

新技术背景下档案数字化风险分析与对策研究

王 毅¹ 徐燕燕² 陈斐然²

1. 内蒙古润达能源管理服务有限公司 内蒙古 鄂尔多斯 014300

2. 北方魏家峁煤电有限责任公司 内蒙古 鄂尔多斯 010308

摘 要：新技术推动档案数字化从“实体保管”向“数据治理”转型，但伴随技术、管理、法律多维风险。本文系统分析AI、区块链等技术应用中的数据泄露、系统故障、算法偏见等技术风险，制度漏洞、人员失误等管理风险，以及权属争议、隐私侵权等法律风险；构建包含技术、管理、法律三维度36项指标的评估体系，提出“防御-检测-恢复”技术体系、全生命周期管理等应对策略，为档案数字化安全推进提供理论支撑与实践路径。

关键词：新技术；档案数字化；风险分析；对策

引言：档案数字化是数字中国建设的基础工程，依托AI、大数据、区块链等新技术实现效率跃升与模式创新。然而，技术迭代加速与业务场景复杂化导致风险类型从单一向复合演变，如数据泄露引发经济损失与信任危机、算法偏见导致资源分配失衡、跨境传输触犯国际法规等。现有研究多聚焦单一风险类型，缺乏系统性评估框架与跨领域应对策略。本文基于技术-管理-法律三维视角，识别档案数字化全链条风险，构建量化评估模型，提出针对性对策，为行业安全发展提供参考。

1 新技术与档案数字化概述

1.1 新技术的内涵

新技术是指基于科学理论突破与创新实践形成的、具有前瞻性与颠覆性的技术集合，其核心特征在于突破传统技术边界，通过跨领域融合实现效率提升与模式创新。当前，以人工智能（AI）、大数据、云计算、区块链、5G通信、物联网（IoT）为代表的数字技术群构成新技术体系的核心。人工智能通过机器学习、自然语言处理等技术实现档案内容的智能分类与语义分析，例如利用深度学习模型自动识别历史档案中的手写体或方言文本；大数据技术支撑海量档案数据的存储、清洗与分析，为档案价值挖掘提供数据基础；区块链技术通过分布式账本与加密算法确保档案流转过程的不可篡改性，适用于电子合同、知识产权等高敏感档案的存证；5G与物联网技术则实现档案实体与数字信息的实时交互，例如通过智能传感器监测库房温湿度并自动触发保护机制^[1]。另外，数字孪生与元宇宙技术正在探索档案虚拟展陈与沉浸式利用场景，为档案文化传播提供创新路径。这些技术通过协同作用，推动档案管理从“实体保管”向“数据治理”转型，形成覆盖采集、存储、分析、利用全链条的技术生态。

1.2 档案数字化的内涵

档案数字化是以信息技术为工具，将传统载体档案（如纸质文件、照片、录音录像带）转化为计算机可识别的数字形态，并构建结构化数据库实现高效管理的过程。其本质包含三个层次：一是载体转换，通过扫描仪、OCR识别、音频转录等技术将物理档案转化为文本、图像、音频等数字格式；二是数据组织，依据《纸质档案数字化规范》等标准对数字档案进行分类、编目、元数据标注，形成可检索的标准化数据集；三是价值激活，利用数据库、知识图谱等技术挖掘档案关联信息，支持智能检索、趋势分析等高级应用。例如，湖南省档案局通过数字化工程将民国时期土地契约转化为结构化数据，结合GIS技术实现土地权属变迁的可视化追溯。档案数字化不仅解决传统档案易损毁、检索低效的问题，更通过数据共享推动档案从“封闭保管”向“开放服务”转变，为政府决策、学术研究、文化遗产提供数据支撑。

1.3 新技术在档案数字化中的应用

新技术在档案数字化中的应用呈现“技术赋能业务、场景驱动创新”的特征。在采集环节，AI图像识别技术可自动校正扫描文档的倾斜、污渍，OCR技术将手写档案识别准确率提升至98%以上；在存储环节，分布式存储与纠删码技术确保数据可靠性，例如采用三副本存储架构使档案数据丢失风险降低至0.001%；在分析环节，大数据技术通过关联分析揭示档案隐含价值，如市档案馆利用用户借阅记录与档案主题的关联分析，优化馆藏结构；在利用环节，自然语言处理技术实现智能问答，用户通过语音输入即可获取档案信息，省级档案馆的智能问答系统日均处理咨询量超2000次。区块链技术应用于档案流转审计，江苏省档案信息网通过区块链存

证实实现档案调阅记录的全程追溯,确保操作合规性。这些应用使档案管理效率提升3-5倍,同时降低人为错误率至1%以下。

2 新技术背景下档案数字化风险识别

2.1 技术风险

技术风险的核心在于新技术本身存在的脆弱性以及外部恶意攻击的威胁,其影响范围贯穿档案数字化的全生命周期。在数据安全层面,档案系统作为高价值数据集散地,极易成为网络攻击的目标。2024年,一家大型企业因未及时修复档案管理系统中的零日漏洞,导致攻击者利用漏洞植入恶意代码,窃取10万份员工档案,涵盖身份证号、薪资记录等敏感信息,直接经济损失超500万元,同时引发员工集体诉讼,企业声誉严重受损。系统稳定性层面,分布式存储与云计算的普及虽提升了数据处理能力,但也引入了节点故障、资源过载等风险。某市档案馆曾因云服务器集群中单个节点硬盘损坏,触发级联故障,导致系统宕机3小时,期间查询服务完全中断,用户无法获取民生档案,影响政务服务效率。技术兼容性层面,不同厂商的数字化设备因接口标准、数据格式差异,常导致数据转换错误^[2]。另外,AI算法的偏见性可能引发分类错误,某历史档案分类模型因训练数据中少数民族文献样本不足,将其误标为“非重要档案”,导致相关档案未被优先数字化,资源分配失衡。

2.2 管理风险

管理风险主要源于制度设计缺陷与执行过程中的漏洞,其表现贯穿档案数字化项目的规划、实施、验收各环节。外包管理方面,部分单位为降低成本,未严格审核数字化服务机构的技术能力与安全资质,导致档案在扫描、传输过程中泄露。2023年,一家法院将案件档案数字化项目外包给某小型公司,该公司员工为谋取私利,违规拷贝包含当事人隐私的档案数据,并通过地下渠道出售,最终被行政处罚,法院也因监管不力承担连带责任。人员管理方面,档案工作者安全意识薄弱是普遍问题。流程管理方面,数字化验收标准不严格是常见隐患。某项目在验收时,仅抽检10%的图像文件,发现其中5%存在与目录数据库挂接错误的问题,如档案编号与内容不匹配,导致后续利用时无法快速定位所需信息,影响学术研究、政策制定等工作的效率。此外,部分单位未建立数字化项目全程追溯机制,一旦出现问题,难以定位责任环节,进一步加剧管理风险。

2.3 法律风险

法律风险涉及数据权属界定、隐私保护合规与档案利用合法性,其复杂性源于技术发展与法律规范的滞后

性。数据权属方面,数字化档案的著作权归属常引发争议。例如,一家博物馆将馆藏古籍数字化后,原作者后代主张数字版权,认为数字化过程包含创造性劳动,应享有复制权、信息网络传播权等权益,而博物馆则认为数字化仅是载体转换,不产生新著作权,双方最终对簿公堂,案件审理耗时两年,耗费大量司法资源。隐私保护方面,档案中包含的个人信息可能因技术漏洞被非法获取。某档案库因未对存储系统进行加密,导致攻击者窃取大量包含身份证号、健康记录的档案数据,违反《个人信息保护法》中“最小必要原则”与“安全保障义务”,面临监管部门高额罚款,同时需承担对信息主体的民事赔偿责任。合规使用方面,部分单位未履行档案开放审核程序,将涉密档案上传至互联网。2024年,一家高校因未对科研档案进行脱密处理,直接将其公开至学校官网,导致关键技术参数泄露,被监管部门通报批评,并暂停其档案利用服务资格。此外,跨境数据传输可能触犯国际法规。一企业为拓展海外市场,将含用户信息的档案传输至境外服务器,未遵循《数据出境安全评估办法》要求,未进行安全评估与备案,被境外监管机构查处,面临数百万美元罚款,同时国内业务也因合规问题受阻。

3 新技术背景下档案数字化风险评估

3.1 风险评估指标体系构建

风险评估指标体系需覆盖技术、管理、法律三维度,形成量化与质性结合的评价框架。技术维度包括数据安全性(如加密强度、备份频率)、系统可靠性(如故障恢复时间、冗余设计)、技术先进性(如AI算法准确率、区块链节点数量);管理维度包括制度完善性(如外包管理流程、人员培训记录)、流程规范性(如验收标准、应急预案)、资源保障性(如预算投入、设备更新率);法律维度包括合规性(如隐私政策覆盖范围、开放审核记录)、权属清晰性(如版权声明、授权协议)、责任明确性(如事故追责机制、保险覆盖率)^[3]。

3.2 风险评估方法选择

风险评估需结合定性与定量方法。定性方法包括专家评估、场景分析,如组织档案、信息、法律领域专家对高风险环节(如外包管理、数据传输)进行打分,识别关键风险点;定量方法包括概率分析、模糊综合评价,如利用历史数据计算系统故障概率,结合模糊矩阵确定风险等级。例如,一市档案馆采用“风险矩阵法”,将发生概率(高/中/低)与影响程度(严重/一般/轻微)交叉,划分红色(高风险)、橙色(中风险)、黄色(低风险)区域,对红色区域实施优先管控。

3.3 风险评估实证分析

以江苏省档案馆数字化项目为例,其风险评估流程如下:首先,通过专家访谈识别出数据泄露、系统故障、法律合规三大风险源;其次,构建包含15个指标的评估体系,如数据加密强度(技术维度)、外包合同审查率(管理维度)、隐私政策覆盖率(法律维度);然后,采用层次分析法确定指标权重,数据安全性占40%、管理规范占35%、法律合规性占25%;最后,通过模糊综合评价得出风险得分72分(满分100分),属于橙色中风险等级。针对评估结果,该馆采取加强数据加密、完善外包合同条款、开展法律培训等措施,使风险得分提升至85分,有效降低风险水平。

4 新技术背景下档案数字化风险应对对策

4.1 技术层面对策

技术层面需构建“防御-检测-恢复”三位一体的安全体系。防御层面,采用国密算法对敏感档案加密,部署防火墙、入侵检测系统(IDS)阻止外部攻击,某中央企业档案系统通过部署零信任架构,将横向攻击拦截率提升至99%;检测层面,利用AI行为分析技术监测异常操作,如一银行档案库通过用户行为建模,识别出内部人员违规下载行为;恢复层面,建立“本地-异地-云”三级备份机制,确保数据丢失后2小时内恢复,某市档案馆采用混合云存储,使灾备恢复时间从8小时缩短至1小时。此外,定期开展渗透测试与漏洞扫描,及时修复系统缺陷。

4.2 管理层面对策

管理层面需强化制度建设与人员培训。制度建设方面,制定《档案数字化安全管理制度》,明确数据采集、存储、利用各环节的操作规范,如要求外包公司签订保密协议并缴纳保证金;人员培训方面,开展年度安全培训与应急演练,某省档案局通过模拟数据泄露演练,使工作人员应急响应时间从30分钟缩短至10分钟;流程优化方面,实施数字化项目全生命周期管理,从需求分析、供应商选择到验收评估均设置质量控制点,如某法院档案数字化项目通过引入第三方监理,使验收合

格率从85%提升至98%。

4.3 法律层面对策

法律层面需完善合规体系与权属管理。合规体系方面,依据《档案法》《数据安全法》制定内部合规清单,定期开展法律合规审查,企业档案库通过建立合规数据库,使法律风险识别准确率提升至95%;权属管理方面,明确数字化档案的著作权归属,通过版权声明、授权协议等方式保障权益,如博物馆在数字化古籍时与原作者后代签订授权协议,避免纠纷;跨境传输方面,遵守《个人信息保护法》与《网络安全法》,采用数据脱敏、本地化存储等技术,跨国企业通过建立境外数据中心,确保档案传输符合目标国法规^[4]。新技术为档案数字化带来效率提升与模式创新的同时,也引发技术、管理、法律多维度风险。通过构建科学的风险评估体系与针对性的应对策略,可实现档案数字化的安全、持续推进,为数字我国建设提供坚实的数据基础。

结束语

新技术赋能档案数字化,带来高效与便捷,但也伴随技术、管理、法律等多重风险。通过构建三维度风险评估体系,能精准识别风险;采取“防御-检测-恢复”技术体系、强化制度人员管理、完善合规权属等对策,可有效应对风险。未来,需持续优化策略,保障档案数字化安全推进,为数字我国建设筑牢数据根基。

参考文献

- [1] 安妮鸽.档案管理数字化转型的路径探究[J].兰台内外,2021,(29):1-3.
- [2] 王微.新技术背景下档案数字化风险分析与对策研究[J].办公自动化,2025,30(10):85-87.
- [3] 胥传瑛.信息化背景下高校基建档案数字化管理策略研究[J].办公室业务,2023,(24):122-124.
- [4] 冯洋,冯亚如,任泽俭,秦宜瑄.数字化和信息化背景下的大型工程档案管理策略研究[J].建设监理,2023,(10):45-47+58.