文章编号：2617-6084 (2025) 04-0091-05

高校数据安全与治理策略探讨

张　亮，赵云飞，辛　艳

（沈阳药科大学 信息中心，辽宁 沈阳 110016）

摘　要：随着信息技术在高校的广泛应用，应用系统数据量呈现爆发式增长，数据安全与治理已成为高校信息化建设面临的重要挑战。通过分析高校数据多源异构、隐私敏感、增长迅速且动态变化的特性，指出当前高校数据安全存在管理体系混乱、防护技术落后、处理环节风险高以及制度不完善等问题，提出完善数据安全管理、加强数据分类分级保护、强化安全意识等一系列有针对性的数据治理策略，旨在为高校构建全面且有效的数据安全与治理体系提供理论支持与实践参考，从而保障高校教学、科研、管理等业务的稳定运行，有力推动高校信息化建设的可持续发展。

关键词：高校信息化；数据安全；数据治理

中图分类号：TN915.08　　**文献标志码：**A

在数字化进程迅猛发展的当下，数据已成为驱动各领域前行的关键力量。高校作为知识传承与创新的重要阵地，积累了海量的教学、科研、管理等多方面的数据。这些数据不仅是高校日常运转的关键支撑，更是推动高校教育创新、科研突破的战略资源。然而，随着网络技术的不断演进，高校数据面临着前所未有的安全挑战，数据泄露、滥用、管理混乱等问题日益凸显，严重威胁着高校的稳定发展以及师生的合法权益。如何在保障安全的前提下，有效管理和应用数据资源，已成为高校信息化发展的重大挑战[1]。因此，深入研究高校数据安全与治理策略，构建安全可靠、规范有序的数据环境，充分释放数据价值，已成为保障高校数字化转型顺利推进、实现可持续发展的迫切需求。

1　高校数据特点

1.1　多源异构性

高校的数据来源广泛复杂，涵盖教务管理系统、研究生管理系统、科研管理系统、学工系统、协同办公系统、财务系统、医疗信息管理系统等多个不同的业务系统。这些系统由不同厂商开发，采用不同的数据结构和存储方式，数据格式包括结构化数据（如数据库中的字段和表格数据）、半结构化数据（如 XML、JSON 格式数据）和非结构化数据（如文本、图像、音频和视频等），这些数据的数据存储格式和传输格式也不尽相同，导致数据在整合和共享过程中存在困难，需要进行复杂的数据清洗、转换和集成工作。

1.2　敏感性和隐私性

高校数据中包含大量敏感信息，这些数据兼具高度敏感性与隐私特质，如学生的个人身份、成

投稿日期：2025-01-07

作者简介：张亮（1983−），男（汉族），山东泰安人，工程师，研究方向：网络安全、信息化，**E-mail** 176998661@qq.com。

绩、健康状况，教职工的基本信息资料，科研项目的核心技术、研发实验数据和未公开的实验成果等。这些数据一旦泄露可能会对个人隐私、学术声誉和学校安全等造成严重损害，可能直接危害公众健康与扰乱产业秩序，影响公共安全、经济安全和社会稳定。因此，对数据的保密性要求极高，需要采取严格的访问控制和加密措施防止数据被非法获取和利用。

1.3 数据增长迅速

随着高等教育的普及、科研项目的增多以及学生教育的信息化发展，高校的数据量呈现快速增长趋势。尤其是教学、科研、管理等各重要业务系统的数据，如实验数据、个人照片等图像数据以及课堂教学录像等视频数据，单个文件大小可达几十兆甚至上百兆，加上长期积累的历史数据和不断更新的业务数据，都在不断扩充数据总量，对数据存储、传输和处理能力提出了很高的要求，同时，也增加了数据管理的复杂性和安全风险。

1.4 数据的动态性

高校的数据具有鲜明的动态性，随着学科知识的持续更新换代，教学大纲、课程内容不断优化调整，与之相对应的业务系统数据处于动态变化中。在科学研究领域，科研数据也会随着研究进展不断产生新的实验结果和分析数据，每个环节都促使数据持续迭代。这就要求数据管理系统能够及时处理和反映数据的变化，确保数据的一致性和时效性，同时，在数据更新过程中保证数据的安全性，防止数据丢失或被篡改。

2 高校数据安全现状

当前，高校已迈入数据时代，从信息安全、网络安全逐步聚焦至数据安全领域，数据已跃升为数字经济时代的关键新生产要素，更是高校业务系统价值的核心所在。高校智慧校园建设的一个必经阶段，就是对校内数据进行标准规范的梳理和治理，从而保障数据资产的有效形成[2]。网络空间已然演变为地缘政治冲突的新兴主战场，受经济利益驱使的网络安全事件层出不穷。具有国家背景的境外网络攻击，给网络安全带来了现实且紧迫的威胁。其中，数据泄露问题愈发凸显，成为安全防护工作的重中之重。诸多因政治目的、经济利益以及人为蓄意破坏或失误等因素诱发的数据安全事件频繁上演，高校面临诸多数据安全问题。

2.1 数据管理难度大

高校信息化程度高，涉及大量前沿技术应用，技术体系复杂，缺少统一的标准体系以及顶层设计规划[3]。同时，高校对信息技术依赖程度极高，人员密集、设备繁多、业务系统林立、数据量庞大。由于高校的社会关注度高，往往容易成为网络攻击的主要目标。但与之矛盾的是，高校专业网络安全人员和专项经费相对短缺，管理难度较大。从预算方面看，安全投入在整体经费中的占比明显不足，难以支撑全面且深入的安全防护体系建设。从进度层面看，安全建设常常滞后于业务的快速发展，新业务系统上线时，安全防护措施未能同步到位，致使高校的信息系统数据面临严峻的安全威胁。

2.2　安全防护能力不足

在技术层面，部分高校的网络安全防护设备陈旧，数据安全防护技术手段相对落后，无法有效应对日益复杂的网络攻击和数据安全威胁[4]。例如，入侵检测系统、防火墙等设备的规则库未能及时更新，无法有效识别新型网络攻击；数据加密技术应用范围有限，加密算法和密钥管理不够规范；数据备份与恢复策略不完善，在遭遇数据丢失或损坏时无法保证数据的完整性和可用性。对于一些关键业务数据和敏感信息，未能采取足够强度的加密、访问控制等安全防护手段，而对于一般性数据则可能存在过度保护或保护不足的情况，造成资源浪费和安全风险分布不均。

2.3　数据处理环节风险高

以数据生命周期为基础进行安全保障，是数据安全的核心思想[5]。在数据收集环节，若采集来源不明或未经授权，可能收集到错误或恶意数据，同时，收集方式不当可能侵犯个人隐私。在数据存储环节，存储设备故障、存储介质被盗或未加密存储等，都可能导致数据丢失或泄露。在数据使用环节，权限管理不善，可能导致数据被滥用，如未经授权的科研数据使用，影响科研成果的公正性。在数据加工环节，数据篡改风险较高，加工过程若缺乏监管，可能改变数据原有的真实性和可靠性。在数据传输环节，网络传输协议不安全、传输线路被监听等，会造成数据在传输途中被窃取。在数据提供环节，向外部提供数据时，若未签订严格保密协议，数据可能被非法扩散。在数据公开环节，过度公开或公开敏感数据，会直接侵害个人隐私或泄露高校机密。

2.4　安全管理制度不完善

虽然一些高校制定了相关的数据安全管理制度，但制度内容往往不够全面、细致，缺乏针对性和可操作性。部分制度未能及时更新以适应新的信息技术发展和数据安全形势变化，导致在实际执行过程中存在漏洞，难以对数据全生命周期的各个环节进行有效规范和监管，无法满足学校精细化管理、科学决策的需求。数据未进行清晰准确的分类分级管理，导致无法根据数据的重要性和敏感程度实施差异化的安全保护措施。由于业务系统数据质量不高，共享的数据难以充分利用和挖掘，存在数据孤岛现象，导致数据在跨部门共享和协同应用过程中出现障碍，数据标准化和数据整合优化难以深入，影响了数据的质量和价值发挥。由于缺乏有效的数据质量监管评估机制，难以发现和纠正数据质量问题，使得数据决策分析和业务应用可能产生错误的结果，影响高校的教学、科研和管理效率。

3　高校数据治理策略

高校的数据安全工作尚处于起步阶段，师生的数据安全意识淡薄，家底不清，即对自身数据资产缺乏清晰认知；制度不全，缺乏完善的安全管理制度与流程；目标不明，未确立明确的数据安全防护目标；防护不强，导致数据安全风险极高，个人信息保护更是面临巨大挑战。数据安全治理是

一个巨大、复杂的系统工程[6]。高校的数据安全现状不容乐观，亟待全方位、深层次的改进与完善。

3.1 完善数据安全管理

建章立制，重点管控，深入学习贯彻《网络安全法》《数据安全法》《个人信息保护法》《密码法》《关键信息基础设施保护条例》等网络和数据安全的法律法规。建立数据安全责任制，明确第一责任人、责任部门及分工。不断完善数据安全管理、机构建设、人员管理和数据建设、运维等方面的制度建设，做好管理制度的执行监管。在数据产生、传输和使用过程中实施必要的安全访问控制，对数据活动记录日志，完成安全审计，采用加密传输等技术手段，确保数据在传输过程中的安全性、完整性和合规性。同时，明确数据的权属关系和使用范围，规范数据的使用行为，防止数据的非法访问和使用。

3.2 加强数据分类分级保护

数据分类分级是数据安全治理的基础[7]。梳理数据资产，明确数据的种类、特点、存放位置、访问权限、使用频率等，依据数据安全等级定义对所有数据进行分类定级。通过数据分类和标准化，更好地管理和利用数据资源，提高数据治理的效率。建立统一的数据中台，确定一数一源，提高数据的准确性、完整性、一致性和可靠性，推进全业务对象、全业务流程以及业务规则数字化，建成质量优良的全域数据库，构建数字孪生校园的智慧中枢，即时分析海量数据，智能支撑精准施策，实现数据的价值挖掘和赋能，推进高校管理服务和治理数字化，驱动转型发展，建设智慧校园。

3.3 提升数据安全防护能力

对数据实行分区域管理，确保专网专用，对不同业务系统进行横向隔离，加强纵向防御。强化认证，加强审计，利用防火墙、入侵检测、网闸、WAF 等安全设备进行网络和数据安全防护，加强身份鉴别与访问控制，建立监测预警机制，对数据交互进行重点防护，实施数据加密、数据脱敏、数据防泄漏、数据接口安全等安全措施，做好数据备份恢复和安全审计。对数据的产生、采集、传输、存储、处理、共享和销毁等全生命周期流程进行梳理和优化，消除不必要的数据冗余和重复采集环节，建立数据标准规范体系，确保数据在各业务系统之间的一致性和准确性。

3.4 强化师生安全意识

加强数据治理的宣传教育，定期开展网络与数据安全培训，通过国家网络安全宣传周的讲座研讨等活动，提高师生对数据治理以及网络安全的重要性和必要性认识。制定数据安全职责，设定不同岗位在数据安全中的职责和要求[8]。加强个人信息安全保护，将网络和数据安全教育整合到学校课程中，从被动防御转向主动学习和应对。没有数据安全就没有国家安全，全体师生都应该行动起来，把数据安全置于国家安全的全局性、战略性的高度来把握，将数据安全防线建立在校园内部，不断提升师生的数据安全意识，营造全体师生共同保护数据安全，共筑网络安全防线的良好氛围。

4　结语

高校数据安全与治理是一个持续的复杂工程，关系到高校的教学、科研和管理等各项事业的稳定发展和师生的切身利益。通过完善数据安全管理制度、加强数据分类分级保护以及提升数据安全技术防护能力等策略的实施，可以有效应对当前高校数据安全与治理面临的诸多挑战，构建一个安全可靠、完整统一、规范有序、高效利用的数据生态环境，充分发挥数据资产的价值，为高校的创新发展提供坚实的支撑和保障，推动高校教育信息化再上新台阶。

参考文献：

[1] 马妍, 山杜鹃. 智慧校园背景下高校数据安全治理策略[J]. 数字技术与应用, 2024(5): 92−94.

[2] 刘蓁蓁. 智慧校园建设背景下高校数据安全管理的研究[J]. 网络安全技术与应用, 2021(1): 102−103.

[3] 蔡萌萌, 陈晓, 郑玉娟, 刘静. 大数据背景下智慧校园平台建设研究[J]. 网络安全技术与应用, 2024(8): 83−84.

[4] 王少影, 问朝, 常永娟. 电力企业级数据治理体系的研究[J]. 中国战略新兴产业, 2024(29): 42−44.

[5] 甘清云. 浅谈数据安全之数据分类分级[J]. 网络安全技术与应用, 2025(1): 67−69.

[6] 范江波. 高校数据安全治理痛点与对策[J]. 中国教育网络, 2021(7): 65−67.

[7] 刘博. 以数据全生命周期为核心实现数据安全[J]. 中国信息安全, 2019,120(12): 74−75.

[8] 杨云龙, 郭中梅. 数据安全体系建设的研究及思考[J]. 信息通信技术与政策, 2025,51(1): 40−45.

Discussion on data security and governance strategies in universities

ZHANG Liang, ZHAO Yunfei, XIN Yan

(*Information Center, Shenyang Pharmaceutical University*, *Shenyang* 110016, *China*)

Abstract: With the widespread application of information technology in universities, the data volume of application systems has experienced explosive growth, making data security and governance a crucial challenge in the digital transformation of higher education institutions. By analyzing the characteristics of university data including multi-source heterogeneity, privacy sensitivity, rapid growth, and dynamic variability, this study identifies key problems such as disorganized management system, outdated security technologies, high-risk data processing procedures, and inadequate regulatory frameworks. The paper proposes targeted data governance strategies including improving data security management systems, strengthening classification-based and hierarchical data protection, and raising security awareness education. These strategies aim to provide theoretical support and practical references for establishing a comprehensive and effective data security and governance framework in universities, ensuring stable operation of teaching, research, and administrative activities, and promoting sustainable informatization development in higher education.

Keywords: higher education informatization; data security; data governance