The Risk Regulation Path of AI Agents in Foreign-Related Legal Education

Lijing Wu*, **Zejun Kan**
School of Humanities and Law, North China University of Technology, Beijing, China
**Corresponding Author*

Abstract: With the in-depth application of artificial intelligence technology in foreign-related legal education, AI agents have significantly enhanced educational efficiency through functions such as cross-legal system knowledge integration, multilingual legal analysis, and scenario-based teaching simulation, but they have also raised complex challenges such as data sovereignty conflicts, algorithmic biases, and legal application risks. This study systematically dissects three core risks: cross-border data transmission is likely to trigger compliance conflicts between GDPR and domestic law, value embedding in training data may lead to legal cognitive bias, and decoupling of the physical and digital Spaces causes the "triple compliance dilemma". To address these risks, a hierarchical regulatory approach is proposed: using federated learning and blockchain to build a cross-border data regulatory chain at the technical level, and developing a cultural sensitivity algorithm module; At the institutional level, establish an international algorithm audit mutual recognition mechanism and improve the dynamic informed consent and multi-level accountability system; At the level of international collaboration, we will promote the digital revision of the Cross-border Education Services Agreement and establish a cross-border AI dispute arbitration platform. Research shows that a dynamic closed-loop mechanism of "risk prevention - process control - damage relief" is needed to balance technological empowerment and legal value rationality, providing theoretical support for building a transnational regulatory framework that takes into account both sovereign security and educational effectiveness.

Keywords: Foreign-Related Legal Education; AI Agents; Algorithm Transparency; Transnational Legal Collaboration

1. Introduction

With the deepening of globalization, foreign-related legal education has become an important support for cultivating internationalized legal talents and dealing with transnational legal disputes. The rapid development of artificial intelligence technology has promoted the widespread application of AI agents in foreign-related legal education. Through functions such as simulating foreign-related legal scenarios, providing multilingual interaction support, and generating customized teaching cases, it has significantly improved educational efficiency and resource accessibility. However, the risks of algorithmic bias, ethical misconduct, and sovereign conflict that AI agents face in cross-border data flow, cultural value transmission, and the application of legal interpretation may give rise to problems such as legal cognitive bias, cultural misinterpretation, and alienation of educational goals.

By deconstructing the interaction mechanism between the logic of AI technology and the laws of rule of law education, this study explores the path of risk regulation, which can provide decision-making basis for improving the technical application standards and cross-border collaboration mechanisms of foreign-related rule of law education.

2. The Application Status of AI Agents in Foreign-Related Legal Education

2.1 The Main Functions of AI Agents in Foreign-Related Legal Education

In the field of foreign-related legal education, AI agents have many functions. On the one hand, it can use natural language processing technology to achieve efficient integration and

precise delivery of cross-legal system knowledge, such as generating comparative analysis reports for the teaching of commercial dispute resolution mechanisms in countries along the Belt and Road. On the other hand, its intelligent interactive system uses virtual reality technology to simulate scenarios such as international commercial arbitration tribunals, and uses role-playing and real-time feedback mechanisms to help learners master skills such as writing international legal documents.

The intelligent parsing function of multilingual legal texts can be based on the machine translation system of the legal terminology database to contextualize foreign legal documents and mark differences, improving the efficiency of professional language training such as legal English. The data-driven learning assessment system can collect learners' data and generate personalized ability assessment models, providing a quantitative basis for teachers to adjust teaching strategies [1].

These functions form the technical foundation for the digital transformation of foreign-related rule of law education, but when applied, it is necessary to pay attention to the deep integration with educational laws and ensure the irreplaceability of core values such as humanistic literacy and critical thinking in foreign-related rule of law education while improving teaching efficiency.

2.2 Potential Risks of AI Agent Application

In the field of foreign-related legal education, although the introduction of AI agents can enhance teaching efficiency and the breadth of knowledge dissemination, the combination of its technical characteristics and the particularity of educational scenarios may give rise to multiple risks. First, when AI agents handle foreign-related legal cases, they may trigger data sovereignty disputes in different jurisdictions due to the cross-border flow of data. For example, compliance conflicts involving the EU's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law could put educational platforms under double regulatory pressure without clear data jurisdiction. Secondly, algorithmic black box problems may lead to the unexplainability of legal knowledge output. When AI agents provide learners with content involving the interpretation of international treaties or comparative law analysis, the concealment of their reasoning paths may weaken the verifiable nature of legal arguments, especially in teaching scenarios where common law and civil law systems intersect, cognitive biases are likely to occur. In addition, the real-time and dynamic nature of AI-generated content may increase the risk of legal information lag, especially in rapidly evolving areas such as international trade rules and cyberspace governance involved in foreign-related legal education, where the timeliness gap of algorithm model training data may lead to substantial errors in knowledge transfer. A more covert risk is that AI agents may form implicit value guidance through semantic analysis and knowledge recommendation systems [2]. For example, when teaching international human rights law or investment dispute settlement mechanisms, algorithmic bias may cause the output content to deviate from the legal education goals of a specific country. These risks are becoming more complex in specific application scenarios such as transnational cooperative education and remote legal training, and there is an urgent need to establish a risk identification framework that is compatible with the laws of foreign-related legal education.

3. Risk Types of AI Agents in Foreign-Related Legal Education

3.1 Data Security and Privacy Leakage Risks

The application of AI agents in foreign-related legal education faces significant security risks. In the context of cross-border education, AI systems face three threats when handling sensitive data: technical vulnerabilities leading to unauthorized access, process flaws causing over-collection, and international transmission resulting in compliance conflicts due to differences in privacy standards. In the context of the connection between the GDPR and China's Personal Information Protection Law, platforms need to meet multiple requirements when collecting data from European students, which can easily lead to compliance difficulties. In 2022, a platform exposed the

vulnerability of its technical protection system due to the lack of a cross-border compliance mechanism for data, resulting in the leakage of student information [3].

From a technical regulatory perspective, blockchain's distributed storage architecture and federated learning technology can reduce the risk. In terms of legal coordination, international data classification standards need to be established, with clear processing rules, drawing on the certification systems of Singapore and Switzerland. Educational institutions should establish dynamic risk assessment models and regularly check the security of data interfaces. The Harvard Law School project has demonstrated that the preventive compliance model can effectively reduce the risk of privacy leakage, providing a prevention and control model for the application of AI in foreign-related legal education.

3.2 Risk of Algorithmic Bias and Decision Injustice

The problem of algorithmic bias in AI agents in foreign-related legal education is complex because the training data often comes from judicial precedents in specific countries or regions, and cases such as handling cultural differences are prone to embedding value judgments in the data source country. This algorithmic bias may cause double decision imbalance in the field of foreign-related legal education, affecting learners' construction of legal thinking, evaluation of legal literacy, etc. For the scenario of transnational legal education, risk regulation needs to build a three-layer defense mechanism: establish dynamic cultural embedding algorithms at the technical level, promote mutual recognition of international algorithm auditing standards at the institutional level, and embed bias recognition training modules at the educational application level. In practice, the "Algorithmic Transparency Passport" system and the Agreement on Mutual Recognition of AI in Education in the Asia-Pacific region have exemplary value and can provide effective risk regulation paths for the application of AI in cross-border legal education [4].

3.3 Risk of Legal Application and Jurisdictional Conflict

The cross-border application of AI agents in foreign-related legal education presents a complex risk of legal application and jurisdiction issues. When online education platforms provide cross-country legal case analyses, it is easy to trigger regulations in multiple countries, creating a "triple compliance dilemma". Jurisdictional conflicts arise from the decoupling of the physical and digital Spaces, such as the 2023 European Court of Justice case of AI Counsel, which made traditional principles difficult to apply due to the discretization of elements. The existing international law framework lags behind, the Hague Convention on Jurisdiction does not cover AI services, the UNCITRAL draft does not address AI liability determination, and the "code as law" phenomenon has emerged, giving rise to new types of conflicts.

The path to risk regulation needs to be broken through in three dimensions: promoting the digital revision of the Cross-border Education Services Agreement in substantive law to clarify the obligations of AI education service providers; Establish a complex connection point system in the conflict law area; In procedural law, draw on the Singapore Convention on Mediation to establish an online arbitration platform for cross-border AI disputes.

4. The Theoretical Basis for Risk Regulation of AI Agents

4.1 Basic Theoretical Framework for Risk Regulation

The introduction of AI agents in the field of foreign-related legal education has both technological empowerment advantages and complex risk challenges. The risk regulation theory emphasizes preventive management of potential hazards from the application of technology through systematic mechanisms, and its framework construction needs to be based on three dimensions: First, the risk identification dimension needs to focus on the algorithmic bias risk of AI agents in cross-border legal knowledge dissemination, the privacy leakage risk in cross-border data flow, and the transparency risk of intelligent decision support systems [5]. Second, the regulatory path dimension should establish a dynamic closed loop of "risk prevention - process control - damage relief", establish the

technical verification obligations of educational subjects through the algorithm filing system, build a cross-border teaching data supervision chain based on blockchain, and improve the AI ethical review mechanism for foreign-related legal education scenarios. Third, the collaborative governance dimension requires breaking through the regulatory boundaries of a single sovereign state, promoting mutual recognition of AI education application standards through international organizations, establishing a negative list system for cross-border AI education services, and forming a risk co-governance pattern with the participation of multiple entities. This theoretical framework particularly emphasizes the coupling analysis of technical characteristics and legal attributes. In the context of foreign-related legal education, it is necessary to focus on dealing with complex risk elements such as sovereign jurisdiction conflicts, cultural value differences, and technical ethics violations, laying the theoretical foundation for the subsequent construction of a risk regulation system with international adaptability [6].

4.2 Special Requirements for Foreign-Related Legal Education

The implementation field of foreign-related legal education spans the boundaries of a single legal domain, and its core lies in cultivating compound talents with international legal literacy and cross-cultural communication skills. The peculiarity of this educational model is first reflected in the complexity of the knowledge structure, which requires covering both the basic framework of the domestic legal system and the deep integration of international treaties, foreign legal systems and regional legal coordination mechanisms. Taking international trade law education as an example, the AI-assisted teaching system not only needs to accurately analyze the WTO rule system, but also needs to dynamically track the evolution of new regional agreements such as CPTPP and USMCA, which poses a significant challenge to the update frequency of the AI legal knowledge base and the ability to handle multi-source heterogeneous data. The multicultural background of the educational subjects constitutes the second particularity. When AI agents participate in cross-border legal training, they need to deal with the cognitive differences in thinking patterns of different legal systems. For example, there is an essential difference in the logical path of legal reasoning between learners of the civil law system and the common law system. If teaching cases generated by AI fail to effectively balance codified interpretation with the characteristics of case law, it may lead to legal cognitive bias [7]. This requires algorithms to be designed with cultural sensitivity assessment modules to detect cultural fit in teaching output in real time through natural language processing technology.

In terms of technical ethics, the flow of data in foreign-related legal education scenarios involves multiple sovereign jurisdictions. When AI systems collect and process cross-border learning behavior data, they need to comply with the data localization requirements of the EU GDPR and also take into account the compliance standards of China's Personal Information Protection Law. The reconciliation of such legal conflicts requires the establishment of a dynamic risk assessment mechanism and the automatic adaptation of data rules in different jurisdictions through smart contracts based on blockchain technology to ensure a balance between personal privacy protection and knowledge dissemination efficiency in the teaching process [8].

The interpretability dilemma brought about by the technology black box is particularly prominent in this area. When AI agents simulate international commercial arbitration cases, algorithmic decision-making processes must meet the differentiated requirements for judicial transparency in different jurisdictions. Developing deep learning models with multi-level interpretation capabilities and establishing a visualization system of reasoning paths that conforms to the New York Convention's criteria for recognizing rulings have become key breakthroughs in avoiding technical legal risks.

4.3 Coordination Mechanism Between International Law and Domestic Law

With the global application of artificial intelligence technology, the field of foreign-related legal education faces new legal risks such as cross-border data flows by AI agents

and algorithmic discrimination. The international community has established basic principles through framework documents such as the "Recommendations on AI Ethics", but the implementation of specific rules will rely on the transformation of national legislation. The EU's AI Act creates a three-level risk classification system, requiring member states to establish algorithmic impact assessment mechanisms; The United States promotes industry self-discipline and state legislation coordination through the Blueprint of the Bill of Rights on Artificial Intelligence. This "soft law first, hard law following" model reveals a two-way path for international norms to penetrate into domestic law.

When China's Interim Measures for the Administration of Generative Artificial Intelligence Services introduced the algorithm filing system, it absorbed the transparency requirements of UNESCO's Recommendation on Ethical Issues in Artificial Intelligence and added domestic server storage provisions in line with the principle of data sovereignty. This selective conversion mechanism faces legal application conflicts in practice, such as the difficulty in determining product liability caused by cross-border testing of self-driving cars, which involves both the obligations of the contracting states of the Vienna Convention on Road Traffic and the need to coordinate domestic tort liability laws with industry technical standards.

To establish a dynamic coordination mechanism, a three-tier framework needs to be constructed: participating in the development of ISO/IEC artificial intelligence standards at the international level and promoting the formation of an interwoven model of technical rules and legal norms; At the regional level, establish a mutual recognition mechanism for algorithm review based on the RCEP's digital economy chapter; At the domestic level, improve the joint training system for foreign-related legal talents to enable legal practitioners to master international treaty interpretation methods and cross-border electronic forensics skills. The AI Rule of Law Joint Research Center, established in collaboration between the Law School of Tsinghua University and the National University of Singapore, has initiated the construction of a cross-border facial recognition data compliance case library to provide empirical support for the operation of the coordination mechanism [9].

5. Risk Regulation Pathways for AI Agents In Foreign-Related Legal Education

5.1 Improve the Data Security and Privacy Protection System

The application of AI agents in foreign-related legal education faces challenges in data security and privacy protection. In foreign-related scenarios, cross-border data transmission can easily lead to legal conflicts and ethical risks. If cross-border data flows are controversial due to differences in privacy standards, the improper use of personalized data can violate privacy rights and trigger international disputes [10]. To address these issues, a hierarchical governance framework is needed: establish a classification and grading system for foreign data, clarify the scope and sensitivity level of data accessible to AI agents, and set local storage rules and encryption transmission standards for core data; Strengthen the risk assessment mechanism for cross-border data flows, requiring operators to pre-assess the privacy protection level of the data receiving country and form technical specifications; Design dynamic informed consent mechanisms, use multilingual, interactive authorization interfaces, and introduce privacy-enhancing technologies such as embedding differential privacy modules to reduce risks. At the same time, we should promote international collaborative governance, establish data security committees, cultivate foreign-related legal talents with data security literacy, and form a risk prevention path that combines technical governance with legal regulation.

5.2 Establish Algorithmic Transparency and Accountability Mechanisms

Under the background of globalization, the deep integration of foreign-related legal education and artificial intelligence technology has given rise to new forms of education. However, when AI agents are embedded in legal education scenarios, there are risks such as algorithm black boxes and untraceable decisions. With the EU's Artificial Intelligence Act as a reference, building an interpretable algorithm framework has become the key to resolving compliance conflicts in cross-border

data flows. Educational institutions need to use technical means such as open API interfaces and traceable decision logs to enable the AI legal reasoning process to meet the differentiated transparency requirements of different jurisdictions.

A multi-level accountability system should be established for possible legal application errors caused by agents in foreign-related education scenarios. Developers should conduct algorithmic impact assessments in accordance with ISO/IEC 23894 standards, and educational entities should establish interdisciplinary ethics committees to conduct dynamic reviews of international law case analyses output by agents. In the event of algorithmic discrimination involving students from multiple countries, the Hague Conference on Private International Law mechanism can be used to define the cross-border legal liability of algorithmic service providers through preset jurisdiction provisions.

It is worth noting that algorithmic transparency should not be limited to the level of technical disclosure. The experience of Singapore's Legal Technology sandbox shows that transforming machine learning models into visual legal knowledge graphs can enable foreign legal learners to master the reasoning logic of agents simultaneously. This dual guarantee of "technical transparency" and "cognitive transparency" not only meets the requirements of the Vienna Convention on the Law of Treaties for the certainty of legal interpretation, but also effectively prevents normative conflicts arising from AI in comparative law teaching.

5.3 Build a Framework for Transnational Legal Collaboration

In foreign-related legal education, AI agents face transnational legal challenges such as data sovereignty conflicts and algorithmic ethical differences. The traditional domestic law governance model is limited and requires multi-level international collaboration to achieve regulation.

The predicaments of cross-border legal collaboration include differences in AI regulatory standards among countries, disputes over jurisdiction over cross-border services, and the difficulty in tracing the causal relationship of infringement caused by AI decision-making black boxes. Building a framework for cross-border legal collaboration requires multi-dimensional mechanism innovation: first, establish a rule consultation platform led by international organizations, formulate ethical guidelines, and promote regulatory consensus; Second, promote the construction of regional legal coordination mechanisms and pilot the system of mutual recognition of certifications; Third, improve the transnational judicial cooperation network and establish a cross-border dispute resolution platform; Fourth, create a dynamic risk warning mechanism to monitor changes in the legal environment in real time.

The implementation of this framework requires institutional guarantees: First, establish an international AI rule of law education fund to cultivate versatile talents; Second, the International Organization for Standardization will develop safety certification standards for AI systems in education. Third, establish an AI education governance alliance to enhance collaboration efficiency. In addition, when introducing AI agents, it is necessary to build a cross-language interpretability framework, clarify the attribution of responsible entities, and establish a multi-level accountability system. In terms of international collaboration mechanisms, mutual recognition agreements could be established based on the Hague Conference on Private International Law, an algorithm source code evidence platform could be developed, transnational ethics committees could be set up, and regular audits could be conducted.

6. Conclusions

With the deep integration of globalization and artificial intelligence technology, the application of AI agents in the field of foreign-related legal education has brought about innovations in educational models, as well as complex risks such as ambiguous primary responsibility, algorithmic ethical misconduct, and cross-border data conflicts. Through a three-dimensional analytical framework of technology, law and ethics, this study reveals that the risks of AI agents in foreign-related legal education are essentially the externalization of the tension between technological instrumental rationality and legal value rationality. By constructing a dynamic regulatory system of "risk identification - assessment - response", it is proposed to

achieve traceability of the educational process through algorithmic transparency, clarify the boundaries of multiple subjects' responsibilities through a list of rights and obligations, and balance knowledge sharing and sovereign security through hierarchical management of cross-border data, providing a feasible path for risk governance.

Acknowledgments

This paper is supported by the Ministry of Education's Industry-University-Research Collaborative Education Project "Interdisciplinary Course Design and Teaching Practice of Artificial Intelligence + Foreign-related Rule of Law" (Project No. 2504220712), and supported by the 2025 North China University of Technology's Undergraduate Education and Teaching Reform Research Project "Innovative and Practical Research on the Working Mode of University Graduation Theses Assisted by Agents".

References

[1] Alexandre, F. M. The legal status of artificially intelligent robots Tilburg: Tilburg University, 2017.

[2] Sankari, S., Koulu, R., Hirvonen, H., & Heikkinen, T. S. Artificial intelligence and the law: can we and should we regulate AI systems, In B. Brożek, O. Kanevskaia, & P. Pałka (Eds.), Research Handbook on Law and Technology, 2023.

[3] Zhong M. Construction of an Oral Practice Model for Students Based on AI Intelligent Characters in English Textbooks Teaching and Management, 2025, (11):55-58.

[4] Wang D Q, Chen Z L, Shao Wenhao, et al. From "De-energizing" to "Empowering": Design of Thought Chain Prompting Based on LLMs and Construction of Teaching and Research AI Agents - Taking Intelligent Analysis of Classroom Teaching as an Example Chinese Educational Technology, 2025, (03):111-117 + 125.

[5] Akpobome, O. The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation International Journal of Research Publication, 2024, 5(7):5046-5060.

[6] Georgios I. Z. Economics and Law of Artificial Intelligence: Finance, Economic Impacts, Risk Management and Governance Springer International Publishing, 2021

[7] Kryvytskyi, Y. Artificial Intelligence as a Tool of Legal Reform: Potential, Trends and Prospects Scientific Journal of the National Academy of Internal Affairs, 2021(2):90-101.

[8] Jaemin L. Artificial Intelligence and International LawSpringer Singapore, 2022.

[9] Kostenko, O. M., Bieliakov, K. I., Tykhomyrov, O. O. et al. “Legal personality” of artificial intelligence: methodological problems of scientific reasoning by Ukrainian and EU experts AI & Soc, 2024(39):1683-1693.

[10] Wischmeyer, T., & Rademacher, T. Regulating Artificial Intelligence Springer International Publishing, 2020.

