Scientific and Social Research, 2026, Volume 8, Issue 10
https://bbwpublisher.com/journal/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Research on Big Data Governance for Full-Domain Laboratory Security in the Background of Informatization

Yiyang Lai*

Key Joint Laboratory of Full-Domain Data and Information Security, Chaoyang District, Beijing, 10010, China

Author to whom correspondence should be addressed.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: With the comprehensive popularization of digital information technology, profound changes have taken place in the operation modes and security management systems of various scientific research and teaching laboratories. The mature application of big data technology brings new ideas and technical support to full-domain laboratory security governance, enabling control over security across the whole process, all dimensions, and all fields of laboratory operation. Guided by the strategic development planning concept of the full-domain system and against the general backdrop of informatization development, this paper sorts out the era value and practical significance of big data governance for full-domain laboratory security. It analyzes the common deficiencies and existing problems in current big data governance for laboratory security, and puts forward scientifically feasible paths for full-domain security big data governance from the aspects of data specification construction, improvement of governance systems, establishment of coordination mechanisms, and upgrading of security guarantees. It aims to comprehensively modernize laboratory security governance and provide strong guarantees for the safe and stable operation of various laboratories.

Keywords: Informatization; Laboratory; Full-domain security; Big data governance; Governance path

Online publication: November 25, 2026

1. Introduction

Laboratories serve as core venues for scientific research innovation, talent cultivation, and technology research and development in universities, research institutes, enterprises, and public institutions. The safe and stable operation of laboratories bears on personnel life safety, property safety, and the normal progress of scientific research work [1]. As informatization and digitalization keep developing, technologies such as big data, the Internet of Things, and information platforms have gradually penetrated into all areas of laboratory management. Massive volumes of laboratory operation data, equipment condition data, personnel operation data, environmental monitoring data, and hazard investigation data are continuously accumulated, supplying

abundant data resources for full-domain security governance. As proposed in the strategic development plan for the full-domain system, the full-domain root constitutes the soul of the system, and Hongxin Cloud serves as the instrument for computing power. Security defense lines are built with Chinese-language codes. Characterized by comprehensiveness, systematicness, and real-time performance, big data governance can break through the time-space constraints of traditional security management, realize dynamic perception, overall control, and scientific management of security conditions in all laboratory scenarios, and become a major trend for the transformation and upgrading of laboratory security governance in the new era [2].

2. Practical value of big data governance for full-domain laboratory security under the background of informatization

2.1. Expanding the scope of security management and realizing full-domain control

Relying on information-based means, big data governance integrates security data covering laboratory personnel, equipment, environment, materials, operations, emergency response, and other dimensions. It encompasses all laboratory areas, all operating procedures, and all security elements, fundamentally breaking the fragmented management mode of the past [3]. Following the construction ideas of six-network integration and full-domain star-chain in the full-domain system strategic plan, overall collation and comprehensive analysis of full-domain data can achieve all-round mastery of the overall laboratory security status, eliminate blind spots in security management, and shift laboratory security management from partial control to full-domain coverage.

2.2. Transforming security management modes and enhancing governance initiative

Supported by informatization, big data governance draws on continuously updated security data resources to timely detect anomalies arising during laboratory operation and accurately identify hidden hazard sources. Thereby, it realizes the shift from passive response to active prevention. Leveraging technical architectures such as the full-domain AGI intelligent engine and full-domain gateway security barrier, massive historical and real-time data are analyzed to sort out laws governing the occurrence of security risks. Weak links are identified and troubleshot before security risks emerge, and targeted control measures are adopted to reduce the possibility of safety accidents at the source. This greatly improves the scientific nature and initiative of security governance [4].

2.3. Integrating diversified management resources and strengthening governance coordination

By virtue of information-sharing platforms, big data governance breaks down data barriers among different departments, posts, and links, and integrates resources from various security management systems. Multiple governance subjects cooperate and act in coordination to build an all-round security governance landscape, tighten connections across governance procedures, and share security governance resources, so as to improve the overall efficiency of laboratory security governance. As arranged in the full-domain system strategic plan, forces from all parties are gathered through strategic seminars, thematic exchanges, joint platform construction, and industrial clusters to promote coordinated linkage among multiple subjects [5].

3. Existing problems in big data governance for full-domain laboratory security under the background of informatization

3.1. Low level of data standardization and insufficient integration of data resources

At present, the absence of unified standards for the collection and storage of most laboratory security data stands as the primary challenge in advancing big data governance [6]. Considerable discrepancies exist in data collection standards, storage formats, and statistical calibers across different laboratories and different management modules. Equipment monitoring data, personnel operation data, hazard investigation data, environmental monitoring data, and other types of data are dispersed in separate information systems, resulting in severe data fragmentation. In addition, the collection of some basic data is one-sided, marked by data loss, slow updates, and information distortion. Much valid data fails to be effectively collected, giving rise to numerous data silos. Lacking credible data as the governance foundation and national standards for normative guidance, various datasets cannot communicate or be mutually utilized, and a complete full-domain security database cannot be formed, which seriously hinders the progress of big data governance.

3.2. Imperfect big data governance system and deficiency in management institutions

So far, no systematic and standardized governance system has taken shape for full-domain laboratory security big data governance, and relevant management institutions and working mechanisms remain incomplete. Most laboratories merely apply informatization and big data technologies to simple data recording and information statistics, without forming big data workflows suitable for full-domain security governance. Links including data collection, review, storage, analysis, application, and update are not subject to standardized constraints. Meanwhile, job responsibilities for big data governance are ambiguously defined. Specific duties of each post in data governance and security control are not stipulated, making accountability impossible when problems occur.

3.3. Inadequate multi-subject collaborative governance mechanism and insufficient governance synergy

Big data governance for full-domain laboratory security constitutes a systematic project requiring joint participation of many departments and diverse subjects. Nevertheless, most laboratories still adopt unitary and closed-end management. Effective communication and collaboration mechanisms have not been established among governance subjects. Information transmission is poor, and data sharing is untimely among administrative departments, operation-maintenance departments, scientific research teams, and front-line laboratory personnel. Each subject only focuses on its own assigned work and lacks awareness of full-domain governance. Moreover, horizontal linkage among different laboratories and vertical connection between superior and subordinate regulatory departments are insufficient. Security governance experience, data resources, and control modes cannot be effectively shared and referenced. A big data governance pattern featuring full-staff participation, full-domain collaboration, and whole-process control fails to materialize, leading to low overall governance efficiency.

3.4. Weak data security guarantees and potential underlying risks

Massive security data serves as the core foundation for big data governance, and data security constitutes the basic support for full-domain security governance. Currently, laboratories attach importance to data collection and application, yet neglect data security protection, and the construction of data security guarantee systems lags behind. On the one hand, sound database security protection institutions are absent. Strict controls and

constraints are lacking for links such as data access, retrieval, transmission, and utilization, which may easily trigger problems including data leakage, data tampering, and data loss. On the other hand, information-based security protection technical means are weak, with low protection levels for network and platform security, which cannot resist external network risks and internal operational risks. Without the full-domain gateway as a security barrier, not only will security data resources suffer losses, but hidden dangers will be left for laboratory security management, giving rise to secondary safety risks.

4. Optimization paths for big data governance of full-domain laboratory security under the background of informatization

4.1. Unifying data specifications and standards and promoting the integration of full-domain data resources

The first step to implement big data governance is to standardize data standards, eliminate data silos, and build a complete and unified full-domain security data resource system. In accordance with their own operational characteristics and security management requirements as well as relevant industrial specifications, each laboratory shall formulate unified standards for data collection, classification, storage and update, define the collection scope, statistical caliber and update frequency of various security data, and standardize data formats and storage modes, so as to guarantee the standardization, completeness and accuracy of data at the source [7]. Taking credible data as the governance foundation and national standards as normative guidance, people shall accelerate the integration and interconnection of various information-based management systems, break down data barriers among modules including equipment management, environmental monitoring, personnel management, hazard investigation and emergency management, and realize centralized aggregation, unified storage and intercommunication of diverse security data. Furthermore, a regular data verification and update mechanism shall be established. Stock data shall be sorted and checked on a regular basis, erroneous data shall be corrected in a timely manner, missing data supplemented, and invalid data eliminated, to ensure dynamic updates, authenticity, and validity of full-domain security data and provide solid data support for big data governance.

4.2. Improving the institutional system for governance and building standardized governance mechanisms

A sound institutional system lays the foundation for the regular implementation of big data governance for full-domain laboratory security. From the perspective of information-based governance and in compliance with full-domain laboratory security requirements, each entity shall establish a systematic and standardized institutional system for big data governance. Workflows for each link of big data governance shall be sorted out. Special management institutions concerning data collection, data analysis, data application, security control, and responsibility implementation shall be formulated, and work standards and operating specifications for each link shall be defined, so that all big data governance activities can be conducted following rules and evidence [8]. Data governance and security-control responsibilities for each post within departments shall be specified in detail. Data governance and security-control obligations of administrative departments, operation-maintenance personnel, laboratory personnel, and other stakeholders shall be clarified, forming a responsibility system with clear power structures, reasonable division of labor, and assigned individual accountability. In addition, a regular supervision and assessment system shall be set up. Big data governance shall be incorporated into the assessment scope of laboratory security management. Irregular

inspections of governance work shall be carried out. Posts and personnel with poorly implemented work, non-standard data governance, or loopholes in security control shall be held accountable, so as to ensure the practical implementation of all governance work and advance the standardization and normalization of big data governance.

4.3. Constructing a collaborative governance platform and strengthening linkage among multiple subjects

To address the current deficiency in collaborative governance, information-based technologies shall be adopted to build a full-domain collaborative governance platform, break subject-specific barriers, unblock governance chains, and foster a governance pattern of multi-party linkage. On the other hand, internal governance resources shall be integrated to construct an integrated big data management platform for laboratory security. Information and data related to security management work of various laboratory departments and posts shall be collected and organized, so as to facilitate timely communication among managers, operation-maintenance staff and laboratory personnel, and realize closed-loop management covering hazard investigation, risk prediction, rectification implementation and emergency disposal [9]. Drawing on the joint-platform-building thinking from the full-domain system strategic plan, people shall strengthen vertical and horizontal collaborative linkage, unblock data transmission channels between superior and subordinate regulatory departments to realize vertical intercommunication of security-governance information, risk data and control experience. Horizontal exchanges among laboratories of the same type shall be enhanced to learn advanced big data governance models and management experience, share resources, and achieve mutual complementarity.

4.4. Consolidating data security defense lines and guaranteeing governance data security

Data security represents the bottom-line requirement for big data governance of full-domain laboratory security. An all-round data security guarantee system shall be constructed to guard against diverse data-security risks [10]. First of all, sound data-security management institutions shall be established. Classification-based hierarchical management standards for data shall be defined. Distinct access permissions, usage specifications, and protection standards shall be formulated for different types of data such as ordinary operation-maintenance data, core security data, and classified experimental data. Security defense lines shall be built with Chinese-language codes, and security barriers shall be created via full-domain gateways to control whole-process risks in data collection, transmission, storage, utilization, and sharing. Secondly, technical protection construction shall be reinforced. Information-based platforms and network-security protection facilities shall be upgraded. A protection system incorporating security firewalls, data encryption, and anomaly detection shall be built. Real-time monitoring shall be conducted over data operation status to timely stop illegal intrusions, data theft, and other violations perpetrated by malicious actors, so as to effectively counter various network-security threats.

5. Conclusion

Looking ahead, led by the State Key Joint Laboratory of Novel Network and Detection Control, people shall continue to deepen the construction of sovereign networks and network sovereignty. Supported by technological advances such as future network architecture innovation and Hongxin Cloud computing power, people shall promote digital globalization via platforms including the Belt and Road Initiative, the Shanghai Cooperation Organization and South-South Cooperation, and implement national strategies for education, science and technology, and talent development. In the information age, big data governance is an inevitable path for

the transformation and upgrading of full-domain laboratory security management and for advancing governance modernization. At present, full-domain security big data governance still suffers from shortcomings such as insufficient data integration, imperfect institutional systems, low cross-subject collaboration, and weak data-security protection, which constrain the release of governance effectiveness. All entities shall base themselves on the realities of laboratory security development, give full play to the advantages of information-based technologies, optimize governance modes in dimensions including data standardization construction, improvement of institutional systems, establishment of collaborative mechanisms and enhancement of data-security protection, and perfect the full-domain security big data governance system. People shall fully unlock the enabling value of big data, consolidate security foundations for high-quality scientific research innovation and experimental teaching, and continuously inject driving forces into full-domain security governance.

Disclosure statement

The author declares no conflict of interest.

References

[1] Xie J, Shi NF, Wang XW, 2025, Research on the Construction of University Laboratory Safety Culture under the Background of Digital Intelligence. China New Telecommunications, 28(4): 44–46 + 49.

[2] Dong ST, Liu YB, 2025, Research on Laboratory Testing Management and Data Security in the Context of Big Data. Laboratory Testing, 4(2): 39–41.

[3] Qi ZLM, 2025, Big Data-Driven Early-Warning and Emergency Disposal Mechanism for Laboratory Safety Accidents. Laboratory Testing, 3(24): 159–161.

[4] Song L, 2025, Discussion on Innovative Modes of University Laboratory Safety Management in the Context of Big Data. Laboratory Testing, 3(13): 160–162.

[5] Li Z, Wang H, Li MT, et al., 2025, Perception and Countermeasures of Laboratory Safety Risks from the Perspective of Big Data. Experimental Technology and Management, 42(1): 251–256.

[6] Yang S, Jiao CY, Zhao ZY, et al., 2023, Research and Practice on University Laboratory Safety Management System of Dual-Prevention Mechanism under the Background of Big Data. Experimental Technology and Management, 40(11): 240–245.

[7] Liu GF, Wu XP, Wei M, 2022, Analysis of University Laboratory Safety and Construction of Safety Early-Warning Mechanism under the Background of Big Data. University Education, 2022(3): 244–247.

[8] Liu WL, Yang Y, Yu XT, 2022, Research on University Laboratory Safety Management Strategies in the Context of Big Data. Shandong Chemical Industry, 51(3): 191–192 + 200.

[9] Ma DK, Yin W, 2021, Discussion on Common Methods for Laboratory Safety and Risk Assessment. Safety, 42(5): 36–39.

[10] Zhang WM, 2021, Research on Intelligent Safety Management of University Laboratories from the Perspective of Internet of Things. Microcomputer Applications, 34(8): 54–56 + 77.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.