

档案管理中隐私保护与信息利用的平衡机制构建研究

刘彦麟

衡阳华南出版装璜彩印有限公司, 中国·湖南 衡阳 421600

摘要: 在数字化背景下, 档案信息载体的迭代和使用需求不断增加, 使得网络环境下的数据隐私和数据使用之间的矛盾日益突出。在此基础上, 工作人员需要依据风险管控的全过程逻辑, 结合公众利益和隐私的相关概念, 建立起一套科学的平衡机制, 这样不仅符合法律对个人隐私保护的刚性需求, 也能有效发挥文件信息的公众价值。

关键词: 档案管理; 隐私保护; 信息利用; 平衡机制

Research on the construction of a balanced mechanism between privacy protection and information utilization in archive management

Liu Yanlin

Hengyang South China Publishing Decoration and Color Printing Co., Ltd., China Hunan Hengyang 421600

Abstract: In the context of digitalization, the iteration of archival information carriers and the increasing demand for their use have made the contradiction between data privacy and data usage in the network environment increasingly prominent. Based on this, staff members need to establish a scientific balancing mechanism based on the whole-process logic of risk management and control, combined with relevant concepts of public interest and privacy. This not only meets the rigid legal requirements for personal privacy protection but also effectively leverages the public value of document information.

Keywords: Archive management; Privacy protection; Information utilization; Balance mechanism

0 引言

在建立档案管理隐私保护与信息利用平衡机制的时候, 需要工作人员基于信息生命周期、隐私和公共利益等相关理论展开思考, 分析隐私与利用冲突的产生机理, 明晰合法合规和动态适应性的均衡逻辑。这样不仅可以充实和完善档案管理效率, 构建个人隐私保护领域的学科体系, 还能有效弥补现有制度研究中的缺陷, 能够有效解决当前“保护过度”和“利用不足”之间的矛盾, 切实促进我国档案信息和个人隐私权利的协调保障。

1 法律规制机制: 明确平衡制度边界

1.1 完善法规衔接细则

为解决档案隐私保护方面存在的问题, 需要建立专门的执行细则, 以确定档案中关于“隐私信息”的界定标准, 需要涵盖个人身份信息、财产信息、健康信息等敏感信息, 并以公共健康应急、重大历史研究等为重点, 提出特殊情况下的利用豁免标准。还需要对档案的隐私保护进行规范化处理, 包括脱敏处理、信息留存时限、跨部门共享等隐私控制需求, 以保证不同层级的档案主管部门在执行过程中不会出现模糊地带, 并为档案信息使用划出明确的法律

界限。

1.2 建立分级授权制度

根据档案信息的保密程度不同, 需要建立一个多层次的权限制度, 将档案分为高、中、低三个敏感级别。首先是高敏感档案, 如个人医疗档案和涉密人事档案, 需以信息主体书面授权为核心授权依据, 还要经过档案管理部门的双重审查。其次是敏感档案, 如一般企业经营档案和非涉密行政档案, 档案主管机关应根据使用用途对档案进行核准, 并确定使用时限和使用范围。对于低敏感档案, 如历史档案和与个人无关的公务文件, 可以通过网上的实名认证获取访问权限。

1.3 设定争议解决路径

为了能够在发生纠纷的时候可以顺利解决, 则需要建立档案隐私利用纠纷的专业裁决机构, 建立档案管理专家、隐私保护法学学者和伦理审查专家组成的仲裁机构, 对纠纷的受理范围进行界定, 包括当事人对不当使用的异议、使用单位对权利的投诉等。要按照“高效透明”的原则, 从提交申请、审核材料到现场论证、出具结果, 都要有一个清晰的时间框架, 并对仲裁结果进行监管, 保证档案管

理部门和使用单位能够及时做出相应的反应。同时,还需要建立纠纷协商渠道,对纠纷当事人进行事前的法律指引,简化不必要的仲裁程序,以专业化和规范化的方式解决个人隐私和信息使用之间的矛盾,保障当事人的权利^[1]。

2 技术支撑机制: 协同保护利用关系

2.1 动态脱敏技术

动态脱敏技术需依托档案分类分级结果才可顺利使用,需要在此基础上构建场景化脱敏规则库,根据利用主体身份与利用目的自动调整脱敏强度。如针对学术科研背景下的敏感文件,仅对姓名、身份证号等关键信息进行局部隐藏,并对其进行可视化脱敏。针对高灵敏度的政务核实情景,需要在保持重要商业记录的基础上,实现对身份的全部身份信息的全量脱敏。在此基础上,还需要对加密后的信息进行实时验证,并利用算法对其进行验证,防止由于过度脱敏而造成信息丢失,或者由于不够敏感而造成信息泄露,从而达到“防护程度适合场景,信息价值不损失”的联合效应。

2.2 智能访问技术

智能访问技术需要建立角色、情景、授权的三重验证模式,首先,依据使用对象的职业角色对基本授权范围进行设置,并将其与线下档案查阅、远程访问、跨部门分享等实际使用情景相融合,实现对用户的授权界限的动态调节,然后,通过对用户的操作IP、访问周期、常用操作习惯等进行验证。在此基础上,将实时许可验证模型嵌入到该模型中,在使用者试图进行超越其使用权限的动作,如下载高敏感文件、批量拷贝未经许可的文件时,将会被自动拦截,并引发警报,并将其与异常行为的日志进行同步。同时,还需要在技术上实现授权的暂时调节,以满足突发事件的需要,可以通过批准程序暂时开启特殊文件的存取,以满足安全和突发事件的需要^[2]。

2.3 区块存证技术

区块链存证技术需要涵盖档案利用的整个过程,将重要的资料如使用主体身份、存取时间、操作内容、档案编号等转换到区块链的节点上,以分布的方式来保证资料不被篡改,并使用密码算法来保护凭证的隐私。该技术需要具有可追溯性,一旦发生个人信息泄露,可以通过区块链的节点逆向回溯使用链,精确地找到相关责任人。对于使用中的文件,审批记录,权限调整记录等,都需要同时录入到区块链中,从而构成了一个可追踪的闭环。另外,还需要将区块链存储的数据与文件管理平台进行实时连接,保证每次使用行为均可及时产生证据,为用户的个人隐私

和信息使用合法性提供可证实的证据。

2.4 隐私计算技术

隐私计算技术需要充分考虑文档使用的多样性,融合联邦学习、差异隐私和安全多方计算等多种技术途径。面向科研领域的抽样分析需要,利用差分保密的思想,在保证研究成果真实性的前提下,引入微小噪声,避免个体身份被逆向辨识。面向文档多智能体协同分析的需要,拟采用安全的多方计算方法,使多个参与者以密文方式协同工作,获得相应的分析成果。在实际中,需要对隐私的保护进行严密的控制,在数据使用和安全之间寻求最优的均衡,以防止利用失效和保护漏洞的发生。

3 分类管理机制: 适配不同平衡需求

3.1 制定档案分类分级标准

以隐私敏感性和使用价值作为两个核心维度,建立了一个文件的分类分级系统:其中,隐私敏感性维度从信息可识别性、泄露危害程度和信息主体关注度三个方面进行了分级,其中能够被直接识别并导致用户利益遭受重大损失的文件被列为高敏感类别,而对于无法识别并且泄露后果不大的文件列为低敏感类别。另外,通过价值维度对公共服务需求、学术研究价值和历史传承意义进行评价,将对公共决策具有重大价值的文件归类为高使用价值类别,对个人收藏需要的文件归类为较低使用价值类别。在此基础上,将对各类档案进行详细划分,并制定相应的评价程序,并结合档案形成时间、社会环境变化、法律法规更新等情况,对其进行定期复查,以保证其符合个人隐私和信息使用的动态需要。

3.2 分类施策流程

在档案入库的过程中,需要对文件进行分类、分类和标记,然后,档案管理员将其与分类准则和诸如敏感信息自动化探测系统等智能辨识手段相融合,对文件的内容逐一进行核对,并对其进行归类和等级的标记,同时将标记的结果保存在档案管理系统中,如图1所示。在档案使用过程中,通过对已知信息的注释,实现对档案的保护和使用。对于高敏感性的高价值文件,采用信息主体授权、多级审核、动态脱敏的联合机制,对于较弱的高价值文件,则启动实名验证、公开存取、工作日志的机制。在存档过程中,需要对其进行定期的分级效应评价,根据使用频率、隐私风险事件、用户反馈等信息,判定现行的分级决策的合理性。对于适应性较差的档案,进行类型和相应的响应对策的修正,保证各类文档的防护手段和使用要求的准确匹配^[3]。



图1 档案级别分类及管理框架

4 利用审核机制：把控利用的合规性

4.1 事前审核

事前审核工作的开展需要建立多维度的认证机制，即首先验证使用人的资质，然后通过与政府、学术机构等身份认证系统相匹配的身份验证，确定使用者身份的真伪和归属范围，并将不具备合法使用资格的人剔除。在对使用用途进行重新审查时，使用者需要对其使用情况进行详尽的描述，并对其使用情况进行界定，且要根据文件的分类等级来判定其用途是否满足法律规定和隐私保护底线。最终核实使用范围，按照文件等级和用途确定可查阅的文件目录，防止使用者提出超越需要的资料授权。

4.2 事中监控

事中监控需要依靠档案管理系统来建立一个实时的行为监控制度，在整个过程中都能追踪到使用者的使用情况，记录每一种操作的时间、内容和频率，包括文件访问、查看、复制、下载等操作的时间、内容和频率。对于高敏感性文件，增加了禁止批量下载、限制拷贝内容长度和水印等运算限制，以避免非法扩散问题的出现。该系统需要预先设置异常的警告门限，如果发生对同一敏感文件的高频率使用，跨区域的异常 IP 操作，以及越权的尝试进入等情形，将会自动发出警报，并将使用者的操作中止，然后在

档案管理员的验证下，确定该权限的恢复与否。

4.3 事后追溯

为了实现事后可追溯的要求，需要设立一个日常的稽核和可追踪的制度，档案管理员要对使用的记录进行定期的审查，以确定使用者有没有越权的利用行为，是否符合档案的使用协议。而且要将审计的结论写成一份书面的报表，把合规的利用行为保存起来，并对可疑的违规行为进行深入调查。一旦证实有违法使用行为，则要按照审核记录对有关人员进行追责，并按照有关法律和文件的有关规定对其进行问责，其中有暂停使用许可、通报所属单位和承担法律责任等。在此基础上，还要将使用结果向档案文件信息主体进行反馈，以保证其对相关人员的知情权，从而实现审核核实、责任溯源、结果反馈的监管闭环，并以此为基础加强使用者的合规意识，夯实档案使用安全的防御体系^[4]。

5 结语

综上所述，在档案管理工作中，隐私保护与信息利用的平衡机制在构建的过程中需要通过多领域的交叉融合才能得以完善，做好此项工作能够为我国的档案治理研究和实际应用奠定坚实的基础。在后续的工作中，工作人员也能对各类文件的理论适应性进行深入研究，并根据不断涌现的新技术对均衡逻辑进行不断地优化，使档案信息在保障和使用的动态平衡中更好地发挥价值。

参考文献：

[1] 刘滨. 档案管理信息化建设中的数据安全与隐私保护策略研究[J]. 兰台内外, 2025,(20):36-38.
 [2] 薛利梅. 人事档案开发利用中的隐私保护问题[J]. 山西档案, 2025,(04):91-94.
 [3] 王照润. 大数据时代加强档案管理信息化建设的对策[J]. 价值工程, 2024,43(32):50-53.
 [4] 何丽霞. 数字化技术在档案管理中的应用研究[J]. 信息记录材料, 2024,25(01):47-49.

作者简介：刘彦麟（1991-），男，汉族，湖南祁东人，馆员，硕士，研究方向：档案应用。