REKONSTRUKSI SYARAT *ADMISSIBILITY ALGORITHMIC EVIDENCE* BERBASIS *EXPLAINABLE AI* DALAM PEMBUKTIAN PIDANA INDONESIA

Oleh: **Dheni Anugerah Prasetya**
Universitas Negeri Semarang Jl. Raya Banaran, Sekaran, Kec. Gn. Pati, Kota Semarang, Jawa Tengah, 50229, Indonesia
email: dhenianugerah3@gmail.com

Informasi Artikel *Received*: 06-08-2026 **Accepted:** 25-08-2026

ABSTRAK

Kehadiran *algorithmic evidence* dalam pembuktian pidana menandai pergeseran besar dari bukti elektronik yang bersifat pasif menuju bukti yang lahir dari penalaran mesin. Namun, hukum pembuktian Indonesia masih memandang alat bukti elektronik sebatas medium penyimpanan atau transmisi data, tanpa menyediakan standar keabsahan materiil terhadap proses algoritmik yang menghasilkan suatu kesimpulan. Kekosongan ini berbahaya karena *black box AI* dapat melahirkan bukti yang tampak objektif, padahal menyimpan bias, ketidakjelasan logika, dan potensi kesalahan yang tidak mudah diuji oleh terdakwa maupun hakim. Penelitian ini bertujuan merekonstruksi syarat *admissibility algorithmic evidence* berbasis *Explainable Artificial Intelligence* (XAI) sebagai syarat minimum agar pembuktian pidana tetap tunduk pada *due process of law* dan *fair trial*. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan hukum. Hasil penelitian menunjukkan bahwa *algorithmic evidence* tidak layak diperlakukan sebagai alat bukti yang otomatis sah hanya karena berbentuk digital. Agar dapat diterima di persidangan, bukti tersebut harus memenuhi standar transparansi, auditabilitas, *traceability*, pengujian tingkat kesalahan, serta keterjelasan alasan algoritmik yang dapat diperdebatkan secara yuridis. Tanpa standar XAI, penggunaan AI dalam pembuktian pidana berisiko menggeser hakim dari penguji fakta menjadi penerima pasif hasil mesin. Karena itu, diperlukan rekonstruksi norma pembuktian pidana Indonesia yang menempatkan AI bukan sebagai penentu kebenaran, melainkan sebagai alat bantu yang harus dapat diaudit, diuji, dan dikendalikan oleh hukum.

Kata kunci : *algorithmic evidence, explainable AI,* pembuktian pidana, *fair trial, due process of law.*

ABSTRACT

The emergence of algorithmic evidence in criminal adjudication marks a major shift from passive electronic evidence to evidence generated through machine-based reasoning. However, Indonesian criminal procedure law still treats electronic evidence merely as a medium for storing or transmitting data, without establishing substantive admissibility standards for the algorithmic processes that produce such evidence. This legal gap is problematic because black box AI may generate evidence that appears objective while actually containing bias, opaque reasoning, and errors that are difficult for defendants and judges to examine. This study aims to reconstruct the admissibility requirements of algorithmic evidence based on Explainable Artificial Intelligence (XAI) as a minimum standard to ensure that criminal proof remains consistent with due process of law and fair trial principles. This study employs a normative legal research method using statutory, conceptual, and comparative approaches. The findings show that algorithmic evidence should not be treated as automatically valid merely because it is digital in form. To be admissible in court, such evidence must satisfy additional standards of transparency, auditability, traceability, error testing, and explainable algorithmic reasoning that can be legally challenged. Without XAI standards, the use of AI in criminal proof risks turning judges from fact assessors into passive recipients of machine-generated outputs. Therefore, a reconstruction of Indonesian criminal evidentiary norms is needed to position AI not as a determinant of truth, but as an assistive tool that must remain auditable, examinable, and subject to legal control.

Keywords: *algorithmic evidence, explainable AI, criminal proof, fair trial, due process of law.*

PENDAHULUAN

Kehadiran kecerdasan buatan (*artificial intelligence*/AI) dalam proses peradilan pidana telah bergeser dari sekadar alat bantu administratif menjadi entitas yang turut menghasilkan kesimpulan substantif yang dipakai sebagai dasar putusan skor kecocokan wajah, indeks risiko residivisme, hasil interpretasi campuran DNA berbasis probabilitas genotipe. Uni Eropa, melalui *Regulation (EU) 2024/1689* tentang *Artificial Intelligence Act*, secara tegas mengklasifikasikan sistem AI yang digunakan dalam *law enforcement* dan *administration of justice* sebagai kategori *high-risk* yang tunduk pada kewajiban kepatuhan ketat, sebuah pengakuan tegas bahwa kesimpulan algoritmik membawa risiko yang berbeda dari bukti konvensional (European Parliament, 2024). Di Indonesia, momentum ini berpadu dengan babak baru hukum acara pidana: Undang-Undang Nomor 20 Tahun 2025 tentang Hukum Acara Pidana, disahkan DPR RI pada 18 November 2025, mengubah sistem pembuktian dari tertutup (lima jenis alat bukti menurut Pasal 184 ayat (1) KUHAP lama) menjadi terbuka (delapan kategori dengan klausul residual pada Pasal 235 ayat (1) huruf h)(Undang-Undang Nomor 20 Tahun

2025 Tentang Hukum Acara Pidana, 2025). Pergeseran ini menyelesaikan pertanyaan formal mengenai dapat-tidaknya suatu bentuk bukti diajukan di persidangan, tetapi sama sekali tidak menjawab pertanyaan substantif tentang bagaimana kesimpulan yang dihasilkan melalui proses komputasional seharusnya diuji kekuatan pembuktiannya dan justru pada titik pertemuan inilah *algorithmic evidence* muncul sebagai persoalan hukum baru yang mendesak (Kawamleh, 2025).

Kajian internasional memperlihatkan kesamaan sekaligus perbedaan penting dalam merespons persoalan ini. Garrett dan Rudin mencatat proliferasi model *black box* dalam interpretasi bukti forensik (García-Magariño et al., 2025) dan mengusulkan agar hukum pembuktian mengakui "*a right to a glass box*" preferensi hukum terhadap model AI yang *interpretable* dibanding model tertutup, sebuah pendekatan yang menitikberatkan pada desain sistem itu sendiri sebagai solusi (Garrett & Rudin, 2024). Nugraha, Kristanto, dan Siagian menekankan sisi yang berbeda: perbedaan sistem hukum antarnegara menghasilkan absennya standar *admissibility* yang seragam bagi bukti berbasis AI, sebuah persoalan pada tataran regulasi lintas yurisdiksi, bukan semata desain teknis (Satriya Nugraha et al., 2026). (Allen et al., 2025) mengambil sudut yang lebih fundamental, mengkritik kecenderungan pengadilan mengasimilasi keluaran algoritmik ke kategori pembuktian yang sudah mapan tanpa menguji ulang premis rasionalitas di baliknya. Ketegangan ini mengkristal dalam putusan Mahkamah Agung Wisconsin, (Frank, 2017), yang menguatkan penggunaan skor risiko algoritmik COMPAS dalam penjatuhan pidana meski terdakwa tidak diberi akses menguji metodologi algoritma yang berstatus rahasia dagang. Ketiga kajian tersebut berbeda penekanan desain sistem, harmonisasi regulasi, dan rasionalitas epistemik namun bertemu pada satu simpulan yang sama: pengadilan di berbagai yurisdiksi memperlakukan keluaran algoritmik sebagai perpanjangan bukti yang sudah dikenal, tanpa mempertanyakan apakah justifikasi doktrinal di balik kategori-kategori lama benar-benar berlaku bagi artefak komputasional yang penalarannya kerap tidak dapat diperiksa oleh siapa pun, termasuk perancangnya sendiri (Khadijah, 2025).

Literatur hukum Indonesia mengenai bukti elektronik berkembang pesat sejak berlakunya UU ITE, tetapi sejauh penelusuran pustaka yang dilakukan dalam penelitian ini, perhatian tersebut secara dominan tertuju pada autentikasi dan keabsahan prosedural bukti elektronik yang bersifat pasif rantai penyimpanan rekaman CCTV, integritas nilai *hash* dokumen elektronik sebagaimana tampak dalam kajian (Yuli Anggraini, 2024) atas pembuktian elektronik dalam sistem peradilan pidana Indonesia. Kajian yang lebih baru dan secara eksplisit membahas AI sebagai alat bukti, seperti kajian (Safriansyah Yanwar Rosyadi & Zainal Arifin Hoesein, 2025) serta kajian Al Mahdi, Ridwan, dan Ali keduanya membahas pemanfaatan hasil analisis AI sebagai alat bukti dalam penegakan hukum pidana pertambangan tetap memperlakukan validitas hasil analisis AI sebagai persoalan pemenuhan syarat formal alat bukti elektronik pada umumnya, tanpa mempertanyakan apakah kategori "alat bukti elektronik" itu sendiri memadai untuk menampung kesimpulan yang lahir dari proses komputasional. Kajian yang menyinggung AI dalam konteks pidana pun umumnya berhenti pada persoalan pertanggungjawaban pidana atas kejahatan berbasis AI, sebagaimana tampak dalam

kajian Aditya dan Yusuf mengenai manipulasi bukti digital berbasis *deepfake* dalam sistem pembuktian terbuka KUHAP Baru, yang menyoroti kekosongan regulasi audit forensik digital namun belum masuk ke pertanyaan bagaimana keluaran AI itu sendiri seharusnya diklasifikasikan (Aditya & Yusuf, 2026). Tidak satu pun dari kajian-kajian tersebut baik yang membahas autentikasi bukti elektronik, kredibilitas bukti elektronik secara umum, maupun AI sebagai alat bukti secara spesifik secara tegas menjawab pertanyaan yang lebih mendasar: berkedudukan sebagai apa suatu kesimpulan algoritmik, semisal skor kecocokan wajah 96 persen, dalam sistem pembuktian pidana Indonesia? Petunjukkah ia, keterangan ahlikah, ataukah sekadar bukti elektronik? Kekosongan konseptual inilah yang belum diisi baik oleh KUHAP lama, KUHAP Baru, maupun literatur hukum Indonesia yang ada termasuk literatur yang secara spesifik membahas AI sekalipun.

Kesenjangan inilah yang hendak diisi penelitian ini. Novelti penelitian ini dibangun pada tiga tingkatan: secara konseptual, penelitian ini memperkenalkan *algorithmic evidence* sebagai bukti elektronik generasi kedua (*second generation electronic evidence* kategori yang berbeda secara kualitatif dari bukti elektronik konvensional karena lahir dari proses penalaran, bukan sekadar perekaman atau transmisi; secara teoretis, penelitian ini membedakan secara tegas antara *electronic evidence*, *digital evidence*, *scientific evidence*, dan *algorithmic evidence*, serta menempatkan pembahasan *admissibility* di atas fondasi teori kebenaran materiil dan epistemologi pembuktian; dan secara normatif, penelitian ini merekonstruksi syarat *admissibility algorithmic evidence* dengan menempatkan *explainability* bukan sekadar sebagai kriteria teknis, melainkan sebagai asas hukum pembuktian elektronik yang baru. Kontribusi keilmuan artikel ini karena itu bukan sekadar mengusulkan penerapan *Explainable AI*, melainkan mengonseptualisasikan ulang kedudukan *algorithmic evidence* dalam hukum pembuktian pidana Indonesia sebelum sampai pada pertanyaan bagaimana ia diuji. Bertolak dari uraian di atas, penelitian ini bertujuan menjawab: (1) bagaimana kedudukan *algorithmic evidence* dalam sistem pembuktian pidana Indonesia; (2) mengapa rezim alat bukti elektronik yang berlaku saat ini termasuk sistem pembuktian terbuka dalam KUHAP Baru belum mampu menguji validitas *algorithmic evidence*; dan (3) bagaimana syarat *admissibility algorithmic evidence* seharusnya direkonstruksi berdasarkan prinsip *Explainable AI* untuk menjamin *due process of law* dan *fair trial*

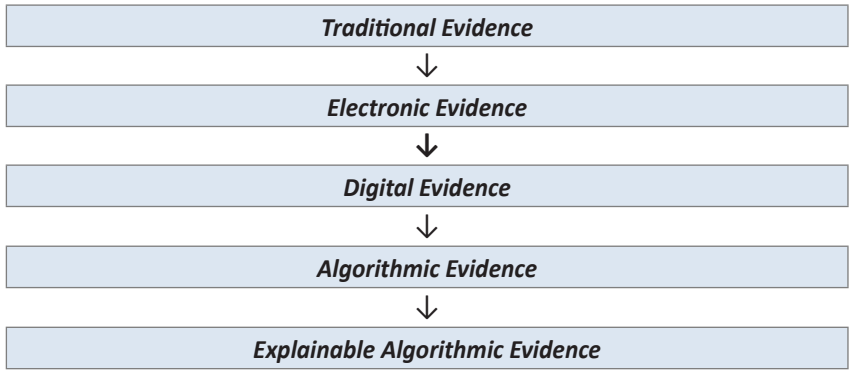
METODE

Penelitian ini merupakan penelitian hukum normatif yang menggabungkan pendekatan perundang-undangan (*statutory approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan hukum (*comparative approach*). Pendekatan perundang-undangan digunakan untuk menganalisis Undang-Undang Nomor 8 Tahun 1981, Undang-Undang Nomor 20 Tahun 2025, dan Undang-Undang Informasi dan Transaksi Elektronik; pendekatan konseptual digunakan untuk merumuskan kedudukan *algorithmic evidence* sebagai kategori pembuktian yang berbeda dari *electronic evidence*, *digital evidence*, dan *scientific evidence*; dan pendekatan perbandingan hukum digunakan untuk menelaah kerangka pengaturan AI

dalam sistem hukum Uni Eropa, Dewan Eropa, serta yurisdiksi lain yang relevan. Bahan hukum yang digunakan mencakup bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, bahan hukum sekunder berupa artikel jurnal dan hasil penelitian sebelumnya, serta bahan hukum tersier berupa kamus dan ensiklopedia hukum. Seluruh bahan hukum tersebut dianalisis secara kualitatif melalui teknik interpretasi gramatikal, sistematis, dan teleologis untuk merumuskan rekonstruksi syarat *admissibility* yang koheren dan dapat dipertanggungjawabkan secara akademik.

HASIL DAN PEMBAHASAN

Bagan 1. ***Evolution of Evidence Paradigm***



Sebelum syarat *admissibility* dapat direkonstruksi, pertanyaan yang lebih mendasar harus dijawab lebih dahulu: apa sesungguhnya *algorithmic evidence* itu? Penelitian ini mendefinisikannya sebagai kesimpulan probatoir yang dihasilkan melalui proses inferensi komputasional atas data, yang nilai pembuktiannya bergantung pada validitas proses inferensi tersebut, bukan sekadar pada keutuhan data yang menjadi masukannya. Definisi ini membawa empat karakteristik yang membedakannya dari bukti pada umumnya: sifat generatif (menghasilkan proposisi baru, bukan merekam fakta yang sudah ada); sifat probabilistik (keluarannya berupa angka kemungkinan, bukan pernyataan biner); opasitas penalaran (proses yang menghasilkannya sering tidak dapat ditelusuri, bahkan oleh perancangnya sendiri, sebagaimana dicatat Garrett dan Rudin atas proliferasi model *black box* dalam forensik algoritmik) (Garrett & Rudin, 2023); dan otoritas yang didelegasikan (pihak yang menyajikannya di persidangan umumnya bukan pihak yang melakukan penalaran itu sendiri).

Karakteristik terakhir inilah yang menciptakan persoalan akuntabilitas epistemik yang membedakan *algorithmic evidence* dari *electronic evidence* maupun *digital evidence* dua istilah yang kerap dipakai bergantian dalam UU ITE tanpa pembedaan tegas (Undang Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2024). Perdebatan terminologis antara "elektronik" dan "digital" bukan yang terpenting; yang luput dari keduanya adalah pembedaan antara bukti pasif dan bukti generatif. Rekaman CCTV, log percakapan, dan surel adalah bukti pasif: kontennya berasal dari peristiwa nyata, dan medium elektronik hanya menyimpan

atau mentransmisikannya, sehingga pengujian keabsahannya berpusat pada integritas penyimpanan. *Algorithmic evidence* berbeda secara kualitatif kontennya tidak eksis sebelum sistem menghitungnya, sehingga yang perlu diuji bukan keutuhan rekaman, melainkan validitas proses yang menghasilkannya.

Algorithmic evidence juga tidak otomatis setara *scientific evidence* seperti pencocokan sidik jari atau profil DNA, sekalipun keduanya sama-sama melibatkan inferensi. Bukti ilmiah konvensional bertumpu pada empat prasyarat yang menopang otoritasnya: metodologi yang telah melalui tinjauan sejawat, seorang ahli manusia yang bersaksi di bawah sumpah atas pengetahuannya sendiri sebagaimana disyaratkan Pasal 1 angka 28 jo. Pasal 186 KUHAP lama atau Pasal 238 ayat (1) UU Nomor 20 Tahun 2025 (Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana, 1981) (Undang-Undang Nomor 20 Tahun 2025 Tentang Hukum Acara Pidana, 2025), keterujian oleh ahli independen, dan pengetahuan tentang tingkat kesalahan metodologi. *Algorithmic evidence* berbasis pembelajaran mesin kerap tidak memenuhi satu pun prasyarat itu: metodologinya dilindungi sebagai rahasia dagang sebagaimana dalam (Frank, 2017), saksi yang menyajikannya tidak melakukan penalaran itu sendiri, dan tingkat kesalahannya sering tidak diketahui publik atau bervariasi tajam antarkelompok populasi Buolamwini dan Gebru menunjukkan disparitas tingkat kesalahan hingga 34,7 persen untuk perempuan berkulit gelap dibandingkan 0,8 persen untuk laki-laki berkulit terang pada sejumlah sistem klasifikasi wajah komersial (Buolamwini & Gebru, 2018). Persoalannya bukan bahwa *algorithmic evidence* pasti tidak dapat dipercaya, melainkan bahwa ia sering memperoleh kewibawaan bukti ilmiah tanpa diwajibkan memenuhi syarat yang menjadi alasan bukti ilmiah itu dipercaya.

Interpretasi campuran DNA melalui perangkat lunak probabilistik, sebagaimana dikaji Garrett dan Rudin, menghadirkan variasi lain dari persoalan yang sama: alih-alih membandingkan pola visual secara langsung seperti sidik jari konvensional, perangkat lunak ini menghitung *likelihood ratio* melalui model statistis yang kompleks dan sering bersifat *proprietary*, sehingga pemilihan model dan asumsi di dalamnya yang dapat memengaruhi hasil secara signifikan tidak dapat diperiksa baik oleh pengadilan maupun ahli yang ditunjuk terdakwa. Contoh ini menegaskan bahwa persoalan *algorithmic evidence* berulang di berbagai ranah forensik, termasuk yang secara tradisional dianggap paling "ilmiah" sekalipun.

Kerangka ini memungkinkan jawaban tegas atas pertanyaan yang diajukan pada bagian Pendahuluan. Skor kecocokan wajah 96 persen bukan petunjuk dalam pengertian Pasal 188 KUHAP, karena ayat (2) pasal tersebut membatasi sumber petunjuk secara limitatif hanya pada keterangan saksi, surat, dan keterangan terdakwa algoritma bukan salah satu dari ketiganya (Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana, 1981). Ia juga bukan keterangan ahli dalam pengertian penuh, sebab keterangan ahli mensyaratkan pengetahuan yang dimiliki ahli itu sendiri, diberikan di bawah sumpah atas nama pengetahuannya sendiri bukan sekadar meneruskan keluaran sistem yang penalarannya tidak ia kuasai. Kesulitan yang sama muncul pada skor risiko COMPAS dalam *Loomis*: hakim yang menerimanya tidak berhadapan dengan

seorang ahli yang dapat ditanya "mengapa 96 persen, bukan 90 atau 99," karena tidak ada manusia yang benar-benar memiliki jawaban itu. Yang tersisa hanyalah kategori bukti elektronik dan di sinilah masalahnya paling telanjang: kategori itu, baik dalam UU ITE maupun Pasal 235 ayat (1) huruf f UU Nomor 20 Tahun 2025, hanya mensyaratkan keabsahan cara memperoleh dan keutuhan bentuk elektroniknya, tanpa satu pun syarat yang menyentuh validitas penalaran yang menghasilkan angka tersebut.

Keberatan yang mungkin diajukan adalah bahwa persoalan ini cukup diselesaikan dengan memperluas cakupan keterangan ahli, sehingga analis yang mengoperasikan sistem algoritmik dianggap "ahli" dalam pengertian luas. Keberatan ini keliru: keterangan ahli mensyaratkan kapasitas menjelaskan dan mempertanggungjawabkan penalaran sendiri di bawah pemeriksaan silang, bukan sekadar status formal. Seorang analis dapat menjelaskan cara kerja umum suatu sistem, tetapi tidak mengapa parameter tertentu menghasilkan skor 96 dan bukan 94 persen untuk kasus spesifiknya penjelasan itu, jika ada, hanya dapat diberikan sistem itu sendiri, dan sistem bukan subjek yang dapat disumpah. Memperluas kategori keterangan ahli bukan solusi, melainkan pengaburan lebih lanjut atas kekosongan kategori pembuktian yang secara khusus dirancang menguji penalaran nonmanusia.

Simpulannya bersifat konseptual: *algorithmic evidence* adalah bukti elektronik generasi kedua. Bukti elektronik generasi pertama memerlukan hukum pembuktian yang menjaga integritas penyimpanan; bukti elektronik generasi kedua memerlukan hukum pembuktian yang menguji validitas penalaran. Pencampuradukan keduanya di bawah satu label "bukti elektronik" adalah akar dari kekosongan hukum yang menjadi fokus artikel ini, dan konseptualisasi inilah yang membedakan penelitian ini dari kajian-kajian sebelumnya yang memperlakukan seluruh persoalan AI dalam pembuktian pidana semata sebagai persoalan penerapan *Explainable AI* (Yeo et al., 2025).

Pembedaan antara bukti pasif dan bukti generatif ini bukan sekadar latihan konseptual tanpa konsekuensi praktis (Darizta et al., 2023). (Sebayang et al., 2024), dalam salah satu kajian paling awal mengenai hubungan *artificial intelligence* dan hukum pembuktian, menunjukkan bahwa hukum pembuktian konvensional dibangun di atas asumsi bahwa setiap alat bukti dapat ditelusuri kembali ke sumber pengetahuan manusia tertentu persepsi seorang saksi, keahlian seorang ahli, atau catatan seorang pencatat dokumen (Seng, 2025). *Algorithmic evidence* meruntuhkan asumsi ini: sumber pengetahuan di baliknya bukan manusia tertentu, melainkan pola statistis yang diekstraksi dari kumpulan data berskala besar, yang tidak dapat direduksi menjadi pengalaman atau keahlian satu orang yang dapat disumpah dan diperiksa silang. Implikasinya, setiap upaya memaksakan *algorithmic evidence* ke dalam kategori pembuktian yang mengasumsikan sumber pengetahuan personal petunjuk, keterangan ahli akan selalu berakhir pada fiksi hukum: seolah-olah ada seseorang yang "mengetahui" sesuatu yang sesungguhnya tidak diketahui siapa pun secara utuh selain sebagai keluaran agregat suatu sistem.

Pemilihan istilah *algorithmic evidence*, alih-alih *AI evidence* atau *computational evidence* yang mungkin tampak sama relevannya, dilakukan secara sengaja. Istilah *AI*

evidence berisiko membatasi cakupan konsep ini hanya pada sistem yang secara populer diasosiasikan dengan "kecerdasan buatan" generasi terbaru, padahal persoalan validitas penalaran komputasional yang dibahas artikel ini juga relevan bagi sistem statistis yang lebih sederhana namun tetap opak, seperti model skor risiko berbasis regresi logistik yang telah digunakan sejak sebelum istilah AI populer digunakan secara luas. Istilah *computational evidence*, sebaliknya, terlalu luas karena berpotensi mencakup pula perhitungan matematis sederhana yang sepenuhnya deterministik dan dapat diverifikasi ulang secara manual tanpa kesulitan berarti situasi yang berbeda secara mendasar dari persoalan opasitas yang menjadi fokus artikel ini. Istilah *algorithmic evidence* dipilih karena secara tepat menangkap ciri yang relevan: bukti yang dihasilkan melalui suatu algoritma, yakni serangkaian langkah komputasional yang menghasilkan kesimpulan dari data masukan, terlepas dari apakah algoritma tersebut disebut "AI" secara populer atau tidak.

Tabel 1. ***Comparison Between Electronic Evidence and Algorithmic Evidence***

Aspek	*Electronic Evidence*	*Algorithmic Evidence*
Sumber informasi	Peristiwa atau tindakan manusia yang direkam	Proses inferensi komputasional atas data
Karakteristik	Pasif (menyimpan/mentransmisikan)	Generatif (menghasilkan proposisi baru)
Bentuk keluaran	Rekaman, dokumen, pesan (bersifat faktual)	Skor, klasifikasi, probabilitas
Metode pengujian	Integritas penyimpanan, keaslian bentuk	Validitas proses penalaran
Objek verifikasi	Rantai penyimpanan (*chain of custody*)	Rantai penalaran algoritmik (*chain of algorithmic custody*)
Tingkat transparansi	Tinggi - konten dapat diperiksa langsung	Rendah - sering bersifat *black box*
Tingkat kesalahan	Terutama risiko manipulasi/ pemalsuan	Risiko bias, kesalahan model, disparitas antarkelompok
Peran manusia	Perekam/pengirim pasif	Otoritas penalaran yang didelegasikan ke sistem

Ketidakmampuan rezim pembuktian elektronik Indonesia menguji *algorithmic evidence* bukan sekadar kelalaian legislatif, melainkan konsekuensi logis dari sejarah pembentukannya. KUHAP lama tidak pernah dirancang untuk mengakomodasi bukti elektronik sama sekali kelima jenis alat bukti dalam Pasal 184 ayat (1) disusun tahun 1981, jauh sebelum internet menjadi bagian kehidupan hukum. Ketika UU ITE kemudian memperluas alat bukti yang sah menjadi mencakup informasi dan dokumen elektronik, perluasan itu dilakukan sebagai *lex specialis* yang ditempelkan pada sistem lama, bukan sebagai reformulasi menyeluruh atas teori pembuktian itu sendiri (Undang Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2024). Konsekuensinya tampak jelas dalam Putusan Mahkamah Konstitusi Nomor 20/ PUU-XIV/2016: Mahkamah menegaskan bahwa informasi atau dokumen elektronik, khususnya hasil penyadapan atau perekaman, hanya sah sebagai alat bukti apabila

diperoleh dalam rangka penegakan hukum dan atas permintaan aparat penegak hukum yang berwenang (Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016, 2016). Putusan ini penting, tetapi ia hanya menjawab pertanyaan tentang siapa yang berwenang memperoleh bukti elektronik persoalan otorisasi dan legalitas akuisisi dan sama sekali tidak menyentuh pertanyaan tentang bagaimana menilai validitas kesimpulan yang dihasilkan suatu proses komputasional. Bahkan yurisprudensi konstitusional paling penting mengenai bukti elektronik di Indonesia tetap berkutat pada persoalan generasi pertama. Kajian-kajian lain mengenai bukti elektronik pun bergerak pada sumbu yang sama: (Yuli Anggraini, 2024) mengkaji kekuatan hukum dan kredibilitas alat bukti elektronik dalam pembuktian pidana, sementara (Yuyun Sri Wahyuni, 2021) mengkaji kepastian hukum alat bukti elektronik dalam perspektif hukum acara pidana baru keduanya membahas bukti elektronik sebagai kategori tunggal yang kredibilitasnya diuji melalui parameter keutuhan dan keaslian, tanpa membedakan antara bukti yang pasif dan bukti yang generatif sebagaimana diusulkan bagian sebelumnya.

KUHAP Baru memperbaiki sebagian persoalan formal ini dengan mengadopsi sistem pembuktian terbuka, tetapi memperbaiki bentuk bukan berarti memperbaiki substansi. (Maharani & Wulandari, 2025), dalam kajiannya atas ketiadaan *exclusionary rules* eksplisit dalam RUU KUHAP, menemukan bahwa penerapan prinsip pengecualian bukti yang diperoleh secara melawan hukum di Indonesia masih sporadis, mekanisme praperadilan belum mampu melakukan uji substantif, dan enam elemen *due process* belum diatur secara eksplisit. Jika mekanisme kontrol yang sudah lama dikenal praperadilan, *exclusionary rules* saja belum mampu menjalankan fungsi ujinya secara memadai untuk bukti konvensional, tidak ada alasan untuk berasumsi bahwa mekanisme yang sama akan mampu menguji sesuatu yang jauh lebih kompleks secara epistemik seperti *algorithmic evidence*. Kekosongan ini berpotensi diperparah oleh pola umum implementasi undang-undang di Indonesia, di mana ketentuan pokok dalam undang-undang induk kerap memerlukan peraturan pelaksana yang baru terbit bertahun-tahun setelah undang-undang itu sendiri berlaku. Apabila pola ini terulang pada KUHAP Baru, ada risiko nyata bahwa Pasal 235 ayat (1) huruf f dan h akan diterapkan di lapangan tanpa pedoman teknis yang memadai selama masa transisi tersebut, sehingga hakim-hakim di berbagai pengadilan negeri akan mengembangkan penafsiran masing-masing atas *admissibility algorithmic evidence* secara independen satu sama lain persis skenario inkonsistensi yang coba dicegah artikel ini.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi turut menyinggung pemrosesan data secara otomatis dan hak subjek data untuk memperoleh penjelasan atas keputusan yang dihasilkan semata-mata melalui pemrosesan otomatis. Namun demikian, rezim ini berorientasi pada perlindungan data pribadi dalam pengertian administratif-preventif mencegah penyalahgunaan data sebelum terjadi bukan pada standar pembuktian pidana yang berlaku ketika keluaran suatu sistem otomatis hendak dijadikan dasar keyakinan hakim di ruang sidang. Hak atas penjelasan dalam UU PDP adalah hak administratif terhadap pengendali data; ia tidak dengan sendirinya menjadi syarat *admissibility* dalam hukum acara pidana. Kekosongan normatif ini juga bersinggungan dengan Pasal 28D ayat (1) UUD 1945

yang menjamin kepastian hukum yang adil bagi setiap warga negara. Tanpa standar *admissibility* yang jelas bagi *algorithmic evidence*, penerapannya di persidangan akan bergantung sepenuhnya pada penilaian kasuistis hakim tanpa tolok ukur normatif yang seragam situasi yang berpotensi bertentangan dengan cita kepastian hukum itu sendiri, sebab dua terdakwa dengan *algorithmic evidence* yang secara teknis setara dapat diperlakukan berbeda semata bergantung pada bagaimana hakim yang menyidangkan perkaranya memandang kredibilitas teknologi tersebut.

Prinsip praduga tak bersalah turut berada dalam risiko yang sama. Prinsip ini mengharuskan beban pembuktian tetap berada di pundak penuntut umum dan menuntut agar setiap keraguan diinterpretasikan demi keuntungan terdakwa. Ketika suatu kesimpulan algoritmik disajikan dengan tampilan angka presisi tinggi kecocokan wajah 96 persen, skor risiko 0,74 tampilan presisi tersebut dapat menimbulkan efek psikologis yang secara diam-diam menggeser beban pembuktian itu: alih-alih penuntut umum harus meyakinkan hakim melampaui keraguan yang wajar, terdakwalah yang justru harus membuktikan bahwa mesin keliru, padahal metodologi mesin itu sendiri tidak transparan baginya. Kekosongan ini juga tidak dapat diisi oleh doktrin keterangan ahli yang ada: ketika seorang penyidik atau ahli IT menyajikan hasil analisis algoritmik di persidangan, sumpah yang diucapkannya menjangkau kejujurannya dalam menyampaikan apa yang ia ketahui tetapi ia tidak "mengetahui," dalam pengertian yang disyaratkan hukum pembuktian, mengapa algoritma menghasilkan kesimpulan tertentu. Inilah krisis yang sesungguhnya: bukan ketiadaan aturan tentang bukti elektronik, melainkan ketiadaan teori pembuktian yang mampu menampung bukti yang lahir dari penalaran nonmanusia.

Persoalan ini diperparah oleh kesenjangan kapasitas teknis di kalangan aparat penegak hukum sendiri. Hakim, jaksa, dan sebagian besar penasihat hukum di Indonesia umumnya tidak memiliki latar belakang pendidikan ilmu komputer atau statistika yang memadai untuk menilai secara independen apakah suatu klaim algoritmik masuk akal secara teknis. Ironisnya, Indonesia sesungguhnya telah memiliki preseden kelembagaan untuk mengatasi kesenjangan semacam ini pada ranah forensik digital konvensional: Pusat Laboratorium Forensik (Puslabfor) Bareskrim Polri telah terakreditasi ISO/IEC 17025 sejak 2014, dan Lembaga Sertifikasi Profesi Polri secara rutin menyelenggarakan sertifikasi kompetensi bagi pemeriksa forensik yang akan tampil sebagai ahli di persidangan (ISO/IEC, 2012, 2015). Infrastruktur ini menunjukkan bahwa model sertifikasi independen bukan hal asing bagi sistem peradilan Indonesia. Yang absen bukan kemampuan kelembagaan untuk membangunnya, melainkan kesadaran bahwa *algorithmic evidence* memerlukan perluasan model akreditasi yang sama ke ranah validitas penalaran algoritmik, bukan sekadar keutuhan data sebagaimana selama ini menjadi fokus akreditasi laboratorium forensik digital.

Lima kerangka internasional memberikan titik pijak yang berbeda-beda untuk merekonstruksi *admissibility algorithmic evidence*, dan perbedaan penekanan di antaranya justru mengungkap elemen mana yang paling relevan dipinjam Indonesia bukan karena satu kerangka lebih unggul dari yang lain, melainkan karena masing-masing menjawab dimensi persoalan yang berbeda.

Regulation (EU) 2024/1689 mengambil pendekatan berbasis risiko: sistem AI dalam *law enforcement* dan *administration of justice* diklasifikasikan *high-risk*, tunduk pada dokumentasi teknis, *automatic logging*, dan pengawasan manusia bermakna sebelum digunakan (European Parliament, 2024). Logika klasifikasi berjenjang ini AI hiburan diperlakukan berbeda dari AI penilai risiko residivisme absen sama sekali dari UU ITE maupun KUHAP Baru, yang memperlakukan seluruh bukti elektronik dengan satu standar seragam. Council of Europe *Framework Convention on AI*, traktat pertama di dunia yang mengikat secara hukum di bidang ini, menegaskan bahwa penerapan AI oleh otoritas publik harus tunduk pada martabat manusia, HAM, demokrasi, dan supremasi hukum secara dapat ditegakkan, bukan sekadar etis pelajaran bahwa prinsip *admissibility* yang diusulkan artikel ini sebaiknya mengikat, bukan sekadar kode etik.

NIST *AI Risk Management Framework* menawarkan logika operasional berbasis empat fungsi berkelanjutan *Govern, Map, Measure, Manage* yang memandu pengujian keandalan sistem sepanjang masa pakainya, bukan pemeriksaan satu kali (Europe, 2024). OECD *AI Principles*, hasil pembaruan Mei 2024, secara khusus memindahkan *traceability* dari prinsip keamanan menuju akuntabilitas, dan merevisi transparansi agar berorientasi pada kemampuan pihak terdampak untuk menantang keluaran AI, bukan sekadar memahaminya rumusan *explainability* paling tepat bagi konteks pembuktian pidana, karena persis fungsi yang idealnya dijalankan pemeriksaan silang. UNESCO *Recommendation on the Ethics of AI*, diadopsi 193 negara pada 2021, menjadikan HAM dan martabat manusia sebagai fondasi, dengan transparansi dan pengawasan manusia sebagai penopangnya. Perkembangan terbaru turut relevan: paket *Digital Omnibus* Komisi Eropa 2026 mengusulkan penundaan tenggat kepatuhan Annex III dari Agustus 2026 ke Desember 2027 bukan tanda kegagalan pendekatan berbasis risiko, melainkan pengakuan bahwa infrastruktur kepatuhan memerlukan waktu, bahkan bagi yurisdiksi paling maju sekalipun. Pelajaran bagi Indonesia: memanfaatkan momentum KUHAP Baru membangun infrastruktur serupa secara bertahap melalui pedoman Mahkamah Agung sejak sekarang, bukan menunggu ekosistem regulasi matang terlebih dahulu.

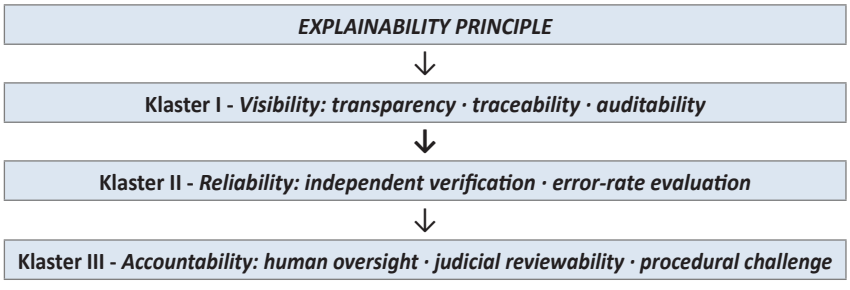
Tidak satu pun dari kelima kerangka ini memaksakan *algorithmic evidence* ke dalam kategori pembuktian konvensional yang sudah ada semuanya memperlakukannya sebagai objek regulasi tersendiri, bukan varian bukti ilmiah atau dokumenter biasa. Konsistensi ini memperkuat argumen bahwa solusi bagi Indonesia bukan memaksakan *algorithmic evidence* ke dalam petunjuk atau keterangan ahli yang sudah ada, melainkan mengembangkan kerangka *admissibility* tersendiri sebagaimana diusulkan bagian berikutnya.

Teori kebenaran materiil yang menjadi rujukan utama hukum acara pidana Indonesia, sebagaimana dirumuskan (H.S. Brahmana, SH., 2012), menegaskan bahwa tujuan pembuktian pidana bukan sekadar memperoleh kepastian formal sebagaimana dalam hukum acara perdata, melainkan mengungkap kebenaran senyata-nyatanya (*materiële waarheid*) melalui proses yang dapat dipertanggungjawabkan secara rasional oleh hakim. Standar ini menuntut lebih dari sekadar keberadaan bukti secara kuantitatif dua alat bukti yang sah sebagaimana disyaratkan Pasal 183 KUHAP

melainkan juga kualitas penalaran yang membentuk keyakinan hakim atas bukti-bukti tersebut. Ketika penalaran itu sendiri berasal dari proses komputasional yang tidak dapat dijelaskan, keyakinan hakim yang terbentuk bukan lagi produk dari penalaran rasionalnya sendiri atas fakta, melainkan produk dari kepercayaan terhadap otoritas teknologi sebuah pergeseran yang, sejauh apa pun presisi numerik yang ditawarkan algoritma, tidak dapat disamakan dengan pencarian kebenaran materiil sebagaimana dimaksud teori ini.

Kontribusi normatif artikel ini adalah menempatkan *explainability* bukan sebagai satu kriteria teknis di antara kriteria lain, melainkan sebagai asas hukum pembuktian elektronik yang menaungi seluruh kriteria *admissibility algorithmic evidence* sebuah prinsip *explainability* yang menjadi turunan langsung dari teori kebenaran materiil tersebut. Jika kebenaran materiil menuntut hakim mencapai keyakinan atas dasar penalaran yang dapat dipertanggungjawabkan, dan bukan atas dasar kepercayaan buta terhadap otoritas teknologi, maka setiap alat bukti yang penalarannya tidak dapat dijelaskan pada dasarnya menghalangi, bukan membantu, pencarian kebenaran materiil itu sendiri. Dari sudut epistemologi pembuktian, persoalannya dapat dirumuskan tajam: apakah keluaran algoritmik menghasilkan *knowledge* yang dapat menjadi dasar keyakinan hakim, ataukah ia sekadar *probability* yang dibungkus otoritas teknologis? Tanpa *explainability*, hakim tidak pernah benar-benar dapat menjawab pertanyaan ini, dan pembuktian pidana bergeser dari pencarian kebenaran menjadi kepatuhan pada mesin.

Bagan 2. *Three Clusters of Algorithmic Evidence Admissibility*



Prinsip *explainability* ini beroperasi melalui tiga klaster kriteria yang saling menopang. Klaster pertama menjamin keterlihatan proses: transparansi mensyaratkan bahwa keberadaan dan fungsi umum suatu sistem algoritmik dalam suatu perkara diungkapkan sejak tahap penyidikan, bukan baru terungkap di persidangan; *traceability* mensyaratkan bahwa setiap keluaran dapat ditelusuri kembali ke data masukan dan versi model yang menghasilkannya, mengingat model pembelajaran mesin dapat dilatih ulang sehingga "sistem yang sama" pada dua waktu berbeda dapat menghasilkan keluaran berbeda; dan auditabilitas mensyaratkan bahwa pihak berwenang termasuk pengadilan memiliki akses untuk memeriksa jejak keputusan sistem, bukan hanya keluaran akhirnya. Ketiganya secara bersama memastikan bahwa "kotak hitam" tidak dapat dijadikan alasan menghindari pemeriksaan, sebagaimana terjadi dalam *Loomis* (Frank, 2017).

Ketiga kriteria klaster pertama ini tidak perlu dibangun dari nol. Indonesia telah mengadopsi standar internasional ISO/IEC 27037 mengenai identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital, serta ISO/IEC 27043 mengenai prinsip investigasi insiden, sebagaimana diterapkan sejumlah laboratorium forensik digital instansi pemerintah yang telah terakreditasi. (Batista et al., 2023) Prinsip *chain of custody* yang telah dikenal dalam kedua standar tersebut untuk bukti digital konvensional dapat diperluas menjadi *chain of algorithmic custody*: setiap tahap mulai dari data pelatihan, versi model, parameter yang digunakan, hingga keluaran akhir harus terdokumentasi dan dapat ditelusuri kembali dengan cara yang sama seperti rantai penyimpanan barang bukti fisik didokumentasikan sejak penyitaan hingga persidangan. Perluasan ini secara teknis dapat dilaksanakan tanpa membangun infrastruktur akreditasi baru dari awal, melainkan dengan memperluas cakupan standar yang sudah berjalan.

Alokasi beban pemenuhan kesembilan kriteria ini juga perlu ditegaskan agar prinsip kesetaraan senjata (*equality of arms*) tidak sekadar retorika. Beban awal untuk memenuhi klaster pertama dan kedua transparansi, *traceability*, auditabilitas, serta penyediaan data tingkat kesalahan seharusnya dibebankan kepada pihak yang mengajukan *algorithmic evidence*, lazimnya penuntut umum, sejalan dengan prinsip bahwa pihak yang mendalilkan sesuatu wajib membuktikannya. Namun demikian, hak menguji atau membantah dalam klaster ketiga verifikasi independen dan kemampuan menantang secara prosedural harus dijamin dapat diakses secara riil oleh terdakwa yang kemampuan ekonominya terbatas, misalnya melalui penunjukan ahli independen oleh negara sebagaimana dikenal dalam mekanisme bantuan hukum, agar prinsip kesetaraan senjata tidak berhenti menjadi hak di atas kertas bagi terdakwa yang mampu membayar ahli sendiri.

Klaster kedua menjamin keandalan yang teruji: verifikasi independen mensyaratkan bahwa pihak lawan termasuk ahli yang ditunjuk terdakwa memiliki kesempatan nyata untuk mereplikasi atau menguji ulang analisis, bukan sekadar menerima laporan hasil; dan evaluasi tingkat kesalahan mensyaratkan bahwa setiap sistem yang diajukan sebagai bukti disertai data tingkat kesalahan yang telah diuji, termasuk sebagaimana ditunjukkan Buolamwini dan Gebru, tingkat kesalahan yang mungkin berbeda antarkelompok populasi (Buolamwini & Gebru, 2018). Tanpa klaster ini, "kewibawaan ilmiah" yang melekat pada *algorithmic evidence* tidak lebih dari sekadar tampilan presisi numerik tanpa substansi yang dapat diuji.

Klaster ketiga menjamin otoritas hukum tetap berada di tangan manusia: pengawasan manusia mensyaratkan bahwa keputusan akhir tetap berada pada penyidik, penuntut, atau hakim yang memahami keterbatasan sistem, bukan sekadar meneruskan keluarannya; dapat ditinjau ulang secara yudisial (*judicial reviewability*) (Atkins, 2024) mensyaratkan bahwa hakim memiliki kewenangan afirmatif untuk menolak *algorithmic evidence* yang tidak memenuhi kriteria di atas, sebagaimana kewenangan menyatakan bukti tidak memiliki kekuatan pembuktian yang telah dikenal dalam hukum acara pidana Indonesia; dan kemampuan menantang secara prosedural (*procedural challenge*) mensyaratkan bahwa terdakwa memiliki hak afirmatif bukan sekadar kesempatan pasif untuk mempersoalkan metodologi algoritmik yang

memberatkannya, meminjam reorientasi OECD dari "menjelaskan" menuju "dapat ditantang" yang telah diuraikan pada bagian sebelumnya.

Kriteria pengawasan manusia perlu dirancang secara hati-hati agar tidak menjadi formalitas belaka. Penelitian psikologi kognitif sejak akhir dekade 1990-an, dipelopori (Skitka et al., 1999), menunjukkan fenomena *automation bias*: kecenderungan pengambil keputusan menjadikan rekomendasi otomatis sebagai pengganti pencarian dan pengolahan informasi yang cermat, bahkan ketika informasi lain yang tersedia bertentangan dengannya. Kehadiran formal seorang hakim atau penyidik yang "mengawasi" keluaran algoritmik karena itu tidak dengan sendirinya menjamin pengawasan yang bermakna, sehingga kriteria ini perlu disertai pelatihan eksplisit mengenai risiko tersebut, dan idealnya tidak berhenti pada pengawasan internal oleh instansi yang sama yang mengoperasikan system baik melalui perluasan mandat Komisi Yudisial untuk turut memantau penggunaan sistem algoritmik dalam proses peradilan, maupun unit pengawasan teknis independen di bawah Mahkamah Agung.

Penerapan kesembilan kriteria ini dapat diilustrasikan melalui skenario kecocokan wajah 96 persen yang telah dibahas berulang kali dalam artikel ini. Di bawah kerangka yang diusulkan, penyidik yang hendak mengajukan hasil tersebut sebagai bukti pertama-tama harus mengungkapkan penggunaan sistem tersebut sejak tahap penyidikan (transparansi), menyertakan catatan versi model dan data pembanding yang digunakan pada saat analisis dilakukan (*traceability*), dan memberi akses kepada pengadilan untuk memeriksa parameter yang mendasari perhitungan tersebut (auditabilitas). Pihak terdakwa kemudian berhak menunjuk ahli independen untuk menguji ulang kecocokan tersebut menggunakan data yang sama (verifikasi independen), dan penuntut umum wajib menyertakan data tingkat kesalahan sistem tersebut, termasuk kemungkinan disparitas tingkat kesalahan antarkelompok demografis (evaluasi tingkat kesalahan). Hakim, pada gilirannya, tetap berwenang menyatakan bukti tersebut tidak memiliki kekuatan pembuktian yang cukup apabila salah satu syarat di atas tidak terpenuhi (dapat ditinjau ulang secara yudisial), sementara terdakwa memiliki hak afirmatif mengajukan keberatan atas metodologi yang digunakan sejak tahap praperadilan, bukan hanya pada saat putusan akan dijatuhkan (kemampuan menantang secara prosedural). Skenario ini menunjukkan bahwa kesembilan kriteria bukan hambatan birokratis bagi penggunaan AI dalam pembuktian pidana, melainkan justru prasyarat agar penggunaan tersebut dapat dipertanggungjawabkan di hadapan hukum.

Analogi dengan asas *unus testis nullus testis* layak ditegaskan: keterangan seorang saksi saja, betapa pun meyakinkan, tidak cukup menjadi dasar pemidanaan tanpa didukung alat bukti lain. Logika yang sama berlaku bagi *algorithmic evidence* keluaran satu sistem, betapa pun tinggi presisi yang ditampilkannya, tidak boleh berdiri sendiri sebagai dasar keyakinan hakim tanpa dukungan bukti independen lain, mengingat presisi numerik justru berisiko mengaburkan kebutuhan korroborasi tersebut di mata hakim yang tidak waspada terhadap *automation bias* (Ruschemeier & Hondrich, 2024).

Kesembilan kriteria ini bukan daftar administratif yang berdiri sendiri-sendiri, melainkan manifestasi dari satu prinsip yang sama: bahwa *algorithmic evidence* hanya

layak menjadi dasar keyakinan hakim apabila penalarannya dapat dijelaskan, diuji, dan dipersoalkan oleh manusia yang bertanggung jawab secara hukum atasnya. Prinsip inilah yang diusulkan penelitian ini sebagai prinsip *explainability* asas baru dalam hukum pembuktian elektronik Indonesia yang berdiri setara dengan asas-asas pembuktian yang telah dikenal seperti asas keyakinan hakim dan asas *unus testis nullus testis* (Baron, 2025).

Rekonstruksi *admissibility* di atas membawa implikasi yang melampaui sekadar penambahan syarat teknis. Bagi kepastian hukum, kerangka ini menggantikan penilaian kasuistis hakim yang berbeda-beda dari satu perkara ke perkara lain dengan tolok ukur normatif yang seragam, sehingga dua terdakwa yang berhadapan dengan *algorithmic evidence* yang secara teknis setara diperlakukan menurut standar yang sama, bukan menurut seberapa besar kepercayaan personal seorang hakim terhadap teknologi tertentu. Bagi keadilan dan perlindungan terdakwa, kerangka ini memulihkan keseimbangan yang tergerus ketika presisi numerik algoritmik menciptakan efek psikologis yang secara diam-diam menggeser beban pembuktian dari penuntut umum kepada terdakwa; dengan mensyaratkan verifikasi independen dan kemampuan menantang secara prosedural, beban itu dikembalikan ke tempat yang semestinya (Holm, 2023).

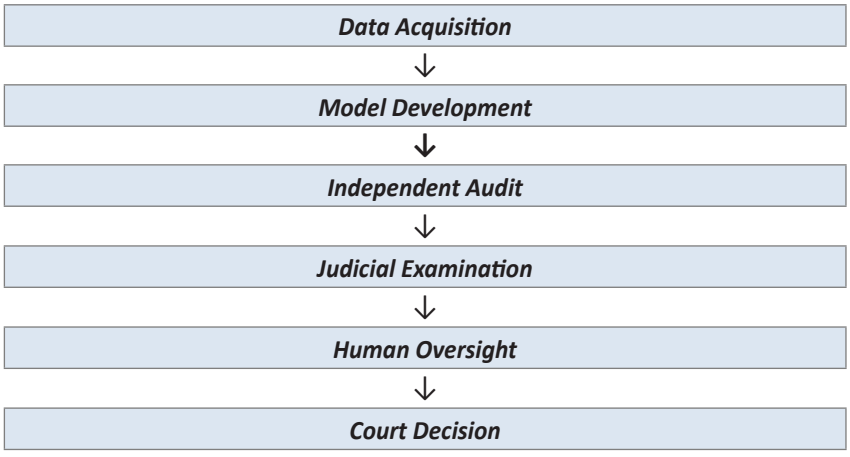
Tanpa kerangka yang diusulkan, dua terdakwa di dua pengadilan berbeda yang dihadapkan pada hasil analisis pengenalan wajah yang identik berpotensi diperlakukan berbeda satu hakim menerimanya sebagai "bukti elektronik yang sah," hakim lain menolaknya karena keraguan pribadi bukan karena perbedaan fakta kasus, melainkan semata sikap personal terhadap teknologi. Disparitas inilah yang hendak dicegah prinsip kepastian hukum, dan akan teratasi apabila kesembilan kriteria diterapkan seragam melalui pedoman Mahkamah Agung (Susatyo, 2023).

Kerangka ini bukan sekadar kebijakan teknis, melainkan pelaksanaan langsung jaminan konstitusional. Pasal 28D ayat (1) UUD 1945 menjamin kepastian hukum yang adil, menuntut tolok ukur normatif seragam bagi *algorithmic evidence*, bukan penilaian kasuistis antarhakim. Pasal 28G ayat (1) menjamin perlindungan diri pribadi relevan langsung dengan hak menguji dan menantang keluaran algoritmik yang memberatkan, yang tanpa verifikasi independen dan *procedural challenge* akan menjadi ilusi. Pasal 24 ayat (1) menjamin kekuasaan kehakiman merdeka, ditopang pengawasan manusia dan *judicial reviewability*: kemerdekaan hakim tidak bermakna apabila keyakinannya didikte keluaran sistem yang tidak dapat ia periksa. Kesembilan kriteria yang diusulkan, dengan demikian, adalah instrumen menegakkan jaminan konstitusional yang sudah ada, bukan pembatasan baru terhadap wewenang peradilan.

Bagi independensi yudisial, implikasinya menegaskan bahwa hakim tetap menjadi penguji fakta yang aktif, bukan penerima pasif keluaran mesin. Prinsip pengawasan manusia dan kewenangan meninjau ulang secara yudisial memastikan bahwa keyakinan hakim, sebagaimana disyaratkan Pasal 183 KUHAP (Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana, 1981), tetap terbentuk melalui penalaran hakim itu sendiri atas alat bukti yang telah teruji, bukan melalui delegasi otoritas kepada sistem algoritmik yang penalarannya berada di luar jangkauan pemeriksaannya. Inilah yang membedakan usulan artikel ini dari sekadar mengizinkan atau melarang penggunaan

AI dalam pembuktian pidana: kerangka ini mengizinkan penggunaannya, tetapi menempatkan AI secara tegas sebagai alat bantu yang tunduk pada kendali hukum, bukan sebagai penentu kebenaran yang berdiri di luar kendali itu.

Bagan 3. ***Implementation Framework for Algorithmic Evidence in Indonesia***



Momentum berlakunya KUHAP Baru dengan sistem pembuktian terbukanya memberikan kesempatan yang tidak akan datang dua kali dalam satu generasi untuk mengintegrasikan kerangka ini sebagai bagian dari arsitektur hukum acara pidana yang baru termasuk membentuk mekanisme sertifikasi independen atas sistem algoritmik yang digunakan aparat penegak hukum, serupa akreditasi laboratorium forensik DNA yang telah dikenal dalam praktik peradilan Indonesia, dan memperluas fungsi praperadilan sebagai forum awal menguji pemenuhan kesembilan kriteria sebelum perkara bergulir ke pokok perkara (Sugiastuti et al., 2023). Penerapannya paling realistis dilakukan bertahap: klaster keterlihatan proses lebih dulu karena hanya memerlukan kewajiban dokumentasi melalui Perma, disusul klaster keandalan yang bergantung pada perluasan akreditasi laboratorium yang sudah ada, dan terakhir klaster akuntabilitas yang memerlukan penguatan kelembagaan paling mendalam. Kerangka ini juga sejalan dengan SDG 16 (*Peace, Justice and Strong Institutions*), khususnya target 16.3 mengenai akses setara terhadap keadilan dan target 16.6 mengenai institusi yang transparan dan akuntabel.

Secara *de lege lata*, kesembilan kriteria tidak memerlukan perubahan undang-undang untuk mulai diterapkan. Pasal 235 ayat (1) huruf f dan h UU Nomor 20 Tahun 2025 menyediakan ruang normatif yang cukup bagi Mahkamah Agung menuangkannya ke dalam Peraturan Mahkamah Agung sebagai pedoman teknis jalur yang telah lazim ditempuh MA untuk mengisi kekosongan teknis penerapan undang-undang tanpa menunggu revisi legislatif.

Secara *de lege ferenda*, kriteria yang sama layak dituangkan secara eksplisit dalam peraturan pelaksana KUHAP Baru pada tingkat yang lebih permanen, mengingat pengalaman *Loomis* menunjukkan bahwa penafsiran hakim kasus demi kasus tanpa tolok ukur eksplisit cenderung menghasilkan standar yang tidak konsisten dan merugikan hak-hak terdakwa

KESIMPULAN

Algorithmic evidence, sebagaimana ditunjukkan penelitian ini, tidak berkedudukan sebagai petunjuk, tidak sepenuhnya setara keterangan ahli, dan tidak cukup diperlakukan sekadar sebagai bukti elektronik konvensional; ia adalah kategori pembuktian tersendiri bukti elektronik generasi kedua lahir dari penalaran komputasional, bukan sekadar perekaman atau transmisi informasi. Baik rezim tertutup KUHAP lama maupun rezim terbuka KUHAP Baru gagal menampung kategori ini, karena keduanya menguji keabsahan cara memperoleh bukti elektronik tanpa pernah menguji validitas penalaran yang menghasilkan kesimpulan algoritmik itu sendiri sebuah kekosongan yang berakar pada sejarah pembentukan hukum pembuktian Indonesia yang tidak pernah dirancang untuk bukti nonmanusia. Dalam perspektif yang lebih luas, temuan ini menunjukkan bahwa tantangan *algorithmic evidence* menuntut hukum pembuktian pidana Indonesia meninjau kembali asumsi paling dasarnya mengenai apa yang dimaksud dengan "mengetahui" dalam proses pencarian kebenaran materiil: sejauh mesin turut serta dalam proses tersebut, hukum pembuktian harus mampu membedakan antara mesin yang membantu manusia berpikir lebih jernih dan mesin yang menggantikan manusia berpikir sama sekali. Untuk mengisi kekosongan itu, penelitian ini merekonstruksi syarat *admissibility algorithmic evidence* dengan menempatkan *explainability* sebagai asas hukum pembuktian elektronik yang baru bukan sekadar kriteria teknis yang beroperasi melalui sembilan kriteria yang terorganisir dalam tiga klaster: keterlihatan proses (transparansi, *traceability*, auditabilitas), keandalan yang teruji (verifikasi independen, evaluasi tingkat kesalahan), dan otoritas hukum yang tetap berada di tangan manusia (pengawasan manusia, *judicial reviewability*, *procedural challenge*). Kontribusi keilmuan artikel ini terletak pada pergeseran fokus dari sekadar mengusulkan penerapan *Explainable AI* menuju pengonseptualisasian ulang kedudukan *algorithmic evidence* dalam teori pembuktian pidana Indonesia sebuah langkah yang menjadikan seluruh rekonstruksi *admissibility* berikutnya berpijak pada fondasi konseptual yang kokoh, bukan sekadar solusi teknis yang berdiri sendiri. Implikasi hukumnya bersifat ganda sebagaimana diuraikan pada bagian *De Lege Lata* dan *De Lege Ferenda*: dapat diintegrasikan segera ke dalam pedoman penerapan Pasal 235 ayat (1) KUHAP Baru melalui Peraturan Mahkamah Agung, sekaligus layak dipertimbangkan untuk peraturan pelaksana yang lebih permanen di masa mendatang. Penelitian ini merekomendasikan tiga langkah konkret. Pertama, Mahkamah Agung segera menyusun pedoman teknis berbasis kesembilan kriteria yang diusulkan sebagai Peraturan Mahkamah Agung, dimulai dari klaster keterlihatan proses yang paling mudah dilaksanakan tanpa investasi infrastruktur baru. Kedua, instansi penegak hukum yang telah memiliki akreditasi laboratorium forensik digital memperluas cakupan akreditasi tersebut untuk turut mencakup validitas penalaran algoritmik, bukan sekadar keutuhan data. Ketiga, penelitian lanjutan diperlukan untuk menguji kelayakan penerapan kesembilan kriteria ini secara empiris pada praktik peradilan yang telah menggunakan sistem algoritmik, khususnya untuk merumuskan pedoman teknis penilaian tingkat kesalahan yang dapat diterapkan secara konsisten oleh hakim yang umumnya tidak memiliki latar belakang teknis ilmu komputer dan kesembilan kriteria yang diusulkan artikel ini adalah upaya menjaga agar pembuktian pidana Indonesia tetap berada pada sisi yang membantu manusia berpikir lebih jernih, bukan sisi yang menggantikan manusia berpikir sama sekali.

REFERENSI

Aditya, R., & Yusuf, H. (2026). Paradoks pembuktian hukum pidana di era transisi : manipulasi bukti digital berbasis *deepfake* dalam sistem pembuktian terbuka KUHAP baru the paradox of criminal law evidence in the transition era : deepfake-based digital evidence manipulation in the new c. *Jurnal Intelek Dan Cendikiawan Nusantara*, *3*(3), 7248–7258. Https://jicnusantara.com/index.php/jicn%0A Allen, R. J., Pardo, M. S., Lawrence, W. J., & Smiciklas, C. K. (2025). Minimal rationality and the law of evidence. *Journal of Criminal Law and Criminology*, *115*(2).

Atkins, S. (2024). Fettering scrutiny on executive discretionary powers? Developments in the judicial reviewability of ministerial non-statutory guidance. *Northern Ireland Legal Quarterly*, *75*(2). Https://doi.org/10.53386/nilq.v75i2.1085

Baron, S. (2025). Trust, explainability and AI. *philosophy and technology*, *38*(1). Https://doi.org/10.1007/s13347-024-00837-6

Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., & Miranda, F. P. De. (2023). Exploring blockchain technology for chain of custody control in physical evidence: a systematic literature review. In *Journal of Risk and Financial Management* (Vol. 16, Issue 8). Https://doi.org/10.3390/jrfm16080360

Buolamwini, J., & Gebru, T. (2018). Gender shades: intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, *81*.

Darizta, F., Sufitri, S., Firdaus, H., Fathony, M., & Sari, D. I. (2023). Barang bukti dalam hukum pembuktian di Indonesia. *Lexstricta : Jurnal Ilmu Hukum*, *2*(2). Https://doi.org/10.46839/lexstricta.v2i2.29

Europe, C. Of. (2024). *Framework convention on artificial intelligence and human rights , democracy and what is the purpose of*.

European Parliament. (2024). Regulation (EU) 2024 / 1689 of the European Parliament and of the council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC) no 300 / 2008 , (eu) no 167 / 2013 , (eu) no 168 / 2013 , (eu) 2018 /. *Offcial Journal of the European Union*, *300*, 1–171. Https://eur-lex.europa.eu/eli/reg/2024/1689/oj Frank, I. (2017). State v. Loomis wisconsin supreme court requires warning before use of algorithmic risk assessments in sentencing. *Harvard Law Review*, *130*(5).

García-Magariño, I., Bravo-Agapito, J., & Lacuesta, R. (2025). Cybersecure xai algorithm for generating recommendations based on financial fundamentals using deepseek. *AI*, *6*(5), 95. Https://doi.org/10.3390/ai6050095

Garrett, B. L., & Rudin, C. (2023). Interpretable algorithmic forensics. *Proceedings of the National Academy of Sciences*, *120*(41). Https://doi.org/10.1073/pnas.2301842120

Garrett, B. L., & Rudin, C. (2024). The right to a glass box: rethinking the use of artificial intelligence in criminal justice. *Cornell L. Rev.*, *109*(3), 561.

H.S. Brahmana, SH., M. . (2012). Teori dan hukum pembuktian. *Pn-Lhoksukon.Go.Id*.

Holm, S. (2023). Statistical evidence and algorithmic decision-making. *Synthese*, *202*(1). Https://doi.org/10.1007/s11229-023-04246-8

ISO/IEC. (2012). 27037:2012 ISO/IEC ternational standard that provides guidelines for the identification, collection, acquisition, and preservation of digital evidence, with a particular focus on the roles of digital evidence first responders (DEFR) and digital evidence s. *ISO/IEC*, *66*(265), 37–39.

ISO/IEC. (2015). 27043: 2015 international standard, information technology — security techniques — incident investigation principles and processes. *ISO.Org*, *1*(1), 1–30.

Kawamleh, S. (2025). Algorithmic evidence in U.S criminal sentencing. *AI and Ethics*, *5*(2). Https://doi.org/10.1007/s43681-024-00473-y Khadijah, K. (2025). Profil berpikir komputasi mahasiswa dari prosedur matematis ke algoritma program: studi kasus metode bagi dua. *Jurnal Ilmiah Matematika (JIMAT)*, *6*(2). Https://doi.org/10.63976/jimat.v6i2.1140

Maharani, S. D., & Wulandari, N. G. A. A. M. T. (2025). Regulation of evidence in the criminal procedure code: A comparison to the draft law on criminal procedure. *Bacarita Law Journal*, *6*(1).

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 (2016).

Ruschemeier, H., & Hondrich, L. J. (2024). Automation bias in public administration – an interdisciplinary perspective from law and psychology. *Government Information Quarterly*, *41*(3). Https://doi.org/10.1016/j.giq.2024.101953

Safriansyah Yanwar Rosyadi, & Zainal Arifin Hoesein. (2025). Pembaruan hukum di era digital: Aspek hukum terhadap validitas hasil analisis artificial intelligence sebagai alat bukti dalam penegakan hukum pidana pertambangan. *Judge : Jurnal Hukum*, *6*(03), 563–577. Https://doi.org/10.54209/judge.v6i03.1569

Satriya Nugraha, Kiki Kristanto, & Fahrizal S.Siagian. (2026). Artificial intelligence in criminal investigations: legal implications for evidence admissibility, accountability, and protection of fundamental human rights. *Journal of Civil Criminal Law*, *1*(3), 24–34. https://doi.org/10.70062/jccl.v1i3.141

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). https://doi.org/10.56128/ljoalr.v3i4.311

Seng, D. (2025). Artificial intelligence as evidence. In *Research Handbook on the Law of Artificial Intelligence: Current and Future Directions, Second Edition*. https://doi.org/10.4337/9781035316496.00026

Skitka, L. J., Mosier, K. L., & Burdick, M. (1999). Does automation bias decision-making? *International Journal of Human Computer Studies*, *51*(5). https://doi.org/10.1006/ijhc.1999.0252

Sugiastuti, N. Y., Desmayanti, R., & Shahin, N. S. A. (2023). Sikap hakim dalam menerapkan Pasal 1321 kuhperdata: studi putusan pengadilan di Indonesia. *Jurnal Hukum Ius Quia Iustum*, *30*(3), 673–691. https://doi.org/10.20885/iustum.vol30.iss3.art10

Susatyo, F. A. (2023). Kriteria alat bukti elektronik yang sah dalam urgensi pembaharuan KUHAP. *HUKUM DAN DINAMIKA MASYARAKAT*, *21*(1). https://doi.org/10.56444/hdm.v21i1.4035

Undang-Undang Nomor 20 Tahun 2025 Tentang Hukum Acara Pidana, Ps. 235 (2025).

Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana, Ps. 1 angka 28 jo. Ps. 186 (1981).

Undang Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Ps. 1 angka 1 (2024).

Yeo, W. J., Van Der Heever, W., Mao, R., Cambria, E., Satapathy, R., & Mengaldo, G. (2025). A comprehensive review on financial explainable AI. *Artificial Intelligence Review*, *58*(6). https://doi.org/10.1007/s10462-024-11077-7

Yuli Anggraini. (2024). Kekuatan hukum alat bukti elektronik dan kredibilitasnya dalam pembuktian hukum pidana. *Jurnal Hukum Dan Kewarganegaraan*, *6*(8).

Yuyun Sri Wahyuni. (2021). Kekuatan hukum pembuktian akta perjanjian pengikatan jual beli tanah (ppjb) dalam kasus sengketa perdata (analisa putusan mahkamah agung nomor : 994/k/pdt/2020 jo putusan pengadilan negeri batam nomor : 218/pdt.g/2017/pn btm). *Indonesian Notary*, *4*.