大数据时代下档案信息安全管理的挑战与对策

李晔

卓资县纪律监察委员会，中国·内蒙古 乌兰察布 012300

摘要：大数据时代，档案信息安全管理呈现范围扩大、风险传导增强、时效性要求提高、安全与共享矛盾凸显的特征，其重要性愈发突出。本文从技术、管理、人员、法律法规与标准四方面，分析了存储传输漏洞、管理体系不完善、复合型人才匮乏、法规标准滞后等核心挑战，提出构建技术防护体系、健全管理流程、加强人才建设、完善法规标准等对策，为相关工作提供参考。

关键词：大数据；档案信息安全；安全挑战

Challenges and Countermeasures of Archives Information Security Management in the Era of Big Data

Li Ye

Zhuozi County Discipline Inspection and Supervision Commission, China Inner Mongolia Ulanqab 012300

Abstract: In the big data era, archival information security management exhibits four key characteristics: expanded coverage, heightened risk transmission, increased timeliness requirements, and intensified conflicts between security and sharing, highlighting its growing significance. This paper analyzes core challenges—including storage and transmission vulnerabilities, inadequate management systems, a shortage of interdisciplinary professionals, and outdated regulations and standards—from four perspectives: technology, management, personnel, and legal frameworks. It proposes countermeasures such as establishing technical protection systems, optimizing management processes, strengthening talent development, and improving regulatory standards to provide actionable references for related initiatives.

Keywords: Big data; Archive information security; Security challenges

0 引言

档案作为承载关键信息的核心资源，其安全直接关系到信息真实性与权益保障，而大数据时代的新型安全场景进一步加剧了管理难度。在此背景下，剖析档案信息安全管理的特征与挑战，探索科学有效的优化路径，是应对安全风险、推动档案管理现代化转型的必然需求，具有重要的实践价值。

1 大数据时代档案信息安全管理的特征与重要性

1.1 大数据时代档案信息安全管理的特征

大数据时代背景下，档案信息安全管理呈现出鲜明的时代特征。其一，安全管理范围显著扩大，突破了传统档案仅聚焦结构化数据的局限，将半结构化的档案流转日志、邮件往来，以及非结构化的音视频档案、图像档案等多类型数据全面纳入管理范畴，管理对象的复杂性大幅提升；其二，安全风险传导性明显增强，档案数据的采集、存储、传输、利用等环节形成紧密关联的链条，单个环节出现的安全漏洞如存储系统防护不足、传输加密缺失等，极易快速传导至全流程，引发系统性安全风险；其三，安全管理时效性要求持续提高，海量档案数据的实时产生与动态更新，对安全监测的响应速度提出更高要求，需实现对数据异常访问、违规操作等风险的即时识别与处置；其四，安全与共享的矛盾愈发凸显，大数据时代档案数据的共享价值被高度重视，跨部门、跨领域的共享需求日益增长，但这与档案信息的安全防护形成尖锐矛盾，如何在保障数据可用的同时筑牢安全防线，成为管理中的核心难题[1]。

1.2 大数据时代档案信息安全管理的重要性

档案信息安全管理在大数据时代具有不可替代的重要性。从档案自身属性来看，档案承载着机构发展历程、社会治理轨迹等关键信息，是具有凭证价值和参考价值的核心信息资源，其安全直接关系到信息的真实性与完整性，一旦出现安全问题，可能导致档案信息篡改、丢失，损害档案的原始凭证效力；从机构运营层面而言，规范有效的档案信息安全管理能够规避数据泄露、滥用等风险，避免因档案安全事故引发的法律责任、声誉损失和经济损失，保障机构各项业务的有序开展；从社会层面考量，档案信

息中往往包含个人隐私、公共利益相关数据，做好安全管理是维护信息主体合法权益、保障社会信息安全秩序的重要支撑，同时也是契合数据安全相关法律法规要求、推动档案事业健康可持续发展的必然前提[2]。

2 大数据时代档案信息安全管理面临的主要挑战

2.1 技术层面挑战

技术层面是大数据时代档案信息安全管理面临的首要挑战。一方面，海量档案数据的存储与传输环节存在显著安全漏洞，分布式存储架构虽提升了数据存储的灵活性与扩展性，但节点分散的特性增加了安全防护的难度，单个节点被攻击或出现故障都可能引发数据泄露；而数据在跨系统、跨部门传输过程中，若加密技术应用不到位、传输通道缺乏有效监管，极易被拦截窃取。另一方面，大数据技术自身存在安全缺陷，数据挖掘与分析过程中，对海量异构数据的整合处理可能无意识泄露隐含的个人隐私或敏感信息，算法设计中的漏洞则可能导致数据处理结果失真，甚至被恶意利用引发安全风险。此外，人工智能、云计算等新兴技术与档案管理的融合，虽提升了管理效率，却也带来了新的安全威胁，如云计算环境下的数据主权归属模糊、人工智能技术被用于批量破解档案访问权限等，如下图所示；传统安全防护技术更是难以跟上数据增长速度，难以实现对海量数据的实时监测与精准防护。

图1 新兴技术与档案管理融合中的安全风险示意图

2.2 管理层面挑战

管理层面的短板进一步加剧了档案信息安全风险。其一，安全管理体系不完善，多数机构尚未建立适配大数据环境的档案信息全生命周期安全管理流程，对数据采集的源头把控、存储阶段的分级防护、利用环节的权限管控以及销毁过程的安全监督缺乏系统性设计，导致安全管理存在诸多盲区。其二，安全管理责任划分不清晰，档案管理涉及多个部门，在大数据共享利用的场景下，容易出现权责交叉或责任真空的问题，一旦发生安全事故，难以明确责任主体，影响问题的快速处置。其三，安全管理制度更新不及时，现有制度多基于传统档案管理模式制定，难以覆盖大数据时代数据共享、跨境流动等新型安全场景，对新型安全风险的约束性不足。其四，应急响应机制不健全，针对数据泄露、系统瘫痪、恶意攻击等突发事件，缺乏完善的应急预案和高效的处置流程，导致事故发生后无法及时控制风险，扩大损失范围[3]。

2.3 人员层面挑战

人员层面的不足成为制约档案信息安全管理成效的关键因素。核心问题在于专业人才的匮乏，大数据时代的档案信息安全管理需要既精通档案管理专业知识，又掌握大数据技术、网络安全技术的复合型人才，而当前行业内这类人才储备严重不足，难以满足复杂的安全管理需求。同时，相关从业人员的安全意识普遍薄弱，对大数据环境下的新型安全风险认知不足，在日常工作中存在违规操作、密码管理松散等问题，人为制造了安全漏洞。此外，人员培训体系滞后，现有培训内容仍聚焦于传统档案管理技能，对大数据安全防护技术、数据安全法律法规等前沿内容覆盖不足，导致从业人员的专业技能无法匹配新时代档案信息安全管理的要求。

2.4 法律法规与标准层面挑战

法律法规与标准层面的滞后为档案信息安全管理带来诸多合规性挑战。在立法层面，针对大数据环境下档案信息安全的专项法律法规尚不完善，现有数据安全相关法律对档案信息的针对性不足，对档案数据泄露、滥用等行为的责任界定不清晰，处罚标准不明确，难以形成有效的法律震慑。在行业标准层面，缺乏统一的大数据档案信息安全标准，不同机构在数据采集、存储、共享等环节的技术规范、安全要求存在差异，导致数据跨领域、跨机构流通时存在安全壁垒，也增加了安全管理的难度。尤为突出的是，跨境档案数据流动的法律监管存在空白，随着全球化进程的加快，档案数据的跨境传输日益频繁，但目前缺乏明确的监管规则和安全评估机制，导致跨境档案数据流动的安全风险难以得到有效管控[4]。

3 大数据时代优化档案信息安全管理的对策

3.1 构建适配大数据的技术防护体系

为精准应对大数据时代档案信息安全管理的多元挑战，需从技术、管理、人才、法规标准四大核心维度构建协同发力的优化对策体系，各维度核心措施与实施目标的对应关系可通过下表清晰呈现（见表 1）。

表1 档案信息安全管理优化对策核心要素对应表

对策维度	核心措施	实施目标
技术防护体系构建	加密存储 / 区块链应用、智能安全监测、精细化访问控制、技术升级迭代	筑牢数据全流程技术防线，实现安全风险实时预警与精准防控
安全管理体系健全	全生命周期流程覆盖、责任体系厘清、制度动态更新、高效应急响应构建	实现管理规范化与精细化，提升安全风险闭环管控能力
人才队伍与意识培育	复合型人才协同培养、全员安全培训、人才激励机制建立	打造专业人才梯队，提升全员安全素养与风险防范能力
法律法规与标准完善	专项立法推进、行业标准统一、跨境数据监管健全	构建法治化、标准化管理环境，规避合规风险

构建适配大数据的技术防护体系是筑牢安全防线的核心支撑。在数据存储与传输环节，应全面采用高强度加密存储技术，结合区块链不可篡改的特性保障档案数据的完整性与保密性，同时优化传输加密协议，防范数据在跨系统流转中的泄露风险；针对海量数据的安全监测需求，需部署融合大数据分析与人工智能技术的智能监测系统，实现对异常访问、违规操作等风险的实时识别与预警；通过建立基于角色的精细化访问权限管理机制，明确不同岗位的访问范围与操作权限，并实现操作行为的全程追溯，从源头遏制内部安全隐患；此外，应加强与科研机构的产学研协同，持续推进安全防护技术的升级迭代，研发适配海量异构档案数据的新型防护技术，弥补传统技术的局限性。

3.2 健全大数据环境下的档案安全管理体系

健全大数据环境下的档案安全管理体系是提升管理效能的关键保障。需以档案数据全生命周期管理为核心，构建覆盖数据采集、存储、处理、传输、销毁等各环节的安全管理流程，明确各环节的安全管控要点与操作规范，实现安全管理的全链条覆盖；通过厘清档案管理部门、技术部门、业务部门等各主体的安全职责，建立跨部门协同管理机制，消除权责交叉或责任真空问题，确保安全管理责任落到实处；建立常态化的安全管理制度更新机制，结合大数据技术发展趋势与新型安全风险变化，及时修订完善管理制度，填补新型安全场景的管理空白；同时，构建高效的应急响应体系，制定针对数据泄露、系统瘫痪、恶意攻击等突发事件的分级应急预案，明确处置流程与责任主体，并定期开展应急演练，提升应急处置的实战能力[5]。

3.3 加强人才队伍建设与安全意识培育

针对复合型人才匮乏的问题，应建立高校、档案管理机构与科技企业协同培养机制，通过高校增设大数据档案安全相关专业方向、企业提供实践实训平台、档案机构开展在岗培训等方式，提升人才的档案管理专业素养与大数据安全技术能力；强化全员安全意识培育，定期组织开展大数据档案安全知识、操作规范及典型风险案例的培训，提升档案管理人员、业务人员等全员的风险认知能力，规范日常操作行为，减少人为安全隐患；建立健全人才激励机制，通过完善薪酬福利体系、搭建职业发展平台、表彰优秀安全管理成果等方式，吸引并留住优秀专业人才，激发人才的创新活力。

3.4 筑牢档案保密廉政防线

强化档案保密管理与廉政风险防控需贯穿全流程，对档案实行密级分级分类管控，涉密档案严格落实“专人保管、专柜存放、专册登记”要求，电子涉密档案采用脱网存储与加密防护技术，传递通过加密传真或机要渠道，查阅实行“双重审批 + 指定场所 + 全程留痕”，销毁履行报批、监销手续并留存记录；同时构建廉政风险防控体系，为档案管理人员建立动态廉政档案，常态化开展廉政警示教育与保密纪律培训，梳理档案查阅审批、数据修改、销毁等关键环节的廉政风险清单，在高风险操作前推送纪律提醒；健全纪检监察协同监督机制，由纪检监察部门与档案管理部门联合开展季度专项检查，搭建数据共享监督平台，对异常访问、违规操作等行为自动抓取比对，对失泄密、廉政违规行为实行“一案双查”，依规给予党纪政纪处分或移送司法机关，筑牢档案信息安全与廉洁管理防线。

3.5 完善法律法规与行业标准体系

加快推进大数据时代档案信息安全管理的专项立法进程，在现有数据安全法律法规基础上，进一步细化档案信息安全的责任界定、权利义务及处罚标准，为安全管理提供明确的法律依据；由行业主管部门牵头，联合科研机构与标杆单位，制定统一的大数据档案信息安全行业标准，明确数据采集、存储、共享、销毁等各环节的安全技术要求与管理规范，消除不同机构间的标准壁垒，提升行业整体安全管理水平；针对跨境档案数据流动的安全风险，健全跨境数据流动监管机制，建立跨境传输的安全评估体系与合规管理流程，明确跨境传输的适用范围、审批程序及安全保障措施，确保跨境档案数据流动的合法合规与安全可控。

4 结语

综上所述，大数据时代为档案信息管理带来机遇的同

时，也使技术、管理、人员、法规标准层面的安全挑战愈发突出。应对这些挑战，需构建“技术－管理－人才－法规标准”四位一体的协同优化体系，通过强化技术防护、健全管理流程、打造专业人才队伍、完善制度保障，全方位化解安全风险。唯有如此，才能平衡档案信息共享与安全防护的关系，保障档案信息的真实性与安全性，为档案事业高质量发展奠定坚实基础。

参考文献：

[1] 梁敏捷，秦爽. 数字化时代高校档案信息安全管理研究[J]. 山西档案，2025(06):137-139.

[2] 张娟. 信息安全视角下的档案管理风险识别与防控维度探析[J]. 兰台内外，2025(17):29-31.

[3] 郑熠. 人工智能在学校档案信息化管理中的有效应用[J]. 中国管理信息化，2025,28(11):174-177.

[4] 张静. 浅析城市管理局档案信息化建设中的安全防护策略[J]. 四川劳动保障，2025(10):36-37.

[5] 陈语. 信息化时代高校档案资源管理模式创新研究[J]. 兰台内外，2025(15):78-80.

作者简介：李晔（1981.04-），女，汉族，内蒙古自治区乌兰察布市卓资县人，毕业于福建师范大学，本科，中级，研究方向：主要从事档案管理方面研究。