Legal Autonomous Web-based Governance (LAW)
Vol. 1, No. 2, October 2026, pp. 175∼186
E-ISSN: XXXX-XXXX | P-ISSN: xxxx-xxxx

Lifecycle Based Legal Governance of Algorithmic Decision Making in Digital Business Platforms

Untung Rahardja[1], Mitra Trima Des Sincer Putri[2], Dwi Cahyono[3], Alfri Adiwijaya[4], Rizky Fredrin Terizla[5*]
[1,2,4] Faculty of Economics and Business, Universitas Raharja, Indonesia
[3] Faculty of Economic and Business, University of Muhammadiyah Jember, Indonesia
[5]Department of Law and Technology, Rey Incorporation, United States
[1]untung@raharja.info, [2]mitra.dessincer@raharja.info, [3]dwicahyono@unmuhjember.ac.id, [4]alfri.adiwijaya@raharja.info, [5]prorizkyyoung@rey.zone
***Corresponding Author**

Article Info

Article history:

Submission March 11, 2026
Revised August 25, 2026
Accepted August 28, 2026
Published August 31, 2026

Keywords:

Algorithmic Decision
Digital Business Platforms
Legal Governance
Transparency
Data Protection

ABSTRACT

The increasing use of algorithmic decision-making in digital business platforms has transformed how organizations evaluate users, personalize services, allocate resources, detect risks, and make commercially significant decisions. Although algorithmic systems improve efficiency and scalability, their expanding role creates legal challenges concerning transparency, accountability, fairness, data protection, and human oversight. **This study examines** the legal governance of algorithmic decision-making in digital business platforms and identifies legal principles required to ensure accountable and responsible algorithmic practices. **The research employs** a normative legal approach using statutory, conceptual, and comparative legal analysis. The study analyzes legal principles concerning algorithmic accountability, transparency, data protection, procedural fairness, and human oversight to develop a comprehensive governance framework. **The findings** indicate that existing regulatory approaches remain fragmented, creating uncertainty regarding legal responsibility among platform operators, technology providers, and other stakeholders. Effective governance therefore requires a lifecycle-based regulatory approach covering algorithmic design, data processing, deployment, monitoring, evaluation, and review. **The proposed** framework integrates transparency obligations, accountability mechanisms, risk-based oversight, data protection safeguards, and meaningful human intervention. This study contributes a conceptual legal governance framework for algorithmic decision-making in digital business platforms and provides a basis for policymakers and platform operators to strengthen legal accountability, protect individual rights, and promote responsible digital business innovation.

This is an open access article under the CC BY 4.0 license.

This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)
©Authors retain all copyrights

1. INTRODUCTION

The rapid expansion of digital business platforms has fundamentally changed how organizations conduct commercial activities, interact with users, and make operational and strategic decisions [1]. Platforms operating in areas such as e-commerce, digital finance, transportation, employment services, and online marketplaces increasingly rely on algorithmic systems to process large volumes of data and support or automate

decision-making [2]. These systems may determine product recommendations, credit assessments, fraud detection, pricing strategies, customer rankings, content visibility, and access to platform services. Algorithmic decision-making has therefore become an important component of digital business infrastructure because it enables platform operators to process information at a scale and speed that would be difficult to achieve through conventional human decision-making [3]. However, the increasing reliance on algorithmic systems also raises significant legal concerns when automated or partially automated decisions affect the rights, opportunities, interests, or economic positions of individuals and businesses [4].

The legal challenges associated with algorithmic decision-making extend beyond the technical performance of algorithms [5]. Decisions generated by algorithmic systems may be difficult for affected parties to understand, challenge, or contest because the underlying logic, data inputs, and decision-making processes are often complex or insufficiently disclosed. This creates concerns regarding transparency and explainability, particularly when algorithmic decisions influence access to financial services, employment opportunities, commercial visibility, platform participation, or other economically relevant outcomes [6]. Algorithmic systems may also reproduce or amplify biases contained in training data or operational datasets, potentially resulting in discriminatory or unfair outcomes [7]. Consequently, the use of algorithmic decision-making within digital business platforms creates a regulatory challenge concerning how legal systems can encourage technological innovation while ensuring that platform-based decisions remain transparent, accountable, fair, and consistent with applicable rights and obligations [8].

The problem becomes more complex because digital business platforms involve multiple actors and layers of technological infrastructure. Platform operators may design or deploy algorithmic systems internally, while other systems may be developed or supplied by external technology providers [9]. Data may also be obtained from users, business partners, third-party services, or other digital sources. As a result, responsibility for an algorithmically generated decision cannot always be attributed to a single actor [10]. Determining who should be legally responsible for unlawful, discriminatory, inaccurate, or harmful algorithmic outcomes is therefore a central issue in legal governance [11]. A regulatory framework that focuses solely on the technical characteristics of algorithms may fail to address the institutional relationships through which algorithmic decisions are developed, implemented, monitored, and challenged [12].

Existing legal frameworks provide several principles that are relevant to these challenges, including data protection, consumer protection, non-discrimination, procedural fairness, transparency, corporate accountability, and administrative oversight [13]. Nevertheless, these principles are frequently distributed across different regulatory instruments and may not directly address the specific characteristics of algorithmic decision-making in digital business platforms [14]. This fragmentation can create uncertainty concerning the scope of transparency obligations, the allocation of responsibility, the requirements for human intervention, and the mechanisms available to individuals or businesses affected by algorithmic decisions [15]. This regulatory gap is particularly important as digital platforms increasingly move from using algorithms merely as supporting tools toward systems that can substantially influence or automate commercially significant decisions [16].

From a legal governance perspective, algorithmic decision-making should therefore be examined as a process rather than as an isolated technological instrument [17]. Effective governance requires legal safeguards throughout the algorithmic lifecycle, beginning with system design and data collection and continuing through deployment, monitoring, evaluation, modification, and review [18]. Such governance should establish clear responsibilities for platform operators and other relevant actors, require appropriate levels of transparency, ensure lawful and responsible data processing, identify and mitigate algorithmic risks, and provide meaningful mechanisms for human oversight and contestability [19]. A lifecycle-based approach is particularly relevant to digital business platforms because algorithmic systems may continuously change in response to new data, user behavior, market conditions, and business objectives [14].

Despite growing scholarly and regulatory attention to artificial intelligence and automated decision-making, an important research gap remains in developing a legal governance perspective specifically focused on algorithmic decision-making within digital business platforms [20]. Much of the existing discussion examines algorithmic fairness, Artificial Intelligence (AI) ethics, data protection, or automated decision-making as separate regulatory concerns. Such approaches provide important foundations but may not sufficiently explain how these legal principles can be integrated into a coherent governance structure for platform-based business environments [21]. The distinctive characteristics of digital platforms, including their data-intensive operations, multi-sided relationships, automated processes, and significant economic influence, require a governance approach that connects algorithmic accountability with the legal responsibilities of platform actors [22].

Accordingly, this study addresses the following research question. How should algorithmic decision-making in digital business platforms be legally governed to ensure transparency, accountability, fairness, data protection, risk-based oversight, and meaningful human intervention? To answer this question, the study employs a normative legal research approach based on statutory, conceptual, and comparative legal analysis. The analysis examines legal principles relevant to algorithmic decision-making and synthesizes them into a governance framework applicable to digital business platforms [23]. The study focuses particularly on the relationship between algorithmic transparency, accountability, data protection, fairness, risk-based oversight, and human intervention [24].

Based on this research question, the study has three objectives. First, it identifies and analyzes the legal principles governing algorithmic decision-making in digital business platforms. Second, it examines how responsibility, transparency, data protection, fairness, human oversight, and risk-based obligations should be allocated across the algorithmic lifecycle [25]. Third, it synthesizes these legal principles into a lifecycle-based governance framework that can guide platform operators, technology providers, and regulators [26]. These objectives directly inform the proposed framework and the subsequent analysis of lifecycle governance, accountability, risk-based regulation, and managerial and legal implications [27].

This study contributes to a lifecycle-based legal governance framework that distinguishes itself from existing approaches by integrating transparency and explainability, accountability, fairness and non- discrimination, data protection, and meaningful human oversight across the successive stages of algorithmic decision-making [28]. Rather than treating these principles as separate dimensions of AI governance, algorithmic accountability, or platform regulation, the proposed framework connects them to system design, data processing, development and testing, deployment, monitoring and evaluation, and review and improvement [29]. This integrated structure provides a legal basis for allocating responsibilities and safeguards continuously throughout the algorithmic lifecycle within digital business platforms.

This study supports the Sustainable Development Goals (SDGs), particularly SDG 16 (Peace, Justice and Strong Institutions) and SDG 9 (Industry, Innovation and Infrastructure). SDG 16 aligns with human-centered legal governance by emphasizing transparency, accountability, effective institutions, and the protection of citizens' rights in AI-based public administration, while SDG 9 relates to the use of AI and digital technologies to promote innovation and strengthen digital public infrastructure. Through the integration of legal safeguards, accountability, and human-centered principles, this study emphasizes that digital transformation in public administration should enhance technological innovation while maintaining public trust and respect for fundamental rights.

2. LITERATURE REVIEW

2.1. Algorithmic Decision Making in Digital Business Platforms

Algorithmic decision-making refers to the use of computational procedures to process data, identify patterns, generate assessments, and support or determine decisions. Its application has expanded rapidly within digital business platforms, where algorithms are used for customer profiling, recommendation systems, fraud detection, credit assessment, pricing, ranking, content moderation, and access management. These applications enable platform operators to process large volumes of data and make decisions rapidly, consistently, and at a scale that would be difficult to achieve through conventional human judgment. Algorithmic decision-making has therefore become an important component of digital business infrastructure and increasingly influences how commercial relationships are established and managed [30].

The role of algorithmic decision-making is particularly significant because digital business platforms operate as intermediaries connecting multiple groups of stakeholders, including consumers, sellers, workers, advertisers, and service providers. Algorithmic outputs may consequently affect not only individual users but also the distribution of economic opportunities across the platform ecosystem. For example, ranking algorithms can determine the visibility of sellers, recommendation systems can influence consumer choices, and automated risk assessments can affect access to financial or platform services [31]. The increasing influence of algorithms therefore creates a need to examine not only their technical performance but also their legal consequences. The complexity of algorithmic systems presents several governance concerns.

Algorithmic decisions may be difficult for affected parties to understand because the underlying models, data inputs, and decision-making processes are often technically complex or commercially protected. In addition, systems trained on incomplete or historically biased data may reproduce or amplify discriminatory

patterns [32]. Algorithmic decisions may also rely extensively on personal and behavioral data, creating concerns regarding lawful data processing, privacy, security, and individual rights. These characteristics demonstrate that algorithmic decision-making within digital business platforms cannot be considered solely a technological issue it is also a matter of legal responsibility, institutional accountability, and protection of affected stakeholders.

2.2. Legal Challenges and Governance Principles

The legal governance of algorithmic decision-making should integrate transparency and explainability, accountability, fairness and non-discrimination, data protection, and human oversight. Transparency and explainability require meaningful and proportionate information about an algorithm's purpose, decision factors, and potential consequences without necessarily disclosing source code or proprietary information [33]. Accountability requires responsibility to remain with organizations and actors involved in developing, procuring, deploying, and managing algorithmic systems, supported by documentation, risk assessment, monitoring, auditing, complaint mechanisms, and remediation [34]. Fairness and non-discrimination are necessary to prevent algorithmic systems from reproducing social or economic inequalities, particularly in access to services, commercial visibility, employment, pricing, and financial products [35].

Data protection must also be embedded throughout the algorithmic lifecycle, ensuring lawful processing, purpose limitation, data minimization, security, and protection of individual rights when personal and behavioral data are collected and analyzed [36]. In addition, human oversight is essential where algorithmic decisions may have significant consequences, requiring qualified personnel with sufficient information and authority to review, modify, or overturn algorithmic outputs when necessary [37]. Collectively, these principles demonstrate that legal governance should regulate not only algorithmic systems themselves but also the organizational and institutional processes governing their development and use.

2.3. Research Gap and Conceptual Framework

Although existing literature has extensively examined algorithmic transparency, fairness, accountability, data protection, and artificial intelligence governance, these dimensions are frequently discussed separately or within broad technological governance frameworks. Less attention has been given to their integration within the specific context of digital business platforms, where algorithmic decisions operate across complex multi-sided ecosystems and can directly influence economic participation, commercial relationships, and access to platform-based services. This creates a research gap concerning how different legal principles can be integrated into a coherent governance framework specifically designed for algorithmic decision-making in digital business environments [38].

This study addresses the gap by conceptualizing algorithmic decision-making as a lifecycle-based legal governance process. The framework integrates five interconnected dimensions, transparency and explainability, accountability, fairness and non-discrimination, data protection, and meaningful human oversight. These dimensions are applied across the algorithmic lifecycle, including system design, data collection and processing, development, testing, deployment, monitoring, evaluation, and review. The framework assumes that effective legal governance requires continuous oversight rather than intervention only after an algorithmic decision causes harm.

The conceptual approach developed in this study positions the digital business platform operator as a central accountable actor while recognizing the involvement of technology providers, data processors, business partners, users, and regulatory authorities. Through this integrated approach, algorithmic governance can move beyond fragmented compliance toward a structured legal framework that establishes responsibilities, protects affected stakeholders, and supports responsible technological innovation. The framework consequently provides the conceptual foundation for examining how legal governance can balance the operational benefits of algorithmic decision-making with the requirements of accountability, fairness, transparency, and protection of rights within digital business platforms [39].

3. RESEARCH METHOD

This study employs a normative legal research approach to examine the legal governance of algorithmic decision-making in digital business platforms. The approach is selected because the study focuses on legal norms, regulatory principles, institutional responsibilities, and governance mechanisms governing the development and use of algorithmic systems. Rather than empirically measuring user behavior or testing algorithmic

performance, this research examines how existing legal principles can be applied and integrated to address the legal risks associated with algorithmically generated decisions in digital business environments [40].

The authors' academic and professional expertise provides the foundation for the legal analysis, supported by scholarship on AI regulation, algorithmic decision-making, digital platforms, data protection, and technology governance. The study employs statutory, conceptual, and comparative approaches. The statutory approach identifies applicable legal rules, the conceptual approach synthesizes key principles such as transparency, accountability, fairness, data protection, and human oversight, while the comparative approach examines international regulatory practices and lessons. Together, these approaches establish the legal norms, analytical dimensions, and comparative insights underlying the proposed lifecycle-based governance framework.

The legal materials comprise primary, secondary, and tertiary sources. Primary materials include legislation, regulations, and authoritative legal instruments on digital platforms, data protection, automated decision-making, and AI governance. Secondary materials consist of peer-reviewed articles, academic books, legal scholarship, institutional reports, and policy documents, while tertiary sources clarify legal terminology and concepts. Materials are selected based on legal relevance, substantive relevance, authority, and analytical usefulness, particularly in relation to transparency, accountability, fairness, data protection, and human oversight. International frameworks are included to provide comparative insights into algorithmic risk and governance, with priority given to authoritative legal instruments and peer-reviewed scholarship.

The analysis is conducted through four stages. First, relevant legal materials are identified and classified according to their legal authority and substantive relevance. Second, the materials are analyzed based on five governance dimensions, transparency and explainability, accountability, Fairness and Non-Discrimination, data protection, and human oversight. Third, regulatory gaps and challenges are identified by examining the extent to which existing legal principles address algorithmically generated decisions within digital business platforms. Fourth, the identified principles are synthesized into a lifecycle-based legal governance framework. The analytical dimensions used in this study are summarized in Table 1.

Table 1. Analytical Dimensions of Legal Governance of Algorithmic Decision Making

Governance Dimension	**Principal Legal Concern**	**Key Analytical** Focus	**Governance Objective**
Transparency and Explainability	Limited understanding of algorithmic decisions	Disclosure, explanation, and documentation	Enable meaningful understanding and contestability
Accountability	Unclear allocation of responsibility	Responsibility, auditing, documentation, and remedies	Establish clear legal responsibility
Fairness and Non-Discrimination	Biased or unequal algorithmic outcomes	Bias assessment, monitoring, and mitigation	Prevent unjustified discriminatory outcomes
Data Protection	Extensive processing of personal and behavioral data	Lawfulness, purpose limitation, minimization, and security	Protect data related rights
Human Oversight	Excessive reliance on automated outputs	Human review, intervention, and appeal mechanisms	Maintain meaningful human control

Table 1 presents the five analytical dimensions that form the foundation of the legal analysis. These dimensions are interconnected rather than independent. Transparency enables affected parties to understand algorithmic decisions, accountability establishes responsibility for those decisions, fairness addresses potentially discriminatory outcomes, data protection regulates the processing of information used by algorithmic systems, and human oversight provides a mechanism for reviewing and intervening in significant decisions. Together, these dimensions provide the analytical basis for assessing whether algorithmic decision-making within digital business platforms can operate within a legally accountable governance structure. The methodological framework consequently treats algorithmic governance as a continuous legal process. Legal requirements are

examined across the algorithmic lifecycle, including system design, data collection and processing, development and testing, deployment, monitoring, evaluation, and review. This approach enables the study to connect substantive legal principles with organizational responsibilities and operational governance mechanisms.

4. RESULTS AND DISCUSSION

4.1. Conceptual Framework of Legal Governance

The analysis indicates that effective legal governance of algorithmic decision-making requires an integrated framework rather than isolated regulatory requirements. Building on the five governance dimensions established in the literature review, the proposed framework positions algorithmic decision-making within digital business platforms as the central object of legal governance. These dimensions operate collectively across the algorithmic lifecycle to establish responsible governance and connect substantive legal principles with organizational responsibilities and operational safeguards.

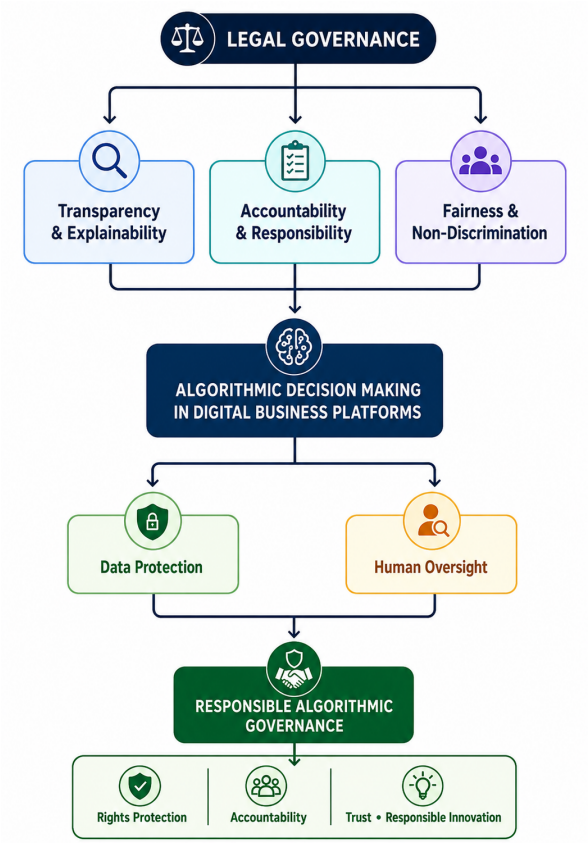

Figure 1. Legal Governance Framework for Algorithmic Decision-Making

Figure 1 illustrates the conceptual framework developed from the legal analysis. The framework places algorithmic decision-making at the center because it represents the primary object of governance within digital business platforms. The five governance dimensions function as interconnected safeguards. Their integration is intended to ensure that algorithmic systems operate with sufficient transparency, clearly allocated responsibility, fair treatment, lawful data processing, and meaningful human control. The framework also establishes a direct relationship between legal governance and broader outcomes, including protection of rights, institutional accountability, user trust, and responsible digital innovation. The framework demonstrates that legal governance should not be limited to regulating the technical characteristics of an algorithm. Instead, governance must address the institutional and organizational processes surrounding the algorithm, including who designs or deploys the system, what data are processed, how decisions are generated, who is responsible for outcomes, and what mechanisms are available when affected parties challenge a decision.

4.2. Lifecycle-Based Legal Governance

The analysis further demonstrates that the five governance dimensions should be applied throughout the algorithmic lifecycle. Legal risks do not emerge exclusively when an algorithm produces a final decision. They may originate during system design, arise from the collection and processing of data, become apparent during testing, or emerge after deployment as the system interacts with users and changing datasets. Consequently, legal governance should operate continuously across the lifecycle rather than being limited to post-decision review. The proposed lifecycle consists of six stages, design, data collection and processing, development and testing, deployment, monitoring and evaluation, and review and improvement. Each stage creates specific legal responsibilities for platform operators and other relevant actors.

Figure 2. Lifecycle-Based Legal Governance of Algorithmic Decision Making

Figure 2 demonstrates that legal oversight should operate continuously across all stages of the algorithmic lifecycle. During the design stage, platform operators should identify the purpose, potential risks, and legal implications of the intended system. During data collection and processing, compliance with applicable data protection requirements becomes essential. Development and testing should address accuracy, reliability, and potential discriminatory outcomes. During deployment, appropriate transparency and accountability mechanisms should be established. Monitoring and evaluation should identify emerging risks and unexpected outcomes, while review and improvement provide mechanisms for correcting or modifying systems when necessary. The lifecycle model also demonstrates that the responsibility of platform operators does not end when an algorithm is deployed. Because algorithmic systems may continuously process new data and produce changing outputs, governance must remain adaptive. Continuous monitoring, documentation, auditing, human review, and corrective measures are therefore essential components of responsible algorithmic governance.

The comparative analysis identifies both similarities and differences between the European Union's risk-based approach to artificial intelligence governance and the GDPR's approach to profiling, automated decision-making, and personal data processing. Both regulatory approaches emphasize accountability, transparency, proportionality, and safeguards for decisions that may significantly affect individuals. However, their regulatory emphasis differs, the risk-based AI governance approach differentiates obligations according to the level and nature of algorithmic risk, whereas the General Data Protection Regulation (GDPR) primarily establishes safeguards through data protection principles and specific requirements concerning profiling and

automated decision-making. These differences demonstrate that algorithmic governance requires both risk-sensitive obligations and data protection safeguards. The principal lesson for digital business platforms is that legal duties should be proportionate to the potential impact of an algorithmic system while remaining integrated with requirements for transparency, accountability, human oversight, and lawful data processing. The proposed framework incorporates these lessons by connecting proportional legal obligations to the stages of algorithmic design, data processing, development and testing, deployment, monitoring, and review.

4.3. Transparency, Explainability, and Accountability

Transparency and explainability are fundamental to the legal governance of algorithmic decision-making because affected individuals and businesses need meaningful information about how significant decisions are produced and why they occur. In digital business platforms, algorithms may determine service access, rankings, pricing, fraud assessments, or content visibility. Legal governance should therefore require proportionate transparency concerning the algorithm's purpose, data categories, key decision factors, and review or contestation mechanisms, without necessarily requiring disclosure of source code, trade secrets, or security-sensitive information. Explainability should enable affected parties to understand outcomes, identify errors, and challenge unjustified decisions, particularly where significant economic consequences arise. Transparency provides information, while accountability assigns responsibility for algorithmic consequences. Platform operators should remain accountable for systems they develop, procure, deploy, or manage, supported by preventive measures such as impact assessments, documentation, testing, governance policies, and assigned responsibilities, as well as corrective mechanisms including audits, complaints, human review, remediation, and appropriate sanctions.

Accountability should also reflect the roles and control exercised by different actors within the algorithmic ecosystem. Platform operators bear primary responsibility for lawful purposes, deployment, monitoring, governance, and remediation; technology providers are responsible for the technical characteristics, documentation, testing, security, and known limitations of systems they supply; data processors are accountable for lawful and secure processing within their assigned functions; and business partners or third parties remain responsible for activities and data under their control. Regulatory authorities provide oversight and enforcement according to their legal mandates. Responsibility should therefore be allocated according to each actor's function, degree of control, and capacity to prevent or remedy risks. Although contracts may distribute operational duties, they should not be used to obscure accountability for harmful or unlawful algorithmic outcomes.

4.4. Fairness, Data Protection, and Human Oversight

Fairness, data protection, and human oversight are essential dimensions of responsible algorithmic governance. Algorithmic unfairness may arise from biased or incomplete data, inappropriate variables, flawed system design, or embedded assumptions, potentially affecting service access, seller visibility, employment, pricing, and credit assessments. Legal governance should therefore require bias identification and mitigation throughout the algorithmic lifecycle, including data and variable assessment during development, testing for disproportionate effects, continuous monitoring after deployment, and corrective measures or remedies when harmful outcomes emerge. Data protection is equally important because digital platforms rely on extensive personal and behavioral data, including registration, transaction, browsing, location, communication, and interaction data. Governance should ensure legitimate and defined processing purposes, proportional data use, appropriate security safeguards, transparency regarding relevant processing, and mechanisms for exercising applicable data rights, particularly when algorithmic decisions significantly affect individuals.

Human oversight provides an additional safeguard where automated decisions may produce errors or inappropriate outcomes, especially those with significant legal, economic, or social consequences. Meaningful oversight requires competent and authorized personnel who can understand, review, and intervene in algorithmic decisions rather than merely approve automated outputs. Affected parties should also have mechanisms to request human review and challenge significant decisions through procedures that consider individual circumstances rather than simply reproduce the original outcome. Together, these dimensions demonstrate that responsible algorithmic governance extends beyond technical accuracy, systems must also comply with data protection requirements, prevent unjustified discrimination, and maintain meaningful human control to protect rights, interests, and accountability.

5. MANAGERIAL IMPLICATIONS

The findings show that lifecycle-based legal governance must integrate legal safeguards with organizational decision-making and operational controls. Platform operators should assign responsibilities across design, data processing, development, deployment, monitoring, and review, supported by impact assessments, documentation, testing, auditing, human oversight, and remediation. Technology providers and data processors should fulfill function-specific duties concerning documentation, security, testing, transparency, compliance, and incident reporting, while contracts should clearly allocate these responsibilities without transferring the platform operator's ultimate accountability. At each lifecycle stage, operators should identify risks and legal requirements, ensure lawful and proportionate data processing, assess accuracy, bias, reliability, and robustness, provide meaningful transparency and human intervention, continuously monitor performance and complaints, conduct periodic audits, and document corrective actions. Regulators can use these records for proportional supervision, while users and business partners should receive understandable information about algorithmic use, relevant decision factors, and available review or challenge mechanisms. Regulation should therefore establish preventive obligations across the lifecycle rather than addressing harm only after it occurs.

The framework further supports a risk-based regulatory model that differentiates algorithmic systems according to the severity, scale, likelihood, and reversibility of their impacts. Lower-risk systems may require baseline documentation, transparency, data protection, and monitoring; medium-risk systems should undergo additional assessment, testing, documentation, and periodic review; and high-impact systems affecting financial services, employment, platform participation, commercial visibility, or other significant interests should face stronger requirements, including formal impact assessments, enhanced documentation, meaningful human oversight, continuous monitoring, qualified independent auditing, and accessible review and remediation. These findings contribute to AI governance, technology law, digital policy, and platform governance by clarifying responsibilities among operators, providers, processors, and regulators while integrating transparency, accountability, fairness, data protection, and human oversight. Ultimately, accessible explanations, human review, challenges, and remedies can turn transparency into an effective rights safeguard, strengthen accountability and trust, and preserve the benefits of algorithmic innovation. support the sustainable growth of Indonesia's digital economy.

6. CONCLUSION

This study concludes that the legal governance of algorithmic decision-making in digital business platforms requires an integrated, risk-based, and lifecycle-oriented approach. The analysis establishes that transparency and explainability, accountability, fairness and non-discrimination, data protection, and meaningful human oversight should be applied consistently throughout the algorithmic lifecycle, from system design, data collection and processing, development and testing, to deployment, monitoring, evaluation, review, and improvement. These safeguards should function as interconnected legal requirements rather than isolated principles, ensuring that algorithmic systems remain subject to continuous legal and organizational control as their purposes, data, risks, and impacts evolve.

The principal legal finding is that responsibility should be distributed according to the functions performed and the degree of control exercised by platform operators, technology providers, data processors, and other relevant actors. At the same time, regulatory obligations should be proportionate to the potential severity, scale, likelihood, and reversibility of algorithmic impacts. This study contributes to legal scholarship by framing algorithmic governance as a continuous legal process and integrating core governance principles into a lifecycle-based framework specifically designed for digital business platforms. Practically, the framework provides a basis for implementing algorithmic impact assessments, documentation, testing, auditing, monitoring, meaningful human review, transparency mechanisms, and remediation, while supporting policymakers and regulators in establishing clearer and proportionate risk-based obligations.

Despite these contributions, the study is limited by its normative legal research design and therefore does not empirically evaluate how the proposed framework would operate across specific digital platform environments or measure its effectiveness in practice. Future research should address this limitation through empirical investigations, case-based studies, and comparative assessments of different regulatory regimes, particularly concerning risk classification, algorithmic impact assessment, auditing standards, human oversight, transparency mechanisms, and legal remedies. Further research may also examine how organizations can

translate the framework into measurable compliance indicators and operational procedures. Such studies would strengthen the empirical foundation of the framework and contribute to more precise, adaptable, and effective standards for responsible lifecycle-based algorithmic governance.

7. DECLARATIONS

7.1. About Authors

Untung Rahardja (UR) https://orcid.org/0000-0002-2166-2412

Mitra Trima Des Sincer Putri (MP) https://orcid.org/0009-0007-2493-3808

Dwi Cahyono (DC) https://orcid.org/0000-0001-9951-560X

Alfri Adiwijaya (AA) https://orcid.org/0009-0008-4049-5286

Rizky Fredrin Terizla (RT) https://orcid.org/0009-0009-7817-0265

7.2. Author Contributions

Conceptualization: UR; Methodology: AA; Software: MP; Validation: RT, AR and UR; Formal Analysis: MP and AA; Investigation: RT; Resources: UR; Data Curation: MP and UR; Writing Original Draft Preparation: RT and AR; Writing Review and Editing: AA, UR and RT; Visualization: MP; All authors, UR, MP, AR, AA, and RT, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] N. Alnemr, "Democratic self-government and the algocratic shortcut: the democratic harms in algorithmic governance of society: N. alnemr," *Contemporary political theory*, vol. 23, no. 2, pp. 205–227, 2024.

[2] É. S. F. Azevedo, D. F. de Souza, and J. R. C. de Mendonça, "Algorithmic management in digital work platforms: A systematic literature review," *Contextus–Revista Contemporânea de Economia e Gestão*, vol. 21, pp. 1–14, 2023.

[3] G. B. R. Duggireddy, "Integrated data and ai governance framework: A lifecycle approach to responsible ai implementation," *Journal of Computer Science and Technology Studies*, vol. 7, no. 7, pp. 771–777, 2025.

[4] R. T. H. Safariningsih, U. Rahardja, M. T. D. S. Putri, N. Azizah, E. Harris *et al.*, "Advanced big data analytics for proactive cyber threat mitigation in large scale computer networks," *Journal of Computer Science and Technology Application*, vol. 3, no. 2, pp. 199–212, 2026.

[5] S. Ehsan, "Ai bias in streaming platform recommendation systems: Exploring the impact on corporate reputation," Ph.D. dissertation, Virginia Polytechnic Institute and State University, 2025.

[6] S. Alkhoudi, S. Shaer, and F. Salem, "The artificial intelligence smes ecosystem in the uae: Overcoming challenges, expanding horizons," *Expanding Horizons (April 15, 2025)*, 2025.

[7] N. Lutfiani, S. Wijono, U. Rahardja, A. Iriani, and E. A. Nabila, "Artificial intelligence based on recommendation system for startup matchmaking platform," in *2022 IEEE Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2022, pp. 1–5.

[8] G. Grote, S. K. Parker, and K. Crowston, "Taming artificial intelligence: A theory of control-accountability alignment among ai developers and users," *Academy of Management Review*, vol. 51, no. 2, pp. 278–299, 2026.

[9] B. Hallinan, C. Reynolds, Y. Kuperberg, and O. Rothenstein, "Aspirational platform governance: How creators legitimise content moderation through accusations of bias," *Internet Policy Review*, vol. 14, no. 1, pp. 1–28, 2025.

[10] N. Lutfiani, S. Wijono, U. Rahardja, A. Iriani, Q. Aini, and R. A. D. Septian, "A bibliometric study: Recommendation based on artificial intelligence for ilearning education," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2, pp. 109–117, 2023.

[11] A. James, D. Hynes, A. Whelan, T. Dreher, and J. Humphry, "From access and transparency to refusal: Three responses to algorithmic governance," *Internet Policy Review*, vol. 12, no. 2, pp. 1–28, 2023.

[12] A. Küsters, "Future-proofing the eu: ordoliberal governance and algorithmic regulation: A. küsters," *Constitutional Political Economy*, vol. 36, no. 4, pp. 469–494, 2025.

[13] J. Laux, "Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of ai governance under the european union ai act," *AI & society*, vol. 39, no. 6, pp. 2853–2866, 2024.

[14] N. Lutfiani, I. Sembiring, I. Setyawan, A. Setiawan, U. Rahardja, and S. Sulistio, "Exploring the relationship between artificial intelligence and business performance," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 19, no. 1, pp. 1–12, 2025.

[15] C. Novelli, M. Taddeo, and L. Floridi, "Accountability in artificial intelligence: what it is and how it works," *Ai & Society*, vol. 39, no. 4, pp. 1871–1882, 2024.

[16] S. Sterz, K. Baum, S. Biewer, H. Hermanns, A. Lauber-Rönsberg, P. Meinel, and M. Langer, "On the quest for effectiveness in human oversight: Interdisciplinary perspectives," in *Proceedings of the 2024 ACM conference on fairness, accountability, and transparency*, 2024, pp. 2495–2507.

[17] A. Rizky, U. Rahardja, M. Muhtarom, D. N. Ramadhan, S. Triandari, and R. F. Terizla, "Responsible ai governance in decentralized web systems," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 123–133, 2026.

[18] K. Wiedemann, "Profiling and (automated) decision-making under the gdpr: A two-step approach," *Computer Law & Security Review*, vol. 45, p. 105662, 2022.

[19] G. Zhu, M. Tang, X. Jian, and T. Mu, "A study of government regulation's strategy for solving the algorithmic black-box puzzle of digital platforms: a complex network-based perspective," *Frontiers in Physics*, vol. 13, p. 1538742, 2025.

[20] B. S. Adelusi, A. C. Uzoka, Y. G. Hassan, and F. U. Ojika, "Reviewing data governance strategies for privacy and compliance in ai-powered business analytics ecosystems," *Journal Not Specified*, vol. 6, no. 4, pp. 101–118, 2023.

[21] N. V. Patel, "An end-to-end, stage-wise life-cycle framework for mitigating algorithmic bias in two-sided marketplaces," *Power System Technology*, vol. 49, no. 3, pp. 434–457, 2025.

[22] U. H. Yulianti, Y. I. Tanjung, U. Rahardja, N. Lutfiani, and A. Valerry, "Integration of iot and blockchain for business data security," *Blockchain Frontier Technology*, vol. 6, no. 1, pp. 62–73, 2026.

[23] A. Meesala, "Machine learning enabled governance framework for autonomous enterprise platforms and intelligent data ecosystems," *International Journal of Computer Technology and Electronics Communication*, vol. 7, no. 6, pp. 9899–9909, 2024.

[24] C. T. Okolo, "Governance of ai-based algorithms," in *Handbook of Human-Centered Artificial Intelligence*. Springer, 2025, pp. 1–39.

[25] H. Cahyadi, A. Kho, F. A. Yusuf, R. A. Sunarjo, and U. Rahardja, "Ai maturity in business: Bibliometric analysis and sustainable development goals," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2024, pp. 1–6.

[26] P. Casanovas, "A regulatory framework for legal ecosystems in the context of emerging web-based systems and the european ai value chain regulations," *Governance and Control of Data and Digital Economy in the European Single Market*, vol. 23, 2025.

[27] U. Kango, "Algorithmic governance," in *Handbook of Human-Centered Artificial Intelligence*. Springer,

2025, pp. 1–26.

[28] S. Kosasi, I. D. A. E. Yuliani, U. Rahardja *et al.*, "Boosting e-service quality of online product businesses through it leadership," in *2022 International Conference on Science and Technology (ICOSTECH)*. IEEE, 2022, pp. 1–10.

[29] A. K. Zharova, "Achieving algorithmic transparency and managing risks of data security when making decisions without human interference: legal approaches," *Journal of Digital Technologies and Law*, vol. 1, no. 4, pp. 973–993, 2023.

[30] M. Kretschmer, T. Margoni, and P. Oruç, "Copyright law and the lifecycle of machine learning models: M. kretschmer et al." *IIC-International Review of Intellectual Property and Competition Law*, vol. 55, no. 1, pp. 110–138, 2024.

[31] Central Digital and Data Office, "Uk government publishes pioneering standard for algorithmic transparency," Nov. 2021. [Online]. Available: https://www.gov.uk/government/news/uk-government-publishes-pioneering-standard-for-algorithmic-transparency

[32] L. Sanbella, I. Van Versie, and S. Audiah, "Online marketing strategy optimization to increase sales and e-commerce development: An integrated approach in the digital age," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 54–66, 2024.

[33] K. Yu, N. S. Malik, and T. Yang, "The legal issue of deterrence of algorithmic control of digital platforms: the experience of china, the european union, russia and india," *BRICS Law Journal*, vol. 10, no. 1, pp. 147–170, 2023.

[34] B. R. Mendez, "Algorithmic governance and digital ethics: An organizational approach to automated decision-making," *International Journal of Management Science and Operations Research*, vol. 10, no. 1, pp. 86–97, 2025.

[35] E. S. Pramudito, R. Widayanti, S. Purnama, and K. A. Al-Farouqi, "Reinventing human resource practices through digital marketing platforms and remote work technologies," *APTISI Transactions on Management*, vol. 9, no. 3, pp. 267–277, Oct. 2025.

[36] X. Zheng, G. Zhou, and D. D. Zeng, "Platform governance in the era of ai and the digital economy," *ENGINEERING Management*, vol. 10, no. 1, p. 177, 2023.

[37] R. Zahid, A. Altaf, T. Ahmad, F. Iqbal, Y. A. M. Vera, M. A. L. Flores, and I. Ashraf, "Secure data management life cycle for government big-data ecosystem: Design and development perspective," *Systems*, vol. 11, no. 8, p. 380, 2023.

[38] S. L. Sitorus, A. Hermawan, A. W. Widjaja, and M. P. Berlianto, "Enhancing digital fashionpreneurship through innovation capability and market sensing," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 645–658, 2026.

[39] Y. Han and L. Xie, "Sustainable governance of digital platform ecosystem: A life cycle perspective through multiple governance parties," *Sustainability*, vol. 17, no. 8, p. 3628, 2025.

[40] A. S. Anita, T. Kuusk, G. Nicola, M. Hardini, and U. Rahardja, "Advancements in artificial intelligence and their contributions to sustainable development goals: A multidisciplinary review," *Smart Human-centered Emerging Research in Machine Intelligence*, vol. 2, no. 1, pp. 37–47, 2026.