

Civil Liability for Artificial Intelligence-Induced Harm in Indonesia: Reconstructing Fault, Causation, and Evidentiary Responsibility through a Control-Risk-Evidence Model

Tauhid^{1*}, Dipo Fathullah Saputra², Muhamad Redo Idra³, Amar Bintang⁴, Zikrian⁵

^{1,2,3,4,5} Faculty of Law, Universitas Merangin

*Correspondence: tauhidtauhid824@gmail.com

Received: 04 January 2026

Accepted: 03 September 2026

Published: 16 September 2026

Abstrak

Pemanfaatan kecerdasan artifisial dalam layanan keuangan, perdagangan elektronik, kesehatan, transportasi, pendidikan, dan pengambilan keputusan berbasis data memperluas risiko kerugian yang tidak lagi dapat ditelusuri hanya kepada tindakan langsung satu manusia. Artikel ini menganalisis kecukupan kerangka pertanggungjawaban perdata Indonesia terhadap kerugian yang dihasilkan atau diperantarai sistem kecerdasan artifisial dan merumuskan model rekonstruksi yang tetap kompatibel dengan perbuatan melawan hukum, wanprestasi, perlindungan konsumen, transaksi elektronik, dan perlindungan data pribadi. Penelitian hukum normatif menggunakan pendekatan perundang-undangan, konseptual, dan perbandingan terbatas. Hasil penelitian menunjukkan bahwa Pasal 1365, 1366, dan 1367 Kitab Undang-Undang Hukum Perdata tetap relevan, tetapi menghadapi kesenjangan atribusi dan pembuktian ketika sistem bersifat opak, adaptif, multiaktor, dan bukti teknis dikuasai tergugat. Artikel ini mengembangkan Model Kendali-Risiko-Bukti yang mengalokasikan tanggung jawab berdasarkan kendali praktis, manfaat ekonomi, kemampuan mencegah risiko, dan penguasaan bukti; model tersebut menggabungkan kewajiban dokumentasi, praduga kausalitas yang dapat dibantah, tanggung jawab yang lebih ketat untuk penggunaan berisiko tinggi, serta mekanisme regres antaraktor.

Kata Kunci: kecerdasan artifisial; pertanggungjawaban perdata; perbuatan melawan hukum; kausalitas; ganti rugi.

Abstract

The deployment of artificial intelligence in financial services, electronic commerce, health care, transportation, education, employment, and data-driven decision-making expands the possibility of harm that can no longer be explained solely through direct human conduct. This article examines the adequacy of Indonesia's civil-liability framework for losses caused or mediated by AI systems and develops a reconstruction model compatible with tort, breach of contract, consumer protection, electronic transactions, and personal-data protection. Using normative legal research with statutory, conceptual, and limited comparative approaches, the article finds that Articles 1365, 1366, and 1367 of the Indonesian Civil Code remain doctrinally relevant but encounter serious attribution and evidentiary gaps where AI systems are opaque, adaptive, distributed across multiple actors, and technically documented by defendants rather than victims. The article proposes a Control-Risk-Evidence Model

that allocates responsibility according to practical control, economic benefit, capacity to prevent harm, and access to evidence. The model combines documentation duties, rebuttable presumptions of causation, stricter liability for high-risk deployment, and contribution-based recourse among responsible actors. It therefore preserves the corrective and preventive functions of civil liability without treating AI either as a new legal person or as a universal excuse for human and corporate actors.

Keywords: artificial intelligence; civil liability; tort; causation; compensation.

INTRODUCTION

Artificial intelligence has moved beyond the role of a passive computational tool that merely executes predetermined human instructions. Machine-learning systems now classify, predict, recommend, generate content, and influence decisions that can directly affect private rights and economic interests. When an AI system is used to assess creditworthiness, price insurance, screen employment candidates, support medical diagnosis, moderate electronic-commerce transactions, or automate safety-critical functions, the resulting harm may emerge from a chain involving model developers, data providers, cloud infrastructure, system integrators, professional deployers, platform operators, and end users. This distributed architecture challenges a civil-liability model that is often applied as though one identifiable actor performed one wrongful act and caused one readily observable loss. Recent law-and-economics scholarship accordingly frames the core problem not as whether ordinary private law can reach AI, but how liability should allocate risk when control, information, and preventive capacity are divided among multiple actors.¹

Indonesian private law already contains several doctrinal entry points. Article 1365 of the Civil Code provides the general basis for liability arising from an unlawful act; Article 1366 extends responsibility to negligence and lack of due care; and Article 1367 recognizes forms of responsibility associated with persons and things under one's supervision. In contractual relations, Articles 1239 and 1243 and the broader law of non-performance provide a basis for damages where a promised obligation is not properly performed. These provisions are technologically neutral. Their difficulty lies not in the absence of a cause of action, but in attribution: whose conduct counts as legally relevant conduct, whose standard of care should govern, and when a technical malfunction, an unreasonable deployment choice, or a failure to preserve evidence becomes a civil wrong.

The problem becomes more acute because AI-related harm is frequently multi-causal. A harmful output may originate in training-data quality, model architecture, design choices, inadequate testing, deficient safety guardrails, integration errors, local fine-tuning, misleading user interfaces, an operator's deployment decision, a user prompt, a failure to update the system, or interaction among several components. A developer may have little control over the final context of use, whereas a deployer may have no realistic access to the model's internal logic. Allocating all liability to the last human in the chain may therefore target the actor with the least information about systemic risk. Conversely, treating the developer

¹Miriam Buiten, Alexandre de Streel, and Martin Peitz, "The Law and Economics of AI Liability," *Computer Law & Security Review* 48 (2023): 105794, <https://doi.org/10.1016/j.clsr.2023.105794>.

as the universal guarantor of every downstream use would ignore misuse, unauthorized modification, and context-specific operational choices. Liability should instead follow relative control over risk and relative awareness of how that risk can be prevented.²

Evidentiary asymmetry is the second structural challenge. A claimant may know that an automated decision denied a loan, misclassified a medical image, exposed personal data, or triggered a physical loss, while the information needed to explain the outcome model logs, training provenance, version histories, configuration files, evaluation metrics, incident reports, and human-intervention records remains in the exclusive possession of the defendant or a third-party provider. If the claimant must prove the entire internal technical sequence before disclosure is available, formal rules of proof can become a structural barrier to a remedy. Indonesian scholarship has already identified this difficulty when Articles 1365-1367 are applied to systems whose autonomy and black-box characteristics obscure the responsible human or corporate actor.³

Sectoral legislation adds several layers of responsibility. Consumer-protection law requires business actors to provide safe services, accurate information, and compensation in circumstances regulated by Law No. 8 of 1999, while Article 28 provides a burden-of-proof rule favorable to consumers in relevant compensation disputes. The Electronic Information and Transactions regime, as amended by Law No. 1 of 2024, and Government Regulation No. 71 of 2019 impose duties concerning reliable, secure, and accountable electronic systems. Law No. 27 of 2022 on Personal Data Protection creates an additional remedial pathway where AI harm is connected with unlawful collection, profiling, disclosure, security failure, or other personal data processing. These regimes show that AI liability in Indonesia is not located in a legal vacuum; rather, it is fragmented across rules with different protected interests, standards, and evidentiary consequences.

The government's 2023 Circular Letter on Artificial Intelligence Ethics introduced principles of inclusiveness, humanity, security, accessibility, transparency, credibility and accountability, personal-data protection, sustainable development, and intellectual property. In 2026, the government continued preparing presidential regulations on AI ethics and a national AI roadmap, indicating a shift from non-binding ethical guidance toward a more structured governance framework. As of the date of this article, however, those instruments were still reported as draft presidential regulations rather than an enacted comprehensive AI-liability statute. The distinction matters: ethical governance can shape standards of reasonable conduct, but it does not by itself answer who must compensate a victim, what proof is required, or how contribution among multiple AI actors should be allocated.

Comparative developments provide useful calibration without dictating Indonesian law. The European Union AI Act adopts a risk-based regulatory

²Shu Li, Michael Faure, and Katri Havu, "Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach," *European Journal of Risk Regulation* 13, no. 4 (2022): 618–634, <https://doi.org/10.1017/err.2022.26>.

³Yolanda Simbolon, "Pertanggungjawaban Perdata terhadap Artificial Intelligence yang Menimbulkan Kerugian Menurut Hukum di Indonesia," *Veritas et Justitia* 9, no. 1 (2023): 246–273, <https://doi.org/10.25123/vej.v9i1.6037>.

approach, while Directive (EU) 2024/2853 modernizes product-liability rules and expressly treats software, including AI systems, as products for the purposes of no-fault product liability in its field of application. The comparative lesson is not that Indonesia should copy the European model wholesale; it is that digital products, continuous software control, technical complexity, and evidentiary asymmetry can justify differentiated rules concerning defect, disclosure, and causation.⁴

This article therefore shifts the analytical focus away from the question whether AI should become a legal person. Effective civil liability does not require machine personality. AI can remain a system through which legally recognized persons and entities develop, deploy, control, benefit from, and document risk. The relevant legal inquiry is more concrete: who controlled the stage at which the risk arose, who derived economic benefit, who was objectively able to prevent or mitigate the harm, and who controlled the evidence necessary to explain what occurred. This study labels that approach the Control-Risk-Evidence Model (CRE Model).

The article addresses three questions. First, how can Indonesian civil-liability doctrine be applied to harm generated or mediated by AI systems? Second, where do the principal difficulties arise in proving fault, causation, and responsibility in opaque and multi-actor systems? Third, how should liability be reconstructed so that victims have an effective path to compensation while innovators retain predictable standards of conduct? The central argument is that Indonesia should preserve ordinary private-law doctrine as the foundation but adapt attribution and proof through role-sensitive duties, documentation obligations, conditional presumptions, and stricter treatment of professionally deployed high-risk systems.

RESEARCH METHOD

This study employs normative legal research and treats statutes, legal principles, doctrinal concepts, and institutional allocation of responsibility as its principal materials. The statutory approach examines the Indonesian Civil Code; Law No. 8 of 1999 on Consumer Protection; Law No. 11 of 2008 on Electronic Information and Transactions as most recently amended by Law No. 1 of 2024; Law No. 27 of 2022 on Personal Data Protection; Government Regulation No. 71 of 2019 on Electronic Systems and Transactions; and Ministerial Circular Letter No. 9 of 2023 on Artificial Intelligence Ethics. The research also considers the status of Indonesia's ongoing 2026 AI-governance initiatives only as policy context and does not treat draft presidential regulations as positive law.

The conceptual approach evaluates fault, negligence, risk control, causation, information asymmetry, product defect, operator responsibility, strict liability, evidentiary presumptions, contribution, and recourse. The comparative component is deliberately limited. It uses the EU AI Act and the 2024 Product Liability Directive, together with peer-reviewed AI-liability scholarship, as functional comparisons for issues of risk classification, continuing software control, defect, disclosure, and

⁴European Parliament and Council of the European Union, Directive (EU) 2024/2853 of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC.

burden of proof. Comparative material is used to test design options against Indonesian doctrine rather than to import foreign legal categories automatically.⁵

Secondary materials were selected on the basis of relevance, academic credibility, and verifiable publication data. Priority was given to peer-reviewed articles carrying DOIs and to recent Indonesian scholarship addressing civil liability, electronic contracts, product liability, personal data, and provider responsibility. The analysis proceeds in four stages: mapping the applicable Indonesian causes of action; allocating legal duties by actor and sphere of control; testing classical fault and causation doctrine against AI opacity and multi-actor supply chains; and constructing a prescriptive model that aligns compensation, prevention, proportionality, and innovation. Because the study is doctrinal, it does not claim to measure the frequency of AI failures or the empirical behavior of Indonesian courts.

RESULTS AND DISCUSSION

The Fragmented Basis of Civil Liability for AI-Induced Harm

The first finding is that AI does not create an immunity zone within Indonesian private law. Where harm occurs in a contractual relationship, the relevant obligation can be traced to the promised performance, service level, security assurance, quality representation, or professional standard incorporated into the parties' agreement. A business cannot avoid contractual responsibility merely by stating that an algorithm generated the harmful output. From the standpoint of performance, AI is part of the method chosen by the debtor to discharge its obligation. The harder question arises where the contract only promises probabilistic assistance, contains broad disclaimers, or allocates technical risk to the user. In those situations, good faith, consumer-protection rules, transparency, and the substantive fairness of standard clauses become central to determining whether contractual risk allocation should be respected.

For third-party loss outside contract, Article 1365 remains the principal doorway. An unlawful act in the AI context need not be the final physical event that immediately precedes the injury. It can include a decision to design, train, release, integrate, deploy, continue operating, or market a system despite a known and unreasonable risk; a failure to implement appropriate safeguards; or a failure to correct a material defect after notice. Indonesian scholarship increasingly supports attribution to human or corporate actors rather than recognizing AI itself as the bearer of private-law responsibility.⁶

Article 1366 is especially important because many AI disputes are better characterized as failures of due care than intentional misconduct. A role-sensitive standard of care may include reasonable testing, validation for the intended context, security controls, bias evaluation, meaningful human oversight, monitoring after deployment, incident response, preservation of logs, and communication of material limitations. These duties should not be identical for every actor. A foundation-model

⁵Martin Ebers, "Truly Risk-Based Regulation of Artificial Intelligence—How to Implement the EU's AI Act," *European Journal of Risk Regulation* 16, no. 2 (2025): 684–703, <https://doi.org/10.1017/err.2024.78>.

⁶Angie Natasya Hirawan and Indah Parmitasari, "Civil Liability for Losses Resulting From the Use of Artificial Intelligence," *Journal of Private and Commercial Law* 3, no. 1 (2026): 1–20, <https://doi.org/10.20885/JPCOL.vol3.iss1.art1>.

provider, a system integrator, a hospital, a bank, and an ordinary end user occupy different positions in relation to risk. A single abstract negligence standard would obscure rather than clarify their obligations.

Article 1367 should be used cautiously. Its language concerning responsibility for persons and things under supervision does not automatically turn all AI use into strict liability, and software is not necessarily equivalent to a traditional tangible thing. Yet the provision reflects a broader private-law intuition: responsibility can arise from control over a source of risk even where the controller did not directly perform the final harmful act. For AI disputes, that intuition is more useful than attempting to classify every autonomous output as a separate act of a machine. The legal focus should remain on supervision, control, capacity to intervene, and the relationship between the actor and the risky system.

Consumer law strengthens the remedial position of individuals who receive AI-enabled goods or services. Article 19 of Law No. 8 of 1999 supports compensation for legally recognized consumer loss, while Article 28 demonstrates that Indonesian law already accepts evidentiary adjustments in relationships characterized by business-consumer asymmetry. That structure is highly relevant to AI because a consumer normally cannot inspect source code, training data, model cards, incident logs, or internal validation records. A rebuttable presumption tied to a proven breach of documentation or safety duties would therefore extend an existing Indonesian policy logic rather than create an entirely foreign principle.

Personal-data law operates in parallel, not as a substitute for general civil liability. Where an AI system harms an individual through unlawful profiling, excessive processing, unauthorized disclosure, insecure data handling, or a violation of data-subject rights, Law No. 27 of 2022 can provide a direct basis for redress. But many AI harms do not depend on unlawful data processing. A lawful dataset can still support an unsafe decision model; a system can cause physical or economic harm without processing the victim's personal data at all. Accordingly, data-protection liability should be treated as one component of a broader liability architecture, not as the universal answer to AI harm.⁷

Electronic-system regulation supplies additional evidence of the expected standard of conduct. Government Regulation No. 71 of 2019 requires electronic systems to meet standards of reliability, security, and accountability. These terms should not be misread as a guarantee that an AI system must be perfectly accurate. Legal reliability should instead be assessed in relation to the system's intended purpose, foreseeable risk, representations made to users, validation practices, security posture, and available alternatives. Residual error can be legally tolerable; unmanaged, undisclosed, or avoidable risk may not be.

The main weakness is therefore not the absence of legal sources, but fragmentation. A single incident can simultaneously raise contract, tort, consumer, electronic-system, and data-protection issues. If attribution depends only on the label chosen in the statement of claim, outcomes may vary for formal reasons unrelated to the underlying harm. The law needs cross-cutting attribution factors that remain relevant across regimes. Control over the risky function, economic

⁷Junaidi Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil, "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory," *Journal of Law and Legal Reform* 5, no. 2 (2024), <https://doi.org/10.15294/jllr.vol5i2.3437>.

benefit, capacity to prevent harm, and control over technical evidence provide such factors and form the foundation of the CRE Model.

Fault, Causation, and the Evidentiary Problem of Opaque Multi-Actor Systems

Fault remains normatively important because it differentiates accidents that should remain with the victim from losses that ought to be shifted to an actor who failed to exercise reasonable care. In the AI context, however, fault should be assessed as a failure of risk governance rather than as actual knowledge that one particular output would be wrong. The relevant inquiry is whether the defendant knew or reasonably should have known the category of risk, whether it possessed means to reduce that risk, and whether it deployed or continued the system without safeguards proportionate to the foreseeable consequences. This formulation preserves negligence doctrine while making it operational for probabilistic technology.

Duties should therefore be role-specific. Developers are best placed to address model architecture, safety design, testing, cybersecurity, documentation, and communication of material limitations. Integrators control compatibility, local configuration, fine-tuning, and the interaction between the AI component and the surrounding system. Professional deployers decide whether the system is suitable for a particular use, whether human review is meaningful, what decision thresholds apply, and what remedies exist when outputs are challenged. End users may bear responsibility where they intentionally disregard warnings or use a system in an obviously prohibited manner. This role differentiation is supported by recent Indonesian work proposing provider-centered and risk-based approaches to AI accountability.⁸

Opacity creates both a substantive and procedural problem. Some opacity is technical, arising from complex model architectures; some is organizational, caused by poor recordkeeping and fragmented vendor relationships; and some is legal, arising from trade-secret claims and contractual confidentiality. The law should distinguish these forms. A defendant should not gain an evidentiary advantage from deliberately maintaining an unauditable deployment. At the same time, disclosure should not require public release of proprietary source code. Courts can protect trade secrets through limited production, independent experts, confidentiality orders, or technical summaries sufficient to test the contested causal pathway.

AI causation is difficult in at least four recurring ways. First, multi-causality arises where data, design, integration, and human choices jointly contribute to loss. Second, probabilistic causation means that a system can be reasonably designed while still producing occasional incorrect outputs. Third, update causation requires identification of the model version and configuration that existed when the loss occurred. Fourth, intervention causation arises where an AI recommendation is followed by a human decision. None of these problems is solved by asking only who made the final click. The court must ask who possessed meaningful control at each causal stage and whether a later intervention was genuinely independent or merely formal.

⁸Ninik Zakiyah et al., "Who Bears the Risk? Mapping the Legal Liability of Artificial Intelligence Providers in Indonesia's Regulatory Landscape," *Journal of Indonesian Legal Studies* 11, no. 1 (2026): 111–146, <https://doi.org/10.15294/jils.v11i1.31133>.

The concept of human-in-the-loop requires particular care. A physician, analyst, employee, or content moderator may formally approve an AI output but lack the information, time, or institutional authority needed to evaluate it independently. In that situation, a final human approval should not automatically sever causation from the system designer or deploying organization. Conversely, a trained professional who receives a transparent decision-support recommendation and disregards contrary evidence may become a concurrent cause. Liability should therefore depend on the quality of human oversight rather than its nominal existence.⁹

Burden of proof is where technical asymmetry becomes procedural inequality. Requiring a claimant to identify the precise code path, hidden parameter, or training example responsible for a decision before obtaining access to technical records can make a legally valid claim impossible to litigate. Comparative literature increasingly supports disclosure duties and rebuttable presumptions where technical complexity lies largely within the defendant's sphere of information. The economic justification is straightforward: the party that can preserve and produce evidence at the lowest cost should not externalize the consequences of non-documentation to the injured party.¹⁰

The CRE Model therefore proposes a conditional evidentiary presumption rather than an automatic reversal in every AI case. The claimant should first establish a threshold showing of legally cognizable harm, material use of an AI system in the process that generated the harm, and either a documented safety failure, a violation of a relevant duty, or an unexplained failure to preserve records that should reasonably exist. Once that threshold is met, causation may be presumed unless the defendant demonstrates that the harm was more likely produced by an independent cause or that the relevant duty was complied with and the loss arose from residual risk. This preserves disciplined proof while preventing opacity from functioning as immunity.

Documentation is consequently both a governance obligation and an evidentiary infrastructure. High-impact deployments should record the relevant model version, material inputs, testing outcomes, configuration changes, human interventions, override events, security incidents, and remedial actions. A party that maintains a credible audit trail should be better able to rebut a claim. A party that fails to preserve information under its exclusive control should face the possibility of an adverse inference. The rule creates an ex ante incentive to build accountable systems before litigation occurs.

Causation doctrine should also retain limiting principles. Rebuttable presumptions should facilitate proof of connection, not eliminate the requirement of actual loss. Foreseeability, proximity, mitigation, and the distinction between physical injury, property damage, pure economic loss, reputational harm, and data-related injury remain relevant to defining recoverable damages. Civil liability should

⁹Caroline Jones, James Thornton, and Jeremy C. Wyatt, "Artificial Intelligence and Clinical Decision Support: Clinicians' Perspectives on Trust, Trustworthiness, and Liability," *Medical Law Review* 31, no. 4 (2023): 501–520, <https://doi.org/10.1093/medlaw/fwad013>.

¹⁰Sam Whittam, "Mind the Compensation Gap: Towards a New European Regime Addressing Civil Liability in the Age of AI," *International Journal of Law and Information Technology* 30, no. 2 (2022): 249–265, <https://doi.org/10.1093/ijlit/eaac013>.

not transform every inaccurate AI output into a compensable wrong; it should respond where a legally protected interest was harmed through a risk that can fairly be attributed to an actor or combination of actors.

Comparative Calibration: Risk-Based Regulation and Modern Product Liability

Comparative developments illuminate two complementary ideas. The first is risk differentiation. The EU AI Act classifies certain uses according to risk and imposes more demanding governance duties where systems can seriously affect health, safety, or fundamental rights. The second is modernization of product liability. Directive (EU) 2024/2853 recognizes software as a product and treats continuing software control, updates, and digital complexity as relevant to modern liability. Indonesia need not reproduce the EU categories, but the functional logic is transferable: a liability framework should become more demanding as potential harm increases and as victims lose practical capacity to control or understand the risk.¹¹

The revised European product-liability framework is especially instructive because it recognizes that software producers may retain post-market control through updates and remote services. Traditional product-liability doctrine often assumes that a manufacturer's control ends when a product leaves the factory. That assumption is increasingly inaccurate for AI. A provider may change model behavior remotely, disable features, alter safety filters, or update weights after deployment. In such circumstances, legal responsibility should follow continuing technical control rather than a formal date of sale. This supports the CRE Model's insistence on assessing control at the time the harmful risk materialized.

Academic analysis of defective AI similarly emphasizes that defect should be evaluated in light of relative control and awareness of risk between producer and user. An AI system should not be deemed defective merely because it made one incorrect prediction; otherwise product liability becomes a guarantee of perfect performance. But neither should a producer escape merely because probabilistic error is inherent to machine learning. The legal question is whether safer design, better warnings, improved monitoring, different human-machine interaction, or post-market correction was reasonably available in light of the actor's knowledge and control.¹²

Recent Indonesian scholarship points in a similar direction. Studies published in 2025 and 2026 increasingly reject the notion that AI itself should bear liability and instead allocate responsibility among developers, providers, owners, or users through risk, control, and evidence. These studies also highlight the black-box problem and advocate stricter responsibility, evidentiary adjustment, or transparency obligations for professional providers. The convergence is significant

¹¹European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).

¹²Miriam C. Buiten, "Product Liability for Defective AI," *European Journal of Law and Economics* 57 (2024): 239–273, <https://doi.org/10.1007/s10657-024-09794-z>.

because it suggests that a risk-sensitive attribution model can be developed from within Indonesian doctrine rather than imported as a foreign transplant.¹³

Comparative law also cautions against universal strict liability. Soyer and Tettenborn argue for a differentiated model in which strict liability is especially defensible for death and personal injury while other types of loss may remain fault-based. The insight is valuable for Indonesia: the intensity of liability should reflect the gravity of the externalized risk and the victim's ability to avoid it. A low-risk generative writing assistant and an autonomous system controlling a medical device should not automatically be governed by identical liability rules.¹⁴

Table 1. Control-Risk-Evidence Allocation Matrix

Actor	Typical sphere of control	Core duty	Key evidence	Indicative liability focus
Developer / model provider	Architecture, training process, safety design, updates, system-level documentation	Reasonable design, testing, security, warnings, corrective updates	Model documentation, testing records, version history, incident reports	Design defect, negligent development, misleading capability claims, failure to update
Integrator / fine-tuner	Local configuration, data integration, adaptation, interoperability	Context validation, secure integration, compatibility testing	Configuration records, local datasets, integration tests	Integration fault and local adaptation risks
Professional deployer	Purpose of use, decision thresholds, workflow, human oversight, user interface	Suitability assessment, monitoring, meaningful oversight, correction mechanism	Deployment logs, policies, override records, complaints	Primary user-facing responsibility where deployer selects and controls use
End user	Prompts, direct use, compliance with warnings	Reasonable use within stated limits	User actions, warnings received, interaction logs	Misuse or independent intervention where meaningful control existed
Multiple actors	Overlapping stages	Cooperation, preservation of evidence, contribution	Cross-vendor audit trail and contracts	Joint or concurrent liability with internal recourse where causation cannot reasonably be separated

¹³Mashuri, Dwi Afni Maileni, Rizki Tri Anugrah Bhakti, and Indra Sakti, "Civil Liability for Losses Caused by Artificial Intelligence under Indonesian Civil Law," *Jurnal Cakrawala Hukum* 17, no. 2 (2026): 155–168, <https://doi.org/10.26905/idjch.v17i2.16124>.

¹⁴Baris Soyer and Andrew Tettenborn, "Artificial Intelligence and Civil Liability—Do We Need a New Regime?," *International Journal of Law and Information Technology* 30, no. 4 (2022): 385–397, <https://doi.org/10.1093/ijlit/eaad001>.

The Control-Risk-Evidence Model for Indonesian Civil Liability

The CRE Model reconstructs liability without treating AI as a new legal subject. It uses four cumulative questions. First, who had practical control over the technological stage from which the material risk arose? Second, who obtained the principal economic benefit from deploying that system? Third, who was objectively best placed to prevent or mitigate the harm at reasonable cost? Fourth, who controlled the evidence needed to explain the failure? The answers identify the actor who should bear the primary duty to the victim, the standard of care applicable to that actor, and the evidentiary consequences of missing information.

The first axis is practical control. Ownership is relevant but not decisive. A model provider may not own the user's device yet retain control over updates, safety guardrails, access policies, and core architecture. A deployer may not possess source code but control the purpose of use, local data, human-review requirements, and thresholds that convert an AI score into a legal or economic decision. An end user may control a prompt but not the system's underlying design. Mapping these control points prevents simplistic attribution to whoever formally owns the software or physically interacted with it last.

The second axis combines risk and economic benefit. A professional entity that deploys AI at scale to reduce costs, automate decisions, or increase revenue is differently situated from a passive person exposed to those decisions. Where the enterprise internalizes the economic benefit but externalizes a difficult-to-avoid risk onto individuals who cannot inspect the system, private law has a stronger justification for placing preventive and compensatory responsibility on the enterprise. This does not mean that profit alone creates liability; it means that economic benefit helps identify the party expected to invest in precautions and insurance.¹⁵

The third axis is preventive capacity. Liability should encourage precautions by the actor who can most efficiently reduce the relevant risk. Developers may be best positioned to correct model-wide vulnerabilities; deployers may be best positioned to decide whether a model is appropriate for a hospital, financial institution, school, or transportation system; and users may be best positioned to avoid a clearly prohibited use. The point is not to identify one actor for every case, but to align duties with the stage at which prevention is practically possible.

The fourth axis is evidentiary control. A party that possesses logs, evaluation results, configuration history, or model documentation should have a corresponding duty to preserve and disclose the material necessary to test a plausible claim. Evidentiary responsibility is not a separate form of tort liability; it is a mechanism that prevents private control of technical information from defeating substantive rights. Failure to preserve expected records can support an adverse inference or trigger the conditional presumption of causation proposed above.

For consumer-facing applications, the professional deployer should ordinarily function as the primary contact point for compensation because it selected the system, integrated it into the service, communicates directly with the consumer, and benefits from its use. This rule improves procedural accessibility. It does not

¹⁵Miriam Buiten, Alexandre de Streel, and Martin Peitz, "The Law and Economics of AI Liability," *Computer Law & Security Review* 48 (2023): 105794, <https://doi.org/10.1016/j.clsr.2023.105794>.

immunize the developer. A deployer that compensates the victim may seek recourse against a developer or provider where the loss originated in a defect or breach within the developer's control. The external relationship with the victim and the internal allocation among commercial actors should therefore be separated.

Direct developer responsibility remains appropriate where harm originates predominantly from model-level design, deficient security, materially misleading capability claims, failure to disclose a known limitation, or failure to provide a safety update that remained within the provider's technical control. Indonesian scholarship on AI product liability similarly emphasizes that provider, developer, and user responsibilities should be differentiated rather than collapsed into a single category.¹⁶

For high-risk deployments, the model supports a stricter liability standard. This category should be defined functionally rather than by technology brand. Relevant factors include the potential for death or serious physical injury, automatic determination of access to essential services, high-impact financial or employment decisions, large-scale processing of sensitive data, and circumstances in which the affected person cannot realistically avoid or monitor the risk. Where a professional actor intentionally deploys such a system and captures its benefits, requiring the victim to prove traditional fault in full may be disproportionate.

Stricter liability need not mean unlimited liability. The defendant may retain defenses based on extraordinary external events, claimant misconduct, independently sufficient third-party intervention, or a showing that the damage is outside the legally protected risk. Statutory caps may be considered in narrowly defined contexts, but they should not be used to externalize predictable mass harms. Mandatory liability insurance or financial guarantees may complement the system for high-risk deployments by ensuring compensation capacity while allowing insurers to price governance quality into premiums.

The model also addresses concurrent causation. Where an unsafe model design and negligent deployment materially contribute to the same harm and the victim cannot reasonably isolate their technical shares, the law should permit claims against one or more responsible actors, followed by contribution or recourse among defendants. Internal apportionment can consider comparative fault, control, benefit, preventive capacity, and the degree to which each actor complied with documentation duties. This avoids requiring the least informed party the victim to solve the supply chain before obtaining a remedy.

Table 2. Risk-Sensitive Liability and Evidentiary Design

Risk profile	Liability baseline	Evidentiary adjustment	Illustrative governance expectation
Low-risk assistive use	Ordinary fault / contract rules	No special presumption absent information abuse	Basic warnings, security, ordinary records
Material consumer or economic decision	Fault-based plus consumer-law safeguards	Conditional presumption where	Decision notice, complaint channel,

¹⁶Dewi Asri Puannandini et al., "Liabilitas Produk AI dalam Sistem Hukum Indonesia: Implikasi bagi Pengembang, Pengguna, dan Penyedia Layanan," *Iuris Studia: Jurnal Kajian Hukum* 6, no. 1 (2025): 24–34, <https://doi.org/10.55357/is.v6i1.808>.

		documentation/safety duty is breached	logs, meaningful review
High-risk professional deployment	Stricter or risk-based responsibility for professional deployer	Enhanced disclosure, rebuttable causation presumption, adverse inference	Risk assessment, independent testing, audit trail, human oversight, incident reporting
Multi-actor high-risk system	External victim protection plus joint/concurrent responsibility where appropriate	Evidence duties allocated by control; internal recourse later	Interoperable logs, contractual audit rights, allocation of update/incident duties

Implementation within Indonesian Law

The CRE Model can be implemented incrementally. In the short term, courts can use control, risk, and evidence as interpretive factors when applying Articles 1365-1367, contractual liability, consumer protection, electronic-system duties, and data-protection rules. This approach does not require judicial creation of a new cause of action. It refines existing elements—wrongfulness, negligence, causation, and proof—by asking which actor controlled the material risk and which actor had access to the evidence.

In the medium term, implementing regulation should expressly require documentation for material AI decisions. The obligation should cover at least system identity and version, the purpose of deployment, relevant input categories, testing and validation, known limitations, significant configuration changes, human intervention, complaint handling, and material incidents. The required level of detail should be proportionate to risk. An internal writing assistant should not face the same documentation burden as an AI system used in medical triage or automated credit exclusion.

Regulation should also establish a right to meaningful review where an automated or AI-assisted decision materially affects legal or economic interests. Meaningful review does not require every system to explain its internal mathematics in natural language. It requires sufficient information to identify the decision basis, permit correction of material data errors, reveal the role of AI, and enable a qualified human to reconsider the outcome. This procedural protection links transparency with an actual remedial pathway rather than treating transparency as a purely symbolic notice obligation.

Consumer contracts require additional scrutiny. Standard terms should not allow a business to advertise AI as automated, accurate, and efficient while simultaneously shifting all output risk to the consumer. Article 18 of the Consumer Protection Law and the broader principle of good faith provide doctrinal tools to control unfair clauses. B2B agreements among sophisticated actors may allocate indemnities and insurance more freely, but those internal allocations should not extinguish the rights of third parties who never consented to them.

Personal-data governance should be integrated into, rather than separated from, AI liability. A violation of processing law, security duties, purpose limitation, or data-subject rights can constitute evidence of wrongfulness and negligence. But the CRE Model remains applicable even where no personal data are involved. This avoids a sectoral silo in which physical or economic AI harm falls outside meaningful

responsibility simply because the incident did not involve a data-protection violation.

Technical expert evidence will become increasingly important. Courts should preserve the distinction between technical and legal judgment. Experts can explain system architecture, error rates, model versions, security controls, and plausible technical causes; the court must determine whether the applicable standard of care was breached and whether causation is legally sufficient. Neutral or court-appointed technical review may be useful where both parties face extreme information imbalance, particularly if confidentiality arrangements can protect trade secrets while preserving adversarial testing.

The model is technology-neutral. It does not define liability by specific machine-learning architectures, model brands, or temporary technical vocabulary. Instead, it asks functional questions about control, benefit, preventive capacity, and evidence. This approach allows the framework to remain relevant as AI evolves from predictive systems toward generative models, autonomous agents, multimodal systems, or future architectures not yet contemplated by current regulation. Technology neutrality also reduces the risk that detailed legislation becomes obsolete before it is consistently applied.

The framework also gives businesses *ex ante* legal certainty. Liability rules should not be understood only as litigation threats; they can operate as governance instructions. A company that performs risk assessment, validates the system, preserves logs, discloses material limitations, provides meaningful human review, monitors incidents, and corrects known failures is better positioned both to prevent harm and to defend itself if litigation occurs. By contrast, a firm that launches a high-impact AI system without adequate testing or records should not be able to invoke the complexity of its own system as a defense. *Ex-post* liability thus complements *ex-ante* governance by creating incentives for responsible innovation.¹⁷

Indonesia's 2026 policy process reinforces the need for this distinction. Government statements described draft presidential regulations on AI ethics and the national AI roadmap as intended to move AI governance from ethical aspiration toward a stronger national framework. Until those instruments are enacted and their relationship with private-law remedies is clarified, civil courts and sectoral regulators will continue to rely on the existing legal architecture. A principled liability model can provide continuity during that transition while remaining adaptable to future legislation.

CONCLUSION

Civil liability for AI-induced harm in Indonesia does not require recognition of AI as a new legal person. The Civil Code, particularly Articles 1365, 1366, and 1367, remains capable of grounding responsibility for unlawful conduct, negligence, and control-related risk, while contractual remedies remain applicable where AI is part of the method by which a debtor performs an obligation. Consumer protection, electronic-system regulation, and personal-data law provide additional sectoral

¹⁷Guido Noto La Diega and Leonardo C. T. Bezerra, "Can There Be Responsible AI without AI Liability? Incentivizing Generative AI Safety through Ex-Post Tort Liability under the EU AI Liability Directive," *International Journal of Law and Information Technology* 32 (2024): eaae021, <https://doi.org/10.1093/ijlit/eaae021>.

duties. The principal weakness of the current framework lies in attribution and proof rather than in a complete absence of legal norms.

AI systems complicate conventional doctrine because they are probabilistic, frequently opaque, continuously updated, and embedded in multi-actor supply chains. A rigid application of fault and causation may allow the actor controlling all relevant technical evidence to enjoy a procedural advantage over the injured party. Liability should therefore be assessed through risk governance: what the actor knew or should have known, what it could reasonably control, what precautions were available, and whether it preserved the evidence necessary to explain the disputed event.

The Control-Risk-Evidence Model developed in this article allocates responsibility through practical control, economic benefit, preventive capacity, and evidentiary control. Professional deployers should ordinarily function as an accessible responsibility point for user-facing services, without immunizing developers from defects or failures within their control. Conditional presumptions of causation should become available where a claimant establishes harm, material involvement of AI, and breach of a relevant safety or documentation duty. High-risk professional deployment justifies stricter responsibility, while low-risk use can remain primarily fault-based.

The principal reform agenda is therefore not the creation of machine personality but the construction of auditable human and corporate responsibility. Indonesia should strengthen documentation and audit-trail duties, meaningful review mechanisms, risk-sensitive disclosure, consumer protection against unfair disclaimers, rules for contribution among multiple actors, and the possibility of insurance or financial guarantees for high-risk activities. Such a framework preserves innovation by making the applicable standard predictable while ensuring that technical complexity does not become a structural reason to deny compensation.

REFERENCES

- Anovanko, Uria Bernandus, Andika Wijaya, and Satriya Nugraha. "Implikasi Hukum Perdata terhadap Penggunaan Kecerdasan Buatan (AI) dalam Kontrak Komersial." *Innovative: Journal of Social Science Research* 5, no. 2 (2025): 3637–3653. <https://doi.org/10.31004/innovative.v5i2.18718>.
- Ardiyanti, N., Rizka Nur Khoirunnisa Azmi, Nabil Ramadhan, and Ahmad Jamaludin. "Legal Responsibility for the Use of Artificial Intelligence in Medical Practice." *Jurnal Hukum De'rechtsstaat* 10, no. 1 (2024): 121–132. <https://doi.org/10.30997/jhd.v10i1.11323>.
- Brożek, Bartosz, Michał Furman, Marek Jakubiec, and Bartłomiej Kucharzyk. "The Black Box Problem Revisited: Real and Imaginary Challenges for Automated Legal Decision Making." *Artificial Intelligence and Law* 32 (2024): 427–440. <https://doi.org/10.1007/s10506-023-09356-9>.
- Buiten, Miriam C. "Product Liability for Defective AI." *European Journal of Law and Economics* 57 (2024): 239–273. <https://doi.org/10.1007/s10657-024-09794-z>.

- Buiten, Miriam, Alexandre de Streel, and Martin Peitz. "The Law and Economics of AI Liability." *Computer Law & Security Review* 48 (2023): 105794. <https://doi.org/10.1016/j.clsr.2023.105794>.
- Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence—How to Implement the EU's AI Act." *European Journal of Risk Regulation* 16, no. 2 (2025): 684–703. <https://doi.org/10.1017/err.2024.78>.
- European Parliament and Council of the European Union. Directive (EU) 2024/2853 of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC.
- European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).
- Gredka-Ligarska, Iwona. "Employer as an AI System Operator and Tortious Liability for Damage Caused by AI Systems: European and US Perspectives." *The Chinese Journal of Comparative Law* 12 (2024): cxae015. <https://doi.org/10.1093/cjcl/cxae015>.
- Hasibuan, Rangga Hotman, Aurelya Jessica Rawung, and Fidel Jeremy Wowiling. "Indonesian Law and Artificial Intelligence: Balancing Accountability, Ethics, and Innovation." *Jurnal Penelitian Hukum De Jure* 24 (2024): 121–132. <https://doi.org/10.30641/dejure.2024.V24.121-132>.
- Hirawan, Angie Natasya, and Indah Parmitasari. "Civil Liability for Losses Resulting From the Use of Artificial Intelligence." *Journal of Private and Commercial Law* 3, no. 1 (2026): 1–20. <https://doi.org/10.20885/JPCOL.vol3.iss1.art1>.
- Indonesia. Kitab Undang-Undang Hukum Perdata.
- Indonesia. Law No. 8 of 1999 on Consumer Protection.
- Indonesia. Law No. 11 of 2008 on Electronic Information and Transactions, as most recently amended by Law No. 1 of 2024.
- Indonesia. Law No. 27 of 2022 on Personal Data Protection.
- Indonesia. Government Regulation No. 71 of 2019 on the Administration of Electronic Systems and Transactions.
- Indonesia, Ministry of Communication and Informatics. Circular Letter No. 9 of 2023 on Artificial Intelligence Ethics.
- Jones, Caroline, James Thornton, and Jeremy C. Wyatt. "Artificial Intelligence and Clinical Decision Support: Clinicians' Perspectives on Trust, Trustworthiness, and Liability." *Medical Law Review* 31, no. 4 (2023): 501–520. <https://doi.org/10.1093/medlaw/fwad013>.
- Junaidi, Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil. "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory." *Journal of Law and Legal Reform* 5, no. 2 (2024). <https://doi.org/10.15294/jllr.vol5i2.3437>.

- Li, Shu, Michael Faure, and Katri Havu. "Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach." *European Journal of Risk Regulation* 13, no. 4 (2022): 618–634. <https://doi.org/10.1017/err.2022.26>.
- Ma, Jinbo. "Causation in AI Tort Litigation: Legal Dilemmas of Algorithmic Black Boxes and Burden of Proof Allocation." *Legal Compliance* 1, no. 2 (2025). <https://doi.org/10.63808/lc.v1i2.127>.
- Mashuri, Dwi Afni Maileni, Rizki Tri Anugrah Bhakti, and Indra Sakti. "Civil Liability for Losses Caused by Artificial Intelligence under Indonesian Civil Law." *Jurnal Cakrawala Hukum* 17, no. 2 (2026): 155–168. <https://doi.org/10.26905/idjch.v17i2.16124>.
- Noto La Diega, Guido, and Leonardo C. T. Bezerra. "Can There Be Responsible AI without AI Liability? Incentivizing Generative AI Safety through Ex-Post Tort Liability under the EU AI Liability Directive." *International Journal of Law and Information Technology* 32 (2024): eaae021. <https://doi.org/10.1093/ijlit/eaae021>.
- Nurzaman, Jajang, and Dwi Fidhayanti. "Keabsahan Kontrak yang Dibuat oleh Artificial Intelligence Menurut Hukum Positif di Indonesia." *Al 'Adl: Jurnal Hukum* 16, no. 1 (2024): 140–159. <https://doi.org/10.31602/al-adl.v16i1.12710>.
- Puannandini, Dewi Asri, Raihan Ma'ruf Fabian, Reival Andhika Putra Firdaus, Muhammad Zainal Mustopa, and Indra Herdiyana. "Liabilitas Produk AI dalam Sistem Hukum Indonesia: Implikasi bagi Pengembang, Pengguna, dan Penyedia Layanan." *Iuris Studia: Jurnal Kajian Hukum* 6, no. 1 (2025): 24–34. <https://doi.org/10.55357/is.v6i1.808>.
- Putranti, Deslaely, and Kurnia Dewi Anggraeny. "Tanggung Jawab Hukum Inventor Atas Inovasi Kecerdasan Buatan (Artificial Intelligence) di Indonesia." *Jurnal Hukum & Pembangunan* 52, no. 3 (2022): 781–792. <https://doi.org/10.21143/jhp.vol52.no3.3375>.
- Qurrahman, Shofika Hardiyanti, Safira Ayunil, and Tsabita Aurelia Rahim. "Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence dalam Hukum Positif Indonesia." *Unes Law Review* 6, no. 4 (2024): 12687–12693. <https://doi.org/10.31933/unesrev.v6i4.2108>.
- Rodríguez de las Heras Ballell, Teresa. "The Revision of the Product Liability Directive: A Key Piece in the Artificial Intelligence Liability Puzzle." *ERA Forum* 24 (2023): 247–259. <https://doi.org/10.1007/s12027-023-00751-y>.
- Simbolon, Yolanda. "Pertanggungjawaban Perdata terhadap Artificial Intelligence yang Menimbulkan Kerugian Menurut Hukum di Indonesia." *Veritas et Justitia* 9, no. 1 (2023): 246–273. <https://doi.org/10.25123/vej.v9i1.6037>.
- Soyer, Baris, and Andrew Tettenborn. "Artificial Intelligence and Civil Liability—Do We Need a New Regime?" *International Journal of Law and Information Technology* 30, no. 4 (2022): 385–397. <https://doi.org/10.1093/ijlit/eaad001>.

- Wagner, Gerhard. "Liability Rules for the Digital Age—Aiming for the Brussels Effect." *Journal of European Tort Law* 13, no. 3 (2023): 191–243. <https://doi.org/10.1515/jetl-2022-0012>.
- Whittam, Sam. "Mind the Compensation Gap: Towards a New European Regime Addressing Civil Liability in the Age of AI." *International Journal of Law and Information Technology* 30, no. 2 (2022): 249–265. <https://doi.org/10.1093/ijlit/eaac013>.
- Zakiyah, Ninik, Budi Santoso, Muh. Afif Mahfud, Edmon Makarim, and Try Hardyanthi. "Who Bears the Risk? Mapping the Legal Liability of Artificial Intelligence Providers in Indonesia's Regulatory Landscape." *Journal of Indonesian Legal Studies* 11, no. 1 (2026): 111–146. <https://doi.org/10.15294/jils.v11i1.311133>.