PUNGGAWA
GLOBAL RESEARCH:
JURNAL MULTIDISIPLIN

Punggawa Global Research: Jurnal Multidisiplin
Volume 1, Nomor 6, 2026
E-ISSN: 3164-0117
Open Access: punggawajournal.com/pgr

Kewajiban Pengungkapan Bukti Algoritmik dalam Sengketa Perdata Akibat Artificial Intelligence: Rekonstruksi Mekanisme Pembuktian dalam Hukum Indonesia

Junichirou Adhigana Joko Laksito[1], Achmad Davy[1], Ronaldi Ziliwu[1]
[1] Universitas Pamulang, Indonesia
Korespondensi: junichirou126543@gmail.com

Informasi Artikel

Riwayat artikel:
Received Oct 1th, 2026
Revised Nov 12th, 2026
Accepted Nov 21th, 2026

Keyword:
Bukti algoritmik; Kecerdasan buatan; Hukum acara perdata; Dokumen elektronik; Pengungkapan bukti; Preservasi bukti

ABSTRAK

Penggunaan kecerdasan buatan dalam kegiatan ekonomi dan layanan publik menimbulkan kerugian yang sulit dibuktikan karena proses pengambilan keputusannya tertutup, sehingga pihak yang dirugikan menghadapi ketimpangan informasi. Penelitian ini bertujuan menilai kecukupan hukum pembuktian perdata Indonesia dalam menghadapi ketimpangan tersebut dan merumuskan model pengungkapan bukti algoritmik yang proporsional. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan secara terbatas. Hasil penelitian menunjukkan bahwa pengakuan informasi dan dokumen elektronik dalam Undang-Undang Informasi dan Transaksi Elektronik belum menyediakan prosedur untuk memerintahkan pengungkapan informasi teknis yang dikuasai pihak lawan, sedangkan Pasal 137 Herzien Inlandsch Reglement hanya menjangkau surat yang telah diajukan ke persidangan. Penelitian ini mengusulkan model pengungkapan bertahap yang terdiri atas preservasi terbatas, permintaan spesifik, uji proporsionalitas oleh hakim, pengungkapan berjenjang, perlindungan kerahasiaan, dan penilaian atas ketidakpatuhan secara kasus per kasus. Model ini memperkuat akses terhadap keadilan tanpa mewajibkan pembukaan seluruh rahasia algoritma.

© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

PENDAHULUAN

Kecerdasan buatan (*artificial intelligence*, selanjutnya AI) telah mengubah cara keputusan diambil dalam banyak kegiatan ekonomi dan sosial. Sistem ini dipakai, misalnya, untuk menilai kelayakan kredit, menyaring pelamar kerja, mendeteksi penipuan, memberi rekomendasi komersial, dan mengotomatisasi layanan. Keputusannya cepat dan konsisten, tetapi bila keliru, kerugiannya dapat menimpa individu maupun badan usaha. Masalah hukumnya tidak berhenti pada siapa yang harus bertanggung jawab. Dalam banyak kasus, pihak yang dirugikan bahkan kesulitan mengetahui bagaimana keputusan yang merugikannya dihasilkan.

Kesulitan itu bersumber dari sifat teknis AI. Keputusan sistem dipengaruhi oleh data masukan, versi model, konfigurasi, pembaruan, parameter, dan interaksi dengan operator manusia, dan sebagian besar informasi tersebut hanya ada di sistem internal penyedia atau pengguna AI. Pihak yang dirugikan biasanya hanya melihat hasil akhir, seperti penolakan kredit atau pemutusan layanan, tanpa catatan yang cukup untuk menguji prosesnya. Akibatnya timbul ketimpangan informasi dan bukti yang menyulitkan pemenuhan beban pembuktian dalam perkara perdata.

Hukum acara perdata Indonesia mengenal alat bukti berupa tulisan, saksi, persangkaan, pengakuan, dan sumpah (Republik Indonesia, 1847, Pasal 1866; 1927, Pasal 284; 1941, Pasal 164), sedangkan pembagian beban pembuktian diatur dalam Pasal 163 HIR, Pasal 283 RBg, dan Pasal 1865

KUHPerdata (Republik Indonesia, 1847, 1927, 1941). Perkembangan teknologi kemudian diakomodasi melalui pengakuan informasi dan dokumen elektronik sebagai alat bukti yang sah dan sebagai perluasan alat bukti menurut hukum acara (Soroinda & Nasution, 2022). Namun, diakuinya suatu informasi sebagai alat bukti berbeda dengan tersedianya cara untuk memperolehnya ketika informasi itu dikuasai lawan. Karena itu, persoalan utamanya bukan hanya dapat diterimanya dokumen elektronik (*admissibility*), melainkan juga akses, preservasi, relevansi, autentikasi, dan perlindungan informasi teknis.

Pasal 137 *Herzien Inlandsch Reglement* (HIR) memberi hak kepada para pihak untuk menuntut agar surat-surat pihak lawan yang diserahkan kepada hakim dapat mereka lihat, dan Pasal 163 RBg memuat ketentuan serupa (Republik Indonesia, 1927, 1941). Sebuah tulisan yang dimuat di laman Mahkamah Agung tentang dokumen elektronik di persidangan perdata mengaitkan prinsip ini dengan kebutuhan memperlihatkan dokumen elektronik kepada lawan (Waruwu, 2018). Mahkamah Agung juga telah mengatur administrasi perkara dan persidangan secara elektronik melalui Peraturan Mahkamah Agung Nomor 1 Tahun 2019, tetapi cakupan peraturan itu adalah administrasi perkara dan tata cara persidangan elektronik (Mahkamah Agung Republik Indonesia, 2019). Meski begitu, ketentuan-ketentuan tersebut belum menjelaskan cara memperoleh catatan teknis yang belum diajukan sebagai bukti, termasuk log sistem yang tersimpan di infrastruktur digital dan dapat berubah atau terhapus seiring waktu.

Penelitian ini dibatasi pada bukti algoritmik yang berguna untuk menguji proses pengambilan keputusan AI dalam sengketa perdata. Istilah ini tidak berarti bahwa algoritma atau kode sumber harus selalu dibuka seluruhnya. Yang dimaksud adalah rekaman dan dokumen teknis yang membantu merekonstruksi proses keputusan, yakni log peristiwa, waktu pemrosesan, identitas dan versi model, konfigurasi yang relevan, data masukan yang sah untuk diperiksa, catatan intervensi manusia, serta dokumentasi pengujian atau audit yang berkaitan langsung dengan peristiwa yang disengketakan.

Literatur terdahulu telah membahas sejumlah aspek yang berdekatan. Grossman dan Grimm (2025) mengkaji pendekatan pengadilan terhadap bukti yang dihasilkan AI beserta persoalan autentikasinya, dengan panduan praktis singkat tentang *discovery* dan perintah perlindungan bagi klaim rahasia dagang, tetapi dalam kerangka hukum pembuktian Amerika Serikat. Ameen et al. (2026) menelaah *judicial review* atas sistem administrasi algoritmik dan menekankan pentingnya log, riwayat konfigurasi, dan jejak audit, namun dalam konteks hukum administrasi. Soroinda dan Nasution (2022) mengkaji pengakuan, keabsahan, dan kekuatan pembuktian alat bukti elektronik dalam hukum acara perdata Indonesia, sedangkan Fakhriah (2020) menunjukkan bahwa hakim dapat menemukan hukum melalui analogi atau penafsiran agar bukti elektronik dapat dipakai sebagai alat bukti. Waruwu (2018) menyoroti penyerahan dokumen elektronik di persidangan perdata dan cara memperlihatkannya kepada lawan. Fokus penelitian ini berbeda, yaitu pada akses dan preservasi bukti teknis AI. Di tingkat regulasi, *Artificial Intelligence Act* Uni Eropa mewajibkan dokumentasi teknis dan pencatatan log bagi sistem berisiko tinggi, tetapi tidak dirancang sebagai aturan pengungkapan bukti dalam sengketa perdata (European Parliament & Council, 2024). Penelitian ini tidak mengklaim bahwa isu transparansi algoritma atau bukti digital belum pernah dikaji. Kebaruannya lebih sempit, yaitu menyusun tahapan permintaan dan pengungkapan bukti algoritmik untuk sengketa perdata Indonesia dengan menghubungkan Pasal 137 HIR, rezim bukti elektronik, preservasi bukti, dan mekanisme perlindungan informasi rahasia.

Penelitian ini bertujuan menjawab tiga persoalan. Pertama, bagaimana pengaturan pembuktian elektronik dalam hukum acara perdata Indonesia terhadap sengketa yang melibatkan keputusan sistem AI. Kedua, bagaimana kedudukan dan akses terhadap bukti algoritmik yang dikuasai penyedia atau pengguna AI. Ketiga, bagaimana model pengungkapan dan pelestarian bukti algoritmik yang proporsional dapat dirumuskan agar akses terhadap keadilan terjamin sekaligus rahasia dagang dan data pribadi terlindungi. Kontribusi penelitian ini berupa kerangka yang dapat dijadikan bahan penyusunan pedoman teknis Mahkamah Agung dan pembaruan hukum acara perdata.

METODE PENELITIAN

Penelitian ini bersifat normatif (doktrinal), dengan peraturan perundang-undangan, asas hukum, dan doktrin sebagai objek analisis. Pendekatan perundang-undangan dipakai untuk menelaah HIR, *Rechtsreglement Buitengewesten* (RBg), Kitab Undang-Undang Hukum Perdata (KUHPerdata), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta

perubahannya (Republik Indonesia, 2008, 2016, 2024), Undang-Undang Pelindungan Data Pribadi beserta peraturan pelaksanaannya (Republik Indonesia, 2022, 2026), ketentuan rahasia dagang (Republik Indonesia, 2000), dokumen perusahaan (Republik Indonesia, 1997), dan peraturan Mahkamah Agung tentang persidangan elektronik (Mahkamah Agung Republik Indonesia, 2019). Pendekatan konseptual dipakai untuk menganalisis beban pembuktian, relevansi bukti, penguasaan bukti, kewajiban preservasi, dan proporsionalitas pengungkapan.

Pendekatan perbandingan digunakan secara terbatas, yaitu dengan melihat prinsip dokumentasi dan pencatatan dalam *Artificial Intelligence Act* Uni Eropa (European Parliament & Council, 2024, Pasal 11, 12, dan 19) serta praktik pengungkapan dokumen pada sistem hukum yang mengenal *discovery*. Tujuannya bukan mencangkokkan aturan asing, melainkan mengidentifikasi prinsip yang dapat disesuaikan dengan struktur hukum acara perdata Indonesia. Bahan hukum primer dianalisis secara preskriptif, sedangkan bahan sekunder berupa artikel ilmiah dan literatur dipakai untuk memperjelas konsep dan perkembangan diskursus.

Analisis dilakukan dalam tiga tahap. Pertama, mengidentifikasi norma tentang alat bukti elektronik dan akses terhadap dokumen lawan. Kedua, menguji kecukupan norma tersebut ketika bukti teknis AI dikuasai satu pihak dan rawan berubah atau terhapus. Ketiga, merumuskan model pengungkapan bertahap berdasarkan relevansi, kebutuhan, proporsionalitas, dan perlindungan kepentingan yang sah.

HASIL DAN PEMBAHASAN

Pengakuan Bukti Elektronik Tidak Sama dengan Hak Memperoleh Bukti

Pasal 5 UU ITE, sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024, mengakui informasi elektronik, dokumen elektronik, dan hasil cetaknya sebagai alat bukti hukum yang sah serta sebagai perluasan alat bukti menurut hukum acara Indonesia (Republik Indonesia, 2024). Ketentuan ini penting karena catatan sistem AI pada umumnya berbentuk data elektronik. Pasal 6 menambahkan bahwa informasi elektronik harus dapat diakses, ditampilkan, terjamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Dengan demikian, log sistem atau dokumentasi digital dapat menjadi bukti yang relevan selama memenuhi persyaratan hukum serta dapat diuji keandalan dan kaitannya dengan perkara. Pengakuan serupa bahkan telah lebih dahulu dikenal dalam Undang-Undang Dokumen Perusahaan, yang menyatakan dokumen perusahaan yang dimuat dalam mikrofilm atau media lainnya dan/atau hasil cetaknya sebagai alat bukti yang sah (Republik Indonesia, 1997, Pasal 15 ayat 1; Waruwu, 2018).

Namun, pengakuan normatif tersebut tidak otomatis memberi hak atas seluruh data yang dimiliki pihak lain. UU ITE menjawab soal pengakuan dan syarat informasi atau dokumen elektronik, sedangkan hukum acara harus menjawab bagaimana pihak dapat meminta bukti yang relevan, bagaimana hakim menilai permintaan itu, dan bagaimana kepentingan kerahasiaan dilindungi. Tanpa prosedur akses, pihak yang secara formal memikul beban pembuktian berada dalam posisi timpang, karena bukti penentu ada di luar kendalinya (Waruwu, 2018).

Pasal 137 HIR menjadi landasan bahwa para pihak dapat menuntut untuk melihat surat lawan yang diserahkan kepada hakim, dan ini mendukung keterbukaan pembuktian di persidangan (Republik Indonesia, 1941). Akan tetapi, rumusan dan konteksnya berpusat pada dokumen yang sudah diajukan untuk perkara. Pasal ini belum secara tegas membentuk prosedur permintaan pra-persidangan atas bahan yang belum diajukan, perintah preservasi data, atau pemeriksaan terbatas atas informasi yang memuat rahasia dagang. Mekanisme permintaan data yang belum diajukan karenanya merupakan usulan pengembangan prosedural dalam penelitian ini, bukan bunyi eksplisit pasal, dan penerapannya pada bukti algoritmik memerlukan penafsiran hati-hati dan/atau pengaturan prosedural tambahan. Pendekatan penafsiran semacam itu sejalan dengan penemuan hukum oleh hakim terhadap bukti elektronik yang menurut Fakhriah (2020) dapat dilakukan melalui analogi atau penafsiran, meskipun kajian tersebut berfokus pada pengakuan bukti elektronik dan bukan pada akses terhadapnya.

Perlu pula dibedakan antara bukti yang *dihasilkan* AI dan bukti tentang *cara kerja* AI. Keluaran AI, misalnya skor risiko atau rekomendasi, adalah hasil sistem. Bukti tentang cara kerjanya dapat berupa log input-output, versi model, konfigurasi, dokumentasi pengujian, catatan pembaruan, atau rekaman intervensi manusia. Dalam sengketa yang mempersoalkan apakah keputusan otomatis diambil secara keliru, kategori kedua sering kali lebih penting untuk merekonstruksi proses dan menguji

hubungan sebab akibat. Pembedaan ini sejalan dengan kajian Grossman dan Grimm (2025) yang membedakan bukti yang diketahui dihasilkan AI dari bukti yang keasliannya dipersoalkan, meskipun kajian tersebut berfokus pada autentikasi dan admisibilitas, dengan pembahasan akses terbatas pada panduan praktis tentang *discovery* dan perintah perlindungan.

Karakteristik Bukti Algoritmik dan Ketimpangan Penguasaan Informasi

Bukti algoritmik memiliki empat ciri. Pertama, tersebar, karena informasi relevan bisa berada di aplikasi, server, penyedia *cloud*, sistem pencatatan, atau pihak ketiga. Kedua, dinamis, karena log dapat tertimpa, konfigurasi berubah, dan model diperbarui. Ketiga, teknis, sehingga pemahamannya dapat memerlukan ahli. Keempat, berpotensi sensitif, karena bukti dapat memuat data pribadi pengguna lain, rahasia dagang, informasi keamanan siber, atau informasi bisnis yang tidak terkait sengketa (Ameen et al., 2026). Sifat sistem AI yang tertutup atau berstatus kepemilikan sehingga sulit dijelaskan kepada para pihak dan pengadilan juga disoroti dalam literatur (Grossman & Grimm, 2025).

Ciri-ciri itu menimbulkan ketimpangan antara pihak yang dirugikan dan pihak yang mengendalikan sistem. Penggugat mungkin mengetahui waktu dan akibat keputusan, tetapi tidak mengetahui versi model atau data yang diproses. Sebaliknya, perusahaan menguasai catatan sistem dan dapat berdalih bahwa pembukaan informasi akan membongkar rahasia dagang atau data pihak ketiga (Republik Indonesia, 2000, 2022). Ketimpangan ini tidak berarti semua informasi internal wajib dibuka. Yang dibutuhkan adalah mekanisme seleksi agar hanya informasi yang relevan dan perlu untuk menguji dalil perkara yang dapat diakses.

Undang-Undang Pelindungan Data Pribadi menunjukkan bahwa pembentuk undang-undang telah menyadari risiko keputusan otomatis, karena memberi hak kepada subjek data untuk mengajukan keberatan atas keputusan yang hanya didasarkan pada pemrosesan otomatis, termasuk pemrofilan, yang menimbulkan akibat hukum atau berdampak signifikan (Republik Indonesia, 2022, Pasal 10 ayat 1). Hak tersebut dijabarkan lebih lanjut dalam Peraturan Pemerintah Nomor 33 Tahun 2026 (Republik Indonesia, 2026), tetapi pelaksanaannya diajukan kepada pengendali data pribadi (Republik Indonesia, 2022, Pasal 14), sehingga tidak menjawab bagaimana pihak yang dirugikan memperoleh bukti di persidangan perdata.

Untuk keperluan analisis, bukti algoritmik dapat dikelompokkan menjadi enam jenis. Jenis pertama adalah log peristiwa dan waktu, yaitu catatan kapan sistem menerima masukan dan menghasilkan keluaran. Kedua, identitas dan versi sistem, termasuk versi model atau perangkat lunak saat kejadian. Ketiga, catatan konfigurasi dan parameter yang relevan. Keempat, data masukan yang berkaitan langsung dengan penggugat, dengan data pihak lain disamarkan. Kelima, catatan intervensi atau pengawasan manusia. Keenam, dokumentasi validasi, pengujian, atau audit yang berhubungan dengan fungsi yang disengketakan. Pengelompokan ini merupakan kerangka analitis penulis, bukan daftar kewajiban pengungkapan yang saat ini berlaku umum di Indonesia, dan disusun dengan merujuk pada prinsip dokumentasi dan pencatatan dalam regulasi Uni Eropa (European Parliament & Council, 2024) serta kajian Ameen et al. (2026).

Pembukaan kode sumber secara menyeluruh pun tidak selalu diperlukan. Dalam banyak perkara, ringkasan teknis yang dapat diverifikasi, log peristiwa, dokumentasi versi, atau pemeriksaan oleh ahli independen sudah cukup menjawab pertanyaan hukum tanpa membuka seluruh arsitektur sistem. Prinsip pengungkapan minimal (*minimal disclosure*) penting agar hak untuk membuktikan tidak berubah menjadi akses tanpa batas terhadap aset intelektual perusahaan.

Kesenjangan Prosedural dalam Hukum Indonesia

Kesenjangan pertama adalah belum adanya prosedur khusus untuk meminta bukti algoritmik yang dikuasai lawan. Pasal 137 HIR dapat dipakai untuk melihat dokumen lawan yang telah diajukan, tetapi tidak mengatur permintaan terarah sebelum dokumen diajukan (Republik Indonesia, 1941; Waruwu, 2018). Padahal kebutuhan mengetahui keberadaan log dan dokumentasi dapat muncul sejak awal sengketa, bahkan sebelum gugatan didaftarkan, karena data teknis berpotensi terhapus oleh kebijakan retensi rutin.

Kesenjangan kedua berkaitan dengan preservasi. Bukti elektronik mudah berubah atau hilang. Jika penguasa sistem tidak punya kewajiban jelas untuk menahan penghapusan data setelah sengketa dapat diperkirakan secara wajar, pembuktian berisiko kehilangan bahan yang justru paling relevan. Kewajiban preservasi yang diusulkan bukan berarti seluruh data disimpan selamanya, melainkan dibatasi pada data yang relevan, jangka waktu yang proporsional, dan keadaan ketika pihak mengetahui

atau patut menduga sengketa akan timbul. Undang-Undang Dokumen Perusahaan mewajibkan penyimpanan dokumen keuangan selama sepuluh tahun dan menetapkan jangka waktu simpan dokumen lainnya menurut nilai gunanya melalui jadwal retensi (Republik Indonesia, 1997, Pasal 11), serta membebankan tanggung jawab atas kerugian kepada pimpinan perusahaan yang memusnahkan dokumen padahal diketahui atau patut diketahui dokumen itu masih harus disimpan (Pasal 19 ayat 3 huruf b). Definisi dokumen perusahaan yang luas (Pasal 1 angka 2) membuka kemungkinan log sistem tergolong dokumen lainnya, tetapi ketentuan ini tidak boleh ditafsirkan sebagai kewajiban khusus menyimpan seluruh log AI dalam setiap sengketa.

Kesenjangan ketiga adalah standar pemeriksaan rahasia. Data teknis dapat bercampur dengan rahasia dagang, data pribadi, atau informasi keamanan (Republik Indonesia, 2000, 2022). Tanpa prosedur penyaringan, pengadilan menghadapi dua risiko, yaitu menolak seluruh permintaan sehingga penggugat tidak dapat membuktikan dalilnya, atau memerintahkan pembukaan yang terlalu luas sehingga merugikan kepentingan sah penguasa data. Diperlukan pemeriksaan bertingkat yang mencakup penyamaran, ringkasan, pembatasan akses, dan pemeriksaan oleh ahli yang terikat kewajiban kerahasiaan.

Kesenjangan keempat berkaitan dengan akibat kegagalan mengungkapkan bukti. Hukum pembuktian perdata Indonesia tidak boleh diasumsikan otomatis menerapkan *adverse inference* pada setiap penolakan, karena ketentuan beban pembuktian tidak dengan sendirinya menetapkan akibat otomatis atas kegagalan membuka bukti (Republik Indonesia, 1847, Pasal 1865; 1927, Pasal 283; 1941, Pasal 163). Meski demikian, dapat dipertimbangkan pedoman bagi hakim untuk menilai perilaku penguasa bukti, alasan penolakannya, kewajiban penyimpanannya, dan apakah bukti hilang setelah sengketa dapat diperkirakan. Penilaian itu bertumpu pada kewenangan hakim menilai alat bukti, termasuk persangkaan (Republik Indonesia, 1927, Pasal 310; 1941, Pasal 173), dan hanya menjadi salah satu faktor dalam menilai seluruh alat bukti, bukan pengganti otomatis atas pembuktian unsur gugatan.

Pelajaran dari Perbandingan: Dokumentasi dan Pencatatan Sistem AI

Artificial Intelligence Act Uni Eropa mewajibkan dokumentasi teknis dan pencatatan log untuk kategori sistem AI tertentu, terutama yang berisiko tinggi (European Parliament & Council, 2024, Pasal 11, 12, dan 19). Hal ini menunjukkan bahwa dokumentasi dan log dipandang penting untuk keterlacakan, pemantauan, dan pengawasan. Namun, kewajiban tersebut dirancang dalam kerangka tata kelola dan kepatuhan AI, bukan sebagai aturan lengkap *discovery* dalam sengketa perdata. Aturan Eropa itu lebih tepat dijadikan rujukan tentang jenis dokumentasi dan pentingnya pencatatan, bukan disalin sebagai mekanisme acara perdata Indonesia.

Literatur tentang peradilan algoritmik juga menekankan bahwa pengujian legalitas keputusan algoritmik membutuhkan log, riwayat konfigurasi, dan jejak audit yang memadai; tanpa catatan, pengadilan sulit menilai bagaimana suatu keputusan terbentuk (Ameen et al., 2026). Kajian tersebut berada dalam konteks hukum administrasi pada sistem *common law*, sehingga dipakai di sini sebagai analogi, bukan sebagai padanan langsung bagi hukum acara perdata Indonesia. Pelajarannya, perlu dibedakan antara informasi yang dibutuhkan pihak yang dirugikan untuk memahami keputusan individual dan informasi lebih luas yang mungkin cukup diperiksa hakim atau ahli.

Dari sini lahir prinsip diferensiasi akses. Penggugat tidak selalu memerlukan seluruh dokumentasi teknis; ia memerlukan informasi yang cukup untuk mengidentifikasi dasar keberatan dan menguji keputusan yang berdampak padanya. Hakim mungkin memerlukan akses lebih luas untuk menilai relevansi, sementara ahli independen dapat memeriksa bagian yang terlalu sensitif untuk dibuka langsung kepada pihak lawan. Dengan begitu, tingkat pengungkapan dapat disesuaikan dengan tujuan dan sensitivitas informasi.

Rekonstruksi Model Pengungkapan Bukti Algoritmik

Berdasarkan analisis di atas, penelitian ini mengusulkan model pengungkapan enam tahap yang dapat diwujudkan melalui pedoman Mahkamah Agung atau pembaruan hukum acara perdata. Tahap pertama adalah preservasi terbatas. Pihak yang menguasai sistem mengambil langkah wajar untuk mencegah penghapusan atau perubahan bukti relevan setelah menerima pemberitahuan sengketa atau ketika secara objektif dapat memperkirakan proses hukum. Cakupannya meliputi log peristiwa, versi model, konfigurasi relevan, dan catatan intervensi yang terkait kejadian, dengan batas relevansi dan masa simpan agar tidak menjadi beban berlebihan. Standar "diketahui atau patut diketahui" yang sudah

dikenal dalam Pasal 19 ayat (3) huruf b Undang-Undang Dokumen Perusahaan (Republik Indonesia, 1997) dapat dijadikan analogi bagi pemicu kewajiban preservasi.

Tahap kedua adalah permintaan yang spesifik. Pemohon menguraikan keputusan AI yang disengketakan, rentang waktu, kategori informasi yang diminta, relevansinya dengan dalil gugatan atau bantahan, dan alasan mengapa informasi itu tidak dapat diperoleh dengan cara yang lebih ringan. Permintaan yang bersifat *fishing expedition*, atau meminta seluruh kode sumber tanpa penjelasan relevansi, patut ditolak atau dipersempit. Tahap ketiga adalah uji proporsionalitas oleh hakim. Hakim menimbang relevansi, kebutuhan, penguasaan atau kendali atas informasi, beban teknis dan biaya, risiko terhadap keamanan sistem, serta kemungkinan cara alternatif. Bila informasi dapat dibuktikan melalui ringkasan, sampel, atau laporan ahli, pembukaan data mentah yang lebih luas tidak perlu diperintahkan.

Tahap keempat adalah pengungkapan bertingkat. Tingkat pertama berupa ringkasan keputusan, identitas sistem, versi model, waktu pemrosesan, dan penjelasan faktor utama yang relevan. Tingkat kedua berupa log atau dokumentasi terpilih yang disamarkan. Tingkat ketiga berupa pemeriksaan terbatas oleh ahli independen (lihat juga Pasal 154 HIR tentang keterangan ahli; Republik Indonesia, 1941) atau pemeriksaan tertutup oleh hakim bila informasi sangat sensitif. Kode sumber hanya dipertimbangkan dalam keadaan luar biasa, ketika benar-benar diperlukan dan tidak ada alternatif yang memadai. Gagasan pembedaan penerima informasi, yaitu pihak yang dirugikan, pengadilan, dan ahli di bawah perlindungan, sejalan dengan matriks pengungkapan bertingkat yang dikembangkan Ameen et al. (2026) untuk *judicial review* keputusan algoritmik dan di sini diadaptasi ke hukum acara perdata Indonesia.

Tahap kelima adalah perlindungan kerahasiaan. Pengadilan dapat memerintahkan penyamaran data pribadi pihak ketiga, pembatasan penggunaan informasi hanya untuk perkara, larangan penyebarluasan, akses terbatas bagi kuasa hukum atau ahli, dan penyimpanan dokumen pada sarana yang aman. Rahasia dagang tidak boleh menjadi alasan otomatis menolak seluruh permintaan, tetapi menjadi faktor penting dalam menentukan bentuk dan tingkat akses (Republik Indonesia, 2000, 2022). Undang-Undang Rahasia Dagang sendiri memungkinkan hakim memerintahkan sidang tertutup atas permintaan para pihak dalam perkara perdata (Republik Indonesia, 2000, Pasal 18), dan praktik peradilan di Amerika Serikat mengenal perintah perlindungan (*protective orders*) untuk mengatasi klaim rahasia dagang dan kerahasiaan terkait bukti AI (Grossman & Grimm, 2025). Tahap keenam adalah konsekuensi atas ketidakpatuhan. Jika penguasa bukti tidak mematuhi perintah pengungkapan atau menghilangkan bukti relevan tanpa alasan yang dapat dibenarkan, hakim dapat mempertimbangkan perilaku itu dalam menilai bobot pembuktian dan kredibilitas penjelasan pihak tersebut. Penilaian harus memperhatikan apakah bukti memang dalam penguasaannya, apakah kewajiban preservasi sudah timbul, apakah kehilangan disebabkan kelalaian atau alasan teknis yang wajar, dan apakah pemohon telah menunjukkan relevansi bukti. Konsekuensi ini tidak boleh otomatis memenangkan penggugat.

Model tersebut dapat dituangkan dalam pedoman teknis yang mengatur format permintaan, tenggat jawaban, standar preservasi, tata cara pemeriksaan tertutup, penggunaan ahli, dan pengamanan data. Dalam jangka panjang, pembaruan hukum acara perdata dapat memberi dasar yang lebih tegas bagi perintah pengungkapan dokumen dan data elektronik yang dikuasai pihak lawan. Tabel 1 merangkum rancangan model yang diusulkan.

Tabel 1 Rancangan Mekanisme Pengungkapan Bukti Algoritmik

Tahap	*Tindakan*	*Pengaman Hukum*
Preservasi	Menahan penghapusan log dan dokumentasi relevan setelah sengketa dapat diperkirakan	Relevansi, batas waktu, dan beban wajar
Permintaan	Menyebut kategori data, periode, peristiwa, dan kaitannya dengan dalil	Larangan permintaan spekulatif
Penilaian hakim	Menguji relevansi, kebutuhan, penguasaan, biaya, dan risiko	Uji proporsionalitas
Pengungkapan	Ringkasan, data tersamarkan, atau pemeriksaan ahli bertingkat	Akses minimum yang diperlukan
Kerahasiaan	Pembatasan akses, penyamaran, perintah kerahasiaan	Perlindungan data pribadi dan rahasia dagang
Ketidakpatuhan	Menilai alasan penolakan atau hilangnya bukti dalam pembuktian	Tidak ada kemenangan otomatis; penilaian kasus per kasus

Implikasi terhadap Asas Pembuktian dan Perlindungan Para Pihak

Model ini tidak menghapus prinsip bahwa pihak yang mendalilkan suatu hak atau peristiwa wajib membuktikannya; beban pembuktian tetap menjadi titik tolak (Republik Indonesia, 1847, Pasal 1865; 1941, Pasal 163). Yang perlu diperhatikan adalah siapa yang secara nyata menguasai bukti dan apakah pemohon punya peluang yang wajar untuk memperolehnya. Akses terhadap bukti adalah prasyarat agar beban pembuktian dapat dijalankan secara bermakna. Usulan pengungkapan dalam penelitian ini dimaksudkan untuk mengatasi ketimpangan akses bukti, bukan menghapus beban pembuktian pihak yang mendalilkan hak.

Model ini juga tidak menjadikan penyedia AI selalu bertanggung jawab atau selalu wajib membuka seluruh sistem. Kewajiban pengungkapan melekat pada pihak yang menguasai atau mengendalikan informasi relevan, baik penyedia, pengembang, operator, maupun pengguna institusional, menurut fakta perkara dan hubungan hukumnya. Jika data berada pada pihak ketiga, hakim perlu mempertimbangkan dasar hukum dan prosedur yang tersedia untuk memperolehnya.

Dari sisi pelindungan data pribadi, pengungkapan harus bertujuan sah, terbatas pada data yang diperlukan, dan disertai pengamanan; informasi pribadi pihak lain dapat disamarkan atau dipisahkan (Republik Indonesia, 2022). Dari sisi rahasia dagang, perlindungan hanya diberikan bagi informasi yang bersifat rahasia, bernilai ekonomi, dan dijaga kerahasiaannya (Republik Indonesia, 2000, Pasal 3 ayat 1), sehingga klaim rahasia dagang perlu diuji terhadap unsur-unsur tersebut, dan akses dapat diberikan hanya kepada ahli atau kuasa hukum yang terikat kewajiban kerahasiaan. Jadi, transparansi prosedural tidak sama dengan transparansi publik atau pembukaan seluruh rahasia komersial.

Pada akhirnya, ukuran keberhasilan model ini bukan banyaknya data yang dibuka, melainkan apakah informasi yang diperlukan untuk menguji keputusan AI dapat diperoleh secara adil, aman, dan proporsional. Pengadilan harus mampu menyeimbangkan hak pihak untuk membuktikan dalilnya dengan hak pihak lain atas kerahasiaan, keamanan sistem, dan pelindungan data.

KESIMPULAN

Hukum Indonesia telah mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah melalui UU ITE, sehingga catatan sistem AI pada prinsipnya dapat dipakai sebagai bukti selama memenuhi syarat keutuhan, keterjangkauan, dan keandalan. Pasal 137 HIR juga memberi dasar bagi pihak berperkara untuk melihat surat lawan yang diajukan kepada hakim, tetapi kedua dasar tersebut belum membentuk mekanisme komprehensif untuk memperoleh bukti algoritmik yang belum diajukan, menjaga log ketika sengketa dapat diperkirakan, dan memeriksa informasi teknis yang memuat rahasia dagang atau data pribadi. Karena bukti algoritmik bersifat tersebar, dinamis, teknis, dan berpotensi sensitif, ketimpangan penguasaan dapat menghambat pihak yang dirugikan membuktikan proses keputusan AI. Penelitian ini mengusulkan model bertahap yang meliputi preservasi terbatas, permintaan spesifik, uji proporsionalitas oleh hakim, pengungkapan berjenjang, perlindungan kerahasiaan, dan penilaian ketidakpatuhan secara kasus per kasus. Model tersebut dapat dikembangkan melalui pedoman Mahkamah Agung dan dipertimbangkan dalam pembaruan hukum acara perdata, sementara penyedia

dan pengguna AI perlu menyusun tata kelola dokumentasi dan retensi log yang sebanding dengan risiko sistem agar proses keputusan dapat diperiksa tanpa membuka informasi yang tidak relevan.

DAFTAR PUSTAKA

Ameen, K. S., Towfiq, T. A., Mousa, K. M., & Pooyanmehr, M. (2026). Judicial review of algorithmic administrative systems: Legality, evidence and remedies in the smart city state. *Frontiers in Artificial Intelligence, 9*, Article 1802986. https://doi.org/10.3389/frai.2026.1802986

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.

Fakhriah, E. L. (2020). Penemuan hukum oleh hakim melalui pembuktian dengan menggunakan bukti elektronik dalam mengadili dan memutus sengketa perdata. *Jurnal Bina Mulia Hukum, 5*(1), 89–102. https://doi.org/10.23920/jbmh.v5i1.50

Grossman, M. R., & Grimm, P. W. (2025). Judicial approaches to acknowledged and unacknowledged AI-generated evidence. *Columbia Science and Technology Law Review, 26*(2), 110–155. https://doi.org/10.52214/stlr.v26i2.13890

Mahkamah Agung Republik Indonesia. (2019). *Peraturan Mahkamah Agung Nomor 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan secara Elektronik* (Berita Negara Republik Indonesia Tahun 2019 Nomor 894).

Republik Indonesia. (1847). *Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek), Staatsblad 1847 Nomor 23*.

Republik Indonesia. (1927). *Rechtsreglement Buitengewesten (RBg), Staatsblad 1927 Nomor 227*.

Republik Indonesia. (1941). *Herzien Inlandsch Reglement (HIR), Staatsblad 1941 Nomor 44*.

Republik Indonesia. (1997). *Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan*.

Republik Indonesia. (2000). *Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang*.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

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

Republik Indonesia. (2026). *Peraturan Pemerintah Nomor 33 Tahun 2026 tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Soroinda, D. L., & Nasution, A. A. R. S. (2022). Kekuatan pembuktian alat bukti elektronik dalam hukum acara perdata. *Jurnal Hukum & Pembangunan, 52*(2), 384–405. https://doi.org/10.21143/jhp.vol52.no2.1474

Waruwu, R. P. R. (2018). *Eksistensi dokumen elektronik di persidangan perdata*. Mahkamah Agung Republik Indonesia. https://www.mahkamahagung.go.id/id/artikel/3048/eksistensi-dokumen-elektronik-di-persidangan-perdata