数字赋能高校转型下的数据安全风险防控研究

刘克铜 张越 闫智莉 胡新红
河北机电职业技术学院，中国·河北 邢台 054000

摘要：数字赋能促使高校全方位转型，教学科研数字化、管理服务智能化成为高校发展的走向，高校数据量急剧增长、种类日益复杂，数据安全风险防控的紧迫性、重要性愈加突出。本文以数字赋能高校转型的时代背景为出发点，梳理高校数据安全的现实状况，分析转型过程中存在的数据安全风险类型，探究风险产生的深层次原因，从技术、管理、制度、人员等角度提出相应的防控策略。目的在于为高校创建科学完善的数据安全防护体系提供理论依据，使高校在数字化转型过程中实现安全与发展同步推进。

关键词：数字赋能；高校转型；数据安全；风险防控

Research on Data Security Risk Prevention and Control under the Empowerment of Digitalization for University Transformation

Liu Ketong, Zhang Yue, Yan Zhili, Hu Xinhong
Hebei Institute of Machinery & Electricity, China Hebei Xingtai 054000

Abstract: Digital empowerment has driven comprehensive transformation in universities, with the digitalization of teaching and research and the intelligence of management and services becoming the development trend. The volume and complexity of university data have increased sharply, making the urgency and importance of data security risk prevention and control more prominent. This paper starts from the background of digital empowerment for university transformation, sorts out the current situation of university data security, analyzes the types of data security risks in the transformation process, explores the deep-seated reasons for the risks, and proposes corresponding prevention and control strategies from the perspectives of technology, management, system, and personnel. The aim is to provide a theoretical basis for universities to create a scientific and complete data security protection system and achieve the synchronous advancement of security and development during the digital transformation process.

Keywords: Digital empowerment; University transformation; Data security; Risk prevention and control

0 引言

数字技术深度融入、持续革新应用，使高校从传统的办学模式向数字化、智慧化方向发展。数字赋能不仅是高校教学范式、科研路径、管理机制的重塑者，而且是海量师生个人信息、科研数据、教学资源数据、校园管理数据的产生者。此类数据是高校的战略资源，属于核心的战略资源，其安全保障关系到高校的稳定运行以及长远的发展。目前高校在数字化转型过程中存在着技术漏洞、管理短板等数据安全隐患，这些问题并未得到系统解决。加强数字赋能高校转型下数据安全风险防控研究，是教育数字化发展的必然要求，也是高校高质量发展的必要举措。

1 数字赋能高校转型的内涵与数据安全态势

1.1 数字赋能高校转型的核心内涵

数字赋能是以大数据、云计算、人工智能、区块链等信息技术为动力，促使高校从办学理念、组织架构、教学模式、科研创新、管理服务等方面进行系统性的变革与重构。数字技术冲破传统课堂时空的束缚，慕课、虚拟仿真实验、智慧课堂等新教学方式出现，个性化教学、精准育人得以实现。在科研方面，数字赋能使得科研手段得到提升，跨学科、跨地域的协同科研平台也渐渐建立，科研数据的采集、分析、共享效率也得到提高。智慧校园建设不断推进管理服务领域的建设，招生就业、学籍管理、后勤保障等工作用数字化系统进行流程优化，管理效能得到提高。

1.2 高校数据安全的现实发展态势

随着高校数字化转型的不断深入，数据资源的战略价值越来越明显，高校数据安全受到的关注也越来越高。高校数据类型越来越丰富，涉及师生个人敏感信息、科研机密数据、教学核心资源、校园管理数据等众多种类，数据的开放性、共享性需求越来越大，数据安全的保护边界变

得越来越模糊。高校数据安全防护能力虽然有所提高，但是仍然存在许多不足。高校安全防护技术跟不上数字化转型的需要，老旧的安全防护系统抵抗不了新的网络攻击。另外高校的数据管理体系还不健全，数据采集、存储、传输、使用等各个环节权责不明容易造成数据泄露、滥用等问题。

2 数字赋能高校转型下的数据安全风险类型

2.1 技术层面的潜在风险

技术是数字赋能高校转型的重要支撑，同时也是数据安全风险的重要来源。数据存储环节存在风险。部分高校采用分布式存储架构，存储设备异构性较大，不同设备之间的兼容性问题容易造成数据丢失或者损坏。云存储技术被越来越多的高校所采用，但是云端数据控制权的一部分已经移交给服务商，高校无法对云端数据进行全流程监管，存在数据泄露的风险。数据传输环节有风险。高校内部各个系统之间数据的交流频繁，数据在传输过程中容易被截获、篡改。无线网络在校园内实现全覆盖，使得数据传输的开放性增大，未加密的传输数据很容易成为黑客攻击的目标。技术迭代带来的风险。新一代信息技术的快速发展促使高校技术架构不断更新，新旧系统融合过程中容易出现安全漏洞，高校对新技术安全特性的认知存在滞后性，不能及时建立起有效的防护屏障。

2.2 管理层面的固有短板

管理体系的不健全是高校数据安全防护能力提高的主要障碍。数据全生命周期管理机制的缺失，造成数据从产生到销毁的全过程缺少有效的监管，数据采集阶段存在过度采集现象，大量的非必要数据被收集，增加了安全管理的成本。数据存储阶段没有进行分类分级管理，核心敏感数据和普通数据没有做差异化防护，容易造成核心数据泄露。数据使用阶段权限管理混乱，部分人员超越权限范围访问数据，数据滥用、盗用的风险较大。另外，高校数据安全管理的协同机制还没有形成，信息技术部门、教学部门、科研部门、管理部门之间没有有效的沟通协作，数据安全问题出现后不能快速响应和处置，导致风险影响范围扩大。

2.3 制度层面的滞后问题

制度保障是数据安全风险防控的基础，目前高校数据安全相关制度建设明显滞后。高校数据安全管理制度的制定不能完全适应数字化转型的实际需要，制度内容比较模糊，缺少针对性、可操作性。数据安全责任制度不健全，没有把数据安全责任落实到具体的部门和个人，一旦出现安全问题，容易出现推诿扯皮的现象。数据安全应急处置制度不健全，没有科学合理的应急预案，当发生数据泄露、系统崩溃等突发安全事件的时候，应急响应能力差，不能很好地控制风险损失。另外，高校数据安全相关制度更新不及时，不能适应技术发展、转型的要求，制度滞后性使数据安全防控工作缺乏有效的制度依据。

2.4 外部环境的侵袭威胁

随着高校数字化转型的不断深入，高校与外部环境的联系越来越紧密，外部环境的侵害威胁成为高校数据安全风险的主要来源。网络黑客的恶意攻击属于主要威胁之一，黑客利用网络钓鱼、植入恶意软件的方式攻击高校信息系统。部分黑客对高校科研数据进行攻击的行为是有目的的，给高校的科研工作造成严重影响。另外第三方合作机构带来的风险也不能忽视。高校在数字化转型的过程中，会和企业、科研院所等第三方机构进行合作，在数据共享、交换的过程中，第三方机构的数据安全防护能力参差不齐，容易成为数据安全的薄弱环节。部分第三方机构缺少完善的数据安全管理制度，容易造成高校共享数据泄露。

3 数字赋能高校转型下的数据安全风险成因

3.1 技术架构更新与安全防护不同步

数字赋能使高校的技术架构快速迭代，新技术的应用速度远远大于安全防护体系的建设速度。高校在引进大数据、人工智能等新技术的时候，常常重视技术的应用效果和效率的提高，而对技术应用过程中存在的安全风险重视不够。安全防护技术的研发和部署需要大量的资金和人力投入，部分高校由于经费预算、人才队伍的限制，不能实现安全防护技术与转型技术架构的同步更新。除此之外，新技术的安全特性具有很强的专业性、复杂性，高校相关技术人员对于新技术安全风险的认识和应对能力不足，不能及时发现、修复技术架构中的安全漏洞，造成技术层面的安全风险一直存在。

3.2 数据管理权责划分不清晰

数据管理权责不明是造成管理层面安全风险的主要因素。高校的数据涉及到各个部门、各个领域，数据的产生、流转、应用等环节涉及不同的主体，但是目前的高校没有建立明确的数据管理权责体系。数据的所有权、管理权、使用权界定不清，各个部门之间管理职责交叉重叠，容易造成管理真空地带。信息技术部门作为数据安全管理的主要责任部门，没有对其他部门的数据使用行为进行有效的监管，教学、科研、管理等部门对数据安全的重视程度不高，缺少主动防护的意识和能力。权责划分不清造成数据

安全管理工作缺少抓手，不能形成协同防控的合力。

3.3 相关制度建设缺乏前瞻性

高校数据安全制度建设缺乏前瞻性，没有很好地预见到数字化转型带来的新风险、新问题。在制度制定过程中，以传统的数据管理模式为参照，没有考虑到数字化转型背景下数据的开放性、共享性、动态性等特点。制度内容重在事后追责，缺少事前预防、事中控制的规定，不能形成全流程的风险防控体系。高校数据安全制度的制定缺少跨部门、跨领域调研论证，没有充分吸纳技术、教学、科研、管理等各方面的专业意见，制度的科学性、合理性有待提高。制度建设的滞后性、前瞻性不够，造成数据安全防控工作缺少有效的制度保障。

3.4 师生数据安全意识薄弱

师生数据安全意识薄弱属于造成高校数据安全风险的人为因素。高校师生是数据的主要生产者和使用者，他们的数据安全意识影响着数据安全防护的效果。部分师生对数据安全的重要性认识不够，在日常的工作学习中存在着很多不安全的行为。设置简单的账户密码、随意点击不明链接、违规共享敏感数据等，这些行为给数据安全风险的发生埋下了隐患。高校对于师生的数据安全教育培训缺乏，培训内容单一，缺少针对性、实用性，不能有效地提高师生的数据安全防护能力及意识。师生数据安全意识的薄弱，造成高校数据安全防线存在明显的人为漏洞。

4 数字赋能高校转型下的数据安全风险防控策略

4.1 构建适配的技术防护体系

创建合适的技术防护体系，是应对数据安全技术风险的主要办法。高校应加大技术研发和投入力度，使安全防护技术同数字化转型技术架构同步更新。从数据存储角度出发，对重要的敏感数据采用加密存储的方式，采用分布式存储、集中管理的方式保证数据存储的稳定性、安全性。使用区块链技术，依靠其去中心化、不可篡改的特点来完成数据全生命周期的溯源管理。数据传输时使用安全传输协议，对传输的数据进行加密、校验，防止数据被截获或者篡改。加强无线网络安全防护，安装入侵检测系统、防火墙，实现对网络传输行为的实时监控。另外高校要创建技术漏洞动态监测体系，定时开展信息系统安全扫描及漏洞修补工作，及时消除技术层面的安全隐患。

4.2 完善精细化的数据管理机制

建立精细化的数据管理机制，是解决管理层面的安全风险的有效方法。高校创建数据管理权责体系，对数据采集、存储、传输、使用等各个阶段中各个部门所承担的责任及权限进行明确界定，并将数据安全责任落实到具体的岗位和人员身上。根据数据的敏感程度和重要性把数据分为不同的级别，实行分类分级管理，采取不同的安全手段对不同等级的数据进行保护。加强数据采集环节的管理，按照最小必要原则，防止过度采集不必要的数据。优化数据权限管理机制，用基于角色的访问控制方式来控制数据访问权限，达到数据按需共享的目的。建立跨部门的数据安全协同管理机制，加强信息技术部门和其他部门之间的沟通协作，形成数据安全管理的合力。定期进行数据安全管理工作中的不规范行为进行纠正的审计工作。

4.3 健全动态化的制度保障体系

健全动态化的制度保障体系，是加强数据安全风险防控的重要保证。高校要根据数字化转型的实际需要，修订完善现有的数据安全管理制度，配套建立制度执行监督检查机制，定期核验制度落实情况，及时发现并纠正执行偏差，提高制度的针对性和可操作性。制定数据安全全生命周期管理制度，对数据从产生到销毁全过程的管理要求和操作规范做出规定，形成事前预防、事中控制、事后追责的全流程管理体系。建立数据安全责任追究制度，对由于管理不善造成数据安全问题的部门和个人进行严肃追责。健全数据安全应急处置制度，制定科学合理的应急预案，定期开展应急演练，提高高校应对突发数据安全事件的能力。建立制度动态更新机制，根据技术发展、转型进程的变化及时对制度内容进行修改完善，保证制度时效性、前瞻性。

4.4 强化全方位的人员素养培育

全方位人员素养培育是弥补人为漏洞、提高防控效果的重要途径。高校应该将数据安全教育纳入师生日常培训体系，开展多样化的、有针对性的培训活动。对教师群体主要进行科研数据安全管理、教学资源数据保护等知识技能的培训，对学生的群体主要进行个人信息保护、网络安全防范等常识的普及，对管理人员主要进行数据安全责任意识和管理能力的培训。创新培训方式方法，采取线上线下相结合的方式，以专题讲座、案例分析、实操演练等形式提高培训的趣味性和实用性。建立数据安全意识考核机制，将考核结果同师生的评优评先、管理人员的绩效考核挂钩，倒逼师生提高数据安全意识和防护能力。另外高校要引进和培养专业的数据安全人才，建立高素质的数据安全管理队伍，给数据安全风险防控提供人才支持。

5 结语

数字赋能给高校转型注入强大动力，但是也带来了严峻的数据安全问题。高校数据安全风险防控是项系统性、长期性的工作，要从技术、管理、制度、人员等各方面共同推进。本文通过对数字赋能高校转型的内涵、数据安全态势的梳理，对风险类型、成因进行分析，提出相应的防控策略，以期为高校创建科学完善的数据安全防护体系提供理论依据。在教育数字化的大背景下，高校只有不断加强数据安全意识，完善防控机制，提高防护能力，在保证数据安全的基础上，充分发挥数据要素的核心价值，才能实现高校的高质量发展。

参考文献：

[1] 赵丽莉，张震. 实践、困境与优化：我国数据出境安全风险防控制度分析[J]. 行政与法，2025,(12):51-65.

[2] 张晓东，刘晓彤. 公共数据授权运营的网络安全风险防控机制研究[J]. 无线互联科技，2025,22(17):94-98.

[3] 刘泽霖. 大数据安全下的企业财务风险防控[J]. 现代企业文化，2025,(06):19-21.

[4] 周斌，咸洁敏. 生成式人工智能与数据安全：技术融合与风险防控[J]. 网络安全和信息化，2025,(02):9-11.

[5] 苏子龙. 生成式人工智能的数据安全风险防控与法律规制研究[J]. 通信与信息技术，2024,(05):95-98+110.

基金项目：课题名称：数字赋能 - 职业院校数字化治理体系研究，课题编号：2024ZJJGGH14。

作者简介：刘克铜 (1982.03-)，男，山东省平邑县，本科，副教授，研究方向：大数据、数据安全。