大数据背景下的档案信息安全管理分析

兰　天
人力资源和社会保障局　湖北洪湖　433200

摘　要：伴随着信息技术的快速发展，特别是大数据时代驱动下的档案信息管理面临着空前的机遇和挑战。大数据技术应用使档案信息采集、储存、整理、利用等工作更加有效方便，但是也给信息安全带来风险及隐患。档案信息是国家与社会重要的信息资源，涵盖了政府、企事业单位与个人等核心数据，档案信息的安全问题不仅关系着档案工作能否顺利开展，更是直接关系着国家机密，组织利益和个人隐私等问题。所以，大数据下档案信息安全管理非常重要。

关键词：大数据；档案信息；安全管理

一、理论基础与相关概念

（一）大数据概念及其特点

大数据是指无法通过传统数据库工具在合理时间内进行捕捉、管理和处理的大量信息集合。其主要特点体现在数据量庞大、数据种类繁多、处理速度快以及价值密度低这几个方面。数据量庞大是大数据的核心特征，随着互联网、物联网等技术的发展，各种设备和平台每天产生海量数据。数据种类多样，涵盖了结构化、半结构化和非结构化数据，诸如文本、图片、视频、音频等多种形式都能构成大数据的一部分。大数据的处理速度也非常重要，实时数据处理能力成为衡量其技术水平的关键，因为及时获取和分析数据对于决策和预测至关重要。尽管大数据带来了丰富的信息资源，但其价值密度较低，即数据中的有用信息比例较小，如何从庞杂的海量数据中挖掘出高价值的信息成为了一项重要的技术挑战。大数据的这些特点不仅使其在数据管理、决策支持等领域具有广泛应用，也给技术开发、信息安全等方面带来了新的挑战。

（二）档案管理的基本概念

档案管理是指对在社会活动中形成的各种档案材料进行系统的收集、整理、保存、利用和保护的过程，是信息管理工作的重要组成部分。档案作为一种历史记录与证据载体，其社会价值极高、法律效力极强，对国家、企业与个人发展都起着举足轻重的作用。档案管理的首要目标就是要保证档案的完整性、真实性以及可用性，让档案在必要的时候可以得到有效的取用以及利用。在信息技术不断发展的背景下，纸质档案传统管理模式正朝着电子化与数字化方向转变，电子档案信息存储、传输与检索呈现出更加高效与灵活的特点。但是电子档案管理同时对于信息安全与隐私保护有较高要求，尤其是存储、备份以及数据迁移过程中，如何确保档案安全性与防篡改性就成了重点。档案管理的中心工作既包括妥善保存现有档案，又要保证档案资源不断更新与高效利用，从而能在社会各个领域为管理与决策提供可靠信息支撑。

（三）信息安全的定义与维度

信息安全就是要通过一系列的技术与管理手段来确保信息的保密性、完整性与可用性，避免未经许可的获取、篡改与损坏，这样就保证了信息的储存、加工、传递过程中不受到威胁。保密性作为信息安全的关键维度，其目的在于保证敏感信息只允许授权人员获取，避免信息泄漏。为了确保信息的完整性和准确性，在其传输和储存的过程中，我们必须防止未经允许的更改或损坏。而可用性是指系统与信息在必要时须能正常存取与利用而不受攻击，失效或人为等因素的影响。在此基础上，信息安全涉及到身份认证、授权管理以及抗拒服务攻击，保证信息系统稳定可靠。在大数据和云计算的新技术环境中，信息安全所受到的威胁与挑战变得越来越复杂，技术进步中如何保持信息的安全成为世界各国研究的重点。信息安全多维度保障需要综合运用技术和管理措施对信息资产安全进行综合保护。

二、大数据背景下档案信息安全的挑战

（一）档案信息安全面临的技术挑战

档案信息安全面临着大数据与信息化大环境下的众多技术挑战，其复杂性与多样性也越来越高。在档案管理

逐渐电子化、数字化的今天，档案信息集中存储、网络化管理使得档案信息成为黑客攻击、网络威胁等重点对象。大规模数据存储系统与云平台在带来管理效率提高的同时，也使档案信息的传递与储存面临篡改、泄露与遗失等危险。随着网络攻击手段变得越来越复杂，例如分布式拒绝服务攻击（DDoS）、恶意软件植入和数据窃取等，档案管理系统面临着更高的技术防护要求。与此同时，档案信息种类繁多，涉及文本，图片，音视频及其他多媒体文件等，安全防护难度加大，尤其是跨平台、多终端接入时，如何确保不同设备、不同网络环境下信息的一致性与安全性，就成了一个技术难题。数据备份和恢复技术是否成熟还直接关系到档案信息是否安全，在自然灾害，硬件故障或者系统崩溃等突发情况下，档案数据恢复能力非常关键。另外，在云计算、大数据等技术应用越来越广泛的情况下，其物理边界越来越模糊，因此如何保障跨境数据传输合法性、安全性等技术问题亟待解决。这些挑战既需要较高水平的技术防护，又需要系统化安全策略和管理机制的结合才能全面提高档案信息安全性。

（二）档案信息共享与隐私保护的矛盾

档案信息是社会的一种重要资源，档案信息的共享与利用可以促进信息流通、提升行政效率、促进社会发展。但是档案信息通常含有大量敏感的数据，涉及个人隐私、商业机密以及国家安全等方面，因此如何保证隐私与数据安全的前提下实现开放共享就成了一项复杂而又棘手的问题。档案信息共享时，访问权限的拓展以及信息流通性的增强将加大敏感信息的泄露风险，尤其是不同平台，不同机构以及跨区域共享场景下，资料的用户可能会对资料进行误用或者不恰当地加工，进而侵犯个人隐私。数据在透明性与隐蔽性间的权衡很难把握，在确保信息公开透明性社会效益的同时，还需要保护个人隐私权不受侵犯。法律与技术手段上的滞后性同样加剧了这种冲突，而现有隐私保护法规面对大数据时代错综复杂的数据共享模式时往往显得力不从心。另外，实际工作中档案管理人员或者信息使用者安全意识淡薄也会造成共享过程中违规获取信息或者误用信息。这一矛盾需要建立更详细的法律规范并辅以数据加密，匿名化等先进技术手段，在强化管理机制及安全教育的前提下平衡档案信息共享和隐私保护的矛盾。

三、大数据背景下档案信息安全管理策略

（一）技术手段

大数据环境下确保档案信息安全技术手段不断革新与发展，涉及多层次防护策略与手段。数据加密技术作为确保档案信息安全的一种核心方法，能够通过加密处理有效地阻止未经许可的存取以及数据泄露等。对称加密与非对称加密都有其独特的优点，特别是对称加密算法，例如AES（高级加密标准），它在加密和解密方面表现出色，特别适用于大规模数据的加密处理。非对称加密技术，例如RSA算法，因其出色的安全特性，在密钥交换和数字签名等多个应用场景中得到了广泛使用。为进一步提高安全性，混合加密技术综合运用了两种方法，使得加密系统具有高效与安全的双重特性。防火墙技术是网络安全中的第一道防线，它可以有效地截获未经授权访问及恶意流量。采用深度包检测（DPI）技术的防火墙能够通过对数据包内容的深入分析来识别并制止可能的攻击活动。在档案信息管理系统的架构中，通过整合防火墙、入侵检测系统（IDS）以及入侵防御系统（IPS），可以构建一个多层次的防护机制，以实时监测网络流量，并有效地检测和制止网络攻击行为。IDS对网络流量异常行为进行分析来确定潜在威胁，IPS可以对恶意操作进行主动介入和制止。数据备份和恢复技术同样必不可少，定期备份可以保证系统遇到攻击，自然灾害或者硬件故障等情况下档案信息可以得到及时的恢复。冷备份和热备份策略相结合可增强备份灵活性，冷备份适合长时间周期性存储，热备份是为了实时备份保证数据在任何时候都可使用。另外，区块链技术因具有分布式存储、不可篡改等特点，正逐渐成为档案管理的一种新兴技术，可以保证档案数据真实、完整，使档案信息安全性得到进一步提高。这几种技术手段有效融合为大数据环境下档案信息安全工作提供有力技术保障，使信息在传递、存储与共享等环节安全风险显著下降。

（二）管理机制

大数据环境中，档案信息安全管理是否有效，不仅仅取决于技术手段，更需要完善的管理机制为其提供全方面保障。权限控制作为一种核心管理机制，它通过设置分级访问权限来保证档案信息访问只限于被授权人员。基于角色的访问控制（RBAC）可以根据用户的身份和职责动态调整访问权限，从而减少不必要的权限暴露，降低数据泄露的风险。除权限管理外，审计机制是关键，审计系统通过对用户操作行为的记录与分析，能够对访问情况进行实时监测，当出现异常行为时，能够及时报警或者采取适当的措施。数据备份与恢复机制保证了意

外发生时档案信息能被及时还原，降低了信息丢失所带来的后果。定期实施全量备份和增量备份两种策略，使数据能够溯源并恢复到各个时间点。对档案管理进行持续性监控同样是至关重要的举措，利用日志记录与持续监控工具能够有效地追踪系统运行状态，及时发现可能存在的风险，并进行维修。同时管理机制中也包含了应急响应计划制定与演练以保证信息安全事件出现后能得到快速有效的应对与修复。综合执行这些管理机制，才能从组织层面充分保障档案信息安全。

（三）人员素质

在大数据背景下，档案信息安全不仅依赖于技术手段和管理机制，还高度依赖于人员素质的提升。档案管理人员作为信息安全的直接执行者和维护者，其专业能力、风险意识和应急处理能力对于保障档案信息的安全至关重要。档案管理人员必须具备较高的信息安全意识，了解信息泄露的潜在风险和后果，这要求组织对管理人员进行持续的信息安全教育和培训。定期的培训课程应涵盖网络安全基础、常见威胁类型、数据加密技术及法律法规等内容，确保档案管理人员能够掌握基础的技术手段和防护措施。档案管理人员还需要具备对新兴技术的敏锐认知能力，随着大数据、人工智能和区块链等技术的快速发展，档案信息管理的方式和风险点都在不断演变。管理人员需要对这些新技术有充分的理解，才能有效应用这些技术来提升信息安全。例如，区块链技术在档案真实性验证中的应用，云存储的安全策略，人工智能对安全漏洞的监控等，都需要档案人员具备相应的知识储备。此外，档案管理中的应急响应能力也尤为重要，档案管理人员必须具备处理紧急信息安全事件的能力，包括快速识别、评估安全事件，并在事件发生后采取有效的恢复和补救措施。档案管理人员的沟通与协作能力同样不可忽视，他们需要与技术部门、法律部门紧密合作，共同制定信息安全的策略和方案，确保档案信息安全防护措施的全面落实。通过不断的学习与实践，档案管理人员不仅能应对当前的安全威胁，还能主动适应未来的信息安全挑战，为档案信息的长期安全奠定坚实的基础。

（四）法律与政策

健全的法律法规对档案管理工作提供有力的制度保证，对档案信息利用范围、保护措施以及对违法行为处罚标准等都有明确规定。国家通过立法可以对档案信息采集、储存、加工、共享等方面制定出严格的规章制度以保证当事人在档案信息处理过程中遵守有关法律，以免信息泄露或者被误用。与信息安全有关的《网络安全法》,《数据安全法》对档案信息管理过程中数据保护、隐私权保障以及跨境数据流动等问题做出了细致的规制，并规定信息泄露之后的法律责任。同时，政策层面上的扶持必不可少，无论是国家还是地方政府都会通过发布政策文件，指导性意见以及行业标准等方式来促进档案信息安全保护工作规范化，标准化。在档案信息管理工作开展期间，政策既对安全管理起到操作指引作用，同时也督促企业与机构履行信息安全防护职责与义务。法律、政策保障的健全保证档案管理活动合法、规范，在通过法律约束、政策指导、加强档案信息安全防护措施等措施使信息安全获得长效保障。

结束语

大数据时代为档案管理带来了前所未有的机遇与挑战。在提高档案管理效率和信息共享便利性的同时，档案信息安全问题日益突出。通过技术手段、管理机制、人员素质提升和法律政策保障的有机结合，能够有效应对档案信息安全面临的多重威胁。然而，随着技术的不断发展，信息安全领域的风险也在持续演变，档案管理需要时刻保持对新技术、新威胁的高度敏感，积极引入创新的安全防护技术和管理策略。

参考文献

[1]张必金.“大数据”时代档案信息安全管理新思考[J].科技经济导刊，2016（36）：2.

[2]王璐.大数据背景下档案管理信息安全问题及对策分析[J].商业2.0（经济管理），2021（8）：0093-0093.

[3]林明香.“大数据”时代档案信息安全管理浅析[J].兰台世界，2018（S2）：169-169

[4]张秀梅.大数据背景下档案管理信息安全问题及对策浅析[J].2021.

[5]李霜，何伟.“大数据”时代档案信息安全管理新思考[J].中外企业家，2018（24）：1.