NEGREI
Academic Journal
of Law and Governance

Institut Agama Islam Negeri (IAIN) Curup, Indonesia
ISSN 2775-8621 (p), 2798-3803 (e)
volume 4, number 1, 2024
DOI: http://doi.org/10.29240/negrei.v4i1.13199

Reconstructing Legal Liability Models for AI Misuse on Personal Data Privacy in Indonesia: A Constitutional Law and Regulatory Perspective

Khiswatul Barokah[1], Yuliati[2], Abdul Madjid[3]
[1,2,3]Universitas Brawijaya Malang, Indonesia
Correspondence: khiswatulbarok_@student.ub.ac.id

Abstract. The increasing use of Artificial Intelligence (AI) in digital environments introduces new challenges to data privacy law. Indonesia's Personal Data Protection Act (Law No. 27 of 2022) does not yet fully address the autonomous and complex nature of AI systems that process personal data without direct human control. This study employs a normative juridical method, integrating statutory analysis of Indonesian legislation, conceptual exploration of legal accountability, and comparative evaluation against the European Union's GDPR framework. By examining these layers, the research identifies gaps in assigning liability among developers, data controllers, and platform providers, particularly regarding algorithmic profiling and automated decision-making. The findings suggest that adopting principles such as vicarious liability, corporate responsibility, and risk-based regulation could enhance Indonesia's legal framework. This proposed accountability model aims to better protect individuals' digital rights and align national regulations with international standards, anticipating the evolving risks of AI technologies.

Keywords: *algorithmic decision-making; data controller accountability; risk-based data governance; legal liability in AI systems; privacy violations in digital platforms*

Introduction

The advancement of Artificial Intelligence (AI) has transformed the way humans interact with technology and has influenced nearly every aspect of life, including the economy, law, education, and governance. AI is no longer merely an auxiliary tool; it has evolved into an autonomous system capable of processing complex data and making independent decisions based on machine learning algorithms. This phenomenon presents profound challenges to the social order, as AI can access, process, and predict individual behavior based on the digital data generated daily.From a philosophical standpoint, the right to privacy is derived from fundamental human rights, and the emergence of AI predicated on the exploitation of personal data raises critical questions regarding the moral and ethical boundaries of its use.[1] When personal information is utilized without an individual's knowledge or consent, violations of personal dignity and autonomy become inevitable.

From a sociological perspective, modern digital society tends to be more interconnected and open in sharing information, whether voluntarily or unconsciously. This behavioral shift has fostered a digital environment that enables the massive and real-time aggregation of data by AI systems. However, the use of such technology is often not accompanied by a critical public awareness of the risks related to data breaches and the misuse of personal information. The growing tendency of individuals to entrust decision-making processes to automated systems also contributes to a power asymmetry between technology providers and users. This imbalance has structural implications, particularly concerning the vulnerability of individual rights protection.[2]

From a legal standpoint, the emergence of AI necessitates the adaptation of existing legal frameworks, particularly in the domains of personal data protection and cybercrime. In Indonesia, Law No. 27 of 2022 on Personal Data

[1] Kirsten Martin, "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics* 137, no. 3 (September 2016): 551–69, https://doi.org/10.1007/s10551-015-2565-9.

[2] Shoshana Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Edn," *PublicAffairs, New York*, 2019.

Protection represents an initial response to the growing regulatory need. However, this legislation does not yet fully address the issue of legal liability for systems that lack legal personhood as juridical subjects. In this context, reconstructing the model of liability becomes an urgent task for modern legal theory, aiming to bridge the normative gap between the law and the rapidly evolving landscape of disruptive digital technologies.

Over the past decade, research on artificial intelligence and its legal implications has grown significantly, particularly regarding personal data protection. Much of the existing literature emphasizes how AI challenges the right to privacy through large-scale data collection and analysis conducted without transparency or explicit consent from individuals.A central issue that arises is the ambiguous legal status of AI as an actor in the violation of such rights, alongside the absence of an adequate system of legal accountability for the misuse of AI technologies by individuals, corporations, or even state institutions.[3] On the other hand, international legal developments such as the European Union's General Data Protection Regulation (GDPR) have served as global references; however, they still leave unresolved questions regarding the limits of liability when AI systems act autonomously based on user-provided input data.

While several studies have examined ethical principles and responsible AI governance, the dominant approach remains largely conceptual and normative, lacking a systematic focus on concrete legal accountability mechanisms. Even within the national legal context, there is a notable scarcity of research that explicitly links Law No. 27 of 2022 on Personal Data Protection with the problematic use of AI systems in critical sectors such as education, business, and public services. This gap becomes significant given the nature of AI as not merely instrumental, but also adaptive and predictive, which complicates conventional fault attribution.[4] This paper aims to address that gap by offering a reconstruction perspective on legal accountability one that not only emphasizes end-user responsibility but also considers the roles of technology

[3] Mariarosaria Taddeo and Luciano Floridi, "How AI Can Be a Force for Good," *Science* 361, no. 6404 (August 2018): 751–52, https://doi.org/10.1126/science.aat5991.

[4] Reuben Binns, "Algorithmic Accountability and Public Reason," *Philosophy & Technology* 31, no. 4 (December 2018): 543–56, https://doi.org/10.1007/s13347-017-0263-5.

providers and the AI systems themselves as mediating entities in personal data violations. This approach positions the Personal Data Protection Law as the primary analytical framework and evaluates the extent to which existing regulations are capable of addressing systemic and undetectable AI misuse that escapes traditional legal mechanisms. In doing so, this study contributes not only to normative discussions on AI but also to building a conceptual and juridical foundation for restructuring legal accountability in the context of AI-driven infringements on personal data protection.

The rapid adoption of artificial intelligence across various sectors of life is not always matched by the readiness of legal systems to anticipate its potential misuse. One of the most fundamental unresolved issues is the ambiguity surrounding who holds legal responsibility when violations occur as a result of AI usage particularly in the context of personal data protection. This situation is exacerbated by the autonomous and adaptive nature of AI, which is not always directly controlled by humans at every stage of its operation.[5] Although legal instruments such as Indonesia's Law No. 27 of 2022 on Personal Data Protection have been enacted, their implementation still faces challenges in addressing cases involving disruptive technologies like AI. Meanwhile, the exponential growth of the AI market and its increasing penetration into sectors such as education, healthcare, and digital justice raise the potential for significant legal and social harm if not promptly addressed through more adaptive regulatory frameworks.[6] This reality underscores the urgent need to develop a legal liability framework capable of addressing the complexities of AI-induced violations, so that the law does not continue to lag behind technological advancements.

The primary legal issue arising from the misuse of artificial intelligence concerns accountability for violations of individual privacy rights, particularly in cases where personal data is used without consent or is exploited for unintended

[5] Peter Wagner, "Mind the Gap(s): Moral Philosophy, International Law and Interpretative Historical Sociology," *European Journal of Social Theory* 26, no. 4 (November 2023): 527–35, https://doi.org/10.1177/13684310231164258.

[6] Andrej J. Zwitter, Oskar J. Gstrein, and Evan Yap, "Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual," *Frontiers in Blockchain* 3 (May 2020): 26, https://doi.org/10.3389/fbloc.2020.00026.

purposes. In situations where AI operates autonomously based on algorithms trained by system providers, it becomes difficult to identify the legally liable party. This problem is further compounded when AI systems are used by individuals or institutions lacking a comprehensive understanding of their legal implications, yet still resulting in legal consequences for affected data subjects.[7] The core challenge lies in determining the appropriate legal subject to hold accountable whether it is the end user, the developer, or a third party accessing the data through the AI system. Within the Indonesian legal framework, no mechanism currently exists that explicitly establishes a hierarchical model of responsibility in AI-related data violations. The absence of such standards leads to legal uncertainty in the enforcement of privacy rights protected under Law No. 27 of 2022. In this context, reconstructing a liability model grounded in the functional relationships and degrees of control over AI systems becomes an urgent necessity.

This study aims to identify the forms of artificial intelligence misuse that result in violations of personal data and to evaluate the existing legal framework in safeguarding the rights of data subjects. In addition, the research analyzes the applicable legal liability for perpetrators of such misuse whether individuals or institutions from the perspective of Indonesian positive law. The study is also intended to formulate a legal liability model that is adaptive to the complexities of AI systems, while simultaneously addressing the normative gaps that remain unregulated under Law No. 27 of 2022.

Research Methods

This study employs a normative juridical approach to critically analyze the legal challenges posed by the misuse of Artificial Intelligence (AI) in relation to personal data violations. The core focus is on Indonesian statutory regulations, especially Law No. 27 of 2022 on Personal Data Protection, complemented by international legal frameworks such as the European Union's General Data Protection Regulation (GDPR). To deepen the analysis, a conceptual approach

[7] Margarita Robles Carrillo, "Artificial Intelligence: From Ethics to Law," *Telecommunications Policy* 44, no. 6 (July 2020): 101937, https://doi.org/10.1016/j.telpol.2020.101937.

is used to clarify foundational legal concepts, including "legal liability," "personal data breach," and the status of "AI entities" as legal objects. Additionally, a comparative method examines liability models from other jurisdictions to identify best practices applicable to Indonesia. [8]

The study draws on three categories of legal materials: primary sources such as laws and international treaties; secondary literature including academic publications and policy reports; and tertiary sources like legal dictionaries and encyclopedias.[9] These sources provide a comprehensive basis for identifying regulatory gaps and exploring potential reforms.[10]

Analytically, the study employs systematic interpretation to ensure coherence among interconnected legal norms and legal argumentation to construct a normative accountability framework.[11] This framework is grounded in principles of justice, legal certainty, and individual responsibility, aiming to adapt legal liability doctrines to the complexities of AI-driven disruptive technologies.[12]

Discussion

Characteristics of AI Misuse in the Context of Personal Data

Artificial Intelligence (AI) operates by utilizing vast amounts of data (big data) to train algorithms in generating predictions, decisions, or automated recommendations. In the process, AI requires access to personal data that reflects individuals' behaviors, preferences, locations, and even biometric information, which are collected through various digital channels such as

[8] Tunggul Ansari Setia Negara, "Normative Legal Research in Indonesia: Its Originis and Approaches," *Audito Comparative Law Journal (ACLJ)* 4, no. 1 (February 2023): 1–9, https://doi.org/10.22219/aclj.v4i1.24855.

[9] Sean Mulcahy, "Methodologies of Law as Performance," *Law and Humanities* 16, no. 2 (July 2022): 165–82, https://doi.org/10.1080/17521483.2022.2123616.

[10] Debasis Poddar, "Genealogy of Legal Research Methodology," *Asian Journal of Legal Education*, February 27, 2025, 23220058251321027, https://doi.org/10.1177/23220058251321027.

[11] John Bouvier, *A Law Dictionary: Vol. I* (BoD–Books on Demand, 2022).

[12] Siobhán McInerney-Lankford, "Legal Methodologies and Human Rights Legal Research: Challenges and Opportunities," in *Research Methods in Human Rights*, ed. Bård A. Andreassen, Claire Methven O'Brien, and Hans-Otto Sano (Edward Elgar Publishing, 2024), 14–35, https://doi.org/10.4337/9781803922614.00011.

mobile applications, smart devices, and websites. This data is often gathered through non-transparent processes and without the explicit consent of users, raising serious concerns regarding the protection of privacy rights.

The mechanisms of data collection and processing by AI are generally passive and continuous, relying on digital tracking systems, cookies, and sensors, over which users have little to no control regarding how their data is utilized. Once processed, AI systems not only build detailed individual profiles but also extract predictive behavioral patterns such as consumer habits, health conditions, or financial risk potential. While such activity enhances system efficiency, it simultaneously amplifies the potential for misuse due to its opaque and largely unauditable nature.

The misuse of AI in relation to personal data becomes particularly vulnerable due to the fact that AI lacks moral awareness or ethical capacity, relying entirely on the values encoded by its developers or system operators. The problem is further exacerbated in commercial practice, where technology developers often lack incentives to prioritize transparency and fairness, focusing instead on efficiency and profitability. This is compounded by the absence of clear regulatory standards that impose strict responsibilities on data processing by AI systems. When AI is deployed for economic or surveillance purposes such as targeted advertising or social risk assessment users are often unaware that their data has been manipulated to generate specific outcomes, which may lead to bias or discrimination.[13] In this context, the relationship between humans and machines becomes increasingly asymmetrical, as individuals lose control over their digital representations, which are managed by automated systems. This condition renders AI not only a technically disruptive technology but also one that challenges fundamental principles of data protection, which place the human being at the center as an autonomous legal subject.

[13] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, “Transparent, Explainable, and Accountable AI for Robotics,” *Science Robotics* 2, no. 6 (May 2017): eaan6080, https://doi.org/10.1126/scirobotics.aan6080.

The misuse of artificial intelligence in relation to personal data generally occurs in various forms, all of which fundamentally violate an individual's right to control over their personal information. One of the most basic forms of violation is the extraction of data without valid consent or without adequate informed consent. Many digital platforms employ AI to access data from users' devices including location, contacts, browsing history, and behavioral preferences without providing clear explanations about the purposes of data collection or the extent to which the data will be processed and stored.[14] In numerous cases, user consent is obscured through lengthy and complex terms of service, making it difficult for individuals to understand that they are passively surrendering their personal data. This practice results in a significant asymmetry of information and control between users and system operators, undermining the foundational principle of autonomy in data governance.

The use of personal data for profiling purposes also constitutes a practice fraught with risk. AI is employed to construct digital representations of individuals based on their online activities, and these representations are then used to segment groups according to perceived risk levels, consumer behavior, or social potential. Such profiles can be applied in decision-making processes with significant consequences, such as employment selection, credit approval, or even predictive policing systems leading to injustice when AI draws conclusions based on discriminatory patterns embedded in its training data.[15] AI technology not only reproduces existing biases but can also amplify them systematically on a broader scale, institutionalizing discrimination under the guise of algorithmic objectivity.

Another form of violation is behavioral surveillance conducted without the user's awareness. AI systems are capable of recording patterns of interaction, clicks, page visit durations, and even emotions captured through device sensors, all of which are utilized to continuously generate behavioral predictions. In such

[14] Alessandro Mantelero, "The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten,'" *Computer Law & Security Review* 29, no. 3 (June 2013): 229–35, https://doi.org/10.1016/j.clsr.2013.03.010.

[15] Solon Barocas and Andrew D Selbst, "Big Data's Disparate Impact," *Calif. L. Rev.* 104 (2016): 671.

practices, individuals are not merely passive data subjects but are entrapped within algorithmic observation systems that shape and influence their choices and behavior. When such surveillance is carried out without transparency and accountability, violations of the principles of privacy, justice, and individual freedom become inevitable.[16] These practices demonstrate that the misuse of AI with respect to personal data is not merely a matter of technical infringement but reflects a systemic pattern requiring stronger and more responsive legal intervention.

The misuse of artificial intelligence in personal data processing poses a serious threat to the core principles of data protection, which fundamentally safeguard the right to privacy in digital society. One of the key principles frequently violated in AI practices is the principle of transparency. Modern AI systems particularly those based on machine learning and deep learning operate through algorithmic structures that are not easily comprehensible to lay users or regulatory authorities. As a result, individuals are often unaware of how their personal data is collected, analyzed, and utilized.[17] This lack of transparency leads to users' inability to exercise control over or understand the consequences of their interactions with predictive and automated systems. Consequently, it weakens their position as data subjects protected under the law, undermining the very foundation of data privacy guarantees in democratic digital governance.

Violations of the principle of purpose limitation also frequently occur. In many cases, personal data initially collected for a specific purpose such as account registration or access to certain services is later repurposed by AI systems for entirely different objectives, such as targeted advertising, risk assessment, or automated decision-making, without obtaining renewed consent from the data

[16] Muhammad Firkan Muhammad Muslim and Indi Izza Afdania, "Legal Construction of Criminal Prosecution Against Perpetrators of Rape in the Metaverse," *Peradaban Hukum Nusantara* 1, no. 1 (August 2024): 59–74, https://doi.org/10.62193/3aga8d22.

[17] Jenna Burrell, "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms," *Big Data & Society* 3, no. 1 (June 2016): 2053951715622512, https://doi.org/10.1177/2053951715622512.

subject.[18] When data is used beyond its original purpose, the legitimacy of the processing becomes weakened and risks infringing on the right to privacy as guaranteed under legal instruments such as Article 5 of the General Data Protection Regulation (GDPR) and Indonesia's Law No. 27 of 2022 on Personal Data Protection.

The principle of accountability, as a key element in data protection systems, is also frequently overlooked within AI-driven technological ecosystems. The absence of a clearly identifiable entity responsible for the consequences of automated decision-making leads to ambiguity in the attribution of legal fault. This reflects a structural gap in regulatory frameworks, which have yet to adequately adapt to the evolving dynamics of emerging technologies. When these three core principles transparency, purpose limitation, and accountability are not consistently upheld, personal data protection becomes severely weakened, placing individual privacy rights in an increasingly vulnerable position under algorithmic exploitation.

One of the fundamental issues in the misuse of artificial intelligence concerning personal data lies in the imbalance of power between end-users and technology controllers, creating a structural asymmetry in terms of control and legal responsibility. AI systems are often developed with complex, opaque architectures that are not independently auditable even by their users. When such systems make automated decisions based on collected personal data, users lack the bargaining power to review, contest, or rectify the outcomes. This condition reinforces what is referred to as asymmetric power, wherein technology corporations hold full access to data and algorithms, while users lack sufficient information to understand how their rights are being processed or potentially violated.

This imbalance is further exacerbated by the lack of explicit accountability mechanisms directed at technology providers. Many AI developers operate within licensing frameworks that shift the entire legal risk to end-users, even

[18] Nikolaus Forgó, Stefanie Hänold, and Benjamin Schütze, "The Principle of Purpose Limitation and Big Data," in *New Technology, Big Data and the Law*, ed. Marcelo Corrales, Mark Fenwick, and Nikolaus Forgó, Perspectives in Law, Business and Innovation (Singapore: Springer Singapore, 2017), 17–42, https://doi.org/10.1007/978-981-10-5038-1_2.

though AI systems often function with a high degree of autonomy and make decisions that users cannot fully control. In numerous instances, AI providers limit their liability through complex terms of service, thereby avoiding responsibility when their systems cause harm such as data breaches or discriminatory outcomes. When such accountability is neither normatively regulated nor accompanied by enforceable mechanisms, a legal vacuum emerges. This gap enables systemic violations to occur without clear legal consequences, undermining the very foundation of personal data protection and the rule of law in the digital age.

Normative Weaknesses in Personal Data Protection Against AI Systems

One of the fundamental shortcomings in Indonesia's legal framework for personal data protection is the absence of explicit regulation regarding the legal status of Artificial Intelligence (AI) as either a subject or object of law. Law No. 27 of 2022 on Personal Data Protection recognizes only two primary categories involved in data processing: data controllers and data processors both of which implicitly refer to human entities or legal persons. There is no legal recognition of AI systems as entities that can bear legal responsibility for autonomous actions, even though AI is increasingly utilized to access, process, and even make decisions based on personal data without direct human intervention. When AI systems cause harm to data subjects, no mechanism currently exists to assign legal liability to the systems themselves, as positive law still relies on classical conceptions of legal subjectivity, which require will and legal consciousness.[19]

In the context of personal data protection, the artificial intelligence ecosystem involves various entities with distinct roles, such as algorithm developers, platform providers, and end-users. Each party holds differing degrees of control and access over personal data. However, the legal framework in Indonesia particularly Law No. 27 of 2022 on Personal Data Protection has yet

[19] Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*, vol. 10, Law, Governance and Technology Series (Dordrecht: Springer Netherlands, 2013), https://doi.org/10.1007/978-94-007-6564-1.

to clearly regulate a multi-layered liability model. When violations of personal data occur through AI systems, the existing legal mechanisms are not equipped to proportionally allocate liability among the involved parties. This creates ambiguity in accountability pathways when AI systems operate autonomously based on technical parameters set by developers, executed by users, or mediated by third-party platforms.

In contrast, the European Union's General Data Protection Regulation (GDPR) provides a clear classification of roles into data controllers and data processors, each bearing distinct but interconnected legal obligations.[20] Under this scheme, liability is not only assigned to the party directly committing the violation but also to those determining the purpose and means of data processing. This layered approach enables more precise attribution of responsibility, particularly in cases involving a combination of technical faults and administrative negligence. It also facilitates collaborative risk mitigation mechanisms and promotes the application of shared accountability principles in personal data governance.

The lack of clarity in regulating layered liability within AI systems in Indonesia hampers the effective implementation of key legal principles. In many cases, end-users become the most likely parties to face legal action, despite the fact that control over AI systems and data processing structures typically rests with other entities that hold greater technical and economic power. This imbalance creates opportunities for systemic violations to go undetected or unaddressed, due to the absence of a legal subject that can be held directly and proportionally accountable. The ambiguity in legal relationships among actors within AI ecosystems undermines core principles such as liability, procedural justice, and legal certainty in the realm of personal data protection in the digital age.

Within the artificial intelligence ecosystem, the process of algorithm training heavily depends on training data used to develop the system's predictive capabilities. This data often includes personal information gathered from

[20] Simant Shankar Bharti and Saroj Kumar Aryal, "The Right to Privacy and an Implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the Companies," *Journal of Contemporary European Studies* 31, no. 4 (October 2023): 1391–402, https://doi.org/10.1080/14782804.2022.2130193.

various sources either directly from users or indirectly through recorded online activities. The problem lies in the absence of specific regulations in Indonesian law that clearly define the legality, origin, and limits of using personal data for AI model training. Although Law No. 27 of 2022 on Personal Data Protection provides general principles, it does not explicitly restrict the use of personal data for algorithmic training purposes, nor does it require separate consent for the use of such data in machine learning processes. When data is used during the training phase without the knowledge or explicit permission of its owner, individuals' rights to control their personal information are systemically disregarded.[21]

Beyond issues during the training phase, further challenges arise in the deployment of AI systems that generate automated decisions such as risk assessment, classification, or recommendation—based on personal data analysis. In many systems, these decisions are made opaquely and without user-accessible or verifiable explanations. Such mechanisms, known as automated decision-making, often have direct impacts on individuals, including in cases of automated recruitment, credit scoring, or behavioral-based market segmentation. When systems make decisions based on profiling without transparency or avenues for appeal, individuals' legal rights become difficult to enforce. The GDPR, for instance, explicitly prohibits fully automated decision-making that produces significant effects on individuals, unless there is a valid legal basis and a mechanism for human intervention.

The absence of similar provisions within the national legal system creates a serious gap in data protection. Automated profiling may be conducted without notification, and personal data may be repeatedly used without renewed consent, resulting in data subjects losing control over the life cycle of their personal information. This presents significant challenges to the implementation of the principles of transparency, accountability, and fairness in AI-driven data processing. Without specific regulations governing training data

[21] Maja Brkan, "Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond," *International Journal of Law and Information Technology* 27, no. 2 (June 2019): 91–121, https://doi.org/10.1093/ijlit/eay017.

and the outcomes of automated decisions, legal protection of personal data in the context of autonomous technologies remains weak and vulnerable to misuse.

Legal Liability Models in the Use of AI: A Normative-Comparative Analysis

Indonesia's legal framework for assigning liability in cases of personal data breaches still rests on a traditional paradigm, in which responsibility can only be attributed to entities possessing legal will and capacity to act. Law No. 27 of 2022 on Personal Data Protection places primary responsibility on two entities: data controllers and data processors. The provisions of this law explicitly impose obligations on these entities, including the requirement to obtain data subject consent, ensure data security, and prevent data leakage or misuse. However, these provisions leave gaps in addressing the realities of artificial intelligence, which operates autonomously and involves decision-making based on personal data without direct human intervention.[22] Meanwhile, Law No. 11 of 2008 on Electronic Information and Transactions (ITE), along with its amendments, attempts to complement the legal responsibility framework in the digital space. Nevertheless, its approach remains largely repressive and individualistic. The national legal system has not yet adequately formulated liability principles that are adaptive to AI systems, which not only process vast amounts of data but also produce legal consequences through automated decisions such as individual classification, behavioral predictions, or policy recommendations. The current liability model fails to account for the technical complexity and architecture of AI, which often involves multiple actors, including algorithm developers, cloud service providers, and institutional users.[23]

[22] Dewi Sulistianingsih et al., "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undangan Perlindungan Data Pribadi)," *Masalah-Masalah Hukum* 52, no. 1 (March 2023): 97–106, https://doi.org/10.14710/mmh.52.1.2023.97-106.

[23] Hari Sutra Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (September 2021): 177, https://doi.org/10.25072/jwy.v5i2.460.

Within the Indonesian legal context, there is currently no normative approach that enables collective or layered liability for harms arising from the use of AI. When AI is employed to generate profiles or make decisions that affect the rights of data subjects, there is no existing legal framework capable of proportionally allocating responsibility between technological entities and human legal persons. This legal vacuum generates uncertainty and hampers the enforcement of privacy rights that should be strictly protected within a rule-of-law-based democratic system. This situation reflects that the national legal system remains in an early stage of responding to the phenomenon of autonomous technology, which is evolving far more rapidly than the legislative capacity of the state.

Table 1 Comparative Models of Legal Liability for the Use of AI in the Context of Personal Data Protection

Aspek	**PDP Law (Indonesia)**	**GDPR (European Union)**	**Additional Models**
Recognition of AI	Not explicitly regulated	Has not recognized AI as a legal subject, but regulates automated profiling	Some countries have started discussing electronic person status (EU 2017)
Liability of Data Controllers	Yes, but limited; not yet responsive to autonomous AI	Clear: controllers and processors are strictly regulated	Concept of strict liability applied to systemic risk
Corporate Liability	No specific provisions for AI	Corporate liability applies in cases of negligence or violation of principles	The concept of corporate accountability is increasingly dominant

Profiling and Automated Decision	Not clearly explained in the context of AI	Regulated under Article 22 of the GDPR prohibition without human intervention	Encouraged to conduct regular impact assessments
Sanctions and Redress for Data Subjects	Limited to administrative and general criminal violations	Administrative and civil remedies; fines can be very substantial	Some jurisdictions are adopting the private right of action

Source: Adapted and developed from the General Data Protection Regulation (EU Regulation 2016/679), Law No. 27 of 2022 on Personal Data Protection, Voigt & Von dem Bussche (2017), Kuner et al. (2020), Yeung (2018), Calo (2015), and Surden (2019).

The European Union's legal system, through the General Data Protection Regulation (GDPR), offers a more structured approach in assigning liability for personal data processing, including those involving artificial intelligence systems. The GDPR clearly distinguishes between the data controller, who determines the purposes and means of data processing, and the data processor, who processes data on behalf of the controller. This distinction provides legal role clarity and forms the basis for proportionate attribution of responsibility to each entity involved in data processing.[24] This approach not only emphasizes the principle of accountability but also introduces the concepts of privacy by design and privacy by default, requiring data controllers to assess privacy risks from the earliest stages of system development, including AI systems.

In addition to clearly defined roles, the European legal system also adopts the concept of strict liability in cases involving harm from unlawful data processing or negligence in data security. In this context, victims are not required to prove

[24] Paul Voigt and Axel Von dem Bussche, "The Eu General Data Protection Regulation (Gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10, no. 3152676 (2017): 10–5555.

subjective fault; it is sufficient to demonstrate that harm resulted from a violation of legal obligations by the data controller or processor. This approach is highly relevant in the context of AI, given that AI systems can make autonomous decisions and pose risks that are not always foreseeable by end-users. The application of strict liability also eases the burden of proof for data subjects, who often struggle to identify the actual responsible party behind complex and opaque technological systems.

Several other jurisdictions, such as Canada and Germany, have begun developing frameworks of corporate accountability for data breaches committed by the technological systems they operate or provide. In this regard, liability does not stop at individual actors but is extended to corporate entities that directly benefit from the operation of AI systems. This model emphasizes the importance of internal controls, system audits, and adherence to ethical standards in the design and deployment of automated systems that interact with personal data. Such an approach reflects the evolution of responsive legal systems that adapt to the structural risks posed by modern artificial intelligence.

In the context of modern law, the concepts of vicarious liability and corporate accountability play a crucial role in addressing liability issues arising from the actions of autonomous technologies such as AI. Vicarious liability enables legal responsibility to be imposed on an entity that did not directly commit the violation but has a relationship of power or control over the primary actor. Although originally applied within employer-employee or hierarchical relationships, this approach can be extended to encompass legal liability for the actions of AI systems operated or developed by human or corporate entities. Within this framework, AI developers or service providers may be held accountable for violations committed by the systems they design particularly when such systems lack adequate oversight or mechanisms to prevent rights infringements.[25]

[25] Harry Surden, "Artificial Intelligence and Law: An Overview," *Georgia State University Law Review* 35 (2019 2018): 1305.

On the other hand, corporate accountability emphasizes the responsibility of corporations as legal entities for any business activities that impact individual rights, including personal data protection. When companies operate AI systems for commercial purposes and derive profit from them, liability for any harm caused by those systems should rest with the corporate entity as a whole not merely with individual developers or end-users. This approach has been widely adopted in environmental law and consumer protection, and is now increasingly relevant in the context of AI-based data violations[26] By imposing collective responsibility on entities with structural control over the system, the law can reach those who actually facilitate technological risks on a systemic level.[27]

The application of vicarious liability and corporate accountability can also reinforce the preventive principle in data protection law, encouraging entities that use AI to implement risk evaluations, internal audit systems, and access restrictions based on hierarchical responsibility. When no legal subject can be held accountable for violations committed by AI, the legal framework loses both its corrective and preventive functions. Therefore, expanding the scope of legal liability through these approaches becomes essential to ensure that autonomous technologies remain subject to the principles of justice and legal certainty within a democratic system that upholds human rights.

The rapid advancement of artificial intelligence (AI) technology has shifted the traditional paradigm of legal liability, which has long relied on the existence of legal subjects possessing intent and culpability. In the context of autonomous AI systems, conventional models of liability are no longer sufficient to anticipate the complex legal implications that arise. Indonesia's legal system must move toward a reconstruction of liability models that are more adaptive to the realities of digital technology, by incorporating the precautionary principle, architectural control over systems, and the proportional distribution of risk. This approach is essential to bridge the gap between technological actors and

[26] Karen Yeung, "Algorithmic Regulation: A Critical Interrogation," *Regulation & Governance* 12, no. 4 (December 2018): 505–23, https://doi.org/10.1111/rego.12158.

[27] Ari Ade Kamula, "Implications of the Non-Involvement of the Cek Bocek Selesek Reen Sury Indigenous Community in the Mining Business Approval Process in Sumbawa Regency," Peradaban Hukum Nusantara 1, no. 2 (2024): 37, 2, https://doi.org/10.62193/4yffpb85.

the legal consequences of deploying AI systems that are opaque, difficult to audit, and prone to producing systemic impacts on civil rights particularly the right to personal data.[28]

Such reconstruction entails legal recognition of collective and layered responsibility among the various actors within the AI ecosystem. Accordingly, there must be normative standards that mandate preventive accountability, rather than relying solely on reactive liability. For instance, AI providers should be required to conduct algorithmic impact assessments, and to implement both internal and external audit mechanisms on a regular basis. Legal instruments of this kind have begun to emerge in other jurisdictions, particularly through risk-based regulation approaches that emphasize prevention according to the intensity of risk posed to fundamental rights.[29] In Indonesia, such provisions are not yet explicitly embedded within the Personal Data Protection Law or its derivative regulations.[30]

Furthermore, liability should not focus solely on end-users, but must also extend to developers, platform providers, and corporations that derive commercial benefits from AI utilization. In doing so, the distribution of legal responsibility becomes more equitable and reflective of the power structure within information technology practices. This is consistent with the principle of procedural justice, which demands that legal systems provide effective avenues for redress to victims of rights violations. Without progressive legal anticipation, the legal system will continue to lag behind in addressing the increasingly complex risks posed by emerging technologies. Legal

[28] Ryan Calo, "Robotics and the Lessons of Cyberlaw," *California Law Review* 103 (2015): 513.

[29] Michael Veale and Lilian Edwards, "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling," *Computer Law & Security Review* 34, no. 2 (April 2018): 398–404, https://doi.org/10.1016/j.clsr.2017.12.002.

[30] Syaifullah Noor, Kamil Ismail Banapon, and Tamboa Ketum Levis, "Distorted Practice of Restorative Justice in the Enforcement of Criminal Law in Indonesia: Distorsi Praktik Restorative Justice Dalam Penegakan Hukum Pidana Di Indonesia," Peradaban Hukum Nusantara 2, no. 1 (June 2025): 19, https://doi.org/10.62193/ze7dhp98.

reconstruction, therefore, is not merely a theoretical imperative it is a practical necessity to uphold the rule of law in the era of artificial intelligence.

Conclusion

The misuse of Artificial Intelligence (AI) technologies in the context of personal data protection has generated new challenges that cannot be fully addressed by traditional legal frameworks. The autonomous nature of AI its capacity to process data on a massive scale and to generate decisions without direct human intervention has created significant risks to individual privacy rights and the security of personal information. This phenomenon is further exacerbated by the imbalance in power relations between technology controllers and end-users, wherein control over data and decision-making processes rests entirely with technological entities, while the legal position of data subjects becomes increasingly weakened and vulnerable.

The core issue lies in the normative gap within Law No. 27 of 2022 on Personal Data Protection, which does not specifically regulate the legal status of AI systems or provide a multi-layered legal liability scheme. The absence of explicit recognition of AI as an entity capable of producing legal consequences, along with the lack of regulation concerning training data, profiling, and automated decision-making, creates a legal grey area in data protection. Indonesia's current legal framework remains overly individualistic, rendering it inadequate to address the relational models and complexity of modern digital systems.

In comparative analysis, the European Union's legal system through the General Data Protection Regulation (GDPR) offers a more progressive model featuring a clear division of roles between data controllers and processors, a prohibition on significant automated decision-making without human intervention, and the application of strict liability to ease the burden of proof on victims. Additionally, corporate accountability and vicarious liability concepts have proven more effective in anticipating systemic risks within AI ecosystems.

Accordingly, the urgency for reconstructing legal liability models within Indonesia's legal system becomes increasingly evident. This reconstruction should involve the expansion of regulatory scope over digital technology ecosystems, the strengthening of accountability principles, and the establishment of preventive and collective responsibility mechanisms in AI system operations. Only through an adaptive and multidimensional legal approach can personal data protection be effectively upheld in the era of artificial intelligence without sacrificing the principles of justice, transparency, and the rule of law that form the foundation of a democratic state

Bibliografi

Barocas, Solon, and Andrew D Selbst. "Big Data's Disparate Impact." Calif. L. Rev. 104 (2016): 671.

Bharti, Simant Shankar, and Saroj Kumar Aryal. "The Right to Privacy and an Implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the Companies." Journal of Contemporary European Studies 31, no. 4 (October 2023): 1391–402. https://doi.org/10.1080/14782804.2022.2130193.

Binns, Reuben. "Algorithmic Accountability and Public Reason." Philosophy & Technology 31, no. 4 (December 2018): 543–56. https://doi.org/10.1007/s13347-017-0263-5.

Bouvier, John. A Law Dictionary: Vol. I. BoD–Books on Demand, 2022.

Brkan, Maja. "Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond." International Journal of Law and Information Technology 27, no. 2 (June 2019): 91–121. https://doi.org/10.1093/ijlit/eay017.

Burrell, Jenna. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." Big Data & Society 3, no. 1 (June 2016): 2053951715622512. https://doi.org/10.1177/2053951715622512.

Calo, Ryan. "Robotics and the Lessons of Cyberlaw." California Law Review 103 (2015): 513.

Disemadi, Hari Sutra. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia."

Jurnal Wawasan Yuridika 5, no. 2 (September 2021): 177. https://doi.org/10.25072/jwy.v5i2.460.

Forgó, Nikolaus, Stefanie Hänold, and Benjamin Schütze. "The Principle of Purpose Limitation and Big Data." In New Technology, Big Data and the Law, edited by Marcelo Corrales, Mark Fenwick, and Nikolaus Forgó, 17–42. Perspectives in Law, Business and Innovation. Singapore: Springer Singapore, 2017. https://doi.org/10.1007/978-981-10-5038-1_2.

Kamula, Ari Ade. "Implications of the Non-Involvement of the Cek Bocek Selesek Reen Sury Indigenous Community in the Mining Business Approval Process in Sumbawa Regency." Peradaban Hukum Nusantara 1, no. 2 (2024): 2. https://doi.org/10.62193/4yffpb85.

Mantelero, Alessandro. "The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten.'" Computer Law & Security Review 29, no. 3 (June 2013): 229–35. https://doi.org/10.1016/j.clsr.2013.03.010.

Martin, Kirsten. "Understanding Privacy Online: Development of a Social Contract Approach to Privacy." Journal of Business Ethics 137, no. 3 (September 2016): 551–69. https://doi.org/10.1007/s10551-015-2565-9.

McInerney-Lankford, Siobhán. "Legal Methodologies and Human Rights Legal Research: Challenges and Opportunities." In Research Methods in Human Rights, edited by Bård A. Andreassen, Claire Methven O'Brien, and Hans-Otto Sano, 14–35. Edward Elgar Publishing, 2024. https://doi.org/10.4337/9781803922614.00011.

Muhammad Muslim, Muhammad Firkan, and Indi Izza Afdania. "Legal Construction of Criminal Prosecution Against Perpetrators of Rape in the Metaverse." Peradaban Hukum Nusantara 1, no. 1 (August 2024): 59–74. https://doi.org/10.62193/3aga8d22.

Mulcahy, Sean. "Methodologies of Law as Performance." Law and Humanities 16, no. 2 (July 2022): 165–82. https://doi.org/10.1080/17521483.2022.2123616.

Negara, Tunggul Ansari Setia. "Normative Legal Research in Indonesia: Its Originis and Approaches." Audito Comparative Law Journal (ACLJ) 4, no. 1 (February 2023): 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Noor, Syaifullah, Kamil Ismail Banapon, and Tamboa Ketum Levis. "Distorted Practice of Restorative Justice in the Enforcement of Criminal Law in Indonesia: Distorsi Praktik Restorative Justice Dalam Penegakan Hukum Pidana Di Indonesia." Peradaban Hukum Nusantara 2, no. 1 (June 2025): 1. https://doi.org/10.62193/ze7dhp98.

Pagallo, Ugo. The Laws of Robots: Crimes, Contracts, and Torts. Vol. 10. Law, Governance and Technology Series. Dordrecht: Springer Netherlands, 2013. https://doi.org/10.1007/978-94-007-6564-1.

Poddar, Debasis. "Genealogy of Legal Research Methodology." Asian Journal of Legal Education, February 27, 2025, 23220058251321027. https://doi.org/10.1177/23220058251321027.

Robles Carrillo, Margarita. "Artificial Intelligence: From Ethics to Law." Telecommunications Policy 44, no. 6 (July 2020): 101937. https://doi.org/10.1016/j.telpol.2020.101937.

Sulistianingsih, Dewi, Miftakhul Ihwan, Andry Setiawan, and Muchammad Shidqon Prabowo. "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undangan Perlindungan Data Pribadi)." Masalah-Masalah Hukum 52, no. 1 (March 2023): 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106.

Surden, Harry. "Artificial Intelligence and Law: An Overview." Georgia State University Law Review 35 (2019 2018): 1305.

Taddeo, Mariarosaria, and Luciano Floridi. "How AI Can Be a Force for Good." Science 361, no. 6404 (August 2018): 751–52. https://doi.org/10.1126/science.aat5991.

Veale, Michael, and Lilian Edwards. "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-

Making and Profiling." Computer Law & Security Review 34, no. 2 (April 2018): 398–404. https://doi.org/10.1016/j.clsr.2017.12.002.

Voigt, Paul, and Axel Von dem Bussche. "The Eu General Data Protection Regulation (Gdpr)." A Practical Guide, 1st Ed., Cham: Springer International Publishing 10, no. 3152676 (2017): 10–5555.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Transparent, Explainable, and Accountable AI for Robotics." Science Robotics 2, no. 6 (May 2017): eaan6080. https://doi.org/10.1126/scirobotics.aan6080.

Wagner, Peter. "Mind the Gap(s): Moral Philosophy, International Law and Interpretative Historical Sociology." European Journal of Social Theory 26, no. 4 (November 2023): 527–35. https://doi.org/10.1177/13684310231164258.

Yeung, Karen. "Algorithmic Regulation: A Critical Interrogation." Regulation & Governance 12, no. 4 (December 2018): 505–23. https://doi.org/10.1111/rego.12158.

Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Edn. PublicAffairs, New York, 2019.

Zwitter, Andrej J., Oskar J. Gstrein, and Evan Yap. "Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual." Frontiers in Blockchain 3 (May 2020): 26. https://doi.org/10.3389/fbloc.2020.00026.