EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:7 |July 2025

DATA COMPLIANCE FRAMEWORK IN AI APPLICATION OF REMOTE EDUCATION: LEGAL PATH BASED ON KNOWLEDGE MANAGEMENT AND EFFECT EVALUATION

Chen Chenwei
PhD, School of Economics and Management, Yunnan Open University (Yunnan Technical College of Industry), Kunming, China

ABSTRACT
The deep integration of artificial intelligence into distance education has triggered a systemic data compliance crisis. This study addresses the unique contradiction where educational data possesses both personal attributes and knowledge value, as well as issues in existing governance models such as the disconnect between technical approaches and institutional regulations, the separation of knowledge management from effectiveness evaluation, and the absence of cross-border rules. It proposes a "knowledge management-effect evaluation" dual-driven framework for legalizing data compliance. First, it analyzes four major challenges: imbalance of rights and responsibilities among stakeholders, regulatory blind spots in data types, risks arising from technological development, and conflicts of sovereignty across borders. Second, it establishes theoretical foundations by clarifying that the knowledge management dimension must balance incentives for knowledge innovation with data security controls, while the effectiveness evaluation dimension should ensure data credibility and algorithmic trustworthiness. These two dimensions achieve synergy through goal alignment, risk complementarity, and tool integration. Third, it designs a legal pathway: establishing three core principles—education-oriented, tiered control, and dynamic informed consent; building an institutional system featuring restructured stakeholder responsibilities, embedded lifecycle processes, and cross-border data flow safety gates; and integrating technical governance tools like privacy-enhancing technologies, algorithm rule parameterization, and blockchain judicial empowerment. Finally, it proposes an implementation safeguard system comprising specialized regulatory mechanisms, optimized responsibility allocation, and closed-loop feedback for effectiveness evaluation. This study provides a theoretically innovative and practically actionable solution to address data governance challenges in educational technology innovation, aiming to strengthen the legal foundation for educational equity and quality in the digital era.

KEYWORDS: *Distance Education; Artificial Intelligence; Data Compliance; Knowledge Management; Effectiveness Evaluation; Rule of Law Path; Dual-Wheel Drive Framework*

I. INTRODUCTION

The intelligent transformation of distance education is profoundly reshaping the global educational ecosystem. As artificial intelligence technology penetrates online learning platforms, adaptive assessment systems, and knowledge management tools, educational data has evolved from auxiliary resources to core production factors. While this data-driven model enhances teaching efficiency, it also triggers multiple compliance crises: the uncontrolled collection of students' biometric information and behavioral profiles increases privacy risks; hidden biases in personalized recommendation algorithms may exacerbate educational inequality; and monopolistic control by technology providers threatens the public nature of knowledge resources. In this context, optimizing knowledge management effectiveness and ensuring credible evaluation of educational outcomes both rely heavily on the legal framework for data governance. This study aims to bridge the theoretical gap between educational technological innovation and data governance, providing institutional pathways for implementing regulations such as the Personal Information Protection Law and Interim Measures for Managing Generative AI Services in educational contexts. Its practical significance extends beyond defining technical ethical boundaries—it directly impacts the foundation of educational equity and quality in the digital age.

1. Literature review and problem proposal

Current research on educational data governance exhibits a pronounced dichotomy: the technological governance approach focuses on instrumental rationalities such as data encryption and anonymization, while the legal governance path emphasizes normative analysis of authority-definition and compliance obligations (Vorecol, 2025). This fragmentation reveals three theoretical shortcomings: First, overemphasis on technical solutions

neglects institutional coordination, failing to establish a "technology-institution" integrated framework for legal governance. Second, the separation of data asset attributes in knowledge management from data validation requirements for effectiveness evaluation weakens the systematic nature of compliance mechanisms. Third, cross-border education cloud platforms lack targeted regulations addressing data sovereignty conflicts, with insufficient research on adapting international rules for domestic contexts. These limitations collectively highlight a core challenge: How to construct a remote education AI data compliance framework that achieves dual objectives of knowledge management value realization and credibility enhancement through effectiveness evaluation? Solving this issue requires confronting the unique characteristics of educational data across dimensions of stakeholder relationships, type attributes, and technical risks.

2. Research methods and innovation points

This study employs a dual-track research methodology combining normative analysis and case comparison. On one hand, it deconstructs regulatory frameworks such as the Cybersecurity Law and Data Outbound Security Assessment Measures to delineate legal boundaries for educational data processing. On the other hand, it compares the EU's GDPR-compliant "Educational Data Protection Certification Mechanism" with China's "Smart Education Demonstration Zone" pilot programs, analyzing discrepancies in technical providers 'compliance obligations. Theoretically innovative, this work introduces the first "Knowledge Management-Evaluation Effect" dual-driven model, breaking through traditional compliance frameworks' unidirectional constraints. Its contributions manifest in three aspects: establishing classification standards for educational data integrating knowledge asset attributes to achieve differentiated governance of teaching resource copyrights and AI-generated content; designing blockchain-based data certification mechanisms for educational outcomes to ensure judicial validity of learning achievement verification chains; proposing cross-border data flow compliance solutions combining federated learning with trusted execution environments to balance international collaboration with data sovereignty protection. These explorations not only provide actionable data compliance guidelines for educational institutions but also reaffirm the rule-of-law foundation of education-centered principles in the era of technological advancement.

II. DATA COMPLIANCE DILEMMA OF AI APPLICATION IN DISTANCE EDUCATION

Driven by artificial intelligence, remote education has experienced explosive growth. However, its data governance system has yet to keep pace with technological advancements, creating multiple compliance challenges. These issues stem not only from the inherent complexity of technology itself, but also from the unique characteristics of educational scenarios, the diversity of stakeholder relationships, and the lag in legal regulation. A systematic overhaul is urgently needed to address these systemic challenges.

1. The Imbalance of Rights and Responsibilities Caused by The Complexity of Subject Relations

The education data ecosystem involves dynamic interactions among educational institutions, technology service providers, educators and students, and regulatory bodies. As nominal data controllers, educational institutions often delegate data processing authority to tech suppliers due to technical limitations. Meanwhile, tech companies establish technical barriers through algorithmic black boxes to evade data security responsibilities. A typical scenario illustrates this: The ownership of student answer data collected by AI-assisted homework grading systems remains legally ambiguous (Zhongnan University Law School, 2025). Educational institutions assert teaching management rights, tech firms emphasize data processing contributions, while students demand personal information autonomy – creating structural conflicts in rights claims. More critically, regulators' lack of technical expertise risks undermining their authority when addressing algorithmic discrimination issues. This imbalance in responsibility allocation leads to cyclical shifts in compliance obligations among stakeholders, resulting in an "organized irresponsibility" state.

2. Regulatory Blind Spots Caused by the Particularity of Data Types

The core contradiction of educational data lies in its dual nature as both personal attributes and intellectual assets. On one hand, dynamic data such as learning behavior profiles and cognitive assessments fall under the definition of sensitive information in China's Personal Information Protection Law, yet current regulations lack specific criteria for "educational sensitive data." For instance, behavioral data like students' attention trajectories and interaction latency in virtual classrooms—while accurately reflecting cognitive patterns—remains outside traditional privacy protection frameworks. On the other hand, knowledge management scenarios present new challenges in data ownership: copyright data from collaborative teaching resources becomes fragmented due to multi-party contributions; while derivative content like AI-generated lesson plans and test materials lacks clear intellectual property rights under the current Copyright Law. This dual nature traps data in regulatory dilemmas between privacy protection and knowledge sharing values.

EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:7 |July 2025

3. The System Lags Behind the Risk of Technology Application

The integration of deep learning technologies has given rise to unforeseen risks in traditional legal frameworks. The opaque nature of algorithmic decision-making particularly exacerbates "technological educational inequity": Personalized recommendation systems, which reinforce path dependence through historical data, may systematically marginalize specific student groups. Empirical studies reveal that an intelligent tutoring system persistently pushes basic practice questions to students in under-resourced areas, creating substantial "digital class stratification". In privacy protection, while federated learning and other distributed training models ostensibly achieve "data non-export", they actually reconstruct original data through gradient parameter inversion – constituting the "indirect data collection" prohibited by Article 11 of China's Interim Measures for the Administration of Generative AI Services (Zou, 2025). More critically, the continuous iteration mechanism of models leads to uncontrolled data lifecycle management, effectively undermining the principle of purpose-based data collection, resulting in a technical paradox of "permanent data retention".

4. Sovereign Conflict in Cross-Border Transmission Compliance

The expansion of international education cloud platforms has sparked a data sovereignty competition. Overseas education tech giants are leveraging SaaS models to control core intellectual property data of Chinese educational institutions. Such data flows not only breach the regulatory red line of China's Data Outbound Security Assessment Measures but also face challenges in applying the "research exception" clause due to the commercial confidentiality of intellectual assets. A case study of an online education platform reveals that its architecture modifications to meet China's data localization requirements resulted in a 37% performance degradation of its adaptive learning system, demonstrating the inverse relationship between technical compliance costs and educational efficiency. The deeper contradiction lies in the absence of a "security-development" balance mechanism for cross-border education data flow: excessive restrictions would hinder international educational collaboration, while unchecked flows risk the loss of strategic national education data resources.

III. THE THEORETICAL BASIS OF THE DUAL-WHEEL DRIVE FRAMEWORK

The data compliance framework for AI applications in remote education must be rooted in the intersection of educational digital transformation's inherent logic and legal governance (Data Governance Team, 2025). The "knowledge management-effect evaluation" dual-driven paradigm proposed in this paper aims to overcome the traditional data governance dilemma where technical approaches and institutional regulations remain disconnected. Its theoretical foundation can be systematically explained through two dimensions: the value conversion of knowledge creation and the legal credibility of educational assessment.

1. The Legal Logic of Knowledge Management Dimension

The governance of educational data compliance must transcend the traditional single-dimensional approach to personal information protection, returning to the fundamental nature of knowledge production and dissemination in educational contexts. Knowledge management theory reveals that educational data essentially serves as a digital carrier for both explicit and tacit knowledge: Explicit knowledge data contains codifiable educational content assets, whose compliance management should align with intellectual property protection and data ownership rules outlined in the Copyright Law and Data Security Law; Tacit knowledge data reflects contextual cognitive construction processes, which require handling in accordance with the special protection principles for sensitive information stipulated in the Personal Information Protection Law.

The theory of educational data assetization further strengthens compliance frameworks. When teaching data is integrated into knowledge management systems, its value extends beyond operational efficiency gains to become crucial for building institutions' core competitiveness. For instance, adaptive learning content generated by generative AI possesses significant derivative intellectual property attributes. Without proper ownership confirmation mechanisms, this could disrupt the "data-knowledge-asset" transformation chain (European Commission, 2024). Therefore, data compliance objectives should balance incentives for knowledge innovation with data security controls: On one hand, establishing licensing frameworks for copyright-protected educational resources ensures sustainable knowledge creation; on the other hand, implementing special control mechanisms guided by "purpose limitation" and "minimal use" principles for high-risk data processing (e.g., cognitive assessment and learning behavior profiling) prevents data abuse from eroding the dignity of educational entities.

2. The Legal Appeal of the Effect Evaluation Dimension

The credibility of educational effectiveness evaluation data directly impacts the legal recognition and public trust in distance education quality. Evidence-based education theory emphasizes that the scientific validity of assessment conclusions must be grounded in the legitimacy of data sources and verifiability of algorithmic processes. From a legal perspective, this manifests in two core requirements: First, the collection and processing

of assessment data must comply with the legal basis stipulated in Article 13 of the Personal Information Protection Law; otherwise, the assessment results will lose legal validity due to evidentiary flaws (Edge-Induced Cohesion Research Group, 2025). Second, the "black box" nature of algorithmic decision-making may raise concerns about educational equity. This necessitates fulfilling obligations such as algorithm registration and explanatory disclosure to ensure auditability throughout the assessment process.

The deeper rationale of compliance lies in the fact that effectiveness evaluation data essentially serves as legal evidence for educational quality. Traditional educational assessments rely on administrative endorsement, whereas AI-driven dynamic evaluations require establishing a mechanism that integrates technical credibility with legal validity. For instance, personalized learning recommendation algorithms containing socioeconomic bias would violate Article 9 of the Education Law, which mandates "ensuring educational equity." Therefore, compliance frameworks must translate algorithmic transparency principles into concrete technical specifications: embedding fairness constraints during model training and retaining decision traceability logs at output stages (Chen, 2024). This ensures evaluation results not only meet the controllability requirements stipulated in Article 12 of the Interim Measures for the Administration of Generative AI Services, but also serve as valid evidence in educational administrative actions or judicial rulings.

3. The Synergistic Mechanism of Dual-Wheel Drive

The compliance linkage between knowledge management and effectiveness evaluation essentially responds to the dual tension in the development of educational technology: it is necessary to release the knowledge innovation efficiency of data elements while preventing the risk of rights infringement in technology application. The synergy between the two aspects is reflected in three theoretical integrations:

3.1. Goal Synergy

Knowledge management seeks to realize the value transformation of educational data assets, while effectiveness evaluation focuses on empirical validation of educational quality. Data compliance creates a closed-loop mechanism within legal frameworks by standardizing data lifecycle processes: The high-quality data assets generated through knowledge management provide analytical foundations for effectiveness evaluation, whereas feedback from assessment results drives iterative optimization of knowledge management strategies.

3.2. Complementarity of Risk Prevention and Control

The knowledge management dimension focuses on preventing data asset loss and intellectual property infringement, while the effect evaluation dimension focuses on controlling algorithmic discrimination and misuse of results. Together, they cover the "process-result" risk spectrum of educational data application, forming an overlapping protection network in system design.

3.3. Integration of Governance Tools

The integration of blockchain technology within the dual-wheel framework serves as a prime example: On the knowledge management side, it establishes copyright ownership for educational resources and solidifies authorship rights for generative AI outputs through on-chain certification. On the effectiveness evaluation front, its immutable nature ensures the legal evidentiary validity of learning certificates and audit trails. This technological empowerment transforms compliance requirements from external oversight into intrinsic operational logic, aligning with the "design-driven compliance" philosophy.

In summary, the theoretical foundation of the dual-wheel drive framework lies in: taking the knowledge value transformation law of educational data as the warp and the legal credibility guarantee of assessment results as the weft. Through deep integration of institutional rules and technological tools, it constructs a new paradigm of data governance that balances educational innovation development with protection of stakeholders 'rights. This theoretical positioning not only avoids the instrumental rationality limitations of pure technical governance but also overcomes the traditional legal framework's neglect of the uniqueness of educational scenarios, providing solid academic support for subsequent institutional design.

IV. THE CONSTRUCTION PATH OF THE RULE OF LAW FRAMEWORK

In the application of AI in remote education, data compliance governance must transcend fragmented rule accumulation and establish a systematic legal framework centered on knowledge management optimization and credible outcome evaluation. This framework should be built upon the unique attributes of educational data and the risk characteristics of AI technologies. Through coordinated efforts in three dimensions—principle guidance, institutional design, and technical governance—it aims to achieve deep integration between data compliance and educational value.

EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:7 |July 2025

1. The Legal Foundation of the Core Principal System

The effectiveness of the legal framework is rooted in establishing core principles tailored to the education sector. The education-oriented principle mandates that data processing must strictly focus on enhancing educational quality, promoting personalized learning, and optimizing teaching management. Any commercialization of data deviating from educational essence or unnecessary monitoring constitutes a fundamental violation. This principle provides an enhanced interpretation of Article 6's "Purpose Limitation Principle" in the Personal Information Protection Law within educational contexts, setting clear boundaries for defining data collection scopes.

The implementation of tiered control principles addresses the "one-size-fits-all" governance challenges in educational data management. By evaluating data sensitivity and knowledge value, a refined classification framework can be established. High-sensitivity data with significant intellectual property rights and core educational value requires strict protection against non-educational sharing (NIST, 2023). High-sensitivity data with limited knowledge value should adhere to the minimum necessary principle for collection controls. Low-sensitivity data with substantial knowledge value enables resource sharing and knowledge innovation under secure conditions. Low-sensitivity data with minimal knowledge value may adopt more flexible management approaches. This classification model provides a scientific benchmark for establishing differentiated compliance obligations.

The dynamic informed consent principle represents an innovation over the traditional "one-time consent" mechanism. Given the long-term nature of educational activities and their evolving contexts, a tiered, updatable consent framework should be established: For basic teaching management data, a summary consent model with opt-out rights can be adopted; when handling sensitive data or modifying usage purposes, explicit reauthorization from teachers and students in specific scenarios must be obtained. The consent management platform should feature visual permission management and real-time revocation capabilities to ensure informed consent remains integral throughout the data lifecycle.

2. The Systematic Development of System Design

2.1. Subject Collaboration and Power and Responsibility Reconstruction

The allocation of rights and responsibilities among diverse stakeholders is crucial for institutional operations. As primary data controllers, educational institutions must assume comprehensive governance responsibilities: establishing internal compliance officer systems, conducting regular data protection impact assessments, and creating negative lists for supplier management. Technology providers must undergo "compliance through-the-pipe supervision," with their AI systems required to pass the Ministry of Education's algorithm filing review, have core code audited by third parties, and commit in service agreements to jointly bear liability for discriminatory outcomes caused by algorithmic flaws (Li & Wu, 2024). Regulatory authorities should spearhead the establishment of cross-institutional collaboration networks, issue model contracts for educational data sharing, and clarify confidentiality obligations and liability-sharing rules for all parties involved in data sharing.

2.2. Process Embedding of Whole Life Cycle Management

Data compliance must be deeply integrated into educational workflows. During data collection, institutions should establish a "Essential Educational Data List" aligned with knowledge management objectives. For instance, personalized learning systems may only collect interaction data directly related to cognitive assessments, while redundant collection of social connections or family background information is prohibited. In processing phases, two key regulations apply: 1) Metadata handling in knowledge graph construction must comply with the "Technical Specifications for De-identified Educational Resources" to ensure teachable logic remains reusable while personal identifiers remain unidentifiable; 2) All algorithmic applications require registration, with the Ministry of Education establishing an AI education algorithm registry that mandates submission of design documents, fairness testing reports, and contingency plans – particularly implementing copyright compliance reviews for generative AI's content generation capabilities. The evaluation phase focuses on creating legally recognized assessment evidence chains. Through blockchain certification technology, it solidifies the creation, transmission, and modification trails of student competency assessment data, ensuring traceable results with judicial admissibility.

2.3. Compliance Gate for Cross-Border Flows

For international education cloud platforms and cross-border MOOCs, it is essential to establish special rules that balance openness with security. Critical research outcomes listed in the Catalog of Important Knowledge Assets and core data from national-level quality courses should undergo localized storage and outbound security assessments. Technologically, a hybrid architecture combining "federated learning + trusted execution

EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:7 |July 2025

environment" should be implemented: Federated learning enables collaborative model training without transferring raw data, while Trusted Execution Environment technology ensures data destruction upon processing in encrypted environments, fundamentally preventing risks of data sovereignty erosion. Additionally, the Ministry of Education should lead the signing of bilateral agreements on cross-border education data flows, establishing reciprocal protection principles and dispute resolution mechanisms.

3. The Realization Path of Rule of Law Enabled by Technology

The effective implementation of legal regulations urgently requires the support of technical governance tools. By deeply integrating privacy-preserving technologies into knowledge management systems—such as applying differential privacy algorithms to add noise protection to student competency assessment datasets, and utilizing homomorphic encryption for collaborative annotation of teaching resources in encrypted states—these measures ensure knowledge preservation while preventing privacy breaches (PCPD, 2025). The evaluation algorithm must translate legal provisions into machine-executable parameters: quantifying "fairness" through threshold controls for resource distribution disparities among student groups, and embodying "transparency" by enabling automated generation of interpretable evaluation reports, thereby ensuring algorithmic decisions comply with Article 11 of the Interim Measures for the Administration of Generative AI Services.

Blockchain's judicial empowerment proves particularly effective in educational credential verification. The technology's dual mechanisms create robust safeguards: First, through asymmetric encryption and timestamping, it permanently records student credentials—including digital badges and micro-certificates—on the education consortium blockchain. Any tampering triggers node alerts, significantly enhancing the legal credibility of academic systems. Second, smart contracts automatically execute critical legal actions like data authorization approvals and consent revocations, with all transactions recorded on-chain. This provides regulators with irrefutable compliance audit evidence, dramatically reducing evidentiary burdens for educational institutions.

V. IMPLEMENTING SAFEGUARD MECHANISMS

In order to ensure the sustainable operation of the data compliance framework, it is necessary to build a multi-dimensional implementation guarantee system, and realize the substantive implementation of the rule of law path through the synergistic effect of innovative supervision mechanism, optimized responsibility allocation and closed-loop feedback of effect evaluation.

1. Innovation of Regulatory Mechanism

The current education data governance faces the challenge of fragmented regulation, urgently requiring the establishment of a unified professional regulatory system with clear responsibilities. It is recommended to set up an Education Data Compliance Office under the Ministry of Education's direct institutions to coordinate comprehensive supervision throughout the entire data lifecycle. This office should possess three core competencies: First, formulate detailed implementation rules for education data classification and grading, dynamically updating sensitive data identification standards in knowledge management scenarios; Second, establish a star-rating compliance evaluation system for educational technology products, authorizing independent third-party agencies to conduct annual compliance audits on AI education products, focusing on reviewing key indicators such as algorithm bias coefficients and privacy protection design, with assessment results serving as mandatory entry criteria for educational institutions' service procurement; Third, lead the formation of an interdisciplinary expert committee to issue judicial interpretative documents addressing emerging legal issues like cognitive assessment data and content ownership rights in generative AI outputs. For instance, we could adopt the "gatekeeper system" from the EU's Digital Services Act, requiring online education platforms with over one million users to fulfill systematic risk assessments and regularly submit transparent compliance reports.

2. Optimization of Responsibility Allocation

Collaborative governance among multiple stakeholders requires clear legal liability boundaries. At the technology provider level, implementing a "compliance-throughout supervision" mechanism is essential. When algorithmic flaws lead to data breaches or discriminatory outcomes, the principle of presumed fault should apply, holding providers primarily liable for compensation. Specifically, service agreements must mandate: providers must open algorithmic decision-making interfaces for regulatory audits. If model training data discrepancies trigger educational equity issues, this would be deemed failure to fulfill algorithmic security obligations under Article 12 of the Interim Measures for the Administration of Generative AI Services. For educational institutions, a tiered administrative penalty system applies: violations of data classification and grading controls receive tiered penalties based on intellectual property loss severity. While minor data breaches (e.g., device operation logs) may require corrective measures within deadlines, core teaching resource copyright data leaks would incur substantial fines (5%-10% of annual budget) with accountability for directly responsible parties. This framework not only

aligns with Article 66's penalty gradient principle from the Personal Information Protection Law but also addresses the unique protection needs of educational data assets.

3. Feedback Closed Loop of Effect Evaluation

The effectiveness of data compliance must be validated through the legal credibility of assessment outcomes, with the key being to establish a dynamic closed-loop mechanism of "evaluation-feedback-correction". Technologically, an education effectiveness evaluation and certification system based on blockchain is constructed: student competency assessment data and learning behavior analysis reports are hashed and recorded on the blockchain as critical evidence. Smart contracts are utilized to set access rules for evaluation data retrieval, ensuring traceability and tamper-proof integrity throughout the process. Institutionally, a dual-track feedback mechanism is established: educational authorities periodically extract blockchain-certified data for compliance verification, focusing on monitoring deviations between algorithmic decisions and manual evaluations; while simultaneously opening dispute appeal channels for teachers and students to request re-examination of certified results. Disputed cases generated during this process should serve as empirical foundations for optimizing compliance rules. When over 20% of personalized learning programs in a region receive appeals due to incomplete data collection, the revision procedure for the Minimum Necessary Scope List is triggered. Ultimately, through an annual Education Data Compliance White Paper, the actual impact of assessment results on teaching reforms is disclosed to society, forming an empirical closed-loop of "compliance empowering educational quality".

VI. SUMMARY AND OUTLOOK

This study addresses systemic data compliance challenges arising from AI-driven remote education by establishing a dual-driven legal framework of "knowledge management and effectiveness evaluation". It provides theoretical support and practical pathways to bridge the structural gap between technological innovation and institutional safeguards. The research profoundly reveals unique contradictions in educational data governance: while dynamic data such as learning behavior profiles and cognitive trait analyses carry highly sensitive personal rights, knowledge assets including teaching resource copyrights and AI-generated content embody core values of educational innovation. Traditional governance models, failing to account for the complex nature of educational contexts, exhibit significant blind spots in defining stakeholders' responsibilities, regulating data types, and addressing technical risks. To resolve these issues, this study integrates knowledge management theory with legal assessment principles to develop a systematic solution that combines educational adaptability with technological foresight.

In the theoretical framework, this study pioneers a dual-analysis model of educational data's "personality attributes and knowledge value," establishing three core principles: education-oriented governance, tiered control mechanisms, and dynamic informed consent. This theoretical breakthrough effectively resolves the binary opposition between technological governance and institutional constraints, embedding data compliance deeply into the intrinsic logic of educational value realization. At the institutional design level, it achieves coordinated governance through a four-dimensional classification control matrix, full lifecycle process standards, and cross-border data flow security gateways, ensuring institutional synergy in knowledge asset conversion and evaluation credibility. Crucially, the research transforms cutting-edge technologies like federated learning architectures, blockchain evidence storage, and privacy-enhanced computing into legal implementation tools. This internalizes compliance requirements as system operational logic, providing technical interfaces for precise enforcement of regulations such as the Interim Measures for the Management of Generative Artificial Intelligence Services in educational contexts.

The practical value of this study lies in providing actionable implementation guidelines for educational institutions and technology providers: The knowledge management system balances data security and knowledge sharing tensions through differentiated governance strategies; the effectiveness evaluation mechanism, relying on algorithm registration and blockchain verification mechanisms, grants judicial credibility to dynamic and personalized learning assessments; cross-border education collaboration achieves organic integration of data sovereignty protection and international resource interoperability under the "federated learning + trusted execution environment" framework. Regulatory innovation mechanisms such as the functional design of the Education Data Compliance Office, penetrating accountability rules, and star-rating evaluation systems further ensure the sustainable operation of the governance framework at the implementation level.

Future research must address several evolutionary challenges. First, as immersive technologies like educational metaverse evolve, the boundaries between learning environments and the real world are increasingly blurred. The legal attributes of emerging sensitive data such as biometric information and neurofeedback require clarification, necessitating the integration of neuroethics into existing tiered regulatory frameworks. Second, as generative AI

transitions from an auxiliary tool to co-creators of educational content, establishing intellectual property rights for generated course materials and assessment reports demands breaking free from the "human-centric creation" path dependency in Copyright Law. This requires creating a shared copyright system combining human guidance with AI-generated content. Finally, under the restructuring of global digital education governance, safeguarding educational data sovereignty must transcend geographical boundaries. Exploring new trust frameworks for cross-border data flows based on distributed digital identities will enable China to shift from adaptive compliance to innovative leadership in international rule-making. These explorations will propel educational data governance from risk prevention to value creation, laying a solid legal foundation for the digital transformation of human educational civilization.

REFERENCES

1. *Chen, J. (2024). Interim Measures for the Management of Generative AI Services: Analysis of AIGC Data Compliance Challenges and Solutions [in Chinese]. Zhong Lun Law Firm.*
2. *Data Governance Team. (2025). How We Built Robust Data Governance at Scale. Databricks Community.*
3. *Edge-Induced Cohesion Research Group. (2025). White Paper: Implementing Filters in AI Systems for Boundary Setting in Training Data and First-Order Logic within Nations and Institutions.*
4. *European Commission. (2024). Ethical Guidelines for Trustworthy AI in Education. Directorate-General for Education, Youth, Sport and Culture.*
5. *Li, J., & Wu, Q. (2024). Curriculum Reform Driven by AIGC: Value Reflection and Implementation Pathways [in Chinese]. Journal of Higher Education, *45*(3), 45–52.*
6. *National Institute of Standards and Technology (NIST). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST Special Publication. https://doi.org/10.6028/NIST.AI.100-1*
7. *Office of the Privacy Commissioner for Personal Data (PCPD). (2025). Hong Kong Privacy Commissioner for Personal Data Completes Compliance Checks on the Use of AI and Data Privacy. PCPD Compliance Report.*
8. *Vorecol. (2025). The Role of Data Privacy and Compliance in LMS Selection: Navigating Regulations. Vorecol E-Learning Blog.*
9. *Zhongnan University Law School. (2025). Empowering Graduate Education with Generative AI: Theoretical Logic, Legal Risks, and Governance Pathways [in Chinese]. Graduate Education Research, (2), 26–33.*
10. *Zou, L. (2025). Ethical Risks and Governance Framework of Generative AI in Intelligent Recommendation of Personalized Learning Resources. Advances in Education, *15*(7), 543–551 https://doi.org/10.12677/ae.2025.1571251*