Legal Autonomous Web-based Governance (LAW)
Vol. 1, No. 2, October 2026, pp. 200∼213
E-ISSN: XXXX-XXXX | P-ISSN: xxxx-xxxx

Data Governance and Digital Rights in AI Driven Business Ecosystems

Qurotul Aini[1], Fitra Putri Oganda[2], Sheila Aulia Anjani[3], Rahayu Pristiwati [4],
Annelinda Septian[5*]
[1,2,3]Faculty of Economics and Business Universitas Raharja, Indonesia
[4]Jurusan Bahasa dan Sastra Indonesia, Universitas Negeri Semarang, Indonesia
[5]Department of Digital Law and Artificial Intelligence Governance, Iliearning Incroporation, United States
[1]aini@raharja.info, [2]fitra.putri@raharja.info, [3]sheila@raharja.info, [4]pristi@mail.unnes.ac.id,
[5]septian_annelinda@ilearning.ee
***Corresponding Author**

Article Info

Article history:

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

Keywords:

Artificial Intelligence
Governance
Digital Rights
Accountability
Transparency

ABSTRACT

The rapid expansion of Artificial Intelligence (AI), big data, and interconnected digital platforms has transformed business ecosystems while creating governance challenges involving data protection, privacy, transparency, accountability, and digital rights. **This study examines** how legal governance principles and organizational mechanisms can be integrated to support responsible and sustainable AI-driven business ecosystems. **A qualitative normative** and conceptual approach was employed using scholarly literature, international standards, regulatory materials, and policy frameworks published primarily between 2023 and 2026, which were thematically analyzed across data lifecycle governance, privacy and data protection, transparency and explainability, accountability, human oversight, and fairness. **The findings demonstrate** that effective AI governance requires an integrated lifecycle-based framework connecting legal principles, organizational mechanisms, and stakeholder responsibilities. Accountability should remain attributable to identifiable actors, while meaningful transparency, human oversight, and access to remedies are essential for protecting individuals affected by AI-supported decisions. **The study proposes** an Integrated Human-Centered AI Legal Governance Framework that positions data governance as an organizational foundation for implementing digital rights and responsible AI principles. The framework provides a conceptual basis for accountable, transparent, rights-preserving, and sustainable AI governance across interconnected and data-intensive business environments while strengthening stakeholder trust and supporting responsible digital transformation.

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 integration of AI, cloud computing, big data analytics, Internet of Things, and digital platforms has transformed contemporary business ecosystems. Organizations increasingly rely on interconnected digital infrastructures to collect, process, exchange, analyze, and monetize large volumes of data for automated decision-making, personalized services, predictive analytics, and strategic operations [1]. Data has therefore

evolved from a conventional organizational resource into a strategic asset influencing competition, innovation, customer engagement, and organizational performance. However, growing reliance on AI and data-driven technologies has also created complex governance and legal challenges involving privacy, data protection, transparency, accountability, security, fairness, algorithmic decision-making, and individual digital rights [2]. These challenges are particularly significant because AI systems and data flows often extend beyond a single organization. Data may circulate among data providers, AI developers, cloud and infrastructure providers, digital platforms, business operators, third-party service providers, and end users. Consequently, responsibility for AI-supported decisions and potential rights violations may be distributed across multiple actors [3]. AI systems may also generate recommendations, classifications, or decisions with limited human intervention, raising concerns about whether affected individuals can understand, challenge, review, or seek remedies for potentially harmful outcomes. Algorithmic opacity, extensive data profiling, secondary data use, and automated decision-making can further intensify power asymmetries between organizations and individuals, particularly when individuals have limited control over how their data are collected, processed, combined, and used [4].

These developments demonstrate that AI governance cannot be reduced to technical risk management or internal data administration. Effective governance requires a legal and institutional framework that connects normative principles with organizational mechanisms throughout the AI and data lifecycle. Principles such as privacy, accountability, transparency, fairness, human oversight, and access to remedy establish obligations and protections while defining responsibilities for relevant AI actors [5]. At the organizational level, these principles must be translated into mechanisms including responsibility allocation, data governance, AI risk assessment, documentation, audit trails, algorithmic monitoring, human review, escalation procedures, and redress mechanisms. Thus, AI governance should establish an institutional connection between legal rights, regulatory obligations, and operational decision-making [6]. The complexity of these issues creates an important research gap. Existing AI governance and responsible AI frameworks provide foundations for risk management, accountability, transparency, human oversight, and rights protection but do not always explain how legal principles can be translated into organizational mechanisms across multi-actor AI-driven business ecosystems [7]. Similarly, data governance approaches often emphasize data quality, access, security, and lifecycle management without sufficiently connecting these mechanisms to algorithmic accountability, individual remedies, and the distribution of legal responsibility among ecosystem participants. The resulting gap concerns not only the identification of responsible AI principles but also their institutionalization through governance arrangements connecting data management, digital rights, legal accountability, and organizational practices throughout the AI lifecycle [8].

This gap is particularly relevant to emerging digital economies such as Indonesia, where AI adoption and data-driven business activities are developing within an evolving legal and institutional environment. The growth of AI-enabled platforms, digital services, financial technologies, and data-intensive business models creates opportunities for innovation and economic development while raising concerns about regulatory coordination, institutional responsibility, data protection, algorithmic accountability, and effective remedies for individuals affected by AI-supported decisions [9]. The Indonesian context therefore illustrates the difficulty of implementing AI governance when technological development may advance faster than comprehensive and sectorally coordinated governance arrangements. A governance framework for Indonesia must consequently address both digital-rights protection and responsibility allocation among organizations and other actors involved in AI development and deployment [10]. Against this background, this study examines the legal governance of AI in sustainable digital business ecosystems by investigating how data governance, digital rights, and responsible AI principles can be integrated into a coherent human-centered governance framework. Data governance is conceptualized as an institutional foundation for controlling data throughout its lifecycle, while digital rights provide a normative basis for protecting privacy, autonomy, fairness, transparency, and access to appropriate remedies [11]. Responsible AI governance provides organizational mechanisms for operationalizing these principles through human oversight, accountability structures, risk assessment, auditability, explainability, monitoring, and corrective procedures. The proposed perspective therefore distinguishes between legal governance principles and organizational mechanisms while establishing their functional relationship within AI-driven business environments.

The study contributes to the emerging discourse on AI governance, technology law, and digital governance by proposing an integrated framework that connects legal principles with practical governance mechanisms across interconnected AI business ecosystems [12]. Its contribution extends beyond treating data governance as a technical or managerial function by positioning it within a broader legal governance structure

in which responsibility remains attributable to identifiable actors rather than delegated to AI systems. The framework also emphasizes meaningful algorithmic transparency while recognizing legitimate interests in intellectual property, trade secrets, and commercial confidentiality. Similarly, meaningful human oversight and accessible mechanisms for review, contestation, and remedy are treated as essential components of accountable AI governance [13]. From a sustainable digital business perspective, responsible technological development depends not only on the capacity to deploy AI efficiently but also on maintaining accountability, rights protection, stakeholder trust, and regulatory compliance over time. Sustainable AI adoption therefore requires governance arrangements that continuously identify and manage risks, assign responsibility, protect digital rights, and provide mechanisms for intervention and remedy throughout the AI lifecycle. Legal governance provides the normative foundation, while organizational governance mechanisms provide the practical means for sustaining responsible technological development [14]. The proposed framework consequently seeks to support AI-driven business ecosystems that are innovative and economically productive while remaining accountable, transparent, rights-preserving, and responsive to the evolving legal and institutional environment.

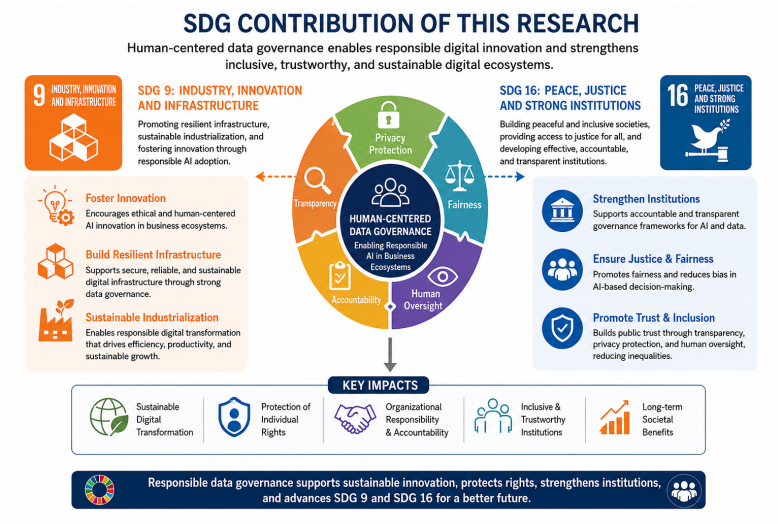

Figure 1. Contribution of AI Legal Governance to the Sustainable Development Goals

Figure 1 illustrates how this research contributes to the Sustainable Development Goals (SDGs), particularly SDGs 9 on Industry, Innovation and Infrastructure and SDGs 16 on Peace, Justice and Strong Institutions. The proposed human-centered AI legal governance perspective supports sustainable digital innovation by integrating data governance, digital rights protection, accountability, transparency, human oversight, and responsible AI practices within business ecosystems [15]. For SDGs 9, the framework promotes responsible technological development by encouraging organizations to manage AI-related risks throughout the data and AI lifecycle while maintaining innovation, resilience, and stakeholder trust. For SDGs 16, it strengthens accountable and trustworthy digital governance through clearer responsibilities among AI ecosystem actors, transparency, human oversight, and mechanisms for review, contestation, and remedy when AI-supported decisions adversely affect individuals [16]. By connecting legal principles with organizational governance mechanisms, the framework also helps address potential inequalities and rights violations arising from opaque, discriminatory, or inadequately governed AI systems. Accordingly, responsible AI legal governance can support sustainable digital transformation while aligning technological innovation with digital rights, organizational accountability, institutional responsibility, and broader societal interests.

2. LITERATURE REVIEW

2.1. Data Governance in AI-Driven Business Ecosystems

Data governance is a fundamental component of AI-driven business ecosystems because AI-based decisions depend on the quality, security, accessibility, and responsible use of data across interconnected actors

[17]. Unlike conventional data management, AI ecosystems involve continuous data flows among organizations, platforms, cloud providers, AI developers, business partners, and users, requiring governance to address data lifecycle management, privacy, transparency, accountability, security, and responsibility allocation [18]. The NIST AI RMF emphasizes continuous governance through the interconnected functions of Govern, Map, Measure, and Manage, while UNESCO promotes transparent, accountable, inclusive, and multi-stakeholder AI governance [19]. In this context, data governance should be understood not merely as an internal administrative function but as a socio-technical and organizational mechanism that connects legal requirements, technological controls, and responsible business practices. Effective data governance therefore provides a foundation for managing data throughout the AI lifecycle while supporting accountability, protecting individual rights, and enabling sustainable AI-driven business development.

2.2. Digital Rights, Privacy, and Data Protection

The expansion of AI-based data processing creates significant concerns regarding privacy, data protection, informational autonomy, transparency, and individual control over personal information [20]. AI systems can combine and analyze large datasets to generate profiles, infer behavioral patterns, personalize services, and support automated decision-making, creating risks when individuals have limited knowledge or control over how their data are collected, processed, or reused. UNESCO emphasizes that privacy and data protection should be protected throughout the AI lifecycle, supported by transparency, accountability, appropriate safeguards, and mechanisms that enable individuals to exercise their rights [21]. In AI-driven business ecosystems, these requirements are particularly important because personal data may flow across multiple organizations and jurisdictions, making individual control more difficult. Digital rights should therefore be embedded into AI governance from data collection and processing through deployment and post-deployment monitoring, including mechanisms for access, correction, appropriate data use, security, human review, and effective redress [22]. Accordingly, data governance provides the organizational means for protecting digital rights, while rights-based principles establish the legal and normative boundaries within which AI-driven business practices should operate.

2.3. AI Accountability, Transparency, and Human Oversight

Accountability, transparency, and human oversight are essential to responsible AI governance because AI systems can influence consequential business decisions while involving multiple actors throughout their development and deployment [23]. NIST identifies accountability and transparency as characteristics of trustworthy AI and emphasizes that organizational roles and responsibilities should be documented and continuously monitored [24]. UNESCO further highlights auditability, traceability, impact assessment, due diligence, human oversight, and mechanisms for investigating and remedying AI-related harms [25]. In AI-driven business ecosystems, accountability should therefore be allocated according to the actual roles of data providers, AI developers, platform operators, business users, and other relevant actors rather than being transferred to the AI system itself. Transparency should provide meaningful information about relevant data practices, AI-supported decisions, responsible actors, and available mechanisms for review or remedy, while human oversight should ensure that authorized and competent individuals can review, intervene in, or override consequential AI-supported decisions. Accordingly, accountability establishes responsibility, transparency enables understanding, and human oversight enables intervention, forming an integrated governance structure for reducing the risks of opaque and highly automated decision-making [26].

2.4. Human-Centered Governance for Responsible AI Business Ecosystems

Human-centered governance provides an integrated perspective for connecting data governance, digital rights, accountability, and responsible AI within contemporary business ecosystems. Rather than treating AI governance solely as a technological or compliance-oriented issue, this approach places human dignity, rights, agency, fairness, and well-being at the center of AI development and deployment [27]. UNESCO emphasizes human dignity, privacy, fairness, transparency, accountability, proportionality, and human oversight, while NIST presents trustworthy AI as a socio-technical objective requiring continuous governance, risk identification, measurement, and management [28]. These principles are particularly relevant to multi-actor business ecosystems because AI-related risks and decisions can affect customers, employees, business partners, and society, while responsibility may be distributed among different organizations. The literature therefore indicates a need to distinguish legal and normative governance principles from organizational mechanisms that operationalize them through risk assessment, documentation, auditing, human oversight, monitoring, and

remediation [29]. The central research gap lies in the limited integration of these dimensions into a business-oriented governance framework that connects data lifecycle management, digital rights, multi-actor accountability, transparency, and human oversight. Accordingly, this study positions human-centered AI governance as a framework through which legal principles and organizational mechanisms can be integrated to support accountable, rights-preserving, and sustainable AI-driven business ecosystems.

Table 1. Key Dimensions of Data Governance and Digital Rights in AI-Driven Business Ecosystems

Literature Dimension	**Core Governance Principle**	**Relevance to AI-Driven Business Ecosystems**	**Expected Governance Outcome**
Data Governance	Data quality, security, access, and lifecycle control	Ensures reliable and responsible management of data across ecosystem actors	Controlled and trustworthy data utilization
Privacy and Data Protection	Privacy, data minimization, and individual control	Protects individuals from unauthorized or excessive AI-based data processing	Stronger digital rights protection
Transparency	Explainability, disclosure, and traceability	Enables stakeholders to understand how AI systems use data and influence decisions	Greater trust and informed participation
Accountability	Clearly defined roles, responsibilities, and audit mechanisms	Establishes responsibility among data providers, AI developers, platforms, and business users	Reduced accountability gaps
Human Oversight	Human intervention, review, and decision control	Prevents excessive dependence on automated decisions in high-impact business processes	More responsible AI decision-making
Fairness and Non-Discrimination	Bias identification and mitigation	Reduces discriminatory outcomes arising from data and algorithmic processes	More equitable AI services and decisions
Risk Management	Continuous identification, measurement, and mitigation of AI risks	Enables organizations to manage technological, legal, ethical, and operational risks	Sustainable and resilient AI adoption

Table 1 synthesizes the principal governance dimensions identified in recent AI governance literature and standards. NIST emphasizes continuous governance through risk identification, measurement, and management, together with accountability, transparency, privacy, fairness, security, and explainability [30]. UNESCO complements this perspective by emphasizing human rights, data protection, auditability, accountability, and human oversight throughout the AI lifecycle [31]. Taken together, these dimensions indicate that AI governance requires an integrated approach in which legal and normative principles are translated into organizational mechanisms rather than implemented as isolated technical controls. In this study, these dimensions provide the conceptual foundation for examining how data governance, digital rights, and responsible AI practices can be aligned to support accountable and sustainable AI-driven business ecosystems.

3. RESEARCH METHOD

3.1. Research Design and Approach

This study employs a qualitative normative and conceptual research approach to examine how data governance, digital rights, and responsible AI principles can be integrated within AI-driven business ecosystems. This approach is appropriate because the study focuses on identifying legal and governance principles, accountability requirements, organizational mechanisms, and human-centered safeguards rather than measuring the performance of a specific AI system [32]. The analysis draws on contemporary scholarly literature, regulatory frameworks, international standards, and policy documents published primarily from 2023 onward. Its methodological foundation is informed by the methodological foundation of this study is informed by the

NIST AI Risk Management Framework (AI RMF), particularly its interconnected functions of Govern, Map, Measure, and Manage [33]. The study also adopts a human-centered governance perspective informed by UNESCO, emphasizing privacy and data protection, transparency, accountability, human oversight, fairness, and multi-stakeholder governance [34]. The research consists of four stages: literature and regulatory identification, thematic analysis, governance dimension synthesis, and conceptual framework development. These stages connect legal governance principles with organizational mechanisms for protecting digital rights and supporting responsible and sustainable AI adoption.

3.2. Data Sources and Literature Selection

The research uses secondary data obtained from peer-reviewed academic publications, international standards, regulatory documents, institutional reports, and authoritative policy frameworks, with particular attention to sources published between 2023 and 2026 to reflect recent developments in AI governance, digital rights, and data regulation [35]. The NIST AI RMF 1.0 is used as a principal reference for AI risk governance because it provides the functions of Govern, Map, Measure, and Manage, while UNESCO provides a complementary human rights perspective addressing privacy, data protection, accountability, transparency, human oversight, and fairness [36]. Literature is selected based on relevance, recency, authority, and conceptual contribution, with sources included when they substantively address data governance, digital rights, AI accountability, privacy and data protection, transparency and explainability, human oversight, fairness, responsible AI, or legal and organizational governance. Sources discussing AI without meaningful relevance to these governance dimensions are excluded. The selected literature and authoritative documents are then organized thematically to identify recurring governance principles, practical mechanisms, stakeholder responsibilities, and unresolved relationships that inform the development of the proposed conceptual framework [37].

Table 2. Literature Selection and Analytical Criteria

Criterion	Inclusion Criteria	Exclusion Criteria	Analytical Purpose
Publication period	Primarily 2023–2026	Sources without sufficient contemporary relevance	Maintain current governance perspective
Source authority	Peer-reviewed journals, international organizations, standards, regulations, and official reports	Unverified websites and non-authoritative sources	Ensure source credibility
Data governance	Data lifecycle, access, quality, security, sharing, and accountability	General data management without governance implications	Identify governance mechanisms
Digital rights	Privacy, data protection, autonomy, transparency, fairness, and redress	General digital transformation discussions	Identify rights-protection requirements
AI governance	Accountability, risk management, explainability, auditability, and human oversight	AI technical studies without governance relevance	Identify responsible AI mechanisms
Business ecosystem	Platforms, organizations, AI providers, users, and interconnected actors	Studies limited to isolated technical systems	Establish ecosystem-level perspective

Table 2 summarizes the criteria used to select and analyze the literature. The emphasis on recent and authoritative sources ensures that the analysis reflects contemporary developments in AI governance while maintaining a reliable methodological foundation. The criteria also focus the analysis on the relationship between data governance, digital rights, and responsible AI rather than treating AI as a purely technological issue. NIST provides a risk-based foundation for continuous AI governance, while UNESCO contributes a rights-oriented perspective emphasizing privacy, accountability, transparency, human oversight, and fairness [38]. These criteria support the identification of governance principles, stakeholder responsibilities, and organizational mechanisms that inform the development of the proposed framework.

3.3. Thematic Analysis and Conceptual Synthesis

Following literature selection, the study applies thematic analysis to identify recurring concepts, relationships, and governance gaps across the selected sources. The analysis focuses on six dimensions: data governance, privacy and data protection, transparency and explainability, accountability, human oversight, and fairness and non-discrimination [39]. Each source is examined to determine how these dimensions are defined and addressed in AI-driven environments. The relevant findings are then compared and grouped according to their governance relevance. The analysis proceeds through three steps: extracting relevant legal and governance principles, grouping related principles into analytical categories, and synthesizing the categories into a conceptual governance framework. Particular attention is given to how governance responsibilities are distributed among data providers, AI developers, platform operators, business organizations, and other ecosystem actors [40]. Consistent with the reviewed governance principles, accountability is treated as attributable to identifiable persons or legal entities, while auditability and traceability provide mechanisms for monitoring and establishing responsibility throughout the AI lifecycle. The synthesis therefore connects legal and normative principles with organizational governance mechanisms and provides the analytical basis for the proposed framework.

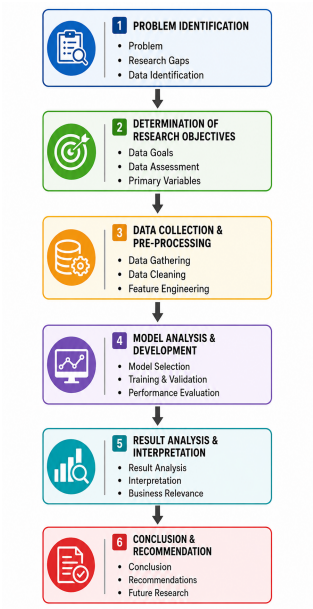

Figure 2. Research Methodological Framework

Figure 2 illustrates the methodological flow of the research, beginning with the identification of governance challenges arising from the interaction between AI, data-intensive business activities, and digital rights. The study then examines recent scholarly and authoritative sources, followed by a thematic analysis of recurring legal and governance principles [41]. The analysis identifies governance gaps concerning accountability, privacy and data protection, transparency and explainability, human oversight, and fairness. These findings are subsequently synthesized by connecting legal and normative principles with organizational governance mechanisms and stakeholder responsibilities. The final output is a conceptual AI governance framework designed to support accountable, transparent, rights-preserving, and sustainable AI-driven business ecosystems [42]. This methodological structure is consistent with the NIST approach, in which governance functions operate across the AI lifecycle and support the continuous identification, measurement, and management of AI-related risks.

3.4. Conceptual Framework Development and Validation

The final methodological stage develops a conceptual AI legal governance framework for sustainable digital business ecosystems by synthesizing themes identified through the literature analysis and mapping them to governance requirements across the AI lifecycle. The framework consists of three interconnected levels. The first represents legal and governance principles, including privacy, transparency, accountability, fairness, human oversight, and access to remedy [43]. The second represents organizational governance mechanisms, including

data lifecycle management, risk assessment, responsibility allocation, documentation, auditability, explainability, monitoring, and human review. The third represents stakeholder and operational application, through which data providers, AI developers, platform operators, business users, and other relevant actors implement these mechanisms throughout AI development and deployment. Conceptual robustness is assessed through triangulation by comparing the proposed dimensions with authoritative perspectives, particularly NIST's risk management and organizational governance approach and UNESCO's human rights-centered approach to AI governance [44]. The framework is considered conceptually supported when its principal dimensions are consistently reflected in the reviewed literature and explain governance requirements across different AI lifecycle stages. This approach does not constitute empirical validation but provides a systematic conceptual basis for integrating legal principles, organizational mechanisms, stakeholder responsibilities, and digital rights within AI-driven business ecosystems.

4. RESULTS AND DISCUSSION

4.1. Data Governance Requirements in AI-Driven Business Ecosystems

The analysis demonstrates that effective data governance in AI-driven business ecosystems requires an integrated structure covering the entire data and AI lifecycle. Six core governance requirements emerge from the analysis: data lifecycle management, privacy and data protection, transparency, accountability, human oversight, and fairness. These requirements are interconnected because weaknesses in one dimension can undermine digital rights and the reliability of AI-supported decisions. The findings indicate that data governance should therefore extend beyond conventional data quality and security controls to govern how data are collected, processed, shared, analyzed, and used in automated decision-making [45]. The analysis also shows that governance responsibilities should correspond to the roles of ecosystem actors: data providers should ensure appropriate data collection and quality. AI developers should address model development and associated risks. platform and business operators should ensure responsible deployment and monitoring; and organizational decision-makers should retain responsibility for consequential decisions. Accordingly, data governance functions as an organizational foundation for implementing legal and rights-based principles because it determines how data are controlled and how responsibilities are maintained throughout the AI lifecycle.

Table 3. Results of the Governance Dimension Analysis

Governance Dimension	Main Finding	Digital Right Protected	Required Governance Mechanism
Data Lifecycle Governance	Data must be controlled from collection to deletion	Informational autonomy and privacy	Data classification, retention, access control
Privacy and Data Protection	AI processing requires appropriate limitations and safeguards	Privacy and data protection	Privacy controls, purpose limitation, security
Transparency	Stakeholders need understandable information about AI processes	Right to information and meaningful participation	Disclosure, explainability, traceability
Accountability	Responsibility must be assigned to identifiable ecosystem actors	Right to remedy and fair treatment	Auditing, documentation, responsibility allocation
Human Oversight	High-impact automated decisions require meaningful human intervention	Human autonomy and procedural fairness	Human review, intervention, escalation
Fairness	AI outcomes must be monitored for discriminatory effects	Equality and non-discrimination	Bias assessment, monitoring, corrective measures

Table 3 summarizes the principal findings from the thematic analysis. The results indicate that pro-

tecting digital rights in AI-driven business ecosystems requires an integrated governance structure rather than a single governance mechanism. Data lifecycle management, privacy and data protection, transparency, accountability, human oversight, and fairness are interconnected because weaknesses in one dimension can affect individual protection and the reliability of AI-supported decisions [46]. The analysis further shows that each governance dimension has corresponding implications for digital rights, requiring organizational data practices to be assessed not only in terms of technical effectiveness but also in terms of their effects on individuals. These findings support the central argument that data governance should function as a rights-preserving organizational mechanism within a broader AI legal governance framework rather than solely as an internal data management function.

4.2. Digital Rights Protection Across the AI Lifecycle

The results show that digital rights protection should be embedded continuously across the AI lifecycle rather than treated as a single compliance activity. The analysis identifies four critical stages: data acquisition, AI development and processing, AI deployment and decision-making, and post-deployment monitoring. During data acquisition, organizations should establish legitimate and transparent data practices and avoid unnecessary collection, while AI development should address data quality, privacy risks, potential bias, and the suitability of datasets for their intended purposes [47]. During deployment, transparency and human oversight become particularly important because AI-supported outputs may affect customers, employees, and other stakeholders. Post-deployment monitoring should identify discriminatory outcomes, privacy incidents, system failures, and emerging risks. The findings further indicate that meaningful transparency requires more than disclosure of AI use; affected individuals should receive understandable information about relevant data practices, decision processes, responsible actors, and available mechanisms for questioning or correcting harmful outcomes. Human oversight is particularly important for high-impact decisions because it enables intervention when automated outputs are inaccurate, unfair, or inconsistent with individual circumstances. Accordingly, digital rights protection should be incorporated throughout the AI lifecycle through governance-by-design, ensuring that privacy, transparency, fairness, human oversight, and access to appropriate remedies are treated as continuous governance requirements.

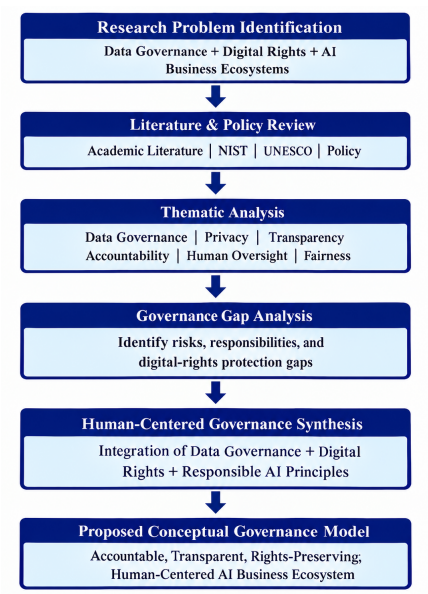

Figure 3. Rights-Based Data Governance Across the AI Lifecycle

Figure 3 illustrates how digital rights protection is distributed across the AI lifecycle. The findings indicate that privacy and individual control are particularly important during data acquisition, while data quality and bias assessment become critical during AI development and processing. During deployment and decision-making, transparency, explainability, and human oversight become essential because AI outputs may directly affect individuals [48]. During post-deployment monitoring, auditing, accountability, and redress mechanisms

provide continued protection against emerging risks and harmful outcomes. These findings demonstrate that digital rights cannot be effectively protected through a single governance intervention but require continuous, lifecycle-based governance across the development, deployment, and operation of AI systems.

4.3. Accountability and Human Oversight in AI-Based Business Decisions

The analysis identifies accountability and human oversight as critical governance mechanisms for addressing responsibility gaps in AI-driven business ecosystems, where data providers, processors, AI developers, cloud providers, platform operators, and business users may jointly contribute to AI-based decisions. The findings indicate that responsibility should be explicitly allocated according to the roles and functions performed by each actor throughout the AI lifecycle, rather than being attributed to the AI system itself [49]. Meaningful human oversight requires more than human presence in the decision-making process; it requires authorized and competent individuals to access relevant information and have sufficient capacity to review, intervene in, or override AI-generated outcomes, particularly in high-impact decisions involving employment, financial services, insurance, essential services, or customer eligibility. The results further indicate that documented responsibility structures, AI impact assessments, audit trails, model monitoring, escalation procedures, and human review mechanisms can establish traceable relationships between AI outputs, organizational decisions, and responsible actors. Explainability supports this process by enabling organizations and affected individuals to understand relevant aspects of AI-supported decisions. However, technical explainability alone cannot ensure accountability without accessible mechanisms for review and remedy. Accordingly, the findings establish an integrated governance relationship in which transparency enables understanding, human oversight enables intervention, and accountability establishes responsibility and access to remedy.

4.4. Integrated Human-Centered AI Legal Governance Framework

Based on the thematic analysis and conceptual synthesis, this study proposes an Integrated Human-Centered AI Legal Governance Framework for sustainable AI-driven business ecosystems. The framework integrates three interconnected levels: legal and governance principles, organizational mechanisms, and stakeholder application. These levels connect privacy, transparency, accountability, fairness, human oversight, and access to remedy with practical mechanisms such as data lifecycle management, risk assessment, documentation, auditability, monitoring, and human review. The framework assigns these responsibilities to relevant actors, including data providers, AI developers, platform operators, business users, and organizational decision-makers, according to their roles throughout the AI lifecycle [50].

The findings demonstrate that these levels must operate as an integrated structure because weaknesses in one dimension can undermine the effectiveness of others. Data governance therefore functions as a core organizational mechanism for protecting digital rights and implementing responsible AI principles. The framework emphasizes that accountability must remain attributable to identifiable actors and that transparency, human oversight, fairness, and access to remedy are essential for addressing AI-related risks and protecting affected individuals. Its principal contribution is connecting legal governance principles with organizational mechanisms and multi-actor responsibilities, providing a structured basis for accountable, transparent, rights-preserving, and sustainable AI governance. The framework can be applied across diverse AI-enabled contexts, including digital commerce, financial technology, platform-based businesses, human resource systems, and other data-intensive environments.

5. MANAGERIAL IMPLICATIONS

The findings provide important managerial implications for organizations operating within AI-driven business ecosystems. Managers should establish governance structures that translate legal and rights-based principles into practical mechanisms across the data and AI lifecycle. These mechanisms should include clear responsibility allocation among data providers, AI developers, technology and platform providers, and business decision-makers, supported by data-quality monitoring, privacy controls, AI risk assessments, documentation, audit trails, human review, and escalation procedures for high-impact decisions. Organizations should also provide stakeholders with meaningful information about relevant data practices and AI-supported decisions while maintaining mechanisms for contestation, correction, and appropriate remedy. Integrating these mechanisms into organizational processes can help reduce legal, ethical, and operational risks, strengthen stakeholder trust, and support sustainable AI adoption. Accordingly, managerial priorities should extend beyond AI efficiency

toward the development of responsible, accountable, transparent, and human-centered AI business ecosystems that align technological innovation with individual digital rights and organizational responsibility.

6. CONCLUSION

This study examined the legal governance of AI in sustainable digital business ecosystems by integrating data governance, digital rights protection, and responsible AI principles within a human-centered governance perspective. The findings demonstrate that effective AI governance cannot be limited to conventional data management, privacy compliance, or technical controls; rather, it requires an integrated approach across the data and AI lifecycle. The study identifies key governance dimensions, including data lifecycle governance, privacy and data protection, transparency and explainability, accountability, human oversight, fairness, and access to appropriate remedies. These dimensions are interdependent, as weaknesses in data governance can increase risks to digital rights, while effective accountability, transparency, and human oversight can strengthen trust and responsible AI adoption. The proposed framework therefore connects legal and governance principles with organizational mechanisms and stakeholder responsibilities, positioning data governance as an important organizational foundation for protecting digital rights and supporting accountable, transparent, and sustainable AI-driven business development.

The research questions are addressed by demonstrating that effective governance of AI-driven business ecosystems requires the integration of legal principles, organizational governance mechanisms, and clearly assigned responsibilities throughout the AI lifecycle. The findings establish that accountability cannot be delegated to AI systems because responsibility must remain attributable to identifiable actors capable of monitoring, reviewing, intervening in, and correcting AI-supported outcomes. The framework further demonstrates that meaningful transparency, human oversight, privacy protection, fairness, and access to remedy are necessary to translate rights-based principles into practical governance. However, the study has several limitations. First, it employs a normative and conceptual methodology based primarily on secondary literature, international standards, regulatory materials, and policy frameworks rather than empirical evidence from organizations. Second, the proposed framework has not yet been quantitatively tested or evaluated through implementation in a specific business ecosystem. Third, differences in national legal systems, institutional arrangements, and sector-specific regulatory requirements may affect how the proposed governance principles are operationalized. Accordingly, the framework should be understood as a conceptual foundation rather than a universally validated operational model.

Future research should empirically examine the proposed AI legal governance framework across different AI-driven business sectors, including digital commerce, financial technology, healthcare platforms, and human resource systems. Quantitative studies could develop measurable indicators of governance maturity, digital rights protection, accountability, transparency, human oversight, and stakeholder trust and subsequently examine their relationships using appropriate statistical methods. Qualitative case studies could further investigate how organizations allocate AI responsibilities and implement risk assessment, algorithmic auditing, privacy controls, human review, contestation, and remedy mechanisms in real-world deployments. Future research should also compare governance and regulatory requirements across jurisdictions, particularly in emerging digital economies, to determine which elements of the framework are broadly applicable and which require contextual adaptation. Further studies could examine the integration of emerging approaches, such as explainable AI, privacy-preserving technologies, and automated auditing, into the proposed governance structure. Such research would strengthen the empirical and practical foundation of the framework and contribute to the development of more transparent, accountable, rights-preserving, and sustainable AI-driven business ecosystems.

7. DECLARATIONS

7.1. About Authors

Qurotul Aini (QA) https://orcid.org/0000-0002-7546-5721

Fitra Putri Oganda (FO) https://orcid.org/0000-0002-4590-0657

Sheila Aulia Anjani (SA) https://orcid.org/0009-0007-9121-1151

Rahayu Pristiwati (RP) https://orcid.org/0000-0001-8399-0238

Annelinda Septian (AS) https://orcid.org/0000-0001-8399-0238

7.2. Author Contributions

Conceptualization: QA; Methodology: FO; Software: SA; Validation: RP, AS and QA; Formal Analysis: FO and SA; Investigation: RP; Resources: AS; Data Curation: QA and FO; Writing Original Draft Preparation: SA and RP; Writing Review and Editing: AS, QA and FO; Visualization: SA; All authors, QA, FO, SA, RP, and AS, 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] P. R. Rajgopal and S. Yadav, "The role of data governance in enabling secure ai adoption," *International Journal of Sustainability and Innovation in Engineering*, vol. 3, no. 1, 2025.

[2] R. Ameria, "The synergistic imperative: Integrating artificial intelligence with master data management for enhanced data quality and governance," *Journal of Computer Science and Technology Studies*, vol. 7, no. 6, pp. 922–929, 2025.

[3] O. Ferli, N. A. Achsani, T. Andati, and Z. Asikin, "Sustainable business innovation in indonesian firms esg disclosure profitability and greenwashing," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 405–419, 2026.

[4] H. Choung, P. David, and J. S. Seberger, "A multilevel framework for ai governance," in *The Routledge Handbook of Global and Digital Governance Crossroads*. Routledge India, 2024, pp. 310–323.

[5] W. Prihandini and S. Safaria, "Digital resilience and financial stability: Rethinking the strategic role of fintech, ai, and cbdc in indonesia and emerging economies," *Journal of Business, Finance, and Banking*, vol. 1, no. 1, pp. 50–70, 2025.

[6] 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.

[7] D. Annam, "Ai-powered data observability & governance agent for cloud analytics: Transforming enterprise data management," *Journal of Computer Science and Technology Studies*, vol. 7, no. 3, pp. 804–811, 2025.

[8] M. L. Rahman, M. I. Alam, R. Anzum, S. Acharjee, M. S. Alam, and S. Shamarukh, "Ai-driven predictive analytics for supply chain resilience, financial risk management, and digital marketing strategy: A unified business intelligence framework," *Journal of Business and Management Studies*, vol. 8, no. 7, pp. 41–55, 2026.

[9] C. Lukita, A. K. Chandra, R. Fahrudin, N. M. Agatha, and D. P. Suci, "Maturity level measurement model of msmes for sustainable economic growth," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 434–442, 2026.

[10] D. Piétron, P. Staab, and F. Hofmann, "Digital circular ecosystems: A data governance approach," *GAIA-Ecological Perspectives for Science and Society*, vol. 32, no. 1, pp. 40–46, 2023.

[11] L. Zhang and W. Wang, "Data governance and digital trust in smart markets," *Journal of Electronic Commerce*, vol. 1, no. 1, pp. 85–104, 2025.
[12] U. Rahardja, M. T. D. S. Putri, N. Septiani, F. Amelia, A. Avandi, and R. Evans, "Human centered legal governance for autonomous ai in digital societies," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 29–41, 2026.
[13] A. K. Sharma and R. Sharma, "Data governance in the age of artificial intelligence: Challenges, best practices and regulatory compliance," *Applied Marketing Analytics*, vol. 10, no. 4, pp. 390–403, 2025.
[14] M. Heikkilä, J. Heikkilä, and F. Ahmad, "Data-driven business model innovation in europe: ethical data practices and ecosystem involvement," *Systems*, vol. 13, no. 3, p. 164, 2025.
[15] S. D. Retnandari, K. Khaeroman, A. T. Winarni, and W. Busse, "Digital innovation and technology driven evaluation of maritime safety systems performance in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 551–564, 2026.
[16] C. Aksoy, "Digital business ecosystems: An environment of collaboration, innovation, and value creation in the digital age," *Journal of business and trade*, vol. 4, no. 2, pp. 156–180, 2023.
[17] R. C. Ångström, M. Björn, L. Dahlander, M. Mähring, and M. W. Wallin, "Getting ai implementation right: Insights from a global survey," *California Management Review*, vol. 66, no. 1, pp. 5–22, 2023.
[18] U. Rahardja and Q. Aini, "Enhancing blockchain security through smart contract vulnerability classification using bilstm and attention mechanism," *Journal of Current Research in Blockchain*, vol. 3, no. 1, pp. 28–45, 2026.
[19] P. Dunleavy and H. Margetts, "Data science, artificial intelligence and the third wave of digital era governance," *Public Policy and Administration*, vol. 40, no. 2, pp. 185–214, 2025.
[20] S. D. Jankovic and D. M. Curovic, "Strategic integration of artificial intelligence for sustainable businesses: Implications for data management and human user engagement in the digital era," *Sustainability*, vol. 15, no. 21, p. 15208, 2023.
[21] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *Sage Open*, vol. 14, no. 2, p. 21582440241258595, 2024.
[22] S. Ramisetty, "Data governance for ai-powered pega applications: Compliance, privacy & reliability," *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, vol. 8, no. 1, pp. 11 574–11 580, 2025.
[23] G. Secundo, C. Spilotro, J. Gast, and V. Corvello, "The transformative power of artificial intelligence within innovation ecosystems: a review and a conceptual framework," *Review of Managerial Science*, vol. 19, no. 9, pp. 2697–2728, 2025.
[24] I. Haryanto, Y. Yunadin, W. Setiawan, F. Agrimiandra, and D. Alam, "Legal governance of technology driven cybercrime in digital society," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 141–154, 2026.
[25] H. S. Mahmood, D. M. Abdulqader, R. M. Abdullah, H. Rasheed, Z. N. R. Ismael, and T. M. G. Sami, "Conducting in-depth analysis of ai, iot, web technology, cloud computing, and enterprise systems integration for enhancing data security and governance to promote sustainable business practices," *Journal of Information Technology and Informatics*, vol. 3, no. 2, pp. 297–332, 2024.
[26] E. M. Ali, F. Dirgantara, and D. Darmawan, "Legal protection of consumers in online transactions: A case study of online fraud in indonesia," *International Journal of Service Science, Management, Engineering, and Technology*, vol. 6, no. 3, pp. 27–38, 2024.
[27] M. Nurkanti, U. Rahardja, M. Lubis, and A. Shukri, "Deep learning-based biology learning with ethnopedagogy and local wisdom to support sustainable development goals," *Jurnal Pendidikan IPA Indonesia*, vol. 15, no. 1, pp. 103–111, 2026.
[28] M. Pathak, "Data governance redefined: The evolution of eu data regulations from the gdpr to the dma, dsa, dga, data act and ai act." *European Data Protection Law Review (EDPL)*, vol. 10, no. 1, p. 43, 2024.
[29] S. Pahune, Z. Akhtar, V. Mandapati, and K. Siddique, "The importance of ai data governance in large language models," *Big Data and Cognitive Computing*, vol. 9, no. 6, p. 147, 2025.
[30] A. H. Rambe, I. Kumalasari *et al.*, "Juridical analysis of legal protection for consumers in e-commerce transactions in indonesia," *IJECK (International Journal Of Economy, Computer, Law, Management And Communication)*, vol. 2, no. 2, pp. 34–42, 2024.
[31] U. Rahardja, M. L. Daeli, S. A. Anjani, L. Pasha, A. Asri, and H. Zainarthu, "Enhancing trust and effi-

ciency in e-commerce transactions through blockchain ai synergy," *ADI Journal on Recent Innovation*, vol. 7, no. 1, pp. 25–37, 2025.

[32] R. Hanifiyah, "Law enforcement of online business fraud crimes according to positive law and islamic law (study on court decision number 975/pid. sus/2018/pn mks)," B.S. thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta, 2022.

[33] F. Yang, M. Z. Abedin, Y. Qiao, and L. Ye, "Toward trustworthy governance of ai-generated content (aigc): A blockchain-driven regulatory framework for secure digital ecosystems," *IEEE Transactions on Engineering Management*, vol. 71, pp. 14 945–14 962, 2024.

[34] D. Derlina, S. Anggoro, R. T. Safariningsih, and C. Perez, "A digital business legal regulation model to create a safe and sustainable digital ecosystem," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 1–14, 2026.

[35] I. D. Kurniawan, P. Suwadi, and J. G. S. Soehartono, "An analysis of economic criminal actions of e-money theft case in e-commerce in indonesia," in *1st INTERNATIONAL CONFERENCE ON LAW, BUSINESS, AND GOOD GOVERNANCE 2024*, 2024, p. 1134.

[36] F. Ji, Y. Zhou, H. Zhang, G. Cheng, and Q. Luo, "Navigating the digital odyssey: Ai-driven business models in industry 4.0," *Journal of the Knowledge Economy*, vol. 16, no. 1, pp. 5714–5757, 2025.

[37] L.-F. Spulbar, "Legal frameworks for ai-driven markets and their challenges and opportunities in the digital economy," *Revista de Ştiinţe Politice. Revue des Sciences Politiques*, no. 86, pp. 288–304, 2025.

[38] S. Widada, S. T. S. Alfian *et al.*, "Utilizing blockchain for electronic wellbeing records," *Blockchain Frontier Technology*, vol. 1, no. 2, pp. 11–22, 2022.

[39] E. E. Akpan, A. FCICN, P. PPGDCA, and L. P. Henry, "Adoption of ai for search of entrepreneurial business opportunities," *Shared Seasoned International Journal of Topical Issues*, vol. 12, no. 2, pp. 1–2, 2025.

[40] M. M. Bühler, I. Calzada, I. Cane, T. Jelinek, A. Kapoor, M. Mannan, S. Mehta, V. Mookerje, K. Nübel, A. Pentland *et al.*, "Unlocking the power of digital commons: Data cooperatives as a pathway for data sovereign, innovative and equitable digital communities," *Digital*, vol. 3, no. 3, pp. 146–171, 2023.

[41] F. Agrimiandra, M. A. Mahdafiqia, D. P. A. Sakti, and D. Alam, "Legal governance of state financial losses in corruption cases," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 155–168, 2026.

[42] D. Marsela, Y. Yudhistira, and B. Fawaid, "Legal protection of consumers in online business: a criminal law perspective in handling fraud and identity theft," *Research Horizon*, vol. 4, no. 3, pp. 99–106, 2024.

[43] N. Vanu, M. Hasan, S. Akter, and M. Faruque, "Legal and ethical frameworks for regulating artificial intelligence in business," *Journal of Business Venturing, AI and Data Analytics*, vol. 1, no. 10.63471, 2024.

[44] J. Bahar, M. A. Prayoga, A. Alamsyah, and D. Alam, "Justice based consumer dispute mediation in the digital economy," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 169–181, 2026.

[45] S. Knight, A. Shibani, and N. Vincent, "Ethical ai governance: Mapping a research ecosystem," *AI and Ethics*, vol. 5, no. 2, pp. 841–862, 2025.

[46] M. A. Camilleri, "Artificial intelligence governance: Ethical considerations and implications for social responsibility," *Expert systems*, vol. 41, no. 7, p. e13406, 2024.

[47] P. Paroli, M. Muhtarom, M. M. Siahaan, D. Derlina, K. Moyo *et al.*, "Smart contract based data strategy for startup growth in digital business systems," *Journal of Computer Science and Technology Application*, vol. 3, no. 2, pp. 117–129, 2026.

[48] A. Yukhno, "Digital transformation: Exploring big data governance in public administration," *Public Organization Review*, vol. 24, no. 1, pp. 335–349, 2024.

[49] D. Eke and B. Stahl, "Ethics in the governance of data and digital technology: An analysis of european data regulations and policies," *Digital Society*, vol. 3, no. 1, p. 11, 2024.

[50] OECD, *Country Digital Education Ecosystems and Governance: A Companion to Digital Education Outlook 2023*. Paris: OECD Publishing, 2023. [Online]. Available: https://doi.org/10.1787/906134d4-en