大数据背景下事业单位档案管理工作优化策略研究

李永志

内蒙古自治区兴安盟扎赉特旗胡尔勒镇综合行政执法队，内蒙古自治区兴安盟，137600；

摘要：大数据背景下事业单位档案管理面临效率低、价值未释放、安全风险高等问题，为推动其从“被动保管”向“主动服务”转型，本文通过分析大数据对档案管理的效率重构、价值拓展、安全强化作用，剖析当前技术适配不足、制度不同步、人才不匹配、安全体系不健全的困境，进而从技术架构、制度保障、人才队伍、安全防护四维度构建优化策略。研究表明，所提策略可有效提升档案管数字化水平，为事业单位数字化改革提供支撑。

关键词：大数据；事业单位；档案管理；优化策略；数字化转型

DOI：10.69979/3041-0673.26.02.082

引言

档案作为事业单位记录履职过程、存储核心信息、支撑决策制定的关键资源，其管理水平直接关系单位运行效率与公共服务质量。随着大数据技术在政务领域的深度渗透，传统以纸质档案为主、人工管理为辅的模式，已难以适应海量档案数据的采集、存储、分析与利用需求。当前，部分事业单位虽启动档案信息化建设，但仍存在技术应用表层化、资源价值未释放、安全风险难管控等问题。在此背景下，系统分析大数据对档案管理的价值赋能，剖析实践困境并构建针对性优化策略，对推动事业单位档案管理从“被动保管”向“主动服务”转型，助力单位数字化改革具有重要意义。

1 大数据对事业单位档案管理的价值赋能

1.1 重构档案管理效率维度

传统档案管理依赖人工录入、手动分类、逐卷检索，耗时耗力且易因操作出错。大数据技术通过自动化采集与智能化处理，大幅提升档案管理全流程效率。一方面，借助 OCR 识别、智能表单将纸质档案转为结构化电子数据，还对接人事、财务、业务系统，实时抓取动态档案信息，替代传统“定期收集-人工录入”模式，减少90%以上重复劳动；另一方面，依托大数据检索算法，实现“多维度组合检索”，秒级定位档案，效率较传统提升数十倍，且操作日志可追溯轨迹，避免人工疏漏。

1.2 拓展档案资源价值边界

传统档案管理多停留在“保管”层面，档案资源静态存放，对决策、服务的支撑价值未充分挖掘。大数据技术通过深度分析与关联挖掘，将其从“静态资源”转化为“动态决策依据”。如人事档案中，分析员工学历、工作经历等数据构建人才能力模型，为优化岗位配置、制定培训计划提供支持；业务档案中，分析历年项目、服务记录，总结规律、识别薄弱环节，助力调整流程、提升服务质量。此外，跨部门档案整合可打破“信息孤岛”，如人事与财务档案关联，核查薪酬与绩效匹配度，提升管理规范性。

1.3 强化档案安全治理能力

档案安全是事业单位档案管理的底线，传统纸质档案面临虫蛀、火灾、丢失风险，电子档案则存在数据泄露、篡改隐患。大数据技术通过分布式存储、加密算法、实时监控等，构建更立体的安全防护体系。一方面，分布式存储将数据分散存于多节点，避免集中存储的“单点故障”，单个节点故障可通过其他节点恢复数据；另一方面，区块链“不可篡改”特性记录档案修改，任何改动都留可追溯痕迹，防人为篡改；同时，大数据监控实时分析访问行为，异常时自动预警、阻断风险，保障档案机密性与完整性。

2 大数据背景下事业单位档案管理的现实困境

2.1 技术架构与大数据适配性不足

部分事业单位档案管理技术架构未跟上大数据发展，存在“硬件滞后、软件单一、标准缺失”三重问题。硬件上，多数用传统服务器存储，未引入云存储、边缘计算，面对海量电子档案常存容量不足、读取慢问题；部分扫描仪老化且型号不统一，致纸质档案数字化格式乱、清晰度差。软件上，现有系统多仅“电子台账”功能，缺大数据分析、智能挖掘及跨系统对接能力，难联动业务与政务平台，且兼容性差，部门间数据难整合。标准上，无统一数据格式、编码与交换标准，如人事档案“工作经历”录入格式不一，无法跨部门关联分析，形成“数据孤岛”。

2.2 管理制度与数字化转型不同步

传统档案管理制度多围绕纸质档案制定，难适应大数据时代需求，存在“覆盖不全、权责不清、执行不力”问题。覆盖上，制度多聚焦档案收集、整理、保管，对数据清洗、智能分析、跨部门共享等新增环节缺规范，如未明确数据清洗标准、共享权限划分，操作随意。权责上，多数单位无专门大数据档案管理岗，传统档案员缺技术与协调权限，致工作“无人牵头、无人负责”。执行上，部分单位虽有信息化制度，但无配套监督考核，如“每月备份”无处罚，制度流于形式，常现备份不及时、数据丢失。

2.3 管理队伍与专业能力要求不匹配

档案管理人员专业能力是大数据技术落地关键，当前事业单位档案队伍存“结构老化、素养单一、培训不足”问题，难满足数字化转型需求。结构上，多数档案员年龄偏大，习惯传统管理模式，对大数据有畏难心理；年轻人员虽懂基础计算机，却缺档案专业知识与大数据分析能力。素养上，人员多掌握传统档案整理技能，缺数据清洗、算法应用等能力，无法处理海量数据或识别系统漏洞。培训上，多聚焦政策与传统流程，少涉大数据技术，且以线下讲座为主缺实战，培训效果不佳。

2.4 安全防护与风险防控体系不健全

大数据时代档案安全风险更复杂，涉及技术层面网络攻击、数据泄露与人为层面操作失误、恶意篡改，部分事业单位防护体系却存“技术薄弱、意识不足、预案缺失”问题。技术上，多数仅部署基础防火墙，缺进阶防护工具，难应对新型威胁；部分仅靠本地硬盘备份，易因灾害、设备故障致数据丢失。意识上，档案人员对安全重视不足，存在弱密码、违规拷贝发送档案等问题。预案上，多数无安全应急预案或内容笼统，事发后无法快速响应，导致损失扩大。

3 大数据背景下事业单位档案管理的优化策略

3.1 构建“云-边-端”协同的技术架构

技术架构是大数据档案管理的基础，事业单位需打破传统“单机存储+简单软件”的技术模式，构建“云平台存储、边缘端处理、终端设备采集”的协同架构，提升技术适配性。在“云平台”建设上，结合单位规模与档案数据量，选择“私有云+公有云”混合云模式：将敏感档案（如人事档案、涉密业务档案）存储于私有云，由单位自主管控，保障数据安全；将非敏感档案（如公开业务记录、宣传档案）存储于公有云，借助云服务商的算力与存储能力，降低硬件投入成本。同时，对接政务云平台，实现与其他政府部门、事业单位的档案数据互通，打破“信息孤岛”。在“边缘端”部署上，在档案数据产生节点（如业务部门、基层站点）部署边缘计算设备，对实时产生的档案数据（如业务系统日志、现场执法视频）进行预处理，筛选有效数据后再上传至云平台，减少数据传输量，提升处理效率。在“终端设备”升级上，统一配置高清扫描仪、智能采集终端（如带 OCR 功能的平板），实现纸质档案“一键数字化”，确保数字化档案格式统一、清晰度达标；为档案管理岗位配备高性能计算机，安装大数据分析工具（如 SPSS、Python 数据分析库），支撑档案数据挖掘与分析。此外，制定统一的档案数据标准，明确数据格式（如电子档案采用 PDF/A 格式、视频档案采用 MP4 格式）、编码规则（如档案编号采用“单位代码-年份-类别-流水号”）、交换协议（如采用 XML 格式进行跨系统数据交换），确保数据整合与共享顺畅。

3.2 建立全生命周期的制度保障体系

制度是档案管理规范化的关键，事业单位需围绕档案“采集-存储-分析-利用-销毁”全生命周期，构建覆盖全面、权责清晰、执行有力的制度体系。

在“采集环节”，制定《档案数据采集规范》，明确采集范围（如人事档案需包含学历、考核、奖惩等 12 类信息）、采集方式（系统自动抓取、人工辅助录入）、数据质量标准（如重复数据率≤0.5%、异常数据率≤0.3%），确保采集数据完整准确；建立“数据溯源机制”，记录每一条档案数据的来源、采集时间、采集人员，实现数据可追溯。在“存储环节”，出台《档案数据存储管理办法》，规范云存储、边缘存储、本地存储的分工，明确不同类型档案的存储期限（如人事档案长期存储、普通业务档案存储 10 年）、备份频率（敏感档案每日备份、非敏感档案每周备份），要求采用“异地备份+离线备份”双重备份模式，定期（每季度）检测备份数据完整性。

在“分析与利用环节”，制定《档案数据挖掘与共享细则》，明确数据挖掘的范围（如仅对非涉密档案进行分析）、工具（如指定使用单位统一部署的分析软件）、成果应用场景（如人才配置、业务优化）；划分档案共享权限，采用“分级授权”模式：单位领导拥有全权限，可查阅所有档案；部门负责人拥有部门内档案查阅权与跨部门非敏感档案查阅权；普通员工仅拥有本人相关档案查阅权，确保共享安全。

在“销毁环节”，制定《档案数据销毁规程》，明确销毁流程（申请-审核-监销-记录），采用“物理销毁

+逻辑销毁”结合方式，对纸质档案进行粉碎，对电子档案进行多次覆写，防止数据恢复，并留存销毁记录，确保可追溯。同时，建立制度执行监督机制，由单位纪检部门、办公室组成监督小组，定期（每半年）检查制度执行情况，对未按规范操作的部门与个人进行通报批评，将制度执行情况纳入绩效考核，提升执行力度。

3.3 打造“技术+管理”双驱的人才队伍

人才是档案管理优化的核心，事业单位需突破传统“单一技能”的人才培养模式，打造兼具档案管理专业知识与大数据技术能力的复合型队伍。

在“人才招聘”上，调整招聘标准，优先录用“档案学+计算机”“信息管理+大数据分析”等交叉专业毕业生，或具有大数据档案管理工作经验的人员；针对现有队伍，通过“内部竞聘”选拔具备学习能力的年轻员工，充实档案管理岗位，优化队伍年龄结构。

在“能力培养”上，构建“理论+实战”双轨培训体系：理论培训邀请高校档案学教授、大数据技术专家，讲解大数据档案管理理论、数据安全法规、智能系统原理；实战培训依托单位档案管理系统，设置“数据清洗实战”“智能检索操作”“安全漏洞排查”等实操课程，安排学员分组完成实战任务，由技术导师现场指导，提升实操能力。同时，与高校、大数据企业合作，建立“培训基地”，定期选派档案员参与进修，学习先进技术与管理经验。

在“激励机制”上，建立“技能认证+绩效奖励”激励体系：开展大数据档案管理技能认证，分为“初级（掌握基础操作）、中级（具备数据分析能力）、高级（能独立设计档案管理方案）”三个等级，认证通过者给予薪资上浮、岗位晋升优先等奖励；设立“档案管理创新奖”，对提出大数据应用创新方案（如档案智能分析模型、安全防护优化建议）并落地见效的人员，给予物质奖励与荣誉表彰，激发人才创新动力。

3.4 完善“技防+人防”融合的安全体系

安全是档案管理的底线，事业单位需构建“技术防护为核心、人员管理为基础、应急响应为保障”的融合安全体系，全面防控安全风险。

在“技术防护”升级上，分层部署安全工具：在“网络层”部署下一代防火墙、入侵检测系统（IDS）、入侵防御系统（IPS），抵御外部网络攻击；在“数据层”采用国密算法（如SM4）对敏感档案进行加密存储与传输，使用区块链技术记录档案修改轨迹，确保数据不可篡改；在“应用层”部署AI智能监控系统，实时分析档案访问行为，识别异常操作（如高频次查阅敏感档案、异地登录下载），自动触发预警（如短信通知管理员、暂时冻结账号）。同时，采用“三备份”模式：在线备份（实时同步至云平台）、离线备份（定期拷贝至专用硬盘，存放于异地保险柜）、冷备份（将核心档案刻录至光盘，长期封存），确保数据万无一失。

在“人员管理”强化上，开展常态化安全培训，每季度组织一次数据安全讲座，结合典型案例（如档案数据泄露事件）讲解安全风险与防范措施；每年开展一次安全实操考核，测试档案员对密码管理、加密操作、应急处置的掌握程度，考核不通过者需补考，直至合格。同时，建立“安全责任清单”，明确档案员、部门负责人、系统管理员的安全职责，签订《数据安全责任书》，将安全责任落实到人，对因个人操作失误引发安全事故的，依规追责。

在“应急预案”完善上，制定《档案安全突发事件应急预案》，明确突发事件分类（如数据泄露、系统瘫痪、自然灾害）、应急响应流程（预警-研判-处置-恢复-总结）、责任分工（如技术组负责系统修复、公关组负责信息发布）；每半年组织一次应急演练，模拟“系统遭DDOS攻击”“档案数据泄露”等场景，检验预案可行性，提升应急处置能力。

4 结论

档案管理是事业单位履职与服务的重要支撑，大数据技术为其革新提供了关键机遇，也带来了技术、制度、人才等层面的挑战。本文系统梳理了大数据对档案管理的价值赋能，明确了当前实践中的核心困境，并针对性提出“云-边-端”技术架构、全生命周期制度、复合型人才队伍、“技防+人防”安全体系的优化路径。这些策略的落地，可推动档案管理突破传统局限，充分释放档案数据价值，不仅能提升事业单位内部运行效率，更能为公共服务质量提升与数字化发展注入动力，助力事业单位实现高质量发展。

参考文献

[1]王芳.大数据时代事业单位人事档案管理创新的思考[J].兰台内外,2024(33):36-38.
[2]刘丽敏.大数据背景下创新事业单位人事档案管理的研究[J].办公室业务,2024(21):129-131.
[3]牛福厚.大数据背景下机关事业单位人事档案管理创新分析[J].兰台内外,2024(11):16-18.
[4]李昕.大数据时代事业单位人事档案管理创新思考[J].陕西档案,2024(1):39-40.
[5]王海燕.大数据背景下行政事业单位信息化档案管理探析[J].中国管理信息化,2024,27(2):206-208.