

Civil Liability for Losses Caused by Artificial Intelligence under Indonesian Civil Law

Mashuri¹, Dwi Afni Maileni², Rizki Tri Anugrah Bhakti³, and Indra Sakti⁴.

^{1,2,3,4} Faculty of Law, University of Riau Kepulauan, Indonesia.

Article history:

Received 2026-06-01

Revised 2026-07-20

Accepted 2026-08-01

Keywords:

Artificial Intelligence; Civil Liability; Electronic Agent; KUH Perdata; Unlawful Act.

DOI:

doi.org/10.26905/idjch.v17i2.16124.

Corresponding Author:

Mashuri.

E-mail:

mashuri@fh.unrika.ac.id.

Abstract: The rapid diffusion of Artificial Intelligence (AI) has outpaced the capacity of Indonesian civil law to allocate responsibility when AI-driven systems cause loss, leaving victims of deepfake fraud, algorithmic misconduct, and automated decision-making without a settled legal remedy. Existing scholarship has extensively debated whether AI may be recognised as a legal subject, yet has rarely translated that debate into a bounded, court-usable liability framework anchored in the Indonesian Civil Code (KUH Perdata) and tested against comparative risk-based regimes such as the European Union's Artificial Intelligence Act. This article addresses that gap by analysing, through a normative-juridical method with statutory and comparative-conceptual approaches, how civil liability for AI-caused losses should be constructed under Indonesian law. The findings show that AI remains an intangible object, not a legal subject, so liability is properly attributed to the creator, owner, or user of the AI system through the unlawful-act doctrine of Articles 1365 and 1367 of the KUH Perdata, applied together with the data-protection obligations of Government Regulation 71/2019. The article's novelty lies in integrating quantified domestic harm data with a three-track (developer-owner-user) liability model calibrated against the EU AI Act's risk tiers, from which it derives specific regulatory and adjudicative recommendations.

1. Introduction

Indonesia adheres to the principle of a state governed by law (*rechtsstaat*), under which every legal subject is bound to submit to, and is protected by, applicable legal provisions. Gustav Radbruch's classical account holds that law serves three cumulative purposes: legal certainty, justice, and expediency.¹ Civil liability, as one operational expression of these purposes, presupposes a legal subject capable of bearing rights and obligations; only such a subject can be made to answer, in law, for harm inflicted on another.² This is the normative ought that governs Indonesia's civil

¹ N. Ardiyanti et al., "Legal Responsibility for the Use of Artificial Intelligence in Medical Practice," *Jurnal Hukum De'rechtsstaat* 10, no. 1 (2024): 122, <https://doi.org/10.30997/jhd.v10i1.11323>, discussing Gustav Radbruch's three purposes of law.

² I. A. Filipova and V. D. Koroteev, "Future of the Artificial Intelligence: Object of Law or Legal Personality?," *Journal of Digital Technologies and Law* 1, no. 2 (2023): 359–386, 361, <https://doi.org/10.21202/jdtl.2023.15>.

liability system: whenever loss occurs through fault or an unlawful act, the law ought to identify a legal subject who bears responsibility, so that the injured party is not left without recourse.

The empirical reality has, however, moved further and faster than this normative architecture anticipated. Artificial intelligence, understood as computational systems engineered to approximate human cognitive functions such as pattern recognition, natural-language understanding, and autonomous decision-making, has migrated from a decision-support tool into an increasingly autonomous actor across healthcare, finance, transportation, and public administration. Because AI systems are trained on data and can adapt their own outputs, they do not merely execute a human instruction the way a conventional machine does; they can generate outcomes that neither their developer nor their user specifically anticipated.³ When those outcomes cause loss, a discriminatory credit decision, a misdiagnosis, a fraudulent deepfake transaction, the classical civil liability architecture, built on the duality of a human actor and a traceable fault, is placed under strain, because AI itself has no legal personality capable of bearing that fault.⁴

This is not a speculative concern. Indonesia's Financial Services Authority (Otoritas Jasa Keuangan/OJK) recorded roughly 274,000 digital financial-fraud reports between late 2024 and 2025, with aggregate public losses exceeding Rp6 trillion, a majority of which exploited AI-generated deepfake technology to defeat digital-banking identity-verification systems.⁵ The Ministry of Communication and Digital Affairs (Komdigi), through Deputy Minister Nezar Patria, separately reported that OJK-recorded losses from AI-enabled digital fraud, including deepfake impersonation, reached approximately Rp9 trillion in the current year.⁶ In April 2025, the East Java Regional Police (Polda Jatim) uncovered a concrete case in which three perpetrators used deepfake video and audio of the sitting Governor of East Java, Khofifah Indar Parawansa, to solicit fraudulent transfers over a three-month period, netting an illicit gain of Rp87,600,000 from victims across East Java, West Java, Central Java, and North Maluku who reasonably believed the video was genuine.⁷ These cases illustrate precisely the liability puzzle this article addresses: AI was instrumental in causing quantifiable, victim-specific financial loss, yet Indonesian positive law contains no provision naming AI, an AI developer, or an AI deployer as a liable party. The urgency of the topic is therefore not merely conceptual; it is measured in trillions of rupiah in documented annual losses and in identifiable victims who currently have no AI-specific civil remedy.

Indonesian and comparative legal scholarship has responded to this gap along three broad, only partially connected strands. The *first strand* debates whether AI could, in principle, be recognised as a legal subject. Maharani and Masnun frame AI as a possible "quasi-legal subject" un-

³ Dewi Asri Puannandini, 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" [Liability of AI Products in the Indonesian Legal System: Implications for Developers, Users, and Service Providers], *Iuris Studia: Jurnal Kajian Hukum* 6, no. 1 (2025): 26, <https://doi.org/10.55357/is.v6i1.808>.

⁴ Filipova and Koroteev, "Future of the Artificial Intelligence," 362–364.

⁵ "OJK Ungkap Bahaya Deepfake AI di Sektor Keuangan, Kerugian Penipuan Digital Tembus Rp6 Triliun," *GadgetDIVA.id*, May 14, 2026, <https://www.gadgetdiva.id/news/ojk-ungkap-bahaya-deepfake-ai>, reporting a statement by the OJK's Head of Banking Regulation and Development Department, Indah Iramadhini, at the "AI, Risk and Regulation" forum in Jakarta.

⁶ Nezar Patria, Deputy Minister of Communication and Digital Affairs, remarks at the Indonesia Ethical AI Summit, June 17, 2026, as reported in "Penipuan AI dan Deepfake Kian Marak, Komdigi: Kerugian Capai Rp9 T," *Harian Jogja*, June 17, 2026, <https://news.harianjogja.com/r-1260091/penipuan-ai-dan-deepfake-kian-marak-komdigi-kerugian-capai-rp9-t>.

⁷ "Polda Jatim Ungkap Kasus Penipuan Deepfake AI Kepala Daerah, Pelaku Kantongi Keuntungan Hingga Rp87 Juta," *Dinas Komunikasi dan Informatika Provinsi Jawa Timur*, April 29, 2025, <https://kominfo.jatimprov.go.id/berita/polda-jatim-ungkap-kasus-penipuan-deepfake-ai-kepala-daerah-pelaku-kantongi-keuntungan-hingga-rp87-juta>.

der Indonesian civil law, arguing that the classical human/legal-entity dichotomy may eventually need to accommodate a third, *sui generis* category.⁸ Wen and Tong's negative-theory analysis concludes that AI presently lacks the legal capacity (*rechtsbevoegdheid*) required of any legal subject and must instead be treated as an object of legal relations under human supervision.⁹ Internationally, this personhood debate is equally unsettled: Filipova and Koroteev review individual, collective, and gradient models of AI legal personality and ultimately recommend classifying AI as an object of law while carving out a narrower "electronic agent" category for functionally autonomous systems,¹⁰ while Wen and Tong's analysis of legal-subject theory concludes that AI cannot yet qualify as an "original" legal subject, though it might, in a strictly derivative sense analogous to a corporation, eventually be formulated as one.¹¹

The *second strand*, closer to this article's own focus, examines how liability should be constructed under existing doctrine while AI remains a non-subject. Simbolon argues that, absent AI-specific legislation, Indonesian courts must rely on the general unlawful-act doctrine of Article 1365 of the KUH Perdata, supplemented by Article 1367's rule on liability for persons and things under one's supervision.¹² Qurrahman, Ayunil, and Rahim reach a structurally similar conclusion but emphasise the practical evidentiary difficulty of proving fault against an opaque algorithmic process.¹³ Internationally, Ebers demonstrates that even the European Union's far more developed AI Act does not yet achieve a fully risk-proportionate liability architecture, meaning Indonesia cannot simply import the EU model wholesale without first correcting the same proportionality gaps identified in the EU's own implementation.¹⁴ Noto La Diega and Bezerra go further, arguing that the EU's proposed AI Liability Directive under-delivers on harmonised tort protection because its fault-based, discovery-focused design cannot keep pace with the unpredictable behaviour of advanced generative systems, strengthening the case for strict liability in high-risk contexts.¹⁵

The *third strand* addresses sector-specific and privacy-adjacent consequences of AI deployment. Anovanko, Wijaya, and Nugraha examine the civil-law implications of AI in commercial contracts, highlighting risks to contractual validity and consumer protection.¹⁶ Nurzaman and Fidhayanti separately question the validity of contracts autonomously generated by AI under

⁸ Bintang M.D. Maharani and Muh. Ali Masnun, "Prospek Artificial Intelligence Sebagai Quasi Subjek Hukum: Dinamika Pengaturan Hukum Perdata di Indonesia" [Prospects of Artificial Intelligence as a Quasi-Legal Subject: Dynamics of Civil Law Regulation in Indonesia], *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora* 4, no. 2 (2024): 6–9, <https://doi.org/10.53697/iso.v4i2.2063>.

⁹ Zhifeng Wen and Deyi Tong, "Analysis of the Legal Subject Status of Artificial Intelligence," *Beijing Law Review* 14 (2023): 74–86, 75–76, <https://doi.org/10.4236/blr.2023.141004>.

¹⁰ Filipova and Koroteev, "Future of the Artificial Intelligence," 370–375.

¹¹ Wen and Tong, "Analysis of the Legal Subject Status of Artificial Intelligence," 82–84.

¹² Yolanda Simbolon, "Pertanggungjawaban Perdata Terhadap Artificial Intelligence Yang Menimbulkan Kerugian Menurut Hukum di Indonesia" [Civil Liability for Artificial Intelligence Causing Losses According to Law in Indonesia], *Veritas et Justitia* 9, no. 1 (2023): 250–255, <https://doi.org/10.25123/vej.v9i1.6037>.

¹³ Shofika Hardiyanti Qurrahman, Safira Ayunil, and Tsabita Aurelia Rahim, "Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence dalam Hukum Positif Indonesia" [The Position and Concept of Artificial Intelligence Liability in Indonesian Positive Law], *Unes Law Review* 6, no. 4 (2024): 12689–12691, <https://doi.org/10.31933/unesrev.v6i4.2108>.

¹⁴ Martin 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, 690–695, <https://doi.org/10.1017/err.2024.78>.

¹⁵ Guido 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, no. 1 (2024): eaae021, sec. 3, <https://doi.org/10.1093/ijlit/eaae021>.

¹⁶ Uria Bernardus Anovanko, Andika Wijaya, and Satriya Nugraha, "Implikasi Hukum Perdata terhadap Penggunaan Kecerdasan Buatan (AI) dalam Kontrak Komersial" [Civil Law Implications of the Use of Artificial Intelligence (AI) in Commercial Contracts], *Innovative: Journal of Social Science Research* 5, no. 2 (2025): 3640–3644, <https://doi.org/10.31004/innovative.v5i2.18718>.

Indonesian positive law.¹⁷ Lim examines the urgency of personal-data protection in the context of AI-driven data processing in Indonesia,¹⁸ while, internationally, Kusche shows that the EU AI Act's own delineation of "harm" in terms of fundamental rights produces internal tensions that complicate, rather than resolve, questions of redress,¹⁹ and Magrani and de Miranda argue for a "right to reasonable inferences" as an extension of data-protection law that could similarly inform Indonesia's approach to AI-driven profiling under Government Regulation 71/2019.²⁰

Read together, these three strands remain largely parallel rather than integrated. Studies in the first strand debate AI's abstract legal status without translating that status into an operative liability rule; studies in the second strand construct a liability rule but do not test it against a quantified account of domestic harm or against the EU's most recent risk-tiered instrument, Regulation (EU) 2024/1689; and studies in the third strand address specific sectors (contracts, privacy) without connecting them back to the general unlawful-act framework of Articles 1365 and 1367. No study identified in this review combines (i) a bounded doctrinal liability construction under the KUH Perdata, (ii) a comparative risk-tiering analysis benchmarked against the finalised EU AI Act, and (iii) an evidentiary account of the scale of AI-caused loss in Indonesia.

This article makes three principal contributions to the existing literature. First, unlike Simbolon and Qurrahman, Ayunil, and Rahim, who each construct a single, undifferentiated liability rule, this article develops a three-track liability model that separately allocates responsibility to the creator/developer, the owner/operator, and the end user of an AI system, mapped onto the fault categories already available under Articles 1365 and 1367 of the KUH Perdata. Second, unlike Maharani and Masnun's forward-looking quasi-subject proposal, this article deliberately confines its claim to the object-based liability rule enforceable under current positive law, treating personhood reform as a suggestion for future legislation rather than a present-day legal conclusion. Third, this article is, to the authors' knowledge, among the first Indonesian civil-law studies to benchmark its liability construction against the finalised EU AI Act, Regulation (EU) 2024/1689, and against 2024–2025 comparative literature on the EU's AI Liability Directive, rather than against the Act's earlier draft stages relied upon in prior Indonesian scholarship.

Building on this positioning, this article aims to analyse the form of civil liability for losses caused by Artificial Intelligence under Indonesian civil law. Specifically, it addresses three bounded sub-questions: *first*, what is the legal status of AI within Indonesia's positive legal system, and does that status permit AI itself to bear civil liability; *second*, through which doctrinal mechanism under the KUH Perdata can liability for AI-caused loss be attributed, and to which party; and *third*, what can Indonesia's civil liability framework learn from the European Union's risk-tiered regu-

¹⁷ Jajang Nurzaman and Dwi Fidhayanti, "Keabsahan Kontrak yang Dibuat oleh Artificial Intelligence Menurut Hukum Positif di Indonesia" [The Validity of Contracts Made by Artificial Intelligence According to Positive Law in Indonesia], *Al 'Adl: Jurnal Hukum* 16, no. 1 (2024): 145–150, <https://doi.org/10.31602/al-adl.v16i1.12710>.

¹⁸ Jonathan Lim, "The Urgency of Personal Data Protection Related to Data Processing in the Form of Artificial Intelligence in Indonesia" (Bachelor's thesis, Faculty of Law, Lancang Kuning University, 2024), 12–15.

¹⁹ Isabel Kusche, "Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk," *Journal of Risk Research* (2024): 9–11, <https://doi.org/10.1080/13669877.2024.2350720>.

²⁰ Eduardo Magrani and Paulo Rodrigo de Miranda, "The Right to Reasonable Inferences in Automated Decision Systems as an Unfolding of the Fundamental Right to the Protection of Personal Data in Brazil and Beyond," *International Review of Law, Computers & Technology* 39, no. 1 (2025), sec. 2, <https://doi.org/10.1080/13600869.2024.2351676>.

latory model, and from Indonesia's own data-protection regime under Government Regulation 71/2019, in designing a more legally certain response to AI-caused harm.

2. Method

This research employs a normative-juridical method, examining law as a system of written norms, combined with a statutory approach and a conceptual approach.²¹ The statutory approach traces the positive-law provisions applicable to AI-caused civil loss, principally Articles 1365, 1367, and 1654 of the Kitab Undang-Undang Hukum Perdata (KUH Perdata/Indonesian Civil Code),²² Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, insofar as it defines the "electronic agent",²³ and Government Regulation Number 71 of 2019 on the Administration of Electronic Systems and Transactions.²⁴ The conceptual approach draws on legal-subject theory (natural-law and positive-law perspectives on legal personality) and on comparative liability theory, principally the European Union's Regulation (EU) 2024/1689 (the Artificial Intelligence Act),²⁵ and its accompanying liability-directive literature, to test whether Indonesia's existing doctrinal tools are adequate or require legislative supplementation.

Data were collected through library-based (doctrinal) research. Primary legal materials comprised the statutory provisions listed above. Secondary legal materials comprised peer-reviewed journal articles, indexed either in Scopus or in Indonesia's national Sinta index, selected using three criteria: (a) direct thematic relevance to AI civil liability, legal personhood, or AI-related data protection; (b) recency, with priority given to sources published in 2024–2025, while foundational theoretical works on the general theory of legal subjects were retained regardless of publication year; and (c) traceability via a DOI, Google Scholar, or Scopus record. Tertiary materials comprised official regulatory statements and verifiable regulator-adjacent news reporting (OJK, Komdigi, and the East Java Regional Police), used solely to substantiate the empirical scale and concrete occurrence of AI-related harm in Indonesia rather than as legal authority; each source was re-verified against its original publication.

Data analysis followed a qualitative, prescriptive-analytical technique appropriate to normative legal research: statutory provisions and secondary literature were read, categorised by theme (legal-subject status, liability construction, comparative regulation, and privacy/data protection), and then synthesised to test the internal consistency of applying Articles 1365 and 1367 of the KUH Perdata to AI-caused loss, before being evaluated against the comparative EU framework. This analysis is doctrinal rather than empirical: no fieldwork, observation, or interviews were conducted, and the term "qualitative" refers strictly to the non-numerical character of the legal-textual and literature data analysed.

²¹ Sidi Ahyar Wiraguna, "Eksplorasi Metode Penelitian dengan Pendekatan Normatif dan Empiris dalam Penelitian Hukum di Indonesia," *Lex Jurnalica* 22, no. 1 (2025): 66, 70–71, <https://doi.org/10.47007/lj.v22i1.8801>.

²² Kitab Undang-Undang Hukum Perdata [Indonesian Civil Code], arts. 1365, 1367, 1654.

²³ Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, art. 1 angka 8 (definition of "agen elektronik").

²⁴ Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

²⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), [2024] OJ L 168/1.

3. The Legal Status of Artificial Intelligence and the Construction of Civil Liability under Articles 1365 and 1367 of the KUH Perdata

3.1 The Legal-Subject Status of Artificial Intelligence in Indonesian Positive Law

Indonesian positive law recognises two categories of legal subject: natural persons and legal entities (*recht person*). Article 1 of the KUH Perdata confirms that a natural person's status as a bearer of civil rights attaches from birth and is not conditioned on any grant from the state,²⁶ while Article 1654 defines a legal entity as an association that, like a natural person, is authorised to perform civil legal acts unless a statute provides otherwise.²⁷ Both categories share one structural feature: each is capable of bearing rights and obligations, and each can, in principle, be made to answer for an unlawful act. Comparative scholarship on AI legal personality observes that legal-subject status has historically been a matter of deliberate legal recognition rather than an automatic consequence of any inherent physical or cognitive property, legal systems have extended, withheld, or graded personhood according to the regulatory purpose at hand, a pattern that recurs across the individual, collective, and gradient models of AI legal personality surveyed in comparative literature.²⁸ Van Apeldoorn adds the further requirement of legal capacity (*rechtsbevoegdheid*): the ability of a subject to exercise, and be held accountable for, the rights it holds, a capacity that can be partial (as with a minor) but must exist in some degree for liability to attach.²⁹

Measured against these two requirements, legal recognition and legal capacity, AI does not presently qualify as an Indonesian legal subject. No statute confers legal-subject status on AI, and AI cannot exercise legal capacity independently of the natural or legal persons who create, own, or operate it. Maharani and Masnun's proposal to treat AI as a "quasi-legal subject" is best read, on this evidence, as a normative recommendation for future legislation rather than a description of existing law: they acknowledge that Indonesia's positive-law framework does not currently accommodate a third category of legal subject alongside natural persons and legal entities.³⁰ Internationally, Filipova and Koroteev reach a parallel conclusion, recommending that AI be classified as an object of law, with a narrower "electronic agent" category reserved for functionally autonomous systems whose actions require closer regulatory attention without amounting to full legal personality.³¹

Because AI is not a legal subject, it is properly classified as an object, specifically, an intangible object, since AI exists as software and algorithmic processes with no physical form perceptible to the human senses. This classification is consistent with Simbolon's analysis, which treats AI as an object under the supervision of a legal subject for purposes of civil liability.³² It also resolves the terminological drift found in earlier Indonesian scholarship, where AI is sometimes discussed as an "object" and sometimes, loosely, as if it were already a quasi-subject: this article adopts the object classification as the operative legal position under current law, while treating subject-status reform as a suggestion for future legislation, addressed in the Conclusion below.

²⁶ Kitab Undang-Undang Hukum Perdata, art. 1.

²⁷ Kitab Undang-Undang Hukum Perdata, art. 1654.

²⁸ Filipova and Koroteev, "Future of the Artificial Intelligence," 365-368.

²⁹ Qurrahman, Ayunil, and Rahim, "Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence," 12688, discussing L. J. van Apeldoorn's concept of legal capacity (*rechtsbevoegdheid*).

³⁰ Maharani and Masnun, "Prospek Artificial Intelligence Sebagai Quasi Subjek Hukum," 10-12.

³¹ Filipova and Koroteev, "Future of the Artificial Intelligence," 370-375.

³² Simbolon, "Pertanggungjawaban Perdata terhadap Artificial Intelligence," 256-260.

3.2 Construction of Civil Liability under Articles 1365 and 1367 of the KUH Perdata

If AI is an object rather than a subject, liability for AI-caused loss cannot attach to the AI system itself; it must instead be attributed to a natural or legal person standing behind that object. Indonesian civil law offers two connected doctrinal bases for this attribution. Article 1365 of the KUH Perdata establishes the general unlawful-act (*perbuatan melawan hukum*) doctrine: a person who commits an unlawful act causing loss to another is obliged to compensate that loss, provided the classical elements, an unlawful act, fault, loss, and causal connection, are satisfied. Article 1367 extends this liability to loss caused by persons, or things, under one's supervision or control.³³ Read together, these two articles allow AI-caused loss to be attributed to whichever party exercised supervision or control over the AI system at the relevant time.

This article proposes that this attribution operate through a three-track model, differentiated by the point in the AI life cycle at which the fault-generating conduct occurred. **First**, where loss results from a design or training defect, a flawed algorithm, biased training data, or inadequate safety testing, liability should attach to the creator/developer under Article 1365, since the defect originates in conduct entirely within the developer's control and the developer possesses the technical capacity to have prevented it. **Second**, where loss results from inadequate supervision, deployment in an unsuitable context, or failure to maintain or update a system that was safe as designed, liability should attach to the owner/operator under Article 1367's supervision principle, in a manner analogous to an employer's liability for an employee, or an owner's liability for an animal, under existing Indonesian doctrine.³⁴ **Third**, where loss results from a user's misuse of an AI system outside its intended function or in violation of applicable terms of use, liability should attach to the user directly, on ordinary Article 1365 grounds. Comparative reasoning on liability allocation for AI-related risk supports directing responsibility towards the party best positioned to control the source of harm, ordinarily the developer or operator rather than the individual end user, a conclusion consistent with the doctrinal construction advanced above.³⁵

Applying this three-track model to the empirical cases introduced above clarifies how it would operate in practice. In the Polda Jatim deepfake case, the perpetrators were neither the developers of the underlying generative-AI tool nor the operators of a deployed AI system; they were end users who deliberately misused a publicly available AI capability to fabricate impersonating video and audio for fraudulent gain. Their conduct falls squarely on the third track, giving rise to ordinary Article 1365 liability and, since their conduct is also criminal, to concurrent criminal liability under the ITE Law, without implicating the AI developer, whose product was not defective but was simply misapplied. By contrast, the pattern of loss documented by OJK and Komdigi, concentrated in digital-banking identity-verification failures, points towards the first and second tracks: where a bank's liveness-detection or face-matching system was defeated because it was never designed to withstand deepfake spoofing, the design deficiency implicates the developer of that verification system under the first track; where a technically adequate system was deployed without the layered authentication, real-time anomaly detection, or periodic recalibration that the risk of deepfake fraud already required at the time of deployment, the deficiency implicates the

³³ Qurrahman, Ayunil, and Rahim, "Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence," 12690-12692.

³⁴ Puannandini et al., "Liabilitas Produk AI dalam Sistem Hukum Indonesia," 28-30.

³⁵ Qurrahman, Ayunil, and Rahim, "Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence," 12692-12693.

deploying financial institution as owner/operator under the second track. The three-track model is therefore not merely a taxonomy; it supplies a concrete allocation rule that a court, or a claimant's counsel, can apply to an actual fact pattern to identify the correct defendant, rather than defaulting to an undifferentiated claim against "the AI" or against whichever party happens to be reachable.

The principal practical obstacle to this model is evidentiary. Article 1365 places the burden of proving fault on the injured party, a general evidentiary rule reiterated in Article 1865 of the KUH Perdata, under which a party who asserts a right or a fact bears the burden of proving it. Yet AI systems, particularly those built on machine-learning architectures, are frequently opaque even to their own developers — the well-documented "black box" problem. Qurrahman, Ayunil, and Rahim identify this evidentiary asymmetry as the central practical weakness of relying on unmodified fault-based liability for AI harms.³⁶ Comparative experience with vicarious and strict liability in Indonesian product-liability practice suggests a workable adaptation: courts could apply a rebuttable presumption of fault against the developer or operator once the injured party demonstrates that the loss originated from the AI system's operation, shifting the burden to the defendant to show that the system met an applicable standard of care. This adaptation does not displace Article 1865; it operates within it, by treating proof that a loss originated from a specific AI system's output as sufficient to establish a *prima facie* case, after which the evidentiary burden shifts to the party with actual access to the system's design and operating records, ordinarily the developer or operator, not the claimant. This would preserve the fault-based structure of Article 1365 while addressing the practical difficulty AI's opacity creates for claimants, and it mirrors the logic already familiar to Indonesian courts from Article 1367's supervision-based liability, which likewise does not require the injured party to reconstruct exactly how a supervised person or thing came to cause harm.

4. Result and Analysis 2: Comparative Lessons from the European Union's Risk-Tiered AI Regulation and Indonesia's Data-Protection Regime

4.1 Comparative Perspective: The EU AI Act's Risk-Tiering Model

The European Union's Regulation (EU) 2024/1689 (the Artificial Intelligence Act) offers the most developed comparative model currently available, classifying AI systems into four risk tiers, unacceptable, high, limited, and minimal risk, and calibrating regulatory obligations to each tier.³⁷ High-risk systems, which include AI used in credit scoring, employment decisions, and critical infrastructure, are subject to mandatory conformity assessment, human oversight, and record-keeping obligations designed to make ex-post liability determinations easier by preserving an evidentiary trail. This tiering logic is instructive for Indonesia because it does not require resolving the legal-personhood debate discussed above; it operates entirely at the level of ex-ante regulatory obligation, which then supports, rather than replaces, the ordinary civil liability analysis already developed in this article.

Ebers cautions, however, that the AI Act's own risk-tiering is not yet "truly" risk-based in application: several of its high-risk categories are defined by closed, pre-set lists rather than by an em-

³⁶ Qurrahman, Ayunil, and Rahim, "Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence," 12690-12692.

pirical risk-benefit assessment, and systemic risks from general-purpose AI models are addressed only partially.³⁸ This matters for Indonesia because it counsels against a wholesale transplant of the EU's categorical lists; a more defensible approach would adapt the EU's tiering *logic*, proportioning regulatory and evidentiary obligations to the severity and probability of harm, while defining Indonesia's own risk categories by reference to sectors already identified as high-harm in the empirical data discussed in the Introduction, particularly AI used in financial-sector identity verification and credit decisioning, where the OJK and Komdigi data show the greatest concentration of documented loss.

Noto La Diega and Bezerra's analysis of the EU's proposed AI Liability Directive reinforces this caution from a different angle: they argue that a purely fault-based directive, even with relaxed evidentiary rules, under-delivers on victim protection when applied to unpredictable, self-adapting systems, and that strict liability is better justified for the highest-risk tier.³⁹ Applied to the three-track model developed above, this suggests that Indonesia's first track (creator/developer liability for design defects in high-risk applications, such as AI systems used in digital-banking identity verification) is the strongest candidate for a strict-liability standard, while the second and third tracks (owner/operator supervision failures and user misuse) can remain fault-based, consistent with the general structure of Articles 1365 and 1367. Kusche's finding that the AI Act's own definition of "harm" produces internal tension between a fundamental-rights framing and a product-safety framing⁴⁰ further supports keeping Indonesia's reform proposal narrowly tied to demonstrable financial and physical loss, rather than attempting, in the same instrument, to resolve the broader and more contested question of AI's impact on fundamental rights.

Adapting the EU model wholesale nevertheless faces a distinct obstacle in Indonesia's legal pluralism, which layers customary law, Islamic law, and Western-derived civil law within a single national system. Effective implementation of any risk-tiered AI liability rule would therefore require coordinated oversight involving the Ministry of Communication and Digital Affairs, the Financial Services Authority (OJK), and sectoral consumer-protection bodies, rather than a single regulator acting alone, echoing Puannandini and colleagues' finding that responsibility for AI-related harm in Indonesia is presently distributed across developers, users, and service providers without a single consolidated regulatory authority.⁴¹ A further, Indonesia-specific instrument already available for this coordination is Law Number 8 of 1999 on Consumer Protection, whose provisions on producer liability for defective goods and services⁴² supply a ready-made, sector-neutral analogue to the EU's product-liability logic: an AI-based consumer service that causes loss through a design or operational defect can already be framed, in parallel with the first and second tracks proposed above, as a defective "service" within the meaning of that Law, giving claimants a second, cumulative statutory basis alongside Articles 1365 and 1367 without waiting for AI-specific legislation.

³⁷ Regulation (EU) 2024/1689, arts. 6, 9, and Annex III (high-risk classification criteria).

³⁸ Ebers, "Truly Risk-Based Regulation of Artificial Intelligence," 690–695.

³⁹ Noto La Diega and Bezerra, "Can There Be Responsible AI without AI Liability?," eaae021, sec. 3.

⁴⁰ Kusche, "Possible Harms of Artificial Intelligence and the EU AI Act," 9–11.

⁴¹ Puannandini et al., "Liabilitas Produk AI dalam Sistem Hukum Indonesia," 31–32.

⁴² Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen [Law No. 8 of 1999 on Consumer Protection], arts. 19, 23.

4.2 Data Protection, Privacy, and Commercial-Contract Implications

AI's use of personal data in decision-making, most visibly in the deepfake-enabled fraud documented in the Introduction, but also in ordinary commercial applications such as credit scoring and targeted contract terms, raises a second, closely related civil-law concern: the protection of privacy and personal data. Anovanko, Wijaya, and Nugraha show that AI systems deployed in commercial contracting frequently process sensitive personal data (health status, political views, consumption habits) that is not strictly necessary for the contract's purpose, creating a tension with the principle of data minimisation.⁴³ Nurzaman and Fidhayanti add that where an AI system autonomously generates or modifies contract terms based on such data, the validity of the resulting agreement under Indonesian contract-law doctrine (particularly the requirement of a lawful cause under Article 1320 of the KUH Perdata) becomes uncertain, compounding the civil-liability question addressed above.⁴⁴

Government Regulation Number 71 of 2019 already articulates a privacy-by-design principle for electronic-system operators, requiring that personal data be processed only for purposes consistent with its original collection.⁴⁵ Lim's analysis of AI-driven data processing in Indonesia finds that this principle is regularly honoured in the abstract but rarely operationalised in AI system design, because Indonesian regulators lack a technical standard analogous to the EU's data-protection-impact-assessment requirement for high-risk processing, and because oversight remains fragmented across sectoral regulations rather than consolidated in a single, AI-specific instrument, which weakens both preventive compliance and after-the-fact enforcement.⁴⁶

In the financial sector specifically, the sector most implicated by the OJK and Komdigi data discussed in the Introduction, Ramadhani and Wiraguna's 2025 study of personal-data-protection implementation in financial-services information systems finds that technical safeguards (encryption, access control, anomaly detection) are unevenly adopted across institutions, leaving a compliance gap that directly enables the kind of deepfake-based identity-verification fraud documented above.⁴⁷ Magrani and de Miranda's proposed "right to reasonable inferences", requiring data controllers to justify, *ex ante*, why a given inference drawn from personal data is normatively acceptable for its intended use, offers a transferable model for Indonesia: applied to AI-driven credit and identity-verification decisions, it would require financial institutions to document and justify the inferential logic underlying an AI system's decision before that decision is relied upon, creating exactly the kind of evidentiary record that this article's evidentiary analysis identifies as necessary to overcome AI's evidentiary opacity in subsequent liability litigation.⁴⁸ A comparable non-EU precedent is instructive here: South Korea's 2024 amendment to its Personal Information Protection Act introduced a data-subject right to object to fully automated decisions, but Kim and Park's critical review shows that the amendment still places the burden of invoking that right on the data

⁴³ Anovanko, Wijaya, and Nugraha, "Civil Law Implications of the Use of Artificial Intelligence," 3645-3648.

⁴⁴ Nurzaman and Fidhayanti, "Keabsahan Kontrak yang Dibuat oleh Artificial Intelligence," 151-155.

⁴⁵ Peraturan Pemerintah Nomor 71 Tahun 2019, art. 14 (principle of privacy by design).

⁴⁶ Lim, "Urgency of Personal Data Protection," 40-46.

⁴⁷ Wyanda Kinanti Syauqi Ramadhani and Sidi Ahyar Wiraguna, "Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan," *Perspektif Administrasi Publik dan Hukum* 2, no. 2 (2025): 165-168, <https://doi.org/10.62383/perspektif.v2i2.248>.

⁴⁸ Magrani and de Miranda, "Right to Reasonable Inferences," sec. 2.

subject rather than the controller, a design choice Indonesia should avoid if it wishes the “reasonable inferences” model above to function as intended.⁴⁹

Taken together, this article’s findings answer the three research sub-questions posed in the Introduction. AI is not, under current Indonesian positive law, a legal subject capable of bearing liability in its own right (sub-question one); civil liability for AI-caused loss is properly constructed through a three-track application of Articles 1365 and 1367 of the KUH Perdata to the developer, operator, and user respectively, reinforced, where the harm arises from a consumer-facing AI service, by the cumulative protection of Law Number 8 of 1999 on Consumer Protection – and supported where necessary by a rebuttable presumption of fault to offset AI’s evidentiary opacity (sub-question two); and the EU AI Act’s risk-tiering logic, together with Government Regulation 71/2019’s privacy-by-design principle, offers Indonesia a template for calibrating regulatory and evidentiary obligations to the severity of harm without requiring Indonesia to resolve the contested question of AI legal personhood first (sub-question three). The consistency across these three answers an object-based liability rule, a doctrinally grounded attribution mechanism, and a proportionate regulatory template is what allows the three-track model proposed in this article to function as an integrated response to the research gap identified in the Introduction, rather than as three independent conclusions loosely associated with a common topic.

5. Conclusion

This article set out to analyse the form of civil liability for losses caused by Artificial Intelligence under Indonesian civil law, and the analysis sustains three linked conclusions together with the recommendations that follow from them. First, AI does not qualify as a legal subject under Indonesia’s positive legal system: it lacks both the legal recognition and the independent legal capacity that Indonesian doctrine requires of a bearer of rights and obligations, and is therefore properly classified as an intangible object under the supervision of a natural or legal person. Second, liability for AI-caused loss can and should be constructed through Articles 1365 and 1367 of the KUH Perdata, applied through a three-track model that allocates responsibility to the creator/developer for design defects, to the owner/operator for supervisory failures, and to the user for misuse, supported by a rebuttable presumption of fault to offset the evidentiary difficulty that AI’s technical opacity otherwise creates for injured parties, and reinforced, for consumer-facing AI services, by the cumulative protection already available under Law Number 8 of 1999 on Consumer Protection. Third, the European Union’s risk-tiered regulatory logic under Regulation (EU) 2024/1689, adapted to Indonesia’s own empirically documented risk concentrations, particularly AI-enabled identity-verification fraud in the financial sector, illustrated by the OJK, Komdigi, and Polda Jatim cases discussed above and combined with the privacy-by-design obligations already present in Government Regulation 71/2019, offers a workable template for calibrating Indonesia’s future AI-specific regulation without first requiring resolution of the contested legal-personhood debate. The practical significance of these findings is underscored by the scale of documented harm: with public losses from AI-enabled fraud in Indonesia running into the trillions of rupiah annually, the

⁴⁹ Dong Hyeon Kim and Do Hyun Park, “Automated Decision-Making in South Korea: A Critical Review of the Revised Personal Information Protection Act,” *Humanities and Social Sciences Communications* 11, no. 1 (2024): art. 974, <https://doi.org/10.1057/s41599-024-03470-y>.

absence of an AI-specific civil liability framework is not a theoretical gap but an active source of legal uncertainty for victims, developers, and financial institutions alike, and the three-track liability model proposed in this article is designed to be applied under existing law immediately. Building on this, the article offers three sets of recommendations: for the legislature, Indonesia should enact AI-specific implementing regulation, whether as a government regulation under the amended Electronic Information and Transactions Law or as free-standing legislation, that formally defines the “electronic agent” concept already introduced by Law Number 1 of 2024 in terms sufficient to support the three-track liability model, introduces a rebuttable presumption of fault against the developer or operator of a high-risk AI system once a claimant shows that loss originated from that system’s operation, and adopts a narrow, Indonesia-specific risk-tiering schedule modelled on the EU AI Act’s regulatory logic but anchored in the sectors, beginning with financial-sector identity verification, where OJK and Komdigi data show the greatest concentration of documented harm; for regulators and financial-sector institutions, the Financial Services Authority, in coordination with the Ministry of Communication and Digital Affairs, should require financial institutions deploying AI-based identity-verification and credit-decisioning systems to maintain documented, auditable records of the inferential basis for automated decisions, consistent with the “reasonable inferences” model discussed above, both to reduce deepfake-enabled fraud directly and to create the evidentiary record needed to support future civil claims under Articles 1365 and 1367; and for future research, empirical studies tracking actual Indonesian court decisions applying Articles 1365 and 1367 to AI-adjacent disputes, once such decisions accumulate, would allow the three-track liability model proposed here to be tested against judicial practice rather than doctrinal argument alone, while comparative research extending this analysis beyond the EU to other Asian jurisdictions developing AI-specific liability rules would help refine the regulatory recommendations offered above.

References

- Anovanko, Uria Bernandus, Andika Wijaya, and Satriya Nugraha. “Implikasi Hukum Perdata terhadap Penggunaan Kecerdasan Buatan (AI) dalam Kontrak Komersial” [Civil Law Implications of the Use of Artificial Intelligence (AI) in Commercial Contracts]. *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>.
- Dinas Komunikasi dan Informatika Provinsi Jawa Timur. “Polda Jatim Ungkap Kasus Penipuan Deepfake AI Kepala Daerah, Pelaku Kantongi Keuntungan Hingga Rp87 Juta.” April 29, 2025. <https://kominfo.jatimprov.go.id/berita/polda-jatim-ungkap-kasus-penipuan-deepfake-ai-kepala-daerah-pelaku-kantongi-keuntungan-hingga-rp87-juta>.
- 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. Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 168/1, 2024.

- Filipova, I. A., and V. D. Koroteev. "Future of the Artificial Intelligence: Object of Law or Legal Personality?" *Journal of Digital Technologies and Law* 1, no. 2 (2023): 359–386. <https://doi.org/10.21202/jdtl.2023.15>.
- GadgetDIVA.id. "OJK Ungkap Bahaya Deepfake AI di Sektor Keuangan, Kerugian Penipuan Digital Tembus Rp6 Triliun." May 14, 2026. <https://www.gadgetdiva.id/news/ojk-ungkap-bahaya-deepfake-ai>.
- Harian Jogja. "Penipuan AI dan Deepfake Kian Marak, Komdigi: Kerugian Capai Rp9 T." June 17, 2026. <https://news.harianjogja.com/r-1260091/penipuan-ai-dan-deepfake-kian-marak-komdigi-kerugian-capai-rp9-t>.
- Kim, Dong Hyeon, and Do Hyun Park. "Automated Decision-Making in South Korea: A Critical Review of the Revised Personal Information Protection Act." *Humanities and Social Sciences Communications* 11, no. 1 (2024): art. 974. <https://doi.org/10.1057/s41599-024-03470-y>.
- Kitab Undang-Undang Hukum Perdata [Indonesian Civil Code].
- Kusche, Isabel. "Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk." *Journal of Risk Research* (2024). <https://doi.org/10.1080/13669877.2024.2350720>.
- Lim, Jonathan. "The Urgency of Personal Data Protection Related to Data Processing in the Form of Artificial Intelligence in Indonesia." Bachelor's thesis, Faculty of Law, Lancang Kuning University, 2024.
- Magrani, Eduardo, and Paulo Rodrigo de Miranda. "The Right to Reasonable Inferences in Automated Decision Systems as an Unfolding of the Fundamental Right to the Protection of Personal Data in Brazil and Beyond." *International Review of Law, Computers & Technology* 39, no. 1 (2025). <https://doi.org/10.1080/13600869.2024.2351676>.
- Maharani, Bintang M.D., and Muh. Ali Masnun. "Prospek Artificial Intelligence Sebagai Quasi Subjek Hukum: Dinamika Pengaturan Hukum Perdata di Indonesia" [Prospects of Artificial Intelligence as a Quasi-Legal Subject: Dynamics of Civil Law Regulation in Indonesia]. *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora* 4, no. 2 (2024): 1–19. <https://doi.org/10.53697/iso.v4i2.2063>.
- 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, no. 1 (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" [The Validity of Contracts Made by Artificial Intelligence According to Positive Law in Indonesia]. *Al 'Adl: Jurnal Hukum* 16, no. 1 (2024): 140–159. <https://doi.org/10.31602/al-adl.v16i1.12710>.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [Government Regulation No. 71 of 2019 on the Administration of Electronic Systems and Transactions].
- 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>.
- Qurrahman, Shofika Hardiyanti, Safira Ayunil, and Tsabita Aurelia Rahim. "Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence dalam Hukum Positif Indonesia" [The Position and Concept of Artificial Intelligence Liability in Indonesian Positive Law]. *Unes Law Review* 6, no. 4 (2024): 12687–12693. <https://doi.org/10.31933/unesrev.v6i4.2108>.

- Ramadhani, Wyanda Kinanti Syauqi, and Sidi Ahyar Wiraguna. "Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan." *Perspektif Administrasi Publik dan Hukum* 2, no. 2 (2025): 158–175.
<https://doi.org/10.62383/perspektif.v2i2.248>.
- Simbolon, Yolanda. "Pertanggungjawaban Perdata terhadap Artificial Intelligence yang Menimbulkan Kerugian Menurut Hukum di Indonesia" [Civil Liability for Artificial Intelligence Causing Losses According to Law in Indonesia]. *Veritas et Justitia* 9, no. 1 (2023): 246–273. <https://doi.org/10.25123/vej.v9i1.6037>.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions].
- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen [Law No. 8 of 1999 on Consumer Protection].
- Wen, Zhifeng, and Deyi Tong. "Analysis of the Legal Subject Status of Artificial Intelligence." *Beijing Law Review* 14 (2023): 74–86. <https://doi.org/10.4236/blr.2023.141004>.
- Wiraguna, Sidi Ahyar. "Eksplorasi Metode Penelitian dengan Pendekatan Normatif dan Empiris dalam Penelitian Hukum di Indonesia." *Lex Jurnalica* 22, no. 1 (2025): 66–72.
<https://doi.org/10.47007/lj.v22i1.8801>.
-