档案利用服务中隐私信息保护机制探析

杨　勇

吉林省和龙市房产交易中心 吉林 和龙 133500

【摘　要】：随着信息技术的不断发展，档案利用服务逐渐向数字化和网络化转型，档案管理的效率和便捷性大幅提升。然而，在这一过程中，隐私信息的保护问题愈加突出。本文主要探讨了档案利用服务中隐私信息保护的现状与机制，分析了当前隐私保护面临的挑战，并提出了改进措施。通过对档案管理系统中隐私信息保护技术手段、法律法规保障、以及管理流程优化的综合探讨，提出了建立多层次隐私保护机制的重要性。这不仅有助于提升档案利用的安全性，也确保了个人隐私权益的有效保护。

【关键词】：档案利用服务；隐私信息；保护机制；数字化档案管理；安全性

DOI:10.12417/2811-0722.26.02.055

引言

在数字化和信息化日益加深的今天，档案管理工作面临着前所未有的挑战与机遇。档案利用服务的广泛应用大大提高了工作效率，但与此同时，隐私信息的泄露风险也随之增大。如何在确保档案利用高效便捷的同时，有效保护其中涉及的个人隐私，成为了档案管理领域亟待解决的关键问题。特别是在房地产交易中心等涉及大量个人敏感信息的机构中，隐私保护的难度和重要性更为突出。本文将探讨档案利用服务中的隐私信息保护机制，旨在为提升档案管理的安全性与可靠性提供理论依据和实践指导。

1 档案利用服务中的隐私信息泄露风险分析

在档案利用服务的过程中，隐私信息泄露风险不可忽视。随着信息技术的不断发展，数字化档案管理在提升效率的同时，也带来了越来越多的信息安全隐患。档案中包含了大量个人敏感数据，如身份证号码、联系方式、财务状况等，这些信息一旦被不法分子获取，可能对个人甚至社会造成严重后果。随着档案服务的数字化、网络化进程加快，信息存储和传输过程中可能会出现的漏洞使得隐私信息面临着更高的泄露风险[1]。尤其是在档案系统的设计和管理环节，若未能有效应用加密技术、身份验证机制等手段，便可能导致数据的非法访问与滥用。对于房地产交易中心等具有大量个人信息的机构来说，泄露的风险尤为严重，因为它涉及到诸多具有高敏感度的档案数据，任何一点疏忽都可能引发一系列的法律和信誉问题。

隐私信息泄露的风险不仅仅来自于技术漏洞，管理制度和人员操作的疏忽也在其中扮演着重要角色。许多档案管理机构仍旧依赖传统的纸质文件或简单的数字存储形式，未能有效实施信息安全的统一标准和操作规范。这种情况下，档案的存取权限、管理人员的操作规范等容易产生管理盲区，增加了泄露的可能性。特别是在一些档案借阅和调取的环节，若没有清晰的审计机制和严格的权限控制，工作人员的无意识错误或恶意行为都可能导致隐私信息泄露。档案共享和传递过程中的保密性问题也值得关注。许多档案信息是通过电子邮件、文件传输等方式进行共享的，若传输渠道的安全性无法得到有效保障，便存在被拦截、篡改或泄露的风险，尤其在外部合作中，一旦合作方未采取足够的保护措施，档案中的隐私信息便可能面临泄漏的威胁。

在此背景下，隐私信息保护成为了档案管理中的关键问题。针对这些风险，必须采取一系列防范措施，以确保档案利用服务中隐私信息的安全性。例如，通过应用先进的加密技术，确保信息在存储和传输过程中的安全性，使用多重身份验证和权限管理手段，限制对档案的访问权限，保障信息的访问者身份的唯一性与合法性。建立健全的档案管理制度也是防止隐私泄露的有效手段。加强对管理人员的培训，提高其对信息保护的意识，确保其遵守相关的安全操作规范，才能在根本上减少人为因素带来的泄露风险。在档案利用服务中，隐私信息的泄露风险是一项不容忽视的问题，必须从技术、管理和人员操作等多方面着手，建立起完善的防护机制，以保障个人隐私信息的安全。

2 当前隐私保护机制面临的挑战与不足

在档案管理领域，当前的隐私保护机制仍面临着多方面的挑战，尤其在随着数字化和信息化进程加速的背景下，现有的保护措施难以应对不断升级的隐私泄露风险。首先，技术手段的滞后成为了隐私保护机制的最大短板。尽管现代加密技术、数据脱敏和访问控制等技术已经取得了显著的进展，但在很多档案管理系统中，仍然存在系统安全性不足、加密措施不到位等问题。许多机构未能及时更新和升级其档案管理系统，仍然使用过时的存储和传输技术，无法有效抵御黑客攻击和恶意软件的威胁[2]。部分档案管理系统在数据加密方面存在较大漏洞，尤其是对于数据传输环节的加密保护力度不够，导致信息在传输过程中容易被窃取或篡改。因此，缺乏先进和全面的技术手段，成为当前隐私保护机制面临的主要问题。

隐私保护机制中的制度性缺陷也不容忽视。尽管相关的法律法规逐步完善，但许多档案管理机构在实际操作中仍未能严格执行相应的隐私保护要求。管理制度和操作规范的滞后，导致了隐私保护的缺失。例如，档案管理过程中，关于数据存取权限的规定往往不够明确，存在权限过度集中或滥用的现象，

管理人员在日常工作中往往未能严格遵循访问权限控制规定。对于档案管理人员的安全意识和责任心，也存在着明显的差距。许多从业人员缺乏足够的信息安全培训和隐私保护意识，容易因疏忽大意或者缺乏法律知识而在工作中泄露隐私信息。此外，档案信息在共享与流转的过程中，由于缺乏有效的监控机制，也很容易在未经授权的情况下被外部人员访问，进一步加大了隐私泄露的风险。

隐私保护机制中对人员管理和监督的不足，使得隐私信息保护面临巨大挑战。尽管在技术和制度上已有一定的规定和保障，但一旦进入实际操作环节，便容易出现执行不到位的情况。档案管理人员在信息保护方面的意识薄弱，且缺乏有效的监督与问责机制，导致一些机构未能及时发现和纠正隐私泄露事件。档案信息的安全管理往往局限于部分环节，整体上缺乏综合性与系统性的安全防范措施。即使在实施隐私保护技术手段的同时，如果没有严格的内部监管和完善的审计机制，隐私信息的泄露依然难以避免。因此，要从根本上解决隐私保护机制的不足，除了在技术和制度上加大投入，还需要从管理层面加强对人员的培训与监督，确保隐私保护措施能够落到实处。

3 技术手段在隐私信息保护中的应用与成效

随着信息技术的不断进步，隐私信息保护逐渐依赖于各种高效的技术手段。数据加密技术已经成为档案管理中保护隐私信息的核心手段之一。通过对档案数据进行加密处理，可以确保即使数据被非法获取，也难以被解读或滥用。对存储和传输的数据进行全程加密，尤其是使用 AES 等高级加密标准，能够有效防止数据在存储和传输过程中被窃取或篡改。随着计算能力的提升，现代加密技术的安全性大幅提高，这为隐私保护提供了坚实的技术基础[3]。加密技术还可以结合数字签名和哈希算法等手段，确保数据的完整性和认证，进一步增强档案管理中隐私信息的保护力度。

身份认证技术在隐私信息保护中也发挥着重要作用。传统的单一密码认证方式已无法满足现代档案管理中对隐私保护的需求。多因素认证技术的出现，使得身份验证的安全性大大提升。除了传统的密码输入外，生物识别、手机验证码、硬件令牌等多重认证方式的结合，能够有效阻止未授权人员的访问，确保档案利用服务中的隐私信息只能由授权人员访问。通过加强身份认证和访问控制，可以实现对档案信息访问权限的细粒度管理，确保每个用户仅能访问其所需的最小权限范围，从而大大降低了隐私信息泄露的风险。

数据脱敏技术作为另一种重要手段，也得到了广泛应用。通过对敏感数据进行脱敏处理，使得即使在数据共享和传递过程中，隐私信息也无法被泄露。数据脱敏可以通过删除或替换敏感字段、模糊化处理等方法，使得档案中包含的个人信息无法被直接识别或滥用。例如，个人的身份证号码、联系方式等信息在处理后仅显示部分内容，既保证了数据的可用性，又确保了信息的安全性。在实现档案信息共享时，数据脱敏技术能够有效防止未经授权的访问者获取敏感数据，成为隐私保护的重要保障。随着这些技术手段的不断应用，隐私信息的保护变得更加完善和可控，为数字化档案管理带来了更高的安全保障。

4 法律法规对隐私保护机制的保障作用

随着隐私保护问题的日益严重，法律法规在确保隐私信息保护机制方面起着不可或缺的保障作用。隐私信息的泄露不仅仅会影响个人的利益，还可能对社会和经济秩序带来严重后果。因此，相关法律法规的出台和实施，成为了规范隐私保护的关键。诸如《个人信息保护法》、《数据安全法》等法律的出台，使得隐私保护有了更加明确的法律依据和具体的操作要求[4]。这些法律对数据处理活动进行了严格的规范，明确了数据收集、存储、使用、传输等环节中的合法性要求，对侵犯个人隐私的行为提出了严厉的惩罚措施。同时，法律规定了数据控制者的责任与义务，要求其在处理个人信息时必须采取必要的安全保护措施，确保信息不被泄露、篡改或滥用。

在隐私保护机制的实施过程中，法律法规起到了强有力的约束作用。对于档案管理机构来说，法律要求其必须依法进行个人信息保护，未经个人同意不得随意处理其隐私信息。这种法律约束力迫使档案管理单位在系统建设和运营过程中，必须遵循严格的信息安全标准，确保隐私数据的安全性。法律还规定了信息主体的权利，包括知情权、访问权、删除权等，使个人能够对其隐私信息拥有更多的控制权和知情权。对于违反隐私保护规定的机构和个人，法律提供了明确的惩罚措施，包括罚款、暂停业务等行政处罚，甚至追究刑事责任，从而有效威慑了不法行为的发生。这些法律措施的落实，有助于推动隐私保护机制的完善与落地，确保各方主体在处理个人信息时遵循法律和伦理规范。

隐私保护法律法规在推动跨行业合作方面也发挥着重要作用。在多方共享数据的背景下，不同机构间如何合法、安全地交换和利用个人信息，是当前隐私保护面临的一个重要问题。法律法规明确了跨行业信息流转的法律框架，确保信息共享过程中的隐私保护要求得到充分落实。对于参与信息交换的各方，法律不仅要求其采取适当的技术措施保护数据的安全，还要求其履行告知义务，确保信息提供者知晓其信息的流向与用途。这种法律保障机制促使不同机构在共享数据时，必须进行合规性审核，确保隐私信息在流转过程中的安全性与合法性。此外，法律对第三方服务提供商的监督，也为档案管理系统的隐私保护提供了外部保障，使得整个信息处理生态链都处于合规的法律框架之下，有效降低了隐私泄露的风险。

5 完善隐私信息保护机制的策略与实施路径

为了有效完善隐私信息保护机制，需要从技术、管理和制

度等多个层面采取综合性的措施。技术手段的不断创新和应用是确保隐私信息安全的基础。在信息化、数字化日益普及的今天，档案管理系统必须引入先进的安全技术，如高强度的加密技术、多因素身份验证、数据脱敏等，以增强对个人隐私信息的保护力度。通过采用更为先进的加密算法，如 AES-256 等，可以有效保障数据在存储和传输过程中的安全性[5]。实施严格的访问控制，确保只有经过授权的人员能够访问相关信息，减少数据泄露的风险。加强档案数据的实时监控与审计，能够及时发现和应对潜在的安全威胁，进一步增强数据保护的可靠性。

在管理层面，隐私信息的保护还需要建立健全的制度保障体系。完善的信息安全管理制度是隐私保护的核心支撑。机构应当制定详细的信息安全政策，明确各类档案数据的分类标准和处理要求，确保所有人员了解并遵守隐私保护相关规定。同时，加强档案管理人员的培训与教育，提高其对隐私保护重要性的认识，确保其具备足够的安全防范意识。通过强化信息安全管理人员的专业能力，不仅能够提高日常操作中的数据保护水平，还能够有效预防人为失误或恶意行为的发生。与此同时，建立严格的数据使用、访问和共享规范，确保信息流转过程中每一环节的安全性，从而杜绝因管理漏洞引发的隐私泄露问题。

法律法规在隐私信息保护中同样扮演着至关重要的角色。为了完善隐私保护机制，必须加强相关法律法规的执行力，确保隐私保护措施的落地。国家及地方政府应进一步完善个人信息保护法律体系，明确隐私数据保护的法律责任和违法后果，对不合规的企业和个人实施严厉惩罚。此外，在实施隐私保护措施时，相关机构应确保其档案管理活动符合当地法律法规的要求，尤其是在数据共享和外部合作时，必须确保隐私信息的安全传输与合规使用。随着信息技术的不断发展，法律的更新和完善应同步进行，以应对日益复杂的隐私保护需求，从而为隐私保护机制的优化提供坚实的法律保障。

6 结语

隐私信息保护已成为现代档案管理中不可忽视的重要议题。随着技术的不断发展和信息化进程的推进，隐私信息面临的泄露风险日益增大，这要求各级档案管理机构从技术、管理和法律等多个层面入手，构建一个多元化的隐私保护机制。加强技术手段的应用、完善管理制度以及强化法律保障，将为隐私信息提供全方位的保护。然而，隐私保护仍是一个动态的挑战，随着信息环境的变化，必须不断更新和优化相关措施，确保隐私信息在数字化时代的安全与隐秘。有效的隐私保护不仅有助于提升档案管理的可信度，还能增强公众对数据管理机构的信任。

参考文献：

[1] 李晓芳.基层档案馆提升档案利用服务效能的思考[J].中国档案,2025,(11):44-45.

[2] 姚山季,史雪艳,严锐,等.基于元分析的用户健康隐私信息披露意愿影响因素研究[J].数字图书馆论坛,2025,21(08):35-45.

[3] 王岚.大数据技术在档案利用服务中的应用研究[J].兰台内外,2025,(29):30-32.

[4] 顾玉妮.档案馆档案利用服务问题及对策探究[J].兰台内外,2025,(27):54-56.

[5] 陈宜荣.基于区块链技术的网络用户隐私信息安全防护研究[J].长江信息通信,2025,38(07):141-143.