 DOI: https://doi.org/10.12345/daglyqyfzyj.v3i6.28352

Security and confidentiality risks and countermeasures faced in the process of archive digitization in the AI era

Lijun Zhou[1*] Yifan Zhang[1] Yuxin Zhan[1] Xiaochen Shen[2*] Yuanpeng He[1*]

1. Hubei Institute of Aerospace Chemical Technology, Xiangyang, Hubei, 441003 China

2. Hubei Sunvalor Power Source Aerospace Tech Co., Ltd, Xiang yang, 441003 China

Abstract

This article focuses on the current booming development of AI technology, starting from the perspective of security and confidentiality risks in the entire process of archive digitization, it conducts in-depth analysis of risk points such as source information classification, security technology protection, business process control, and global personnel management. It aims to provide solid theoretical support and practical guidance for information security protection in the field of archive digitization, effectively prevent and resolve potential security and confidentiality risks in archive digitization work under the background of digitalization and intelligence, and safeguard state secrets and work information security.

Keywords

AI era; digitalization of archives; security and confidentiality

AI 时代档案数字化过程中面临的安全保密风险与对策

周力军[1*] 张一帆[1] 詹雨欣[1] 沈晓琛[2*] 何源鹏[1*]

1. 湖北航天化学技术研究所，中国·湖北 襄阳 441003

2. 湖北三沃力源航天科技有限公司，中国·湖北 襄阳 441003

摘　要

本文聚焦于AI技术蓬勃发展的当下，从档案数字化全过程存在的安全保密风险角度出发，通过对源头信息分类、安全技术防护、业务流程管控和全域式人员管理等风险点深入分析，旨在为档案数字化领域的信息安全保障提供坚实的理论支持与实践指导，有效防范化解数字化与智能化背景下档案数字化工作中潜在的安全保密风险隐患，维护国家秘密和工作信息安全。

关键词

AI时代；档案数字化；安全保密

1 引言

在数字化与智能化迅猛发展的 AI 时代，通过“数智融合”推动档案工作数字化转型已成为档案信息化发展的必由之路 [1]。在政策与档案数字化需求双重牵引下，AI 所表现出的自主学习、数据整理、智能决策等能力正在不断驱动档案数字化工作革新发展。然而，与之相伴的是档案数字化失泄密事件的发生，这将对国家安全、社会稳定，甚至国家形象造成严重影响。因此，本文对 AI 时代下档案数字化工作中潜在的安全保密风险隐患分析，提出针对性应对策略，从而确保国家秘密和工作信息安全 [2]。

2 档案数字化领域安全保密风险凸显

近年来，档案数字化工作中安全保密违规行为时有发生，主要风险点在于源头信息分类、安全技术防护、业务流程管控和全域式人员管理等方面。

2.1 档案信息精准合理分类不够

在基于大模型、大数据、大算力等人工智能技术应用过程中，需要海量数据支撑，其中包括个人隐私、商业秘密、工作秘密乃至涉及国家安全的敏感信息等。在数字档案资源管理领域，若缺乏档案信息分级分类机制或现有管理机制和技术防控体系不健全，极容易造成信息泄露，导致知悉范围扩大风险。且大量的工作秘密或敏感信息被收集汇聚分析后，会产生高价值的情报信息，可能对国家安全造成潜在危害，带来档案信息安全保密风险。

2.2 安全技术防护欠缺

数字化档案资源依托于档案管理系统平台实现全生命周期管理，档案数据安全取决于管理系统安全防护体系和网络建设。过去，网络安全技术迭代更新较为缓慢，在 AI 时代，强大的计算、分析、处理和持续学习能力加剧了信息系统、

【作者简介】周力军（1996–），男，中国陕西咸阳人，硕士，工程师，从事保密管理研究。

数据库和应用系统安全防护难度，安全监测、主动预警能力建设面临巨大挑战。档案管理系统平台等多个网络互联互通的信息化综合平台广泛应用，为数字档案高效安全运行提供了便利，同时伴随着“边界防护措施”失效风险，多重网络互联开放的大量服务端口，面临多样且复杂化的网络攻击方式，网络安全“木桶效应”将会给档案信息安全保密风险防范带来极大难度。

2.3 业务流程管控不严

近年来，档案数字化工作中产生的失泄密事件反映了业务工作中全过程保密监管不严、安全保密制度不健全以及管理措施落实不到位等问题，主要表现在从事档案数字化工作的公司不具备保密资质、驻场服务物防技防措施欠缺等方面 [3]。委托单位主体责任意识不强，对档案数字化工作中安全保密风险认识和审查监管重视不够，极大增加了档案数字化全过程安全保密风险隐患。

2.4 驻场服务人员监管不力

为满足档案数字化工作需要，提升档案资源管理水平，越来越多的单位委托档案数字化加工企业开展服务外包工作。部分委托单位安全保密责任意识欠缺，对档案数字化工作中安全保密管理缺乏指导、监督和跟踪，驻场服务人员保密教育监管存在盲区，因此安全保密漏洞隐患突出，窃取涉密数字档案的违法行为时有发生。

3 安全保密风险防控体系建设迫在眉睫

3.1 档案信息精准合理分类提升源头防控水平

为有效防范 AI 时代档案数字化过程中面临的安全保密风险，首先应从源头做好档案信息分类，精准且合理的档案信息分类能够为制定差异化的安全保密风险防控策略提供便利条件 [4]。除国家秘密绝密、机密、秘密分类外，企业或单位应结合实际制定内部动态信息分类标准，降低档案信息密级界定模糊或信息汇聚导致的内部或敏感信息泄露风险。同时，加快与量子加密、区块链等新兴技术融合，构建多层次、多维度、智能化的档案信息分类体系，有效提升档案信息源头管理能力，为档案信息安全保障提供坚实有力的支撑。

3.2 技术赋能助力档案数字化安全保密风险防范能力

加强档案工作数字化转型顶层设计与安全保密管理深度融合，在规划、建设、使用、维护全流程各环节充分考虑安全保密要求，定期开展安全保密风险隐患评估。建立健全档案管理系统安全预警机制。提升档案管理系统安全技术智能化水平，实现在 AI 环境下身份识别、权限控制、资源管控功能，确保数字档案管理安全保密风险可控。提高档案管理系统智能监测和预警能力，利用深度学习和机器学习算法，对系统运行、用户行为进行实时监测和分析，主动识别用户异常行为和潜在威胁。提高档案管理系统自动化响应处理水平，建立基于 AI 的自动化防御系统，发现威胁后迅速决策并采取响应措施。深化风险预警信息共享机制，利用人工智能、大数据、云计算等前沿技术，以安全保密风险为导向，建立合规高效的安全保密风险预警、研判和处置系统，既优化资源配置，又提升档案管理系统风险应对能力，形成系统化、体系化的协同联防体系。

3.3 规范业务流程监管突出“技管并重”

坚持“软硬兼施”和“技管并重”原则，在持续夯实档案信息安全技术管理“硬基础”同时，不断增强安全保密政策保障、制度建设、以及业务领域监管“软实力”。健全数字档案安全保密管理机制，严格安全保密管理制度刚性执行以及档案信息设备及信息系统管理要求落实，避免对驻场服务人员失管失控等低层次事件发生，确保档案信息安全保密管理体系有效运行，维护档案管理系统、网络与数字档案信息安全。加强档案工作数字化转型事前事中事后安全保密风险监管，明确各方责任界面，将安全保密监督检查融入数字档案管理业务流程。

3.4 全域式人员保密管理支撑档案管理人才队伍建设

在抓好档案管理从业人员安全保密教育的同时，要加强外协外包等体制外聘用人员和外包单位驻场服务人员全域式保密管理。档案数字化失泄密案件的发生暴露出委托单位对档案数字化工作中的安全保密风险隐患辨识不到位，缺乏对驻场服务人员保密教育、审查和监管，“人防”措施落实打折扣等问题。因此，一方面要提高档案管理从业人员对新型安全保密风险综合分析与防范能力，另一方面要加快档案管理领域 AI 专业技能和管理人才培养，着力打造一支政治素质高、管理能力强、技术水平高的复合型档案管理人才队伍。

4 档案信息安全发展趋势分析

4.1 风险来源愈发多样

随着 AI 时代档案信息安全领域加速演变，档案信息安全将面临数智化转型带来的新挑战。既有档案管理从业人员或服务外包人员违规违法行为、档案管理体系或制度存在漏洞等因素造成的内部风险以及档案信息化设施设备物理安全防护不到位、档案管理系统遭受网络攻击等外部风险，同时，也面临着信息犯罪、隐私泄露、版权侵犯等新型安全风险 [5-6]。

4.1.1 人员管理风险

一方面，档案管理从业人员可能因管理疏漏或操作失误等无意行为造成档案信息外泄。另一方面，个别人员道德品质缺失、安全保密意识淡薄导致主动违规违法行为仍有发生。此外，对外包驻场服务人员监管不到位也会造成严重的信息安全隐患。对此，应从技术和管理两方面统筹考虑，持续强化档案信息全生命周期安全防护监管，同时做好全域式人员保密管理。

4.1.2 体系管理风险

为适应日益严峻复杂的网络安全形势，应从体制机制层面强化档案信息安全风险防范措施，构建系统化、规范化

的档案信息安全管理体系。持续完善顶层设计，加强档案信息安全责任体系建设，统筹策划档案信息安全重点工作任务，健全档案信息安全管理制度，明确档案信息安全管理职责，建立可操作性强的监督检查和考核机制。

4.1.3 基础设施设备风险

档案信息设施设备稳定是档案信息安全的必要条件。人员误操作、设备失窃、人工电磁干扰等人为因素和地震、火灾、洪水等不可抗力因素是档案信息安全管理面临的潜在风险隐患。为充分应对上述风险，应做好软硬件基础设施设备物理安全防护，加强防灾应急体系建设，推动基础设施设备风险防控关口前移，减少因基础设施设备物理风险导致的档案信息安全事件发生。

4.1.4 网络安全风险

随着大数据、云计算、物联网等技术在档案管理过程中的广泛应用，诸如黑客勒索、病毒攻击、数据窃取等网络信息安全事件频发，档案信息安全形势日益严峻。上述各类威胁因素可通过互联网导致档案管理系统瘫痪、信息设备损坏，从而使重要数字档案信息受损或丢失，造成难以挽回的损失，网络攻击、勒索软件病毒等攻击方式尤为广泛。此外，网络安全“边界防护措施”“木桶效应”应重点关注，要及时升级完善边界防护体系，加强风险因素动态感知和预警信息共享。

4.2 网络攻防对抗体系更加健全

以 ChatGPT、DeepSeek 等大语言模型为代表的生成式 AI 的迅猛发展正在建立起新的网络对抗体系，将网络安全攻防对抗推向了一个前所未有的新高度。AI 时代，攻击者可以利用 AI 实现精准、自动化的攻击，而防御方也能借助 AI 构建更智能、高效的安全防护体系。要实现档案管理系统基于 AI 的自动化防御功能，档案管理从业人员应积极拥抱 AI 并做好准备，既要提高对新型 AI 攻击方式辨识与防范能力，也要加强档案管理团队 AI 技术培训，确保在面对新型 AI 攻击时能够快速响应、有效处置。

4.3 政策引导更加完善

近年来，《中华人民共和国档案法实施条例》《电子档案管理办法》《推进机关数字档案室建设实施办法（试行）》等法规的出台，进一步规范化、制度化档案管理数字化转型进程中电子档案的管理，为确保档案信息化建设提供了法律制度基础，数字档案室建设也已由试点阶段进入常态化推进阶段。可以预见的是，在新一轮科技革命的时代浪潮中，推进数字档案建设，确保档案信息安全是落实“数字中国”战略部署和“数字政府”建设的重要抓手，档案安全主题政策文件相继出台，也将持续为确保档案安全提供坚实保障，为贯彻落实总体国家安全观提供有力支撑 [7]。

5 结语

立足于 AI 时代，从档案数字化全过程存在的安全保密风险视角出发，分析了档案数字化工作中日益增长的安全保密风险。结合大模型、大数据、大算力等人工智能领域新技术，提出构建人防、物防、技防多维度档案信息安全保密防控体系目标。展望档案信息安全未来发展趋势，以提高档案信息安全综合管理水平为出发点，为构建 AI 时代档案数字化领域安全保密新生态提供坚实有力的理论支持与实践指导，为维护国家秘密和工作信息安全保驾护航。

参考文献

[1] 刘思宇.事业档案管理工作对企业发展的重要性研究[J]. 新时代论坛, 2024, 1(2)

[2] 张晓峰.信息安全视角下的档案管理策略研究[J]. 信息与电脑,2021, (6): 34-37.

[3] 王瑞.数字化转型背景下档案信息安全问题分析[J].黑龙江档案,2024,(04):25-27.

[4] 刘建萍.机关事业单位档案管理效能提升策略分析[J]. 档案管理与企业发展研究, 2024, 2(9)

[5] 陈熙满.档案信息安全体系建设风险对策调查与研究[J].中国档案,2025,(01):34-35.

[6] 李晓莉.档案信息安全，筑牢隐私保护防线[J].云端,2025,(11):84-86.

[7] 王照林.国家安全观视域下档案信息安全风险管控研究[J].兰台世界,2025,(05):106-108.