

**PERTANGGUNGJAWABAN PIDANA DALAM MALPRAKTIK ALGORITMA: ANALISIS YURIDIS
AUTENTIKASI BUKTI DIGITAL BERBASIS KECERDASAN BUATAN (ARTIFICIAL INTELLIGENCE)
MENURUT UU NO. 20 TAHUN 2025**

Noor Halina¹, Muhammad Nurcholis Alhadi²

Fakultas Hukum, Universitas Muhammadiyah Kalimantan Timur

Email: Nhlina2525@gmail.com

Abstract

The development of Artificial Intelligence technology has influenced various aspects of life, including the criminal justice system. The utilization of this technology in processing and generating digital information provides significant benefits to the evidentiary process; however, it also raises challenges regarding the authenticity and integrity of digital evidence. The emergence of technologies such as deepfakes and synthetic content further increases the risk of data manipulation, which may affect the validity of evidence presented in court proceedings. This study aims to analyze the regulation of authentication of Artificial Intelligence-based digital evidence in criminal proceedings, as well as the limits of criminal liability for algorithmic malpractice, under Law Number 20 of 2025 concerning the Indonesian Criminal Procedure Code. This study employs a normative legal research method with a statute approach and a conceptual approach. The results indicate that Law Number 20 of 2025 has recognized digital evidence as a lawful means of proof, although its validity must be supported by strict authentication mechanisms, including data integrity verification, digital forensic methods, and the chain of custody principle. Criminal liability for algorithmic malpractice cannot be imposed solely on the end-user, but must instead be traced to the developer corporation or system provider that retains control over the error or bias of the algorithm, with the Identification Theory and Vicarious Liability Theory serving as analytical instruments. Therefore, strengthening regulations and standardizing digital evidence authentication procedures are necessary to ensure legal certainty within the Indonesian criminal justice system.

Keywords: *digital evidence authentication, Artificial Intelligence, criminal evidence, chain of custody, digital forensics*

Abstrak

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*) telah memengaruhi berbagai aspek kehidupan, termasuk sistem peradilan pidana. Pemanfaatan teknologi tersebut dalam pengolahan dan pembentukan informasi digital memberikan manfaat bagi proses pembuktian, namun sekaligus menimbulkan tantangan terhadap keaslian dan integritas alat bukti digital. Kehadiran teknologi seperti *deepfake* dan konten sintetis semakin meningkatkan risiko manipulasi data yang dapat memengaruhi validitas alat bukti dalam persidangan. Penelitian

Article History

Received: Juli 2026

Reviewed: Juli 2026

Published: Juli 2026

Copyright : Author

Publish by : CAUSA



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

ini bertujuan untuk menganalisis pengaturan autentikasi alat bukti digital berbasis kecerdasan buatan dalam proses pembuktian perkara pidana serta batas pertanggungjawaban pidana atas malpraktik algoritma menurut Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa Undang-Undang Nomor 20 Tahun 2025 telah mengakomodasi alat bukti digital sebagai alat bukti yang sah, namun keabsahannya harus didukung melalui mekanisme autentikasi yang ketat, meliputi verifikasi integritas data, penggunaan metode forensik digital, serta penerapan prinsip *chain of custody*. Pertanggungjawaban pidana atas malpraktik algoritma tidak dapat dibebankan semata-mata kepada pengguna akhir, melainkan harus ditelusuri kepada korporasi pengembang atau penyedia sistem yang memiliki kendali atas kesalahan atau bias algoritma tersebut, dengan Teori Identifikasi dan Teori Pertanggungjawaban Pengganti sebagai instrumen analisis. Karena itu, diperlukan penguatan regulasi dan standarisasi prosedur autentikasi bukti digital untuk menjamin kepastian hukum dalam sistem peradilan pidana Indonesia.

Kata kunci: Autentikasi alat bukti digital, kecerdasan buatan, pembuktian pidana, *chain of custody*, forensik digital

PENDAHULUAN

Perkembangan teknologi kecerdasan buatan telah membawa perubahan mendasar dalam berbagai sektor kehidupan, tidak terkecuali sistem peradilan pidana. Kemampuan teknologi ini untuk mengolah data dalam jumlah besar, melakukan pengenalan pola, dan menghasilkan konten digital menjadikannya instrumen yang bernilai dalam mendukung proses pembuktian. Di sisi lain, kehadiran teknologi *deepfake* dan konten sintetis menimbulkan risiko baru terhadap keaslian dan integritas alat bukti digital, karena teknologi tersebut mampu menghasilkan rekaman suara, gambar, maupun video yang tampak nyata meskipun tidak merekam peristiwa yang sesungguhnya terjadi.¹

Persoalan ini menjadi semakin krusial ketika kecerdasan buatan tidak hanya berperan sebagai alat bantu, melainkan turut serta dalam memproduksi maupun memproses informasi yang kelak diajukan sebagai alat bukti di persidangan. Apabila algoritma yang digunakan mengandung cacat desain, bias data latih, atau kegagalan sistem (*algorithmic error*), maka keluaran yang dihasilkan berpotensi menyesatkan proses peradilan. Kondisi tersebut memunculkan dua persoalan hukum yang saling berkaitan, yakni bagaimana menguji keabsahan bukti digital yang dihasilkan atau diproses oleh kecerdasan buatan, dan kepada siapa pertanggungjawaban pidana dapat dibebankan apabila algoritma menghasilkan bukti yang keliru atau telah dimanipulasi.

Pembaruan hukum acara pidana melalui Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana menjadi relevan untuk dikaji karena pengakuan terhadap alat bukti elektronik tidak lagi dapat bertumpu pada bentuk bukti konvensional semata.² Perkembangan kejahatan digital serta pemanfaatan kecerdasan buatan menuntut hukum acara pidana memiliki mekanisme yang mampu menilai keabsahan bukti digital secara

¹ Robert Chesney & Danielle Keats Citron. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), hlm. 1753.

² Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana; Badan Pemeriksa Keuangan, "UU No. 20 Tahun 2025," peraturan.bpk.go.id.

lebih cermat, sekaligus menjawab kekosongan norma mengenai pertanggungjawaban pidana atas kegagalan sistem otonom.

Kajian-kajian terdahulu mengenai kecerdasan buatan dalam hukum pidana cenderung bersifat parsial, dengan menempatkan teknologi tersebut sebatas sebagai objek penyalahgunaan atau sekadar alat bantu pembuktian, tanpa mengkaji secara mendalam implikasi kesalahan algoritmik terhadap konstruksi pertanggungjawaban pidana maupun keabsahan alat bukti digital itu sendiri.³ Penelitian ini menawarkan kebaruan dengan memposisikan malpraktik algoritma sebagai isu yuridis yang menguji sekaligus batas pertanggungjawaban pidana dan standar autentikasi bukti digital dalam hukum acara pidana.

Berdasarkan uraian tersebut, penelitian ini dirumuskan untuk menjawab dua permasalahan pokok: pertama, bagaimana pengaturan autentikasi alat bukti digital berbasis kecerdasan buatan dalam proses pembuktian perkara pidana menurut Undang-Undang Nomor 20 Tahun 2025; kedua, bagaimana pertanggungjawaban pidana terhadap pihak yang terlibat dalam penggunaan atau pengembangan algoritma kecerdasan buatan yang menghasilkan bukti digital bermasalah dalam praktik peradilan pidana.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang dilakukan dengan menelaah bahan pustaka atau data sekunder yang terdiri atas peraturan perundang-undangan, literatur hukum, serta bahan hukum lain yang relevan dengan permasalahan yang dikaji. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), yang dilakukan dengan menelaah ketentuan hukum acara pidana terkait pembuktian, dan pendekatan konseptual (*conceptual approach*), yang digunakan untuk mengkaji konsep bukti digital, autentikasi, dan kecerdasan buatan dalam perspektif hukum pidana.

Bahan hukum primer dalam penelitian ini mencakup Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Bahan hukum sekunder berupa buku teks hukum pidana, jurnal ilmiah, dan hasil penelitian yang berkaitan dengan kecerdasan buatan, bukti digital, dan forensik digital, sedangkan bahan hukum tersier berupa kamus dan ensiklopedia hukum. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), yang kemudian diklasifikasikan dan dianalisis secara sistematis sesuai kebutuhan penelitian, dengan bertumpu pada Teori Integritas Bukti Digital (*Digital Evidence Integrity Theory*) sebagai kerangka analisis utama.

HASIL DAN PEMBAHASAN

Pengaturan Autentikasi Alat Bukti Digital Berbasis Kecerdasan Buatan dalam Proses Pembuktian Perkara Pidana Menurut Undang-Undang Nomor 20 Tahun 2025

Autentikasi alat bukti digital, termasuk yang bersinggungan dengan kecerdasan buatan, pada dasarnya merupakan proses dua tahap: pemeriksaan awal untuk memastikan bahwa bukti sesuai dengan klaim pihak yang mengajukannya, dan analisis lebih lanjut untuk menentukan nilai pembuktiannya (*probative value*) di persidangan.⁴ Guna memastikan mekanisme autentikasi berjalan sesuai standar, diperlukan pengujian ketat terhadap integritas data, yang umumnya dilakukan melalui perbandingan sidik jari digital (*digital fingerprint*) pada saat

³ Noor Halina. (2026). *Pertanggungjawaban Pidana Dalam Malpraktik Algoritma: Analisis Yuridis Autentikasi Bukti Digital Berbasis Kecerdasan Buatan (Artificial Intelligence) Menurut UU No. 20 Tahun 2025*. Universitas Muhammadiyah Kalimantan Timur, hlm. 10.

⁴ Nurlaila Isima. (2022). Kedudukan Alat Bukti Elektronik Dalam Pembuktian Perkara Pidana. *Gorontalo Law Review*, 5(1), hlm. 181.

pengumpulan dengan kondisi bukti pada saat pemeriksaan, menggunakan fungsi *hash* seperti *Message Digest 5* dan *Secure Hash Algorithm*.⁵

Tujuan dari autentikasi yang sah secara forensik adalah memastikan bahwa bukti tidak diubah atau disubstitusi sejak pertama kali dikumpulkan, sehingga dokumentasi menjadi komponen krusial yang mencatat karakteristik unik bukti serta kepemilikan dan kontrol yang berkelanjutan di sepanjang siklus hidupnya.⁶ Hal ini menjadi tantangan tersendiri ketika bukti diproses oleh kecerdasan buatan, sebab sifat data digital yang rapuh membuatnya dapat dimanipulasi tanpa meninggalkan jejak kerusakan yang kasat mata, sementara kehadiran teknologi *deepfake* dan konten sintetis memungkinkan pihak tidak bertanggung jawab merekayasa gambar, audio, dan video yang tampak autentik.⁷

Untuk mengatasi tantangan tersebut, analisis forensik digital tingkat lanjut diperlukan guna menentukan apakah suatu berkas digital telah dimanipulasi atau sepenuhnya dihasilkan oleh komputer (*computer-generated*), melalui evaluasi karakteristik kelas dan karakteristik individu dari bukti yang bersangkutan.⁸ Pelaku kejahatan siber juga kerap menggunakan metode anti-forensik seperti steganografi untuk menyembunyikan data sintetis atau komunikasi rahasia di dalam berkas media yang tampak tidak mencurigakan, sehingga pemeriksa forensik dituntut mampu mendeteksi penyisipan data tersembunyi semacam itu.⁹ Prosedur forensik digital yang sistematis, mencakup akuisisi, identifikasi, evaluasi, hingga penerimaan bukti di persidangan, menjadi krusial dalam kerangka pembaruan hukum acara pidana, mengingat data digital bersifat rapuh (*volatile*) dan menuntut metode pengamanan yang ketat.¹⁰

Guna menjamin keabsahan bukti digital di hadapan majelis hakim, prosedur yang dijalankan wajib berlandaskan Teori Integritas Bukti Digital, yang menuntut pembuktian bahwa bukti tidak mengalami perubahan sejak pertama kali dikumpulkan.¹¹ Standar integritas tersebut tidak akan tercapai tanpa penerapan prinsip *chain of custody*, yaitu proses memelihara dan mendokumentasikan sejarah kronologis penanganan bukti untuk membantah anggapan bahwa bukti telah dirusak selama berada dalam penguasaan aparat.¹² Dokumen rantai penitipan mencatat pihak yang menangani bukti, prosedur yang dilakukan, waktu pengumpulan dan analisis, serta lokasi penyimpanan bukti.¹³ Chain of custody yang terdokumentasi dengan baik memungkinkan bukti diajukan secara sah di pengadilan, sementara ketiadaannya membuka peluang bagi pihak lawan untuk mendalilkan bahwa bukti telah ditangani secara tidak patut, diubah, atau terkontaminasi di luar prosedur.¹⁴

Potensi kesalahan vonis (*miscarriage of justice*) dalam peradilan pidana sangat mungkin terjadi apabila penegak hukum, penasihat hukum, maupun hakim tidak menyadari secara utuh detail esoteris dari ilmu forensik komputer, terlebih di era teknologi manipulasi seperti kecerdasan buatan yang memungkinkan perubahan data tanpa sepengetahuan pemilik

⁵ Eoghan Casey. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press, hlm. 25; Anne Wade. (2019). *Digital Forensics and Investigation: From Data to Digital Evidence*. Syngress, hlm. 2.

⁶ Eoghan Casey. (2010). *Handbook of Digital Forensics and Investigation*. Academic Press, hlm. 16.

⁷ Robert Chesney & Danielle Keats Citron. (2019). *Op. Cit.*, hlm. 1753.

⁸ I Gede Adhi Suwarmas Kawiswara. (2026). Problematika dan Urgensi Hukum Kecerdasan Buatan Ditinjau dari Hukum di Indonesia. *Federalisme: Jurnal Kajian Hukum dan Ilmu Komunikasi*, 3(1), hlm. 48.

⁹ Dennis Fernando, Dini Dewi Heniarti, & Chepi Ali Firman Zakaria. (2025). Transformasi Alat Bukti Elektronik Menggunakan Digital Forensik dalam Pembaharuan Hukum Acara Pidana. *Journal Justiciabelen (JJ)*, 5(1), hlm. 66–67.

¹⁰ Lina Setio Rahayu, Siti Marwiyah, & Bachrul Amiq. (2026). Pertanggungjawaban Pidana Dalam Kejahatan Yang Melibatkan Artificial Intelligence Dalam Sistem Hukum Pidana Indonesia. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 5(3), hlm. 5744.

¹¹ Anne Wade. (2019). *Op. Cit.*, hlm. 26.

¹² Aris Munandar Ar, Wirda, Aditya Slamet Rusbandi, Muhammad Zulhendra, Saiful Bahri, & Danang Fajri. (2024). Peran Niat (*Mens rea*) dalam Pertanggungjawaban Pidana di Indonesia. *JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin*, 1(3), hlm. 244.

¹³ Ibid, hlm. 248.

¹⁴ Lina Setio Rahayu, Siti Marwiyah, & Bachrul Amiq. (2026). *Op. Cit.*, hlm. 5747–5748.

perangkat.¹⁵ Oleh karena itu, aparat penegak hukum dituntut meningkatkan ketelitian ilmiah (*scientific rigor*) dan secara berkala menguji keandalan perangkat, perangkat lunak, serta metode yang digunakan sebelum menjadikannya dasar pembuktian di pengadilan.¹⁶ Meskipun demikian, kesalahan atau kelalaian yang tidak disengaja dalam penanganan bukti digital tidak selalu secara otomatis membatalkan keabsahannya, sepanjang dapat dijelaskan melalui dokumentasi yang rinci, analisis forensik lanjutan, atau kesaksian jujur dari aparat yang bertugas; sebaliknya, upaya menyembunyikan kesalahan prosedural justru dapat menghancurkan kredibilitas penyidikan.¹⁷

Berdasarkan uraian tersebut, autentikasi alat bukti digital berbasis kecerdasan buatan perlu dilakukan melalui pemeriksaan berlapis: pemeriksaan sumber bukti, pemeriksaan teknis atas hash dan metadata, pemeriksaan algoritmik atas kemungkinan bias atau *synthetic generation*, serta pemeriksaan yuridis atas kesesuaian prosedur dengan hukum acara pidana. Dengan pemeriksaan berlapis tersebut, Undang-Undang Nomor 20 Tahun 2025 dapat memberikan kepastian hukum atas keabsahan bukti digital berbasis kecerdasan buatan, sepanjang didukung standarisasi teknis yang memadai dari aparat penegak hukum.

Pertanggungjawaban Pidana terhadap Pihak yang Terlibat dalam Penggunaan atau Pengembangan Algoritma Kecerdasan Buatan yang Menghasilkan Bukti Digital Bermasalah

Dalam hukum pidana, pertanggungjawaban senantiasa diukur melalui ajaran kesalahan atau niat kesadaran (*mens rea*), dengan pemikiran bahwa suatu perbuatan tidak serta-merta mengakibatkan seseorang bersalah kecuali pikirannya terbukti jahat secara hukum.¹⁸ Elemen tindak pidana secara fundamental mensyaratkan perbuatan yang melawan hukum (*actus reus*) sekaligus niat yang melawan hukum (*mens rea*), yang secara harfiah dimaknai sebagai pikiran yang bersalah dan memuat unsur kesengajaan maupun kecerobohan terhadap konsekuensi suatu tindakan, kecuali pada tindak pidana yang menganut asas tanggung jawab mutlak (*strict liability*).¹⁹

Dalam ranah teknologi yang melibatkan kecerdasan buatan, pembuktian *mens rea* menghadapi tantangan struktural akibat potensi kesalahan sistem (*algorithmic error*) yang timbul dari operasi otonom, bukan dari niat jahat manusia secara langsung. Untuk mengatasi celah ini, penegak hukum dapat menerapkan standar kecerobohan (*recklessness*), sehingga pihak yang mengambil risiko tidak dapat dibenarkan (*unjustifiable risk*) dalam merancang atau meluncurkan algoritma tetap dapat dimintai pertanggungjawaban pidana, sepanjang terbukti menyadari risiko tidak masuk akal (*unreasonable risk*) pada sistemnya.²⁰ Tantangan terbesarnya adalah mengurai lapisan sistem otonom untuk menemukan letak kesalahan yang relevan secara hukum, sebab berbeda dengan kejahatan konvensional, beban pembuktian kelalaian atau kesengajaan pengembang menjadi jauh lebih berat ketika kode program dieksekusi oleh mesin.²¹

Penentuan subjek hukum pidana menjadi kompleks karena melibatkan banyak aktor dalam satu siklus operasional, mencakup pengembang yang merancang algoritma, penyedia platform yang menyebarkan dan memelihara layanan, serta pengguna akhir yang memasukkan

¹⁵ Felicia Eugenia, Carla Joycelyne Limanto, & Dave David Tedjokusumo. (2024). Tantangan Praktis dalam Proses Pembuktian Perkara Pidana: Kredibilitas Saksi dan Validitas Bukti Elektronik. *IURIS STUDIA: Jurnal Kajian Hukum*, 5(2), hlm. 500–501.

¹⁶ Eoghan Casey. (2010). *Op. Cit.*, hlm. 21.

¹⁷ Dennis Fernando, Dini Dewi Heniarti, & Chepi Ali Firman Zakaria. (2025). *Op. Cit.*, hlm. 69.

¹⁸ Muh. Endriyo Susila. Malpraktik Medik dan Pertanggungjawaban Hukumnya: Analisis dan Evaluasi Konseptual, sebagaimana dikutip dalam Noor Halina. (2026). *Op. Cit.*, hlm. 13.

¹⁹ Dicky Eko Prasetyo. (2024). *Penerapan Artificial Intelligence dalam Penegakan Hukum*, hlm. 2.

²⁰ Melisa Yulianti, Gusriyanti Nabila, Aldo, Lilis Amelia, & Muh Raditya. (2025). Pemanfaatan Kecerdasan Buatan di Era Digital Analisis Dampak, Tantangan, dan Implikasinya terhadap Regulasi Hukum di Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik*, 3(2), hlm. 370–372.

²¹ Ekinia Karolin Sebayang, Mahmud Mulyadi, & Mohammad Ekaputra. (2024). Potensi Pemanfaatan Teknologi Artificial Intelligence Sebagai Produk Lembaga Peradilan Pidana di Indonesia. *Locus Journal of Academic Literature Review*, 3(4), hlm. 320–321.

perintah atau data.²² Kedudukan subjek hukum ini dapat dianalogikan dengan model tingkat layanan komputasi awan, di mana penyedia platform dan pengembang memiliki kendali penuh atas arsitektur dan keamanan sistem.²³ Apabila kesalahan sistem terjadi murni akibat cacat bawaan pada arsitektur algoritma yang tidak diuji sesuai standar kehati-hatian industri, pertanggungjawaban pidana dapat ditarik kepada korporasi pengembang atau penyedia platform. Sebaliknya, kedudukan pengguna sebagai subjek hukum pidana menjadi relevan apabila pengguna secara sadar mengeksploitasi fungsi kecerdasan buatan sebagai sarana untuk menciptakan, mengubah, atau menyembunyikan bukti digital, sehingga niat kesadaran dan perbuatan jahat sepenuhnya berada di pihaknya.²⁴ Penyedia platform sendiri tidak dapat secara otomatis dijerat pidana atas setiap bukti manipulatif yang dihasilkan sistemnya melalui instruksi pengguna, kecuali terbukti adanya kelalaian parah atau kesengajaan mengabaikan prosedur operasional keamanan.²⁵

Ketika sistem beroperasi secara otonom dan menghasilkan malpraktik tanpa instruksi langsung dari pengguna maupun pengembang, penentuan subjek hukum berdasarkan *mens rea* konvensional sering menemui jalan buntu, sehingga diperlukan kerangka teori yang mampu menarik garis pertanggungjawaban kepada entitas korporasi di balik sistem otonom tersebut.²⁶ Untuk mengatasi kebuntuan ini, hukum pidana dapat mengadopsi Teori Identifikasi (*Identification Theory*) dan Teori Pertanggungjawaban Pengganti (*Vicarious Liability*).²⁷ Berdasarkan Teori Identifikasi, kesalahan yang dilakukan oleh sistem kecerdasan buatan diposisikan sebagai perwujudan *mens rea* atau kelalaian yang melekat pada personel pengendali dalam struktur korporasi pengembangnya, sehingga apabila kerangka operasional agen kecerdasan buatan gagal mematuhi hukum akibat cacat desain, tindakan mesin tersebut diidentifikasi langsung sebagai tindakan korporasi itu sendiri.²⁸ Adapun Teori Pertanggungjawaban Pengganti menekankan tanggung jawab korporasi atas perbuatan sistem otonom yang berada di bawah kendalinya dan dilakukan dalam ruang lingkup operasionalnya, sehingga pengembang tetap dapat dimintai pertanggungjawaban pidana meskipun tidak memiliki niat jahat langsung, selama kegagalan sistem terjadi di dalam batas wewenang yang mereka rilis.²⁹

Kegagalan manusia dalam memantau operasi algoritma dapat dikategorikan sebagai pelanggaran terhadap standar kehati-hatian (*Duty of Care*). Apabila algoritma terbukti memanipulasi atau merusak bukti digital tanpa penjelasan yang dapat diverifikasi secara logis, hal tersebut merupakan pelanggaran mutlak terhadap standar kehati-hatian pengembang maupun operatornya, sehingga pemantauan berkelanjutan menjadi kewajiban esensial bagi administrator sistem.³⁰ Doktrin *Human-in-the-Loop* menjadi parameter penting untuk menentukan konstruksi pemidanaan, di mana manusia sebagai subjek hukum tidak dapat melepaskan tanggung jawabnya dengan berdalih bahwa mesin bertindak di luar kendali, karena kegagalan mengawasi sistem sudah cukup memenuhi unsur kelalaian dalam hukum pidana.³¹

Selain kedua teori tersebut, konsep tanggung jawab mutlak (*strict liability*) juga relevan untuk mengatasi kekosongan norma pada kejahatan teknologi tingkat tinggi, mengingat sifat global dan multi-yurisdiksi kejahatan siber menghadirkan tantangan besar bagi penegak hukum dalam melacak pelaku di balik sistem otonom.³² Ketika sistem algoritma memanipulasi bukti elektronik tanpa instruksi langsung manusia, pencarian pihak yang memiliki niat jahat di dalam

²² Dennis Fernando, Dini Dewi Heniarti, & Chepi Ali Firman Zakaria. (2025). *Op. Cit.*, hlm. 67.

²³ Gian. (2016), sebagaimana dikutip dalam Noor Halina. (2026). *Op. Cit.*, hlm. 62.

²⁴ Dennis Fernando, Dini Dewi Heniarti, & Chepi Ali Firman Zakaria. (2025). *Op. Cit.*, hlm. 67.

²⁵ Ibid.

²⁶ Lina Setio Rahayu, Siti Marwiyah, & Bachrul Amiq. (2026). *Op. Cit.*, hlm. 5748.

²⁷ Ibid, hlm. 5746.

²⁸ Ibid, hlm. 5747.

²⁹ Ibid, hlm. 5747–5748.

³⁰ Ibid, hlm. 5747.

³¹ Ibid, hlm. 5749.

³² Melisa Yulianti, Gusriyanti Nabila, Aldo, Lilis Amelia, & Muh Raditya. (2025). *Op. Cit.*, hlm. 370.

kode komputasi menjadi nyaris mustahil secara teknis, sehingga menciptakan kekosongan norma yang kerap dimanfaatkan pengembang untuk berlindung dari jerat hukum.³³ Karakteristik bukti digital yang rapuh dan rentan terhadap manipulasi yang sulit terdeteksi turut memperberat kesulitan tersebut, sehingga membebankan kewajiban pembuktian niat jahat manusia di balik modifikasi algoritma hanya akan membuat penegakan hukum berjalan di tempat, terutama ketika berhadapan dengan metode anti-forensik canggih.³⁴ Oleh karena itu, konsep *strict liability* perlu diintegrasikan secara khusus untuk membidik korporasi teknologi, pengembang, maupun penyedia layanan kecerdasan buatan, sehingga apabila suatu sistem menghasilkan bukti digital sintetik yang mencederai integritas peradilan, korporasi di baliknya dapat dimintai pertanggungjawaban pidana seketika tanpa perlu membuktikan niat jahat insinyurnya, sekaligus berfungsi sebagai instrumen preventif yang memaksa industri menerapkan standar kehati-hatian tertinggi dalam merancang algoritma.³⁵

PENUTUP

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa, pertama, proses autentikasi bukti digital berbasis kecerdasan buatan dalam persidangan menurut Undang-Undang Nomor 20 Tahun 2025 wajib memenuhi standar validitas formal dan materiil yang ketat melalui metode *digital forensics* yang tersertifikasi, dengan penekanan pada tiga aspek krusial: integritas data, rantai penjagaan bukti (*chain of custody*), dan keandalan sistem algoritma. Bukti digital yang diproduksi atau dianalisis oleh kecerdasan buatan hanya sah dan memiliki kekuatan pembuktian yang mengikat apabila terbukti bebas dari manipulasi, memiliki transparansi algoritma yang dapat diuji (*explainable AI*), dan diproses oleh ahli yang berkompeten sesuai regulasi yang berlaku.

Kedua, pertanggungjawaban pidana terhadap malpraktik algoritma tidak lagi dapat dibebankan semata-mata kepada pengguna akhir, melainkan harus ditekankan kepada korporasi pengembang, penyedia sistem, atau pihak yang memiliki kendali penuh atas kesalahan atau bias algoritma tersebut. Berdasarkan asas pertanggungjawaban pidana atas dasar kesalahan (*liability based on fault*), kesalahan dalam malpraktik algoritma dikategorikan sebagai bentuk kelalaian berat (*culpa lata*) atau kesengajaan terselubung apabila pengembang mengabaikan standar keamanan data dan mitigasi risiko, dengan pendekatan *Human-in-the-Loop* digunakan sebagai dasar untuk menghubungkan kesalahan sistem otonom dengan manusia atau korporasi yang mengendalikannya. Dengan demikian, subjek hukum yang bertanggung jawab adalah aktor manusia atau badan hukum yang memproduksi dan mengoperasikan sistem kecerdasan buatan, bukan teknologi itu sendiri.

Saran

Pertama, pemerintah dan pembentuk peraturan perundang-undangan perlu menyusun regulasi yang lebih komprehensif mengenai penggunaan kecerdasan buatan dalam sistem peradilan pidana, khususnya terkait standar autentikasi alat bukti digital dan mekanisme pertanggungjawaban hukum atas kesalahan algoritma. Kedua, aparat penegak hukum perlu meningkatkan kemampuan dan kompetensi di bidang forensik digital serta teknologi kecerdasan buatan agar mampu melakukan pemeriksaan, validasi, dan penilaian terhadap alat bukti digital secara tepat dan profesional. Ketiga, pengembang dan penyedia platform kecerdasan buatan perlu menerapkan prinsip kehati-hatian, transparansi, dan pengawasan yang memadai dalam proses pengembangan dan penggunaan sistem guna meminimalkan risiko kesalahan algoritma yang dapat menimbulkan permasalahan hukum. Keempat, penelitian lebih lanjut perlu

³³ Nurlaila Isima. (2022). *Op. Cit.*, hlm. 187.

³⁴ Ekinia Karolin Sebayang, Mahmud Mulyadi, & Mohammad Ekaputra. (2024). *Op. Cit.*, hlm. 320.

³⁵ Dennis Fernando, Dini Dewi Heniarti, & Chepi Ali Firman Zakaria. (2025). *Op. Cit.*, hlm. 67–68.

dilakukan untuk mengkaji perkembangan teknologi kecerdasan buatan yang semakin otonom serta implikasinya terhadap konsep pertanggungjawaban pidana dalam sistem hukum Indonesia.

DAFTAR PUSTAKA

Buku

- Cahyani, T. D. (2023). *Hukum Acara Pidana Indonesia (Dalam Teori dan Praktek)*. UMM Press.
- Casey, E. (2010). *Handbook of Digital Forensics and Investigation*. Academic Press.
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet* (3rd ed.). Academic Press.
- National Institute of Justice. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders* (2nd ed.). U.S. Department of Justice.
- Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
- Sari, O. N., Budiyo, Muntazar, A., Girsang, H., Kusumawardhani, D. L. L. H. N., & Amalia, M. (2024). *Pengantar Hukum Pidana: Teori, Prinsip, dan Implementasi*. PT. Green Pustaka Indonesia.
- Soekanto, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Edisi 1 Cetakan ke-15). PT RajaGrafindo Persada.
- Solikin, N. (2021). *Pengantar Metodologi Penelitian Hukum*. Qiara Media.
- Sulianta, F. (2025). *Algoritma & Pemrograman*. Elex Media Komputindo.
- von Solms, S. H., & Louwrens, C. P. (2006). The Relationship Between Digital Forensics, Corporate Governance, IT Governance and IS Governance. Dalam P. Kanellis, E. Kiountouzis, N. Kolokotronis, & D. Martakos (Eds.), *Digital Crime and Forensic Science in Cyberspace* (hlm. 250-262). Idea Group Inc.
- Wade, A. (2019). *Digital Forensics and Investigation: From Data to Digital Evidence*. Syngress.

Jurnal

- Antoro, H., Budhijanto, D., & Somawijaya. (2026). Admissibility of Artificial Intelligence as Electronic Evidence: Comparative Perspectives from Indonesia, The United States, and Japan. *Jurnal IUS Kajian Hukum dan Keadilan*, 14(1), 124-139.
- Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753-1820.
- Eugenia, F., Limanto, C. J., & Tedjokusumo, D. D. (2024). Tantangan Praktis dalam Proses Pembuktian Perkara Pidana: Kredibilitas Saksi dan Validitas Bukti Elektronik. *IURIS STUDIA: Jurnal Kajian Hukum*, 5(2), 492-503.
- Fernando, D., Heniarti, D. D., & Zakaria, C. A. F. (2025). Transformasi Alat Bukti Elektronik Menggunakan Digital Forensik dalam Pembaharuan Hukum Acara Pidana. *Journal Justiciabelen (JJ)*, 5(1), 60-74.
- Isima, N. (2022). Kedudukan Alat Bukti Elektronik dalam Pembuktian Perkara Pidana. *Gorontalo Law Review*, 5(1), 181-189.
- 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.
- Kroll, J. A., et al. (2017). Accountable Algorithms. *University of Pennsylvania Law Review*, 165, 633-705.
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, 3(2), 1-21.
- Munandar Ar, A., Wirda, Rusbandi, A. S., Zulhendra, M., Bahri, S., & Fajri, D. (2024). Peran Niat (Mens Rea) dalam Pertanggungjawaban Pidana di Indonesia. *JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin*, 1(3), 240-252.
- Rahayu, L. S., Marwiyah, S., & Amiq, B. (2026). Pertanggungjawaban Pidana Dalam Kejahatan Yang Melibatkan Artificial Intelligence Dalam Sistem Hukum Pidana Indonesia. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 5(3), 5740-5750.

- Sebayang, E. K., Mulyadi, M., & Ekaputra, M. (2024). Potensi Pemanfaatan Teknologi Artificial Intelligence Sebagai Produk Lembaga Peradilan Pidana di Indonesia. *Locus Journal of Academic Literature Review*, 3(4), 315-325.
- Yulianti, M., Nabila, G., Aldo, Amelia, L., & Raditya, M. (2025). Pemanfaatan Kecerdasan Buatan di Era Digital Analisis Dampak, Tantangan, dan Implikasinya terhadap Regulasi Hukum di Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik*, 3(2), 365-375.

Peraturan Perundang-undangan

- Republik Indonesia. Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.
- Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024.
- Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.