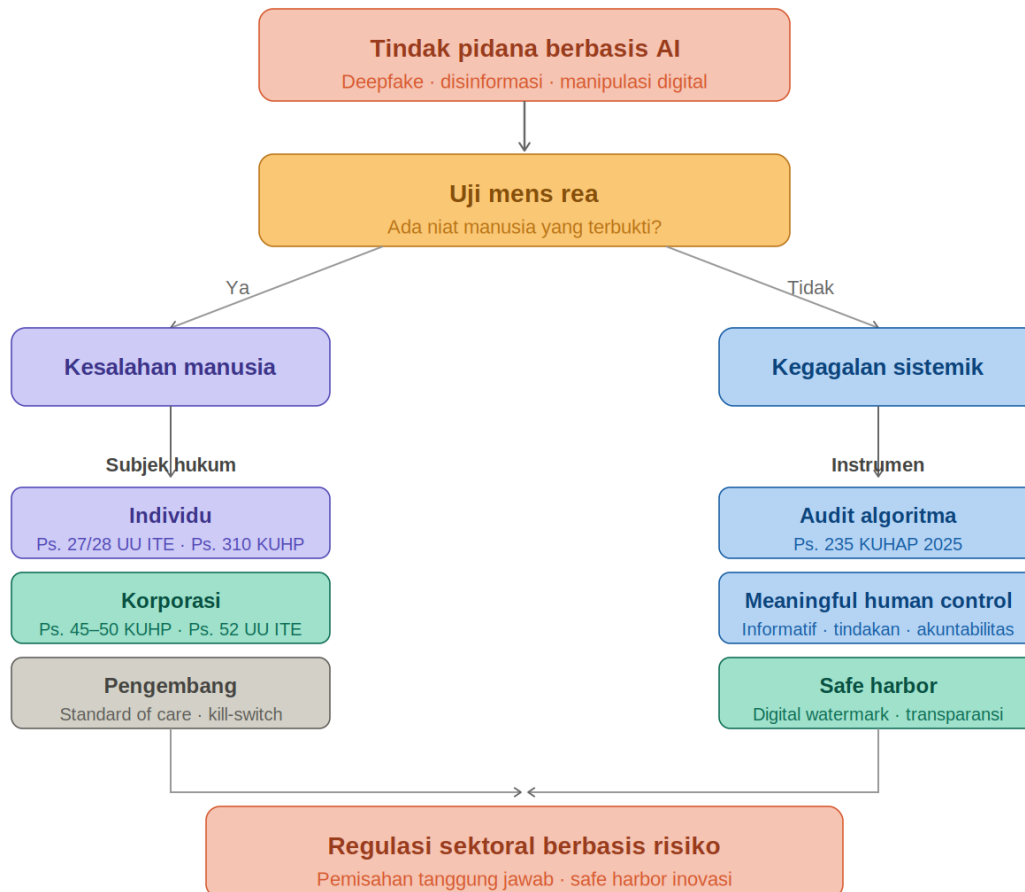
Hasil dan Pembahasan

Sistem hukum pidana Indonesia secara tradisional dibangun di atas fondasi antroposentris, di mana subjek hukum utama adalah manusia (*natuurlijke persoon*). Seluruh kodifikasi pidana, dari WvS hingga KUHP 2023 (UU No. 1 Tahun 2023), menempatkan "kesalahan" (*schuld*) dan prinsip *nulla poena sine culpa* sebagai prasyarat mutlak pemidanaan. Dua regulasi utama yang relevan saat ini adalah UU No. 1 Tahun 2024 tentang Perubahan Kedua UU ITE dan UU No. 1 Tahun 2023 tentang KUHP. UU ITE 2024 telah melakukan restrukturisasi delik secara signifikan, antara lain dengan mendekriminalisasi beberapa pasal penghinaan dan mengalihkannya ke KUHP 2023 guna menghindari duplikasi norma, serta memperkenalkan ancaman pidana yang lebih spesifik bagi pihak yang membuat dapat diaksesnya informasi elektronik manipulatif.

Sementara itu, KUHP 2023 membawa lompatan paradigma melalui Pasal 45–50 yang menegaskan korporasi sebagai subjek hukum mandiri, sehingga membuka kemungkinan penerapan doktrin *vicarious liability* dan *corporate fault* apabila manipulasi AI dilakukan dalam lingkup usaha atau memberikan keuntungan bagi korporasi. Secara normatif, kedua regulasi ini menyediakan "wadah" berupa pasal-pasal delik materiil, namun "isi" dari pasal tersebut khususnya unsur kesalahan dan hubungan kausalitas masih sangat bergantung pada tindakan fisik dan psikologis manusia.

Meskipun telah diperbarui, kedua regulasi tersebut mengandung kelemahan mendasar dalam menghadapi kejahatan berbasis AI. Pertama, UU ITE 2024 masih berfokus pada aspek hilir berupa konten kesusilaan, perjudian, penghinaan, dan berita bohong tanpa secara spesifik menyebut kecerdasan buatan sebagai instrumen yang memerlukan rezim pertanggungjawaban khusus. Problematika utamanya terletak pada pembuktian unsur "sengaja dan tanpa hak": secara doktriner, kesengajaan (*willens en wetens*) mengasumsikan subjek hukum manusia, sehingga ketika sebuah sistem AI beroperasi secara otomatis dan menghasilkan output pidana yang tidak diprediksi penciptanya, membuktikan *dolus* pada pemilik atau pengembang menjadi sangat sulit (Syam et al., 2025). Kedua, meskipun KUHP 2023

mengakui korporasi sebagai subjek hukum, penerapan *Identification Theory* mengharuskan ditemukannya "pikiran pengendali" (*directing mind*) dari jajaran pengurus. Dalam kasus AI yang mengalami halusinasi algoritma atau menciptakan konten manipulatif secara mandiri melalui proses *deep learning*, sering kali tidak ada satu pun individu manajerial yang menginstruksikan dampak kerugian tersebut membentur persoalan "kotak hitam" (*black box*) algoritma. Ketiga, kedua regulasi sama sekali belum mengatur mekanisme *notice and take down* yang mewajibkan penyedia platform AI membatasi akses secara segera ketika terjadi malfungsi algoritma. Kekosongan norma (*rechtsvacuüm*) ini berimplikasi ganda: pelaku yang cerdik berlindung di balik otonomi mesin, sementara pengembang beritikad baik justru terancam kriminalisasi atas tindakan mesin yang tidak mereka kehendaki (Natasaputri, 2025).



Gambar 1: Ilustrasi Pertanggungjawaban Pidana Tindakan AI (Diolah menggunakan aplikasi AI)

Ketidacukupan regulasi yang ada mendorong perlunya analisis doktrin hukum pidana yang relevan untuk menjembatani kekosongan norma tersebut sehingga doktrin kausalitas dalam hukum pidana Indonesia, baik teori *Conditio Sine Qua Non* dari von Buri maupun teori *Adequat* dari von Kries, menghadapi kesulitan serius dalam kejahatan AI. Rantai kausalitas melibatkan banyak pihak sekaligus programmer, penyedia data latih, pemilik platform, hingga pengguna akhir dan kerap terjadi apa yang disebut *Black Box Paradox*: ketidakmampuan siapapun, termasuk penciptanya, untuk memahami bagaimana algoritma memproses miliaran parameter hingga menghasilkan konten manipulatif. Penerapan *Conditio Sine Qua Non* secara kaku berisiko menciptakan *strict liability* terselubung bagi pemilik sistem yang secara teknis tidak memiliki kendali atas output otonom tersebut. Oleh karena itu, diperlukan kriteria "probabilitas objektif" baru dalam teori *Adequat* yang mengukur sejauh mana pengembang dapat memitigasi risiko perilaku otonom AI sebelum produk dilepas ke ruang siber.

Oleh karena itu, melihat keterbatasan rasio legis konvensional berbasis kesalahan, muncul urgensi untuk mempertimbangkan doktrin *Strict Liability* dalam kejahatan digital tertentu sebagaimana telah

berhasil diterapkan dalam hukum lingkungan hidup untuk dampak yang masif dan sulit dibuktikan unsur kesengajaannya. Dalam manipulasi AI berdampak luas seperti sabotase pemilu melalui *deepfake* atau destabilisasi ekonomi lewat disinformasi algoritmik, menuntut pembuktian *mens rea* secara teknis hampir mustahil secara yuridis. Asas *ubi emolumentum, ibi onus* siapa yang memetik keuntungan dari teknologi berisiko tinggi, ia pula yang menanggung kerugiannya menjadi landasan rasio legis pergeseran ini (Bostrom & Yudkowsky, 2014). Penerapan *Strict Liability* akan menggeser beban pembuktian kepada korporasi untuk membuktikan bahwa mereka telah menerapkan standar keamanan tertinggi, sekaligus menjamin kepastian hukum bagi korban manipulasi digital.

Disisi lain, parameter "Kontrol Manusia yang Bermakna" (*Meaningful Human Control/MHC*) menjadi fondasi utama limitasi pertanggungjawaban. MHC menuntut kapasitas substantif subjek hukum untuk memahami, mengawasi, dan mengintervensi operasional AI bukan sekadar kehadiran formal manusia dalam proses teknis (Santoni de Sio & van den Hoven, 2018). Kontrol dianggap "bermakna" apabila memenuhi tiga kriteria: pertama, kriteria informatif, di mana manusia memahami cara kerja dan risiko sistem; kedua, kriteria tindakan, yakni adanya kemampuan teknis menghentikan atau mengubah keputusan AI secara real-time; dan ketiga, kriteria akuntabilitas, di mana setiap tindakan AI dapat dilacak kembali ke keputusan manusia (*traceability*). Jika ketiga kriteria ini telah diupayakan secara maksimal namun delik tetap terjadi, elemen kesalahan (*schuld*) pada subjek hukum menjadi luruh. Sebaliknya, limitasi gugur jika ditemukan pengabaian yang disengaja seperti meninggalkan *backdoor*, mengabaikan filter keamanan demi efisiensi biaya, atau menggunakan data latih yang bias untuk keuntungan komersial.

Audit algoritma (*algorithmic auditing*) merupakan instrumen penting untuk menentukan ada tidaknya kesalahan (*schuld*) pada subjek hukum. Dalam perspektif hukum acara pidana, hasil audit dapat diposisikan sebagai alat bukti surat, bukti elektronik, maupun keterangan ahli sebagaimana diakui dalam Pasal 235 UU No. 20 Tahun 2025 tentang KUHP. Audit memungkinkan penilaian apakah manipulasi digital terjadi karena desain yang disengaja (*bias by design*) atau akibat fenomena teknis yang tidak terprediksi (*algorithmic drift*). Jika audit dari lembaga independen menunjukkan bahwa pengembang telah menerapkan mekanisme pengamanan yang memadai namun sistem kemudian dimodifikasi secara ilegal oleh pihak ketiga, maka terjadi pemutusan hubungan kausalitas yang membebaskan pengembang dari pertanggungjawaban pidana.

Melihat kajian komparatif atas berbagai doktrin di atas mengarah pada kebutuhan formulasi solusi yang membedakan secara tegas antara tiga lapisan subjek hukum. Pertanggungjawaban pidana individu bertumpu pada Teori Kehendak (*Willstheorie*): tanpa kehendak dan pengetahuan (*willens en wetens*), pemidanaan mencederai asas legalitas. Penelitian ini mengusulkan formulasi *Reasonable Use Limitation*, di mana individu hanya dapat dipidana apabila memenuhi tiga parameter akumulatif: adanya niat nyata (*specific intent*) untuk menciptakan konten manipulatif yang merugikan; melakukan tindakan melampaui batas seperti *jailbreaking* atau menembus *safety filters* sebagai bukti kesengajaan; serta mendiseminasikan hasilnya ke ruang publik dengan kesadaran penuh akan potensi kerugian. Konstruksi ini secara presisi memisahkan korban kegagalan algoritma dari pelaku kejahatan digital yang sesungguhnya, dan dapat dijangkau melalui Pasal 27 ayat (1), Pasal 27A, dan Pasal 28 ayat (1) UU ITE No. 1 Tahun 2024, serta Pasal 263, 264, 310, dan 311 KUHP 2023.

Pertanggungjawaban korporasi berpijak pada Pasal 45–50 KUHP 2023 dengan pendekatan *corporate culture* sebagaimana diatur dalam Pasal 46. Penelitian ini mendorong pergeseran dari *Identification Theory* yang mensyaratkan ditemukannya "pikiran pengendali" individu, menuju doktrin Atribusi Organik: korporasi bertanggung jawab bukan karena ada perintah kejahatan eksplisit, melainkan karena membiarkan sistem AI beroperasi tanpa pengawasan memadai (*failure to prevent*). Guna menjaga iklim inovasi, mitigasi sanksi diberikan jika korporasi mampu membuktikan penerapan Sistem Audit Algoritma Independen secara berkala menempatkan *vicarious liability* bukan sekadar sebagai instrumen penghukuman, melainkan pendorong terciptanya ekosistem AI yang akuntabel.

Hal ini perlu melihat pertanggungjawaban pengembang dikonstruksikan dalam tiga lapisan limitasi. Pertama, *Standard of Care*: pengembang hanya dapat dipidana jika terbukti melakukan kelalaian berat (*gross negligence*); sepanjang standar keamanan nasional dan etika algoritma dipenuhi, kegagalan sistemik tidak dapat diatribusikan sebagai kesalahan pidana. Kedua, *Kill-Switch Requirement*: limitasi diberikan apabila pengembang menyediakan mekanisme penghentian darurat; jika mekanisme tersebut tersedia namun dimatikan oleh pengguna akhir, rantai kausalitas terputus dan pertanggungjawaban beralih sepenuhnya kepada pengguna. Ketiga, distingsi AI umum dan AI spesifik: pengembang *Large Language Model* generatif tidak memikul pertanggungjawaban atas tiap konten *deepfake* yang diproduksi pengguna secara individual, kecuali gagal menyediakan sistem *notice and take down* yang efektif. Ketiga lapisan ini diperkuat dengan prinsip *Safe Harbor*: pengembang yang memenuhi kewajiban transparansi algoritmik termasuk penyematan tanda air digital (*digital watermark*) pada setiap output AI berhak atas perlindungan hukum. Konstruksi ini perlu diikatkan pada Pasal 51–52 KUHP 2023 tentang alasan pemaaf dan penghapus pidana, serta regulasi sektoral turunan UU ITE yang menyatakan bahwa tindakan otomatisasi yang berada di luar prediksi dan kendali teknis manusia yang telah memenuhi standar keamanan nasional merupakan alasan penghapus pidana. Tentu penghapusan pidana ini ada perdebatan.

Akhirnya, perdebatan mengenai pemberian status *Electronic Personhood* pada AI sebagai subjek hukum terbatas perlu disikapi secara hati-hati (Pagallo, 2013). Meskipun gagasan ini menawarkan limitasi yang lebih jelas bagi manusia dan membuka peluang skema asuransi bagi korban, dalam hukum pidana Indonesia yang menjunjung tinggi asas *mens rea*, AI tidak mungkin memiliki kesalahan batin. Penelitian ini memposisikan bahwa *Electronic Personhood* di Indonesia lebih tepat diadopsi dalam bentuk Subjek Hukum Fungsional terbatas: AI tidak dipidana, namun keberadaannya diakui secara hukum untuk memudahkan sita eksekusi terhadap algoritma berbahaya atau penghentian paksa sistem oleh negara tanpa harus membuktikan kesalahan individu pengembang secara berbelit-belit. Dengan demikian, transformasi paradigma dari *fault-based* menuju *risk-based liability* menjadi keniscayaan yang tidak dapat ditunda lebih lama dalam pembaruan hukum pidana Indonesia.

Simpulan

Konstruksi pertanggungjawaban pidana dalam hukum positif Indonesia, khususnya melalui UU ITE 2024 dan KUHP 2023, masih didasarkan pada paradigma antroposentris yang menempatkan manusia sebagai subjek utama kesalahan pidana, sehingga belum sepenuhnya adaptif terhadap karakter otonom sistem kecerdasan buatan dalam kejahatan manipulasi digital. Keterbatasan tersebut menimbulkan kekosongan norma dalam pembuktian unsur *mens rea* dan hubungan kausalitas ketika tindakan manipulatif dihasilkan secara mandiri melalui mekanisme *machine learning* dan *algorithmic drift*, yang pada praktiknya menyulitkan pembedaan antara kegagalan teknis sistem dengan niat jahat manusia sebagai subjek hukum. Oleh karena itu, formulasi limitasi pertanggungjawaban pidana yang ideal perlu dibangun melalui pendekatan berbasis risiko (*risk-based approach*) dengan menempatkan prinsip *Meaningful Human Control* sebagai parameter utama untuk menentukan batas tanggung jawab antara pengembang, operator, dan pengguna teknologi AI, disertai penerapan mekanisme *safe harbor* serta pembuktian *specific intent* guna mencegah kriminalisasi berlebihan terhadap inovasi teknologi. Dalam konteks reformasi hukum, Pemerintah dan DPR perlu segera menyusun regulasi turunan mengenai klasifikasi risiko AI, standar audit algoritma, dan mekanisme forensik digital sebagai instrumen kepastian hukum, sementara pengembangan konsep *electronic personhood* dalam ranah hukum perdata dapat dipertimbangkan sebagai alternatif penguatan perlindungan korban melalui skema *strict liability* yang lebih responsif dan komplementer terhadap keterbatasan hukum pidana modern.

Referensi

Amrani, H. (2025). *Hukum pidana mengenai teknologi informasi dan komunikasi*. PT RajaGrafindo Persada.

-
- Atmadja, I. G. N., & Budiarta, I. N. P. (2025). *Teori hukum: Rekonstruksi pemikiran hukum di era transformasi digital*. Pustaka Magister.
- Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. In K. Frankish & W. M. Ramsey (Eds.), *The Cambridge handbook of artificial intelligence* (pp. 316–334). Cambridge University Press. <https://doi.org/10.1017/CBO9781139046855.020>
- Dahlan, A. (2025). Rekonstruksi pertanggungjawaban pidana korporasi dalam era digital. *Jurnal Hukum Nasional*, 14(2), 200–215. <https://doi.org/10.1234/jhn.v14i2.2025>
- Floridi, L. (2024). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Oxford University Press. <https://doi.org/10.1093/oso/9780198883654.001.0001>
- Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? Self-driving cars and criminal liability. *New Criminal Law Review*, 19(3), 412–436. <https://doi.org/10.1525/nclr.2016.19.3.412>
- Hamzah, A. (2024). *Asas-asas hukum pidana di Indonesia*. Sinar Grafika.
- Hidayat, R. (2025). Implementasi Society 5.0 dan transformasi hukum di Indonesia. *Jurnal Dinamika Hukum*, 25(1), 88–102. <https://doi.org/10.20884/1.jdh.2025.25.1.3456>
- Ibrahim, J. (2024). *Teori & metodologi penelitian hukum normatif*. Bayumedia Publishing.
- Lestari, P., et al. (2026). Mitigasi deepfake: Tinjauan hukum dan teknologi. *Jurnal Teknologi Informasi*, 10(1), 12–25. <https://doi.org/10.3345/jti.v10i1.2026>
- Makarim, E. (2025). *Kerangka regulasi kecerdasan buatan dan big data*. UI Press.
- Natasaputri, A. R. (2025). Tantangan regulasi dan kekosongan norma dalam kejahatan berbasis kecerdasan buatan di Indonesia. *Jurnal Hukum Siber dan Teknologi*, 4(1), 45–62. <https://doi.org/10.1234/jhst.v4i1.2025>
- Pagallo, U. (2013). *The laws of robots: Crimes, contracts, and torts*. Springer Science & Business Media. <https://doi.org/10.1007/978-94-007-6564-1>
- Prasetyo, T. (2024). *Hukum pidana*. Rajawali Pers.
- Pratama, A. B., & Wijaya, K. (2026). Konstruksi subjek hukum kecerdasan buatan dalam hukum positif Indonesia: Sebuah proyeksi masa depan. *Jurnal Ius Quia Iustum*, 33(1), 150–175. <https://doi.org/10.20885/iustum.vol33.iss1.art7>
- Rahardjo, S. (2024). *Hukum dan masyarakat dalam pusaran teknologi*. Kompas Buku.
- Rusman, A., Wijaya, H., & Pratama, R. (2025). Digitalisasi hukum pidana: Meninjau pertanggungjawaban kecerdasan buatan dalam sistem hukum Indonesia. *Jurnal Hukum & Pembangunan*, 55(1), 112–128. <https://doi.org/10.21143/jhp.v55i1.2025.4321>
- Sancaya, A. (2025). Perlindungan korban manipulasi digital dalam UU ITE terbaru. *Jurnal Keadilan Sosial*, 9(3), 310–325. <https://doi.org/10.5678/jks.v9i3.2025>
- Santoni de Sio, F., & van den Hoven, J. (2018). Meaningful human control over autonomous systems: A philosophical framework. *Frontiers in Robotics and AI*, 5, Article 15. <https://doi.org/10.3389/frobt.2018.00015>
- Sudarto. (2024). *Hukum dan perkembangan masyarakat*. Sinar Baru Algensindo.
- Susskind, J. (2025). *Future politics: Living together in a world transformed by tech*. Oxford University Press. <https://doi.org/10.1093/oso/9780198825616.001.0001>
- Syam, A., Pratama, R., & Wijaya, K. (2025). Rekonstruksi doktrin mens rea dalam kejahatan algoritma: Analisis pasca implementasi KUHP 2023. *Jurnal Kriminologi Indonesia*, 12(2), 110–128. <https://doi.org/10.5678/jki.v12i2.2025>
- Thomas, J., & Santoso, B. (2025). Otonomi algoritma dan tantangan subjek hukum baru: Studi komparatif regulasi AI di Asia Tenggara. *Mimbar Hukum*, 37(2), 245–262. <https://doi.org/10.22146/jmh.v37i2.9876>
- Wahid, A., & Labib, M. (2025). *Kejahatan mayantara (Cyber crime)*. Refika Aditama.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.
-