International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

Research on Optimization of University Governance Path Based on Campus Big Data Platform

[1]Feng Jianzhu, [2]Xiaoxiao

[1]Department of Training Affairs, Nanjing Sport Institute, Nanjing, Jiangsu, China

[2](Corresponding Author) Schools of Marxism, Nanjing University of Finance and Economics, Nanjing, Jiangsu, China

---

Abstract: *Against the strategic backdrop of the deepening digital transformation of education, campus big data platforms have evolved into core infrastructure advancing the modernization of university governance. Centering its research on the interactive construction relationship between campus big data platforms and university governance, this paper adopts polycentric governance theory, data lifecycle management theory and risk society theory to systematically establish a four-dimensional analytical framework covering current situation diagnosis, risk analysis, strategy optimization and path reconstruction. The research finds that the existing practices of big data governance in universities have achieved phased progress in fields including data integration, intelligent decision-making and targeted services. Nevertheless, they are confronted with multiple structural risks such as data privacy and security threats, algorithmic bias, unbalanced power arising from digital surveillance, ideological security hazards and fragmented governance. Accordingly, this study puts forward systematic coping mechanisms from the technological, institutional and policy dimensions: technologically, strengthen differential privacy protection, block chain encryption and the interpretable design of artificial intelligence; institutionally, build a multi-stakeholder collaborative governance framework and a data ethics review mechanism; and policy-wise, promote in-depth alignment with national digitalization strategies.*

Keywords: Campus Big Data Platform; University Governance; Application of Digital Technology; Risks and Challenges; Path Optimization

I. INTRODUCTION

The wave of digital transformation is profoundly reshaping the organizational form and governance logic of higher education. With the large-scale application of cloud computing, the Internet of Things, artificial intelligence and other technologies, the campus big data platform has evolved from a peripheral issue of information construction into a core supporting system for the modernization of university governance. Theoretically defined, a campus big data platform refers to an integrated digital infrastructure developed by institutions of higher education that relies on diversified digital technologies to realize the unified collection, storage, governance, analysis and application of various heterogeneous campus data resources. Its core features correspond to the five Vs of big data: Volume, Velocity, Variety, Veracity and Value. Compared with conventional information systems, the essential advancement of such platforms lies in the shift from data storage to data-driven operation and from passive record-keeping to proactive empowerment. In the contemporary context, university governance denotes the institutional arrangement whereby universities, within the framework of national educational laws and regulations, effectively integrate educational objectives, resource allocation and organizational order through multi-stakeholder participation, rational division of powers and responsibilities, and scientific decision-making. Fundamentally different from traditional bureaucratic administration, it institutionally highlights democracy, transparency and polycentric coordination. Ostrom's polycentric governance theory furnishes vital theoretical underpinnings, arguing that effective governance of public affairs requires breaking the monopoly of a single

authoritative center and establishing a multi-level, multi-agent network for interaction and negotiation. The integrated paradigm of university governance based on campus big data platforms takes data as a core production factor and intelligent technologies as empowering instruments. It transforms governance decision-making from experience-driven to evidence based, and from one-way administrative control to interactive collaborative governance. This paradigm is also theoretically underpinned by data lifecycle management theory and Beck's Risk Society Theory.

II. Analysis of the Current Situation of University Governance Based on Campus Big Data Platforms

The practices of empowering university governance via campus big data platforms have yielded systematic achievements across multiple dimensions. From five perspectives including data collection and integration, AI predictive analysis, IoT perception, secure data sharing based on block chain, and generative AI application, this section systematically sorts out the phased progress and major constraints of current big-data-driven university governance, so as to lay an empirical foundation for subsequent risk assessment and research.

1. Data Collection and Integration: Digital Restructuring of Governance Foundation

The governance efficiency of campus big data platforms is rooted in the systematic improvement of data collection and integration capabilities. At present, the scope of data collection in universities has expanded beyond traditional administrative management systems to a diversified composite system covering campus IoT sensor terminals, behavioral data from mobile applications, interaction logs from learning management systems, and associated information from social media. The hybrid storage architecture combining data warehouses and data lakes has effectively addressed the long-standing dilemma of "data silos" across heterogeneous systems and enabled data integration across different business domains. Nevertheless, this foundational construction process is still restricted by multiple structural obstacles. In terms of data standards, inconsistent formats and semantic discrepancies among various business systems hinder the formulation of unified norms. From the perspective of data ownership, the ownership and usage authority of teachers' and students' personal information remain ambiguous, with relevant institutional definitions falling far behind technological practice. In respect of data governance, full-lifecycle management mechanisms such as metadata management, data lineage tracking and data quality monitoring have not been fully established in most universities, limiting the in-depth exploitation of the value embedded in data assets.

2. AI-Driven Predictive Analysis: Empowerment and Boundaries of Intelligent Decision-Making

The in-depth embedding of artificial intelligence technology has brought about a fundamental shift in the decision-making paradigm of university governance. In the fields of academic early warning and teaching quality management, modeling and analysis of multi-dimensional learning behavioral data have enabled the construction of an early risk identification system, furnishing empirical evidence for targeted teaching interventions. With regard to the allocation of research resources, performance evaluation models and talent recruitment prediction tools facilitate the optimized strategic deployment of limited academic resources. In student affairs administration, mental health prediction models and graduate employment analysis systems deliver technical support for personalized and precise student services. Practically, AI-enabled governance drastically improves the efficiency and accuracy of decision-making and facilitates an initial paradigm shift from post-incident cause tracing to pre-event risk assessment. Nonetheless, clear constraints persist. The black-box nature of algorithmic decisions undermines the institutional value of governance transparency; historical biases embedded in training data tend to entrench or even exacerbate pre-existing inequities, diverting AI-driven governance away from the core values of fairness and justice.

3. IoT and Smart Campus: Spatial Extension of Perceptive Governance

The large-scale deployment of IoT technology has expanded the spatial perception capacity of campus governance. Scenarios including intelligent access control, energy monitoring, classroom environmental sensing and vehicle

administration lay the perceptual foundation for the digital twin campus, enabling real-time mapping between physical campuses and digital spaces. In terms of resource management, intelligent scheduling systems built upon sensor data deliver prominent efficiency gains in energy consumption, space utilization and facility maintenance. Nevertheless, ubiquitous sensing infrastructure generates massive highly sensitive data concerning the behavioral trajectories of faculty and students, giving rise to unavoidable ethical controversies over digital surveillance and mounting pressure on privacy protection. The structural tension between the coverage density of sensing networks and individual privacy rights stands as one of the most prominent ethical dilemmas in current smart campus governance practices.

4. Block chain and Secure Data Sharing: Technological Construction of Trust Mechanism

Thanks to its features of decentralization, immutability and automatic execution of smart contracts, block chain technology boasts important application value in the secure sharing of university data. In the fields of academic credential verification and confirmation of ownership for academic achievements, the distributed ledger mechanism can effectively curb information forgery and academic misconduct. For cross-institutional data sharing, blockchain-based data exchange protocols enable the orderly circulation of research collaboration data while safeguarding relevant data rights and interests. Currently, its large-scale popularization and application are restricted by high computational overhead, scalability limitations, as well as the complexity of integration with existing university IT infrastructure.

5. Generative AI Empowerment: Frontier Exploration of Intelligent Governance

Represented by large language models, generative AI technologies are emerging as a cutting-edge driving force for the intelligentization of university governance. In practical application, intelligent government assistants and natural language interaction systems lower the information access barriers for teachers and students to obtain governance services; automated report generation and policy text analysis tools improve administrative efficiency; personalized teaching recommendation systems pioneer new approaches for targeted educational services. Meanwhile, structural challenges calling for urgent attention remain in the application of generative AI within university governance, including unreliable information stemming from AI hallucinations, threats to academic integrity posed by deepfakes, and the systematic amplification of value biases embedded in training datasets.

III. Risks and Challenges of University Governance Based on Campus Big Data Platforms

The in-depth advancement of technology-enabled governance and the relative lag in institutional development have jointly spawned multiple structural risks in university big data governance. From the analytical perspective of risk society theory, this section systematically analyzes the mechanisms and root causes of core risks facing current university big data governance across six dimensions: data privacy and security, algorithmic bias, digital surveillance, academic integrity, ideological security and fragmented governance.

1. Data Privacy and Security Risks: Systematic Threats to Information Rights

According to Beck's Risk Society Theory, the widespread proliferation of modern technologies is accompanied by the large-scale generation of risks, whose distribution logic is strongly coupled with the structure of social inequality. This proposition is fully corroborated in the context of campus big data. Personal information of faculty and students covers highly sensitive privacy domains including behavioral trajectories, academic transcripts, physical health status and social connections. Risks of data leakage stem from multiple sources. From a technical perspective, system vulnerabilities, flawed interface security and unauthorized access by internal staff constitute major exposure points. Institutionally, the absence of effective informed consent mechanisms and an ambiguous definition of data usage purposes give rise to excessive data collection and improper exploitation. Legally, there remains an institutional gap between the compliance requirements for sensitive personal data stipulated in the Personal Information Protection Law and the actual data management practices of universities. A more profound concern lies in privacy erosion triggered by data aggregation. While standalone datasets appear innocuous in isolation, cross-correlation analysis of multi-source heterogeneous data enables the construction of

highly granular personal profiles, triggering privacy risks far exceeding the sensitivity of the original raw data, a hazard frequently overlooked under conventional privacy protection frameworks.

2. Algorithmic Bias and Conflicts over Fairness: The Institutional Illusion of Technological Neutrality

The objectivity and neutrality of algorithms are theoretically regarded as the fundamental merits of big data governance over human-based decision-making, yet such an assumption faces severe challenges in practical application. Algorithmic bias originates from three core links: biased historical data perpetuates pre-existing social inequities within training datasets; biased feature selection introduces discriminatory dimensions indirectly via proxy variables; and biased optimization objectives embed specific value preferences into the design of evaluation indicators. Within university governance, typical manifestations of unfair algorithmic outcomes include systematic erroneous risk labeling of students from specific family or ethnic backgrounds by academic early-warning systems, as well as structural exclusion of historically disadvantaged groups in intelligent scholarship and grant allocation models. A unique hazard of algorithmic bias in higher education governance is that algorithms gain institutional legitimacy under the guise of "technical authority", making it harder for affected individuals to identify unfair treatment or obtain remedies through conventional channels, thereby magnifying inequities concealed behind technological rationality. The EU's Artificial Intelligence Act explicitly categorizes AI systems deployed in education as high-risk applications, legally affirming the particular sensitivity of algorithm governance in educational contexts.

3. Digital Surveillance and Power Imbalance: The Structural Compression of Autonomy Space

Foucault's panopticon metaphor illuminates the disciplinary effect of the surveillant gaze on subjects' behaviors. Within digitally transformed universities, the coordinated operation of ubiquitous sensing devices and behavioral data analytics systems has established a highly refined digital surveillance framework that continuously tracks the behavioral footprints of faculty and students across physical and digital spheres. The core risk of such an architecture lies not merely in the inherent sensitivity of collected data, but in the preemptive behavioral modification triggered by the "perception of being watched". Under persistent surveillance, teachers and students may incline toward self-censorship, which in turn shrinks the room for academic freedom, critical expression and innovative thinking. Power imbalance manifests concretely in two respects. First, administrative authorities monopolize data control rights, while faculty and students are denied effective participation in defining data collection purposes, specifying usage scopes and exercising data deletion rights. Second, the pervasive infiltration of algorithmic evaluation logics into student assessment and faculty appraisal systematically erodes the traditional space of academic autonomy, creating a fundamental tension against the principle of equal multi-stakeholder participation advocated by polycentric governance theory.

4. Hidden Dangers of Intellectual Property Rights and Academic Integrity: The Institutional Impacts of Generative AI

The in-depth integration of generative AI technology has exerted unprecedented institutional impacts on the academic ecosystem of higher education institutions. From the perspective of intellectual property rights, existing legal frameworks fail to clarify copyright ownership of AI-assisted outputs, leaving universities caught in an institutional vacuum between AI-enabled research practices and intellectual property protection. In terms of academic integrity, systematic challenges to integrity governance arise from ambiguous demarcation of permissible AI-aided writing, technical limitations in detecting AI-generated content, and the absence of evaluative benchmarks for the emerging human-AI collaborative research paradigm. A more profound hidden risk consists in the strategic leakage of core intellectual assets: high-quality university research datasets used as training materials for AI models may flow to commercial platforms, which could fundamentally undermine the competitive edge of universities as primary knowledge producers.

5. Ideological Security and Deviation of Value Orientation: In-depth Hidden Perils in Digital Governance

Against the institutional backdrop where higher education institutions shoulder the responsibility of ideological education, risks to ideological security arising from big data platforms pose unique governance challenges. Data storage and analytical services provided by overseas big data vendors may involve cross-border flows of educational data, triggering risks to data sovereignty. Algorithm recommendation systems structurally shape how faculty and students access information and may deviate from mainstream value orientations due to commercial logic or technical bias. Furthermore, generative AI systems may produce content inconsistent with core socialist values, leading to systematic deviations in value orientation within educational settings. The principle of localized data storage and critical data protection regime stipulated under the Data Security Law and Cybersecurity Law furnish legal grounds for preventing and mitigating the aforesaid risks. Nevertheless, detailed implementing rules and operational protocols tailored for universities remain to be further refined.

6. Fragmented Governance: Institutional Barriers to the Flow of Data Elements

Fragmented governance refers to a systematic predicament marked by insufficient coordination among governing entities and a lack of integrated governance synergy stemming from institutional demarcation, divergent interests and information barriers. In the field of university big data governance, such risks are manifested in specific ways. Institutional obstacles to cross-departmental data sharing result in decisions being made on fragmented information rather than comprehensive holistic data. Inconsistent data interfaces between universities, competent government authorities and external research institutes hinder the socialized circulation of data elements. Ambiguous designation of accountability subjects for big data governance renders the accountability mechanism ineffective once risk incidents occur. Fundamentally, fragmented governance restrains the full functioning of campus big data platforms and prevents capital investment in technology from being translated into tangible improvements in governance efficiency.

IV. Coping Strategies for University Governance Based on Campus Big Data Platforms

To address the aforementioned multi-dimensional structural risks, effective countermeasures need to generate coordinated synergy across technical, institutional and policy dimensions to achieve systematic improvements in governance capacity. Centered on three main lines constructing secure and trusted digital infrastructure, restructuring a multi-stakeholder collaborative governance framework, and optimizing policies aligned with national strategies—this section puts forward operable systematic solutions.

(I) Technical Dimension: Construction of a Secure and Trustworthy Digital Infrastructure

1. Privacy Protection Technical System of Differential Privacy and Federated Learning

Differential privacy introduces calibrated noise into statistical query outputs to prevent the reverse identification of individual records from aggregated results while preserving the overall statistical characteristics of datasets, thereby providing mathematically rigorous security guarantees for privacy compliance in university data analytics. By contrast, the federated learning framework enables collaborative cross-institutional model training without the exchange of raw data, effectively resolving the privacy paradox in multi-party data sharing: it satisfies the governance demands of inter-university data collaboration while avoiding security hazards stemming from centralized data storage. From the perspective of the full data lifecycle, automated technical workflows covering collection purpose disclosure, usage scope restriction, retention period stipulation and scheduled data destruction upon expiry should be established to enforce standardized lifecycle management through technical means.

2. Block chain-Empowered Trustworthy Data Circulation Mechanism

To tackle the trust deficit plaguing data sharing, universities should develop trusted data circulation platforms built upon consortium block chains. Leveraging the immutability of block chain and the automatic execution mechanism of smart contracts, data access authorization, circulation logs and compliance audits can be transparently recorded and verifiable, effectively facilitating trust building among multi-party data sharing. In specific scenarios such as academic credential verification, confirmation of ownership for research outputs and student file administration, distributed evidence storage removes overreliance on a single centralized authority and mitigates systemic risks within certification frameworks.

3. Transparency Mechanism for AI Explain ability and Algorithmic Auditing

Explainable Artificial Intelligence shall be stipulated as a mandatory technical standard for the procurement and development of AI systems in universities. An explain ability mechanism requires AI systems to deliver not only final decisions but also decision rationales in human-interpretable forms, laying a technical foundation for teachers and students to understand, challenge and appeal against algorithmic outcomes. Meanwhile, an independent algorithmic auditing system ought to be established to conduct regular bias testing, fairness evaluation and performance review on deployed AI systems, so as to sustain their regulatory compliance in practical governance. To mitigate the hallucination risks inherent to generative AI, dedicated content verification tools and source-tracing tagging systems should be deployed, with manual review checkpoints arranged prior to the inclusion of AI-generated content into official governance workflows.

(II) Institutional Dimension: Restructuring the Multi-stakeholder Collaborative Governance Framework

1. Data Ethics Committee and Risk Assessment System

Drawing on the institutional design logic of biomedical ethics review committees, universities should set up dedicated data ethics committees responsible for ethical review of data collection projects, AI system deployment and digital surveillance programs. In line with the multi-stakeholder principle, such committees shall consist of faculty representatives, student representatives, technical specialists, legal experts and independent external participants to prevent ethical judgments from being dominated by a purely administrative perspective. For data projects involving the processing of highly sensitive information, a data protection impact assessment regime shall be enforced to systematically identify, evaluate and document potential privacy risks and corresponding mitigation measures prior to project initiation.

2. Institutional Construction of a Polycentric Collaborative Governance Framework

Based on Ostrom ought polycentric governance theory, the principal structure of university data governance to shift from a centralized hierarchical model toward a five-dimensional polycentric network featuring coordinated participation by administrative management, faculty, students, technical departments and external stakeholders. Specific institutional arrangements are as follows: establishing a data governance committee as the top decision-making body and adopting a multi-participant deliberation mechanism for policy formulation; opening an appeal channel for teachers and students concerning data rights to institutionalize the realization of data subjects' rights to know, access, rectification and erasure; building a regular assessment system for the governance performance of big data platforms and introducing independent third-party audits to guarantee the objectivity of evaluation results.

3. Institutionalization of Full Digital Lifecycle Management Specifications

The institutional system of data governance shall be systematically restructured around full data lifecycle management, covering the following key phases. At the collection stage, the minimization principle shall be followed to gather only data categories indispensable for predefined governance objectives. At the processing stage, the

purpose-binding principle shall be enforced to prohibit data analysis and application beyond the originally consented collection intent. At the storage stage, classified security management shall be implemented with differentiated storage policies formulated in accordance with varying levels of data sensitivity. At the sharing stage, explicit authorization shall be mandated such that any cross-entity data circulation is subject to the data subject's unambiguous consent. At the destruction stage, technical guarantee requirements shall be fulfilled to permanently and irreversibly delete expired data via technical means. The aforementioned principles shall be codified into enforceable institutional documents, and mandatory technical controls shall be deployed to secure institutional compliance.

4. Upgrading and Restructuring of the Digital Governance System for Academic Integrity

Faced with the institutional impacts of generative AI on the academic integrity system, universities should develop a full-chain digital governance framework for academic integrity spanning prevention, detection, sanction and education. At the policy level, clear guidelines shall be formulated to define the permissible scope of AI application in learning and research. At the technical level, multi-dimensional detection tools for AI-generated content should be deployed to complement human review. At the cultural level, data ethics and norms governing AI usage shall be incorporated into the digital literacy curriculum for faculty and students, forming the primary safeguard for academic integrity from a value-based perspective.

(III) Policy Dimension: Optimization Suggestions on Pathways Aligned with National Strategies

1. Advancing Top-level Design of the Educational Data Standard System

The fundamental solution to mitigating fragmented governance risks lies in the unification of data standards and the systematization of institutional norms. Led by the Ministry of Education, the unified development of a standard system for university data should be promoted, covering core elements including data format specifications, semantic labeling criteria, interface protocol standards and security classification benchmarks, so as to lay an institutional foundation for data interconnection among universities as well as between universities and governmental authorities. Meanwhile, compliance requirements stipulated in the Data Security Law and the Personal Information Protection Law shall be translated into concrete operational rules for institutional data governance, establishing well-defined institutional docking channels between national legislative frameworks and university-level implementation.

2. Formulating a Special Policy Framework for Algorithmic Governance

Referring to the classified management logic for high-risk AI laid down in the EU AI Act, competent educational authorities should facilitate the formulation of a dedicated policy framework for algorithmic governance tailored to higher education scenarios. Such a framework shall specify the access review criteria for AI systems deployed in universities, mandatory periodic implementation requirements for algorithmic impact assessments, institutional arrangements for appeal and remedy mechanisms against algorithmic decisions, as well as provisions on information disclosure and compliance liabilities of algorithm system suppliers. Centered on safeguarding educational equity and protecting the legitimate rights and interests of teachers and students, the formulation of the policy framework shall organically integrate the values of technological governance with the objectives of educational governance.

3. Promoting the Systematic Construction of Digital Literacy Education

The long-term effectiveness of technological governance ultimately hinges on the digital cognition and value judgment capabilities of governance stakeholders. Digital literacy education shall be systematically incorporated into university talent cultivation programs and teachers' professional development plans, covering core competency dimensions including awareness of data rights, critical thinking toward algorithms, privacy protection practices and understanding of AI ethics. Capacity building for digital governance among university administrators is equally indispensable; targeted training programs should be launched to strengthen administrators' proficiency in data-driven decision-making, risk assessment and the interpretation of technology-related policies.

4. Promoting Standardized Development of Market-oriented Allocation of Educational Data Factors

Against the national strategic framework for the market-oriented reform of data factors, the factor-based circulation of universities' scientific research and educational data presents a policy opportunity to unlock the potential of the digital economy, while entailing strategic risks such as the spillover of core intellectual assets and the erosion of data sovereignty. A classified management system for the circulation of university data factors shall be established at the policy level: high-sensitive data concerning national security, intellectual property rights and personal privacy shall be subject to stringent protection and localized storage; desensitized educational data with public value shall be openly shared in an orderly manner within the confines of policy frameworks; universities shall be supported to participate in the development of the digital education ecosystem relying on their data assets, with institutional safeguards for data sovereignty retained amid market-oriented explorations.

V. CONCLUSION

From a macro-strategic perspective, optimizing university governance pathways via campus big data platforms not only represents a technical option for universities to improve internal management efficiency but also marks the in-depth convergence of the Strategy for Building a Powerful Country through Education and the Digital China Initiative within higher education. As core hubs of knowledge innovation and strategic bases for cultivating high-caliber talents, universities' digital and modernized governance systems bear direct implications for the bottom line of national innovation capacity and human capital accumulation. Only by anchoring the technological dividends of the era in robust institutional development and restraining the expansion of algorithmic power through rigorous ethical awareness can the digital transformation of university governance evolve toward an advanced human-centered and value-driven modern form. Future research can be further advanced along four strands: the long-term evolutionary rules and institutional response mechanisms behind the in-depth integration of generative AI and university governance; the development of quantitative assessment frameworks and measurement tools for evaluating the effectiveness of university data governance; institutional disparities and the referential value of digital governance models for higher education across nations from a comparative lens; and balanced approaches to safeguarding data sovereignty alongside digital economic growth amid the market-oriented reform of educational data factors. Establishing a secure, trustworthy, fair, transparent, collaborative and efficient big data governance system for universities is not merely a practical necessity to address prevailing technological risks but also a strategic choice to erect institutional safeguards in advance for the sound and sustainable development of the future educational ecosystem.

Acknowledgement

This study is supported by the 2025 Jiangsu University Philosophy and Social Sciences Research Project "Research on Ethical Challenges and Response Strategies in Athlete Ideological and Political Education in the Digital-Intelligent Era" [Grant No. 2025SJYB0277] and the 2025 Nanjing University of Finance and Economics Teaching Reform Project "Research on Optimizing University Governance Path Based on Campus Big Data Platform" [Grant No. XJWC3202521]

REFERENCES

[1]Chen Yuting Research on Student Affairs Based on Smart Campus Big Data [D]. Capital University of Economics and Business, 2020.

[2]Tan Fengxia Research on Service Optimization of Campus Big Data Platform [D]. Huazhong Normal University, 2021.

[3]Zhang Yan Analysis on the Concept and Mode of "Internet plus Education" [J]. China Higher Education Research, 2016, (2): 70-73.

[4]Wang Huixian Exploration and Research on the Construction of Smart Campus in Universities under the Background of

Big Data [J]. Science and Technology Wind, 2018, (19): 76+85.

[5]Luo Ning Design and Application of Big Data Platform in Urban Public Security Risk Prevention and Control [J]. Journal of Henan Normal University (Natural Science Edition), 2025, 53 (1): 100-106.

[6]Wang Shixian, Wen Kunmei, Li Junfeng, etc Design and Construction Practice of Digital Twin Campus Platform in Universities: A Case Study of Huazhong University of Science and Technology [J]. Modern Educational Technology, 2023, 33 (11): 118-126.