Formosa Journal of Applied Sciences (FJAS)
Vol. 5, No. 11 2026: 2361-2374

Artificial Intelligence-Based Evidence in Indonesian Civil Justice: Reconstructing Standards of Admissibility and Reliability

Chandera Halim
Universitas Atma Jaya Yogyakarta
Corresponding Author: Chandera Halim h.chandera@uajy.ac.id

A R T I C L E I N F O

Keywords: Artificial Intelligence, Electronic Evidence, Civil Litigation, Admissibility, Reliability

Received : 10, July
Revised : 12, September
Accepted: 14, November

©2026 Halim: This is an open-access article distributed under the termsof the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

Digital transformation has altered both the transactions that give rise to civil disputes and the materials used to prove them. This article reconstructs standards for admitting and evaluating artificial intelligence-based evidence in Indonesian civil proceedings. Using normative legal research, statutory interpretation, and functional comparison, it examines Indonesian electronic-evidence rules alongside international principles of authentication, technical reliability, and procedural fairness. The findings distinguish evidence generated by artificial intelligence from conventional records merely processed by artificial intelligence and identify gaps concerning provenance, model validation, explanation, and adversarial testing. The article proposes a four-stage judicial assessment encompassing legal admissibility, authenticity, methodological reliability, and contestability, with proportional disclosure obligations and human judicial control. This framework preserves technological neutrality while preventing automated outputs from acquiring unwarranted evidential authority.

DOI prefik: https://doi.org/10.55927/fjas.v5i11.148
ISSN-E: 2962-6447
https://journalfjas.my.id/index.php/fjas

INTRODUCTION

Digital transformation has altered both the transactions that give rise to civil disputes and the materials used to prove them. Contract negotiations occur through messaging platforms, payments generate machine-readable records, and business decisions increasingly depend on predictive systems. Courts consequently encounter electronic correspondence, server logs, automated reports, synthetic media, and analyses prepared with machine-learning tools. These items may look similar when printed or uploaded into an electronic court file, yet they differ fundamentally in how they were produced and how their accuracy can be examined. The essential legal question is no longer whether a document has electronic form, but whether its asserted content is sufficiently connected to a verifiable event, process, or source.

Artificial intelligence (AI) complicates proof in at least three directions. A system may create original-looking text, images, or voices without recording any underlying historical event. It may classify or summarize authentic transaction records while obscuring selection errors and uncertain inferences. Alternatively, an expert may employ a validated analytical tool to examine a disputed image, signature, or account. Each setting presents a distinct evidentiary claim. A generated statement is not automatically evidence that the statement is true, just as an automated classification is not a substitute for explaining the method by which the classification was reached. The technical ability to produce convincing outputs therefore increases the importance of legally meaningful scrutiny (Chesney & Citron, 2019; Surden, 2019).

Indonesian civil procedure possesses an established evidentiary structure but has not been organized specifically around machine-generated inferences. Article 164 of the Herziene Indonesisch Reglement (HIR) and Article 1866 of the Indonesian Civil Code traditionally identify documentary evidence, witnesses, presumptions, admissions, and oaths. Electronic proof subsequently gained express recognition through Law No. 11 of 2008 on Electronic Information and Transactions, as amended, including by Law No. 1 of 2024. Its Article 5 recognizes electronic information, electronic documents, and their printouts as lawful evidence and describes them as an extension of admissible procedural evidence (Republic of Indonesia, 2024). Recognition, however, does not establish that every digital assertion is authentic, methodologically dependable, or persuasive.

Institutional digitalization likewise must not be confused with substantive validation of evidence. Supreme Court Regulation No. 1 of 2019, amended by Supreme Court Regulation No. 7 of 2022, facilitates electronic case administration and hearings. It does not, merely by permitting electronic proceedings, certify the factual accuracy of every file submitted through them (Supreme Court of Indonesia, 2022). The distinction is practically important when a litigant submits an AI-produced reconstruction of a conversation, an automated valuation of disputed property, or a machine-generated chronology. Efficient filing and reliable adjudication are separate legal objectives and must be governed by complementary safeguards.

Current scholarship helps diagnose this problem but does not supply an Indonesian civil-procedure test in ready-made form. Work on algorithmic opacity identifies technical, institutional, and interpretive obstacles to scrutiny, while scholarship on accountable algorithms explains how auditing and procedural verification can improve oversight (Burrell, 2016; Kroll et al., 2017). Research on explanatory models and counterfactual reasoning further suggests that an output may be understandable without revealing every computational parameter (Wachter et al., 2018). Yet the legal consequences of insufficient explanation differ according to whether AI is the alleged source of a fact, a processing instrument, or merely support for an expert opinion. The present inquiry places those differences at the center of evidence doctrine.

This article develops an original, proportionate assessment framework rather than advocating categorical acceptance or exclusion of AI-based materials. It examines how Indonesian courts can distinguish a threshold for receiving evidence from the later determination of evidential weight, require adequate provenance and methodological foundations, and preserve the opposing party's opportunity to challenge contested outputs. It asks how existing Indonesian civil-evidence rules should be interpreted when AI contributes to an exhibit, which comparative principles are functionally transferable, and what procedural safeguards could reconstruct admissibility and reliability without converting judges into software engineers or shifting the burden of proof unfairly.

LITERATURE REVIEW

Electronic Evidence and the Separation of Admissibility from Weight

Admissibility and evidential weight address different legal questions. Admissibility asks whether material may properly enter the judicial record under applicable procedural rules. Evidential weight concerns the degree to which that material supports a disputed proposition after scrutiny of source, integrity, context, and competing explanations. The distinction matters because a legally recognized electronic file may contain false information, an authentic recording may be misleadingly edited, and a technically accurate computation may answer an irrelevant question. The UNCITRAL Model Law on Electronic Commerce makes this separation explicit: Article 9 protects data messages against rejection merely because of electronic form while directing attention to the reliability of generation, storage, communication, integrity, and identification of the originator (UNCITRAL, 1996).

An evidence framework for AI should preserve the same distinction while adding an inquiry into transformation. Ordinary digital records generally purport to document an event occurring outside the computer system. Generative outputs may instead be new informational objects produced through statistical inference. Accordingly, proof that an AI output was genuinely created at a stated time does not prove the event described in the output occurred. Similarly, an algorithmic calculation can be reproducible but based on missing or biased data. Treating the admissibility of a file as conclusive proof of its content collapses these separate inquiries and risks undermining the right to rebut disputed evidence.

Algorithmic Opacity, Reliability, and Explainability

Burrell (2016) distinguishes secrecy, limited technical literacy, and intrinsic computational complexity as sources of algorithmic opacity. This classification has procedural implications. Contractual confidentiality may call for protected judicial disclosure; a lack of technical literacy may justify expert assistance; and complex model behavior may require validation and performance evidence rather than simplistic demands for an intuitive explanation. No single disclosure requirement resolves every problem. The legal aim should be adequate review of the claim actually made, not a theatrical display of computer code that judges and litigants cannot meaningfully use.

Accountability scholarship also cautions against equating transparency with legal correctness. Independent testing, procedural consistency, documentation, and external verification can establish whether a system performs within a justified range even when its internal mechanics are difficult to explain (Kroll et al., 2017). Counterfactual explanations may reveal how changes to relevant inputs affect an automated conclusion, but they cannot by themselves prove that underlying data are true or that an output reliably captures causation (Wachter et al., 2018). In litigation, therefore, interpretability is one component of reliability and contestability; it is neither an automatic admission ticket nor an independent evidentiary category.

The National Institute of Standards and Technology frames trustworthy AI in terms of validity, reliability, safety, accountability, transparency, explainability, privacy, and fairness (Tabassi, 2023). Its generative-AI profile identifies risks particular to probabilistic content generation and deployment contexts (Autio et al., 2024). These frameworks are not Indonesian procedural laws. Their value lies in supplying a vocabulary for evidence-specific questions: whether inputs were representative, whether the relevant model version was recorded, whether known limitations were disclosed, whether errors can be reproduced, and whether the output remains useful for the precise proposition for which it is offered.

Procedural Justice and the Parties' Right to Challenge

Civil evidence is relational: a court evaluates a claim after giving affected parties a meaningful opportunity to respond. When one party relies on an opaque technological process, practical inequality may arise if the other party cannot identify what was analyzed, how the result was obtained, or which assumptions influenced it. Such inequality is not necessarily corrected by formal permission to object. Effective contestation requires a comprehensible claim, access to material explanatory information, and a reasonable opportunity to obtain independent examination. These safeguards translate general ideas of adversarial fairness into concrete procedural obligations without presuming that technology is inherently unreliable.

The conceptual framework adopted here connects four dimensions in sequence: legal permissibility, provenance and authenticity, methodological reliability, and procedural contestability. The first two establish whether an item is properly characterized and sufficiently identified; the third addresses the soundness of any automated inference; and the fourth tests whether asserted foundations can be examined and rebutted. Evidential weight is assessed only after considering all four. Although the sequence provides analytical discipline, serious defects discovered at a later stage can require renewed consideration of admission, targeted disclosure, diminished weight, or exclusion where justified by existing law and procedural fairness.

METHODOLOGY

This study applies normative or doctrinal legal research with statutory, conceptual, and functional-comparative approaches. The primary Indonesian materials are the HIR, the Civil Code, the Electronic Information and Transactions Law as amended through Law No. 1 of 2024, Government Regulation No. 71 of 2019, Law No. 27 of 2022 on Personal Data Protection, and the Supreme Court's electronic-proceedings framework. Comparative reference points include Article 9 of the UNCITRAL Model Law on Electronic Commerce, Rules 901 and 702 of the United States Federal Rules of Evidence, and the European Union Artificial Intelligence Act. Secondary materials comprise peer-reviewed legal and interdisciplinary scholarship and published technical governance frameworks.

The analysis proceeds through three operations. First, doctrinal interpretation identifies the objectives and limits of recognition of electronic information as evidence. Second, functional comparison examines how other instruments separate authentication, expert reliability, judicial oversight, and evidential weight without assuming that foreign procedural rules apply directly in Indonesia. Third, normative synthesis converts these principles into a proposed judicial assessment model tailored to ordinary civil disputes. The unit of analysis is the evidentiary claim made through an AI-related exhibit, not a surveyed litigant or a particular commercial system. Consequently, no interviews, court-file dataset, technical benchmark experiments, or statistical hypothesis tests are claimed.

The research is bounded to civil litigation, particularly contractual, commercial, consumer, and other private-law disputes in which an AI-created or AI-processed item is tendered to prove a fact. It does not propose a new form of evidence outside existing legislation, validate particular AI products, or claim that Indonesian courts have adopted the reconstructed test. Findings are doctrinal conclusions and prospective recommendations; the illustrative scenarios below serve to demonstrate how a procedural rule might operate rather than to represent verified judicial cases.

RESEARCH RESULT

Existing Indonesian Law Recognizes Electronic Form but Leaves AI-Specific Questions Open

The first finding is that Indonesian law supplies a clear starting point for electronic admission but only a partial account of AI reliability. Article 5(1) and (2) of the Electronic Information and Transactions Law, as amended in 2024, recognize electronic information, documents, and printouts and place them within the expansion of evidence admitted by procedural law. Article 5(3) links validity to the use of an electronic system consistent with that law, while Article 5(4) recognizes that another statute may provide otherwise (Republic of Indonesia, 2024). The provision addresses legal form and system conformity; it does not create a universal presumption that content produced by any AI model corresponds to external reality.

Government Regulation No. 71 of 2019 supplies relevant operational criteria. Its Articles 3 and 4 require electronic-system providers to maintain reliable and secure systems and address retrievability, availability, integrity, authenticity, confidentiality, and accessibility of electronic information (Republic of Indonesia, 2019). Such obligations support a provenance inquiry, especially where a document originated within a managed service. Nevertheless, evidence from an appropriately operated platform can still contain inaccurate user inputs, defective algorithms, incomplete source records, or misleading summaries. Compliance evidence should therefore inform authenticity and system integrity, not displace substantive evaluation of an AI-generated inference.

A further source is Law No. 27 of 2022 on Personal Data Protection. Article 64(3) recognizes, in disputes within that law, both procedurally established forms of evidence and electronic information or documents under applicable legislation. Article 64 also allows closed proceedings when needed to protect personal data (Republic of Indonesia, 2022). The implications extend beyond privacy litigation: disclosure of training examples, customer records, or medical information in support of AI evidence may conflict with confidentiality interests. Effective evidentiary scrutiny must consequently employ data minimization, access restrictions, and appropriate protective measures rather than demanding unbounded disclosure of every dataset.

Distinguishing Four Evidentiary Forms

The second finding is that the label 'AI evidence' obscures materially different categories. The first consists of native electronic records subsequently processed by AI, such as an authentic invoice database summarized by a language model. Here, the underlying records are the principal evidence and the summary is a potentially fallible aid. The second consists of AI-generated content offered to prove the fact of its own creation, such as a synthetic advertisement relevant to a consumer-deception claim. The creation of that content may be directly material, provided its origin and timing are demonstrated.

The third category comprises AI-generated representations offered as proof of another event, including recreated voices, imagined contract terms, or reconstructed photographs. This category presents a heightened risk of mistaking simulation for observation. The fourth consists of AI-assisted expert analysis, such as anomaly detection in payment records or automated comparison of disputed images. Its probative value depends on expert competence, valid input data, a method suitable for the task, and intelligible limits. The classification is functional rather than product-based: a single software tool may occupy different categories in different cases, depending on the proposition advanced by the party presenting it.

This taxonomy avoids two symmetrical errors. A court should not exclude every AI-involved record because an algorithm touched it; routine sorting, search, and extraction are familiar features of digital litigation. Yet it should not accept a fluent generated narrative as the equivalent of a contemporaneous record or human witness. The litigant must identify the evidentiary proposition, the original source, the nature and extent of AI intervention, and the inferential distance between output and event. That statement of purpose is the foundation for all subsequent assessment.

Proposed Four-Stage Judicial Assessment

The third finding is a four-stage assessment that is deliberately more precise than a single 'authenticity' question. Stage one, legal admissibility, asks whether the item is relevant to an issue in dispute, capable of lawful presentation under applicable evidentiary rules, and subject to any specific statutory limitation. Legal recognition of electronic documents usually resolves the objection based solely on format, not the merits of the claim. Where material is unlawfully acquired or intrudes upon protected data, the court should separately evaluate the governing legal consequences rather than treating AI involvement itself as the disqualifying factor.

Stage two, provenance and authenticity, asks what the item is and whether it is what the proponent claims. A minimally adequate foundation can include the creator or system operator, date and mode of acquisition, original data source, metadata, file hashes where available, custody history, preservation procedures, and disclosure of modifications. A hash can demonstrate that a file has not changed since a recorded point, but cannot prove that the original information was truthful. Similarly, metadata may be incomplete or manipulated; its significance must be judged alongside corroborating records and testimony. Authenticity is therefore a contextual finding rather than a mechanical box to tick.

Stage three, methodological reliability, applies when a litigant asks the court to draw an inference produced through AI. The judge should examine the system's intended use, relevant model version, input quality, verification procedure, known limitations, performance on comparable data, susceptibility to error, and whether a human checked the output against primary sources. A generative system's verbal certainty is not performance evidence. Nor does an asserted accuracy rate settle reliability when the validation population differs

from the dispute at hand. The appropriate question is whether the method is reasonably dependable for the narrowly defined factual task the output purports to perform (Tabassi, 2023).

Stage four, adversarial contestability, examines whether the opposing party has a realistic chance to challenge those foundations. Required information should be proportionate to the importance of the disputed conclusion and the burden of obtaining it. A disputed automated credit calculation may justify relevant input tables, model documentation, validation summaries, and expert questioning; a minor AI-generated chronology already checked against disclosed emails may require far less. Where trade secrets or personal information are implicated, disclosure to a neutral expert or under confidentiality conditions may protect legitimate interests while maintaining meaningful judicial review.

These stages should be recorded as distinct findings in judicial reasoning. Failure at the threshold of legal admissibility may prevent an item from being received. A remediable weakness in provenance may justify a request for further authentication. A methodological flaw or a failure to disclose limitations may justify reduced weight, expert examination, or, where legally warranted, refusal to rely on the inference. Contestability may demand procedural accommodation before the evidence is assessed. The proposed framework therefore offers graduated responses instead of imposing an inflexible sanction for every informational gap.

Evidentiary Foundation and Proportional Judicial Responses

A practical foundation statement can be attached to AI-related exhibits. It would identify the submitting party, disputed proposition, source records, tool name or category, system or model version if known, date of processing, human operations performed, alteration history, method of validation, and access available for challenge. The statement is not a proposed substitute for existing forms of proof or a guarantee of truth. Its purpose is to make the evidentiary claim inspectable at an early stage, allowing the judge to select proportionate directions for supplementation and reducing surprise in later hearings.

Consider a supplier who files an AI-generated account reconciliation in a payment dispute. The underlying bank statements and invoices may be authentic, while the automated reconciliation mistakenly merges transactions from customers with similar names. Under the proposed test, admissibility of the electronic records would not be the primary problem. Instead, the supplier should produce the underlying entries, describe matching rules, disclose exceptions, and permit comparison of disputed transactions. The judge could accept the original documents while giving little or no independent weight to the unverified automated summary. This response preserves useful technology without rewarding undocumented inference.

A second illustration involves a purported recording of a commercial conversation. If a party tenders an audio file without explaining whether it captures an actual conversation or was reconstructed by a voice-generation model, provenance becomes decisive. Spectral analysis or detection software may assist, but detectors can generate false positives and negatives; they should not be regarded as infallible arbiters of authenticity. Corroborating communications, device records, witnesses, and chain-of-custody information may be more informative than a single detector score (Chesney & Citron, 2019). The court must distinguish proof that a file exists from proof that the speakers actually uttered its contents.

A third illustration concerns property valuation supported by automated predictions. The parties may agree that the program accurately generated the displayed number but disagree whether its training examples, location features, or market period justify application to the disputed property. A qualified expert should explain material assumptions and benchmark the result against appropriate comparable transactions. A model whose methodology is unavailable need not be categorically rejected, but the proponent must provide sufficient substitute validation to make the asserted inference contestable. Otherwise, the court should limit reliance on the automated figure in favor of better-supported valuation evidence.

Table 1. Proposed Judicial Assessment of AI-Based Evidence

Stage	Central Inquiry	Illustrative Foundation
Legal admissibility	Is the exhibit lawfully receivable?	Relevance; applicable procedural rule
Provenance and authenticity	What is the source and alteration history?	Original record; metadata; custody
Methodological reliability	Can the particular inference be trusted?	Validation; inputs; error limitations
Adversarial contestability	Can the opponent meaningfully test the claim?	Explanations; targeted access; expert review

Source: Authors' Normative Synthesis.

DISCUSSION

The Doctrinal Gap Is Inferential, Not Merely Technological

The results show that reconstruction should begin with a conceptual correction. Indonesian electronic-evidence legislation answers an important question about form but does not eliminate the ordinary need to prove a fact. Because AI can generate content and derive predictions, a court must examine the inferential relationship among source data, model operations, and the disputed proposition. That relationship may be direct when a synthetic advertisement itself constitutes the allegedly unlawful representation, but indirect when a chatbot's account of negotiations is advanced as proof that specified negotiations occurred. Reliability standards must track the evidentiary purpose rather than the mere presence of software.

The approach responds to a familiar danger in digital litigation: technical aesthetics can create false confidence. Precise percentages, polished language, interactive dashboards, and apparently scientific images encourage an impression of objectivity. Yet a detailed output may conceal missing inputs, inappropriate proxies, or arbitrary assumptions. Conversely, a technically simple spreadsheet that transparently reproduces documented transactions may be highly persuasive. Judicial reasoning should therefore explain why the method and evidence support the particular inference, rather than treating sophistication as a proxy for truth. In this sense, evidence doctrine disciplines technology without requiring hostility toward it.

Lessons from Comparative Evidence and AI Governance

Comparative sources support a differentiated assessment. Article 9 of the UNCITRAL Model Law explicitly addresses the distinction between the admissibility of data messages and the weight attached to their reliability, origin, and integrity (UNCITRAL, 1996). It is a model law, not a directly applicable Indonesian procedural code. Its functional contribution is nonetheless substantial: electronic form is not itself a reason for rejection, while the process by which information was generated and preserved remains relevant to factual evaluation. This offers a useful interpretive analogy for the treatment of both ordinary and AI-transformed digital records.

United States Federal Rule of Evidence 901(a) requires an adequate basis to identify an item as what its proponent claims, and Rule 901(b)(9) provides an example involving evidence describing a process or system and showing that it produces an accurate result (United States, n.d.-b). Rule 702, including the clarification made in 2023, imposes a reliability-oriented threshold for expert opinions, encompassing sufficient facts, reliable methods, and reliable application (United States, n.d.-a). These rules belong to a different procedural system; Indonesia should not mechanically import their burdens, evidentiary categories, or standards of proof. Their transferable lesson is that computer-generated inferences require demonstrable foundations and that professional expertise does not immunize a methodology from scrutiny.

The European Union Artificial Intelligence Act identifies certain AI systems intended to assist judicial authorities in researching or interpreting facts and law as high-risk systems under Annex III, point 8(a) (European Union, 2024). Its subject is AI governance rather than a comprehensive civil-evidence code, and the classification of judiciary-facing tools should not be confused with a rule governing every party-produced exhibit. Nevertheless, its attention to risk, documentation, human oversight, and governance strengthens the argument that adjudication requires traceable and reviewable machine assistance. Its regulatory design is best treated as comparative policy guidance, not as legislation already effective within Indonesian courts.

Burdens of Production, Expert Assistance, and Access to Information

The party relying on AI-derived evidence should ordinarily explain its source, function, and claimed accuracy because that party selected the material and knows which inference it seeks. This proposed burden of production does not purport to amend existing Indonesian allocations of proof. The opposing party should not be required to disprove an unidentified model before learning what information it processed. When an initial foundation is produced, the court can determine whether an objection identifies a material concern and whether targeted verification is necessary for a fair decision.

Expert assistance is valuable when a dispute turns on model validation, digital forensics, statistical inference, or system architecture. However, expertise should not become an expensive mandatory ritual for every electronic document. A judge can often verify an AI-prepared timeline by checking citations against source correspondence, or test a simple calculation against disclosed ledgers. Specialized assistance is more appropriate when conclusions cannot be independently checked without technical methods. Expert explanations should address the factual question, relevant error mechanisms, comparison data, and uncertainty rather than relying on unexplained confidence scores or prestige derived from software branding.

Disclosure deserves particular care because AI systems may incorporate confidential business records, third-party personal data, or proprietary designs. Unlimited access to complete training datasets or source code may be unnecessary, technically impractical, and harmful. The principle of proportionality calls for the least intrusive disclosure capable of supporting a fair challenge: selected source records, version history, meaningful feature descriptions, validation results, logs, or a confidential expert review. Indonesia's personal-data framework and electronic-system obligations support attention to confidentiality and integrity, though a detailed discovery mechanism would require explicit procedural development (Republic of Indonesia, 2019, 2022).

Cost asymmetry presents a related access-to-justice concern. A major platform may possess sophisticated documentation, while an individual consumer may lack funds to challenge an algorithmic denial or calculation. A formal right to contest can become illusory when the necessary information is controlled by the opposing party. Judicial case management should account for that imbalance through early identification of disputed technical questions, focused requests for information, realistic timelines, and limits on irrelevant demands. A proportionate foundation also benefits smaller litigants because it prevents AI evidence disputes from becoming open-ended contests over every component of a commercial system.

A Structured Reason-Giving Model for Civil Judges

Reasoned judgments should distinguish four propositions often conflated in practice. First, an exhibit may be a legally recognized electronic document. Second, a file may be attributable to a particular source and shown to have remained intact. Third, a technical method may be sufficiently valid for a specified analytical task. Fourth, after examination alongside other proof, its content may support the ultimate factual finding. Recording these propositions separately makes appellate or scholarly review more intelligible and discourages unexplained reliance on automated outputs.

Judges need not reproduce technical manuals. A concise explanation may identify the source records, material method, validation or corroboration, objections considered, and reason for giving particular weight. For example, a judgment might state that an AI-generated spreadsheet was admitted as an electronic document, that its inputs were authenticated by bank records, that a disputed matching procedure remained unvalidated, and that only individually verified entries were relied upon. Such reasoning explains both technological use and judicial independence. It also signals to future litigants which forms of evidentiary preparation are likely to be helpful.

The proposed assessment should avoid a universal numerical reliability threshold. Accuracy figures depend on the task, reference standard, deployment population, and costs of false positives and false negatives. A detector suitable for screening suspicious media may be inappropriate as the sole basis for deciding whether a recording is fabricated. A prediction model validated on national housing data may be weak when applied to one unusual parcel. Judicial standards should therefore ask for justified performance evidence and independent corroboration where available, rather than declaring that every AI system exceeding an arbitrary percentage is legally reliable.

Implementation Pathway and Institutional Safeguards

Implementation could proceed incrementally through Supreme Court guidance, judicial training, and standardized filing information, while matters requiring substantive legal change remain for legislation. Parties could be directed to disclose material AI involvement where a disputed evidentiary proposition depends on synthetic generation or automated inference. The obligation should not extend to incidental spelling correction, formatting, or ordinary document searches. Such tailoring concentrates procedural resources on technologies capable of altering factual conclusions and avoids imposing costly duties on ordinary electronic filings.

Third, court-supported expertise and confidential review mechanisms should be developed cautiously. An independent expert should be appointed for a defined technical question, subject to disclosed qualifications and potential conflicts of interest. Parties need a meaningful opportunity to examine the expert's assumptions and conclusions. Protective arrangements should restrict access to sensitive records while permitting enough scrutiny for fairness. Any procedural direction must remain consistent with existing Indonesian law and cannot be presented as an already enacted discovery regime. Institutional

safeguards are most legitimate when they supplement, rather than silently replace, the judge's duty to determine facts.

CONCLUSIONS AND RECOMMENDATIONS

Indonesian civil-procedure law recognizes electronic information and documents, but recognition of form does not independently establish authenticity or reliability. The principal doctrinal gap lies between source integrity and the inferential validity of AI-generated output. Native records processed by AI, synthetic content offered as an object of dispute, reconstructed representations of alleged events, and AI-assisted expert analysis require different foundations. A rule treating all these materials as equally trustworthy—or equally inadmissible—would fail to respect their differing evidentiary functions and the ordinary demands of civil proof.

This study proposes a four-stage model comprising legal admissibility, provenance and authenticity, methodological reliability, and adversarial contestability. The model draws on Indonesian positive law while using international and comparative instruments only for functional guidance. Judges should make distinct, reasoned findings concerning the disputed proposition, available source records, relevant technical limitations, and opportunities for challenge. Where deficiencies arise, responses should be proportionate: further authentication, targeted disclosure, qualified expert assistance, reduced evidential weight, or exclusion only when warranted by applicable law. Automated output must never substitute for accountable judicial evaluation.

The Supreme Court should consider guidance on disclosure of material AI involvement, proportionate evidentiary foundation statements, technical expert assistance, and protected access to sensitive verification material. Legal practitioners should preserve original records and document meaningful transformations before presenting AI-derived exhibits. Courts should encourage corroboration and assess whether the proposed method fits the facts in dispute. Together these measures would modernize civil proof without changing the fundamental allocation of judicial responsibility or treating any particular technology as inherently trustworthy.

ADVANCED RESEARCH

This doctrinal study does not measure judicial practices, test the accuracy of AI products, or establish how often Indonesian litigants submit synthetic evidence. It also does not resolve every problem of unlawfully obtained data, professional liability, or cross-border production. Further research should examine published civil judgments and anonymized case files, interview judges and practitioners about technical evidentiary disputes, and test the proposed checklist against realistic records with known errors. Comparative inquiry into protective disclosure and expert appointment could help identify procedures compatible with Indonesian civil litigation. Such work should evaluate cost, accessibility, and actual improvement in reason-giving rather than assuming greater disclosure is always better.

ACKNOWLEDGMENT

The author acknowledges the scholarly contributions of the legal and technical literature consulted. No external research funding or empirical collaboration is claimed for this manuscript.

REFERENCES

Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). https://doi.org/10.6028/NIST.AI.600-1.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 1–12. https://doi.org/10.1177/2053951715622512.

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J.

European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689.

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705. https://pennlawreview.com/2017/02/23/accountable-algorithms.

Republic of Indonesia. (2019). Government Regulation No. 71 of 2019 on Electronic Systems and Transactions. https://jdih.komdigi.go.id/produk_hukum/view/id/695/t/common.

Republic of Indonesia. (2022). Law No. 27 of 2022 on Personal Data Protection. https://jdih.komdigi.go.id/produk_hukum/view/id/832/t/crc32.

Republic of Indonesia. (2024). Law No. 1 of 2024 amending Law No. 11 of 2008 on Electronic Information and Transactions.

Republic of Indonesia. (n.d.). Herziene Indonesisch Reglement (HIR), Article 164.

Republic of Indonesia. (n.d.). Indonesian Civil Code (Kitab Undang-Undang Hukum Perdata), Article 1866.

Supreme Court of Indonesia. (2022). Supreme Court Regulation No. 7 of 2022 amending Regulation No. 1 of 2019 on electronic case administration and proceedings. https://jdih.mahkamahagung.go.id/legal-product/perma-nomor-7-tahun-2022/detail.

Surden, H. (2019). Artificial intelligence and law: An overview. Georgia State University Law Review, 35(4). https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8.

Tabassi, E. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1.

UNCITRAL. (1996). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment. United Nations. https://uncitral.un.org/en/texts/ecommerce.

United States. (n.d.-a). Federal Rules of Evidence: Rule 702 (Testimony by expert witnesses). Legal Information Institute.

United States. (n.d.-b). Federal Rules of Evidence: Rule 901 (Authenticating or identifying evidence). Legal Information Institute.

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 841–887.