Modern Management 现代管理, 2025, 15(6), 19-26
Published Online June 2025 in Hans. https://www.hanspub.org/journal/mm
https://doi.org/10.12677/mm.2025.156161

Hans汉斯

档案开放背景下用户个人数据安全风险与应对策略研究

徐宇琳

扬州大学社会发展学院，江苏 扬州

收稿日期：2025年5月12日；录用日期：2025年5月22日；发布日期：2025年6月13日

摘　要

数据时代，数据的价值日渐凸显，与其他资源结合将发挥巨大作用。档案数据与用户个人数据的大量生成及高价值性，使其在生成、采集、储存、管理、分析和使用等过程中，产生了大量的风险。随着公众安全意识的提升，大众对用户个人数据的安全保护更为重视。本文从个人数据安全角度出发，结合个人信息与隐私这两个相关概念，阐释档案开放背景下的用户个人数据的内涵，在研究用户个人数据安全现状的基础上，探究档案开放过程中可能存在的风险类型，并提出完善用户个人数据法律保护体系、增强公众的数据安全素养、加强用户个人数据政策的颁布落实等建议。

关键词

档案开放，数据安全，风险识别

Research on User Personal Data Security Risk Identification and Coping Mechanism under the Background of Archive Opening

Yulin Xu

School of Social Development of Yangzhou University, Yangzhou Jiangsu

Received: May 12th, 2025; accepted: May 22nd, 2025; published: Jun. 13th, 2025

Abstract

In the data age, the value of data is increasingly prominent, and it plays a huge role in combination with other resources. The massive generation and high value of archival data and user personal

文章引用: 徐宇琳. 档案开放背景下用户个人数据安全风险与应对策略研究[J]. 现代管理, 2025, 15(6): 19-26.
DOI: 10.12677/mm.2025.156161

data create significant risks in the processes of generation, acquisition, storage, management, analysis and use. With the improvement of public safety awareness, the public attaches greater importance to the security protection of user personal data. This article starts from the perspective of personal data security and combines the two related concepts of personal information and privacy to define user personal data in the context of archive opening. On the basis of studying the current situation of user personal data security, it explores the possible types of risks that may exist in the process of archive opening, and proposes to improve the legal protection system of user personal data, enhance the public's data security literacy suggestions for strengthening the promulgation and implementation of user personal data policies.

Keywords

Open Archives, Data Security, Risk Identification

1. 引言

档案作为重要的信息资源和独特的历史文化遗产，其价值日益凸显。档案开放是促进档案资源有效利用，总结历史经验、发现历史规律，保障各项事业健康发展的重要活动[1]。在政策及法律法规的支持下，档案的封闭期由 30 年减少至 25 年，档案开放力度明显加大。据统计，“十三五”时期，全国档案馆共开放档案 17,659 万卷(件)。在加快档案开放、扩大档案利用、提供优质高效服务的历程中，不可避免地会给用户个人数据带来安全风险。一方面，散落在档案中的个人数据部分未被隐藏处理，可能会造成个人数据的泄露；另一方面，公众的档案检索需求日益增长，档案平台的服务对象也随之逐渐增多，用户在利用档案的过程中，会产生大量的用户数据，这些数据容易被“默认式”采集、“违规式”泄露和“非法式”传播，安全风险极高。随着公民数据安全意识以及隐私保护意识的提高，对此类事件的关注度也大幅提升，用户个人数据的安全风险问题亟需解决。

2. 文献综述

随着《数据安全法》与《个人信息保护法》的颁布实施，及《档案法》的修订，多位学者依据法律条款，探索档案利用过程中个人信息与隐私的保护。部分学者从单一法律着手，何凡以《个人信息保护法》为抓手，探究该法在档案开放利用中的适用性与局限性[2]。一些学者将多部法律结合起来对比研究，如薛玉洁将《民法典》中的隐私人格权保护与《档案法》“有效保护和利用档案”的立法宗旨结合，提出合理隐私期待、限制使用、利益平衡三大档案隐私权保护原则[3]；王玉珏等对《数据安全法》与《档案法》进行协调研究，分析其内在逻辑联系，结合现存问题与域外经验，提出应对策略[4]。

在个人信息保护研究方面，苗运卫通过法益分层，将档案个人信息分为隐私性、个人性、社会性三类，并据此提出了档案个人信息保护的精准化策略[5]。黄文琼等基于数字档案用户个人信息的特性，从网络空间安全威胁、国家法律规约、用户信息素养等角度分析现实困境的成因，强调应注意防范新型档案传播方式引起的信息安全风险[6]。

在档案用户隐私安全的研究中，多位学者以档案网站的隐私政策为落脚点进行研究分析。孙大东等调查研究了我国 70 个档案网站的隐私声明，对其位置以及内容进行总结归纳，发现我国档案网站的隐私

政策存在公开性差、全面性弱、科学性缺乏等问题[7]。支凤稳等对国内外档案网站的隐私政策进行比较研究，探究中英美澳四国档案网站隐私政策在内容、位置与依据的异同点，并提出建立健全个人信息及隐私保护法律体系等优化建议[8]。周林兴等从隐私声明的名称、位置以及内容出发，对国内档案网站隐私政策的合规性进行研究[9]。部分学者也从用户画像技术角度思考档案用户的隐私安全，如徐承来等提出要从主体治理、授权管理、技术嵌入和隐私立法四条路径来解决问题[10]。

在档案数据开放方面，肖秋会等依托政务公开负面清单制度的基本架构，从内容、过程、保障三个层面构建了档案开放负面清单制度框架[11]。马海群基于政策结构的一般框架，挖掘数据开放政策的内涵与研究动向，据此来尝试构建我国档案数据开放政策的框架结构与核心要素[12]。尹泷杰等探讨数据伦理对档案数据开放的积极影响，分析档案数据开放存在的伦理问题，并提出优化数据伦理发展环境、构建数据伦理配套机制等方法[13]。

之前诸位学者在隐私与个人信息保护方面有大量的研究成果，在档案用户个人数据安全风险方面的研究有待探索填补。本文研究档案开放背景下用户个人数据安全风险的相关问题，以个人数据安全视角，从档案中的个人数据与档案用户数据两方面分析其安全特点与风险类型。在数据时代，从数据着手研究档案开放背景下的用户个人数据安全问题大有可为。

3. 核心概念界定

3.1. 用户个人数据

研究用户个人数据安全风险首先要明确用户个人数据的内涵。本文将从三个方面来阐述其内涵：一是用户个人数据定义；二是本文用户个人数据的具体内容；三是用户个人数据与相关概念(隐私、个人信息)的辨析。

用户个人数据是用于描述或记录与用户个人相关的任何形式的信息集合。用户个人数据载体可以是数字、文本、图像、音频、视频等任何形式的媒介。用户个人数据按内容可分为：生物数据、医疗数据、身份识别数据、财务数据、教育工作数据、网站浏览数据、位置数据、通信数据、设备数据等，其内涵丰富。

本文研究的是档案开放背景下的用户个人数据，它可以分为两大模块。第一部分是档案用户数据，即档案用户在进入档案馆或登入档案馆平台时的注册数据与在利用档案时的检索数据，包括姓名、性别、年龄、居住地址、教育背景、联系方式、地址等个人基础数据与查档路径、访问频率、调卷类目等反映档案用户的利用需求、行为偏好、检索认知、兴趣选择的用户行为数据及判断档案用户实时情形的用户情景数据。第二部分是档案本身所包含的用户个人数据。档案是过去和现在的机关、团体、企业事业单位和其他组织以及个人从事经济、政治、文化、社会、科技等方面活动直接形成的对国家和社会具有保存价值的各种文字、图表、声像等不同形式的历史记录。人作为档案形成的主体，档案中必然包含用户个人数据，如档案管理过程中形成的管理者信息和档案文本中包含的个人数据及各档案联系交织后产生的相关个人数据。

因为语言习惯及语义扩展等原因，“隐私”“个人信息”“个人数据”等概念一般未加区分，常被交替使用。但近些年，随着相关法律法规的出台和完善，它们差异愈见明显。《民法典》将隐私界定为自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。《个人信息保护法》将个人信息定义为以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。与个人数据相比，隐私更强调私人性和不可公开性。相较于隐私而言，个人信息与个人数据的范畴更大一些。个人信息与个人数据的区别就是信息与数据的差别，普遍认为，信息是有语义的数据。

3.2. 用户个人数据安全

用户个人数据安全是指在对用户数据进行采集、管理与传递利用的过程中，为防止用户数据发生盗取、泄露、滥用、篡改与交易等事故，采取措施以确保用户个人数据的真实、可信、完整、保密，维护档案用户的个人数据权益。用户数据安全要素主要分为保密性和完整性。保密性是指确保档案用户数据只交由授权者获得和利用；完整性是指确保档案用户数据不被篡改、删除，使其保持准确完整。

4. 用户个人数据安全现状

进入大数据与互联网时代，用户在享受技术便利的同时，也面临着更为严峻的数据安全风险。下面将从法律法规、平台政策、公众意识三方面对用户个人数据安全现状进行阐述，并总结现存问题。

4.1. 法律法规

维护用户个人数据权益最有力的支撑便是《数据安全法》，该法案厘清了各主体的数据安全保护义务，明确了数据处理者和使用者的法律责任及惩处规则，强调要在维护数据权益的基础上促进数据开发利用。此外，档案领域的基本法——《档案法》也为用户个人数据安全提供保障。档案法第四章也提及有关个人信息档案的开放利用要符合相关法律政策规定。

由于用户个人数据与个人信息的内涵与外延有所交叉，个人信息保护法的相关条例也为用户个人数据的保护提供法律依据。据统计，我国已有 40 部法律、30 余部法规和 200 部规章制度涉及个人信息保护，初步形成了以宪法主体，刑法、民法、经济法等多部法规配套的个人信息保护法规体系[14]。如民法典在“人格权编”中以“隐私权和个人信息保护”专章方式，对隐私权与个人信息保护原则、定义和外延、信息主体权利、信息处理者和行政机关工作人员的信息保护责任等问题做出规定[14]。

虽然，法律法规随着法制进程不断完善，但在部分条款与权责界定方面仍需进一步的细化与删补。《数据安全法》主要是从国家整体的宏观角度出发，考虑国家总体的数据安全，倾向于在维护安全的基础上进行妥善开发，对政务数据安全与开放较为重视，涉及用户个人数据安全较少。《档案法》未曾提及档案数据与档案用户，更没有涉及用户个人数据。在数字环境下，电子档案大量形成，线上检索平台给用户提供便利。档案用户的数据安全需要在法律条款上进一步说明，需要补充用户数据的隐私管理、配套机制与标准规范。在《档案法》中，个人信息档案的使用要求遵照相关法律法规。虽然是法律间的相互印证，但没有明确具体条款，且各法律的侧重点不同，且相互兼容协调性不足。因此，在档案用户个人数据方面存在一些未被法律约束的灰色地带。

4.2. 平台政策

档案信息网是指由国家档案局主导的，省市级档案馆自主建立的面向社会公众提供在线查询、浏览、下载、购买等服务的档案信息公共服务平台。该平台汇聚了档案机构的数字化档案资源，包括历史文献、图片、音视频等多种形式的档案信息，并且提供了便捷的检索和查询功能，为用户在研究、教育、文化、出版等领域的资源需求提供了广泛的支持。

相较于公众号与小程序，档案信息网的发展时间更早，完善程度更高，有更广的公众认同度。且各个档案信息网通过友情链接，将省内档案网站、国内档案网站与国际档案网站联系起来形成了较为完善的传播矩阵。通过全面查询设有隐私政策的档案信息网站，以其首页与查询注册页面为调查范围，对隐私政策名称、位置和内容进行归纳，现总结如下：

隐私政策模块一般独立设置，点击后跳转页面。隐私政策的名称有隐私声明、隐私保护、版权隐私、网站声明等，其中隐私保护出现的频率较高。隐私政策的位置通常设置于网页底端或网页右上角。各档

案信息网的隐私政策的位置、名称、样式有所区别，但都不太引人注目，位置偏僻，字体较小。

隐私政策内容一般包括信息收集范围、信息保护、信息使用与披露、免责声明五大模块。大部分网站都把用户信息的收集说明置于隐私条目的首位，让用户知道在使用网站时会被采集的信息种类。如果用户仅浏览档案网站，网站只会收集用户的非个人识别信息，如用户的域名、软硬件系统类型、访问路径、访问频率、浏览时间等，一般会在用户进入网站后进行，不会征求用户的同意。当用户需进一步获取档案信息服务，如预约查档、咨询投诉、报名活动，网站会通过表格等形式要求用户提供一些个人信息，如姓名、身份证号码、单位、工作、查档原因等，此类数据填写就代表用户同意采集。声明中一般会承诺对用户个人信息进行保护，不会丢失、盗用或窜改，以此来增强用户的信任感。各网站均说明了会向除网站及用户之外的第三方披露用户信息的特殊情况。档案信息平台为了避免承担职权范围之外的责任，在隐私政策正文末尾增加了免责声明，减轻因突发性意外给用户数据带来巨大损失所要承担的追责。

档案网站隐私政策的广度不够。网站隐私政策提供的信息覆盖面不大，仅是简短的几条，较为笼统的概括，没有完全涵盖用户想了解的信息，提及的内容也不易于理解。声明未公示被采集的用户数据的用途，也没有对用户数据使用情况的反馈机制及采集原则进行说明。当这些信息缺失时，用户无法清晰地知晓个人数据的使用情况，也无法在数据被泄露时进行追责，对档案服务机构的信任度与满意度都会直线下降。

档案网站隐私政策的普及率和规范性不高。通过调查研究，大部分省级档案信息网没有设置隐私政策，也没有对隐私保护政策进行公开性说明。但在实际使用这些未设置隐私政策的档案服务平台时，用户仍被索要个人信息，这说明用户仍然在被采集信息，平台却没有做到告知用户的义务。在规范性方面，档案网站隐私政策没有统一的标准，各个网站的隐私政策样式各异，内容也有所出入，需要对档案网站隐私政策的栏目名称、位置及内容设置做统一规定。在制定统一规范的情况下，档案网站的隐私政策才能全面普及并发挥好作用。

档案网站隐私政策的落实缺少监督机制。在被调查的所有档案网站的隐私政策中，均未提及平台是如何落实网站隐私政策，也没有第三方监督机构及主要负责人的信息，所以保护用户数据措施的落实程度无法保证。且技术不足、操作不当、管理人员素质不齐等问题，都可能对用户数据安全造成威胁，所以需要监督机制。现在的隐私政策仅仅发挥了告知的作用，用户个人数据的安全情况仍是未知的，使隐私政策仅浮于表面，流于形式。

4.3. 公众意识

近年来，由于个人数据泄露事件频发，用户的数据安全意识逐渐增强，但其保护能力和维权意识有待提升，处于清醒但放任的悖论状态，即清楚地认识到个人数据的重要性，但不采取行动去保护个人数据。通常，档案用户会因为隐私政策的冗长及利用档案的迫切性，盲目信任平台隐私条款，不认真阅读隐私条款就同意，导致个人信息被过度采集。在遭到个人数据泄露后，大部分用户会因为不了解个人数据的权利或不知道维权途径而望而却步。还有一部分用户在发现泄露问题后积极向相关机构举报、投诉，但得不到妥善的解决方案后，也停止了后续的维权行动。档案领域长期以来更关注档案信息安全防范，而在档案用户数据管理上相对滞后，需要档案工作者提高数据保护意识。

5. 用户个人数据安全风险

5.1. 档案数据安全特征

1. 风险集群性

档案馆作为档案保管中心，贮藏着大量未开放高价值的机密信息。随着档案馆积极推进数据化、网

络化建设，档案数据库与共享服务平台的数据也暴增。因其数据规模，极易形成风险集群效应，即大量高价值的档案比单份档案更易吸引不法分子的注意，数据库被黑客攻击的风险剧增，且数据库被攻击或出故障影响的是全部的档案数据，损失巨大。

2. 综合关联性

档案的载体多样，类型丰富。在档案的形成过程中，档案之间就互为依据，互为参考，在整理实体档案时，会将有联系的档案归置到一起，但在数据库系统中这种关联性或多或少都被破坏了。因为档案的关联性，档案的价值发现才具有隐蔽关联性，即部分碎片化数据只有在聚集和被挖掘之后才能展现其隐含价值。也许部分档案数据单独审阅时意义甚微，但与其他数据结合便更有意义，所以档案的价值鉴定与安全性保护等级的选择一直是档案部门棘手的难题。部分档案数据出现安全问题，另一部分档案数据也可能会随之产生问题。所以档案数据的安全问题也是错综复杂，牵一发而动全身。

3. 动态性

文件生命周期理论揭示了文件从最初形成到最终销毁或永久保存的整个运动过程。档案处于一个动态流转的过程。因其生成流转速度快，难以有效捕捉。数据的实时性和流动性使存在安全隐患的数据易向不同领域、不同部门和不同阶段快速扩散转移，安全问题呈现出移动性，安全风险边界拓展，监测和管控难度增加[15]。

5.2. 用户数据安全特征

用户数据的安全特征就是高价值性。用户在档案服务平台注册时，通常会被要求提供个人身份证明，真实姓名与证件号是必不可少的，所以在档案服务平台上可准确便捷地得到用户的唯一真实身份。用户利用档案时有极强的目的性，通过检索行为极易了解其信息需求，再结合相关个人数据，可分析出高时效性、高价值的信息。一方面，高价值信息的效用极大，会吸引不法分子的注意，被有心之人窃取利用。另一方面，档案馆为了提供精准化服务，会大量采集用户数据，为系统分析提供数据样本。随着用户画像技术的发展，档案馆会利用此技术，构建用户画像，根据其职业与搜索偏好进行精准化知识推送。在分析处理用户数据时，用户的个人数据一直处于动态流转中，对用户数据的安全保障无法到位，极易产生安全风险。

5.3. 用户个人数据风险类型

1. 无效同意风险

出于尊重用户知情权及规避法律风险的考虑，信息采集者通常遵循“告知－许可”制度，即在信息采集前，以隐私声明、服务协议的形式提前告知用户个人数据的采集范围、方式、目的、存储、披露情况等，在用户阅读完声明选择同意后才进行采集。这道程序在实际使用中不太能发挥其应尽的效用。一方面能仔细阅读网站隐私协议的用户较少，大部分用户都是直接勾选同意以期尽快获得服务；另一方面，由于隐私协议的专业性，用户不一定能完全理解。在对数据采集一知半解的情况下，用户无法识别出不合理的条款，进而给用户个人数据带来安全风险。

2. 系统漏洞风险

档案数据与用户数据通常存储在数据库中，由相应的数据管理系统来进行数据控制。数据管理系统由于技术发展水平的限制仍然存在安全漏洞。安全风险如下：一是系统设计无法完全规避不安全因素，如系统需要有一定扩展性以备后续开发，会给系统设计者留有端口，可自由访问、控制、修改、调取；二是网络攻击的复杂多变、迭代频繁，现有数据安全保护技术无法完全应对，数据脱敏、加密、匿名化等数据安全技术有待进一步发展；三是不法分子会利用系统本身的漏洞盗取用户个人数据，更会植入病毒

篡改数据。

3. 人员操作风险

用户数据安全策略的实施依赖于人的管理，用户个人数据风险也来源于管理人员。如果数据处理人员数据安全意识薄弱、操作不规范、受利益驱动非法贩卖用户数据，用户个人数据安全就无法得到保障。个人隐私数据的流出常常是因为管理人员的失误操作，自发性地突破数字档案服务系统的层层安全措施。另一方面，档案人员的学科背景、职业培训未能完全填补计算机科学、档案学、法学等与用户数据保护相关学课的知识空缺。所以，档案人员可能无法有效地对用户数据进行敏感度分级，也无法正确感知用户隐私风险，进而影响到用户数据库管理系统的运行维护。

6. 用户个人数据安全风险的应对策略

6.1. 完善用户个人数据法律保护体系

我国个人数据的保护力度有待加强，需要建立健全用户个人数据法律保护体系。法制时代必然要求立法先行，法律是用户数据权益强有力的保障。在法规修订方面，我国可以借鉴国外数据立法的先进经验，并结合我国国情与发展现状进行增补。关于《数据安全法》的后续修订中，可以增加个人数据、风险评估、安全监督等内容，使数据采集、保存、处理的全过程都有法可依。在实际的司法应用中，由于个人信息与个人数据的语义交叉，常以《个人信息保护法》的部分条例作为法律依据。为避免重复立法，可相互援引，部分概念也可与时俱进。

档案开放背景下的用户个人数据安全更需要档案法的支持。在线上档案用户规模扩大的趋势下，档案用户个人数据管理应当被立法者纳入考量。在监督检查模块中，需要增加档案主管部门对用户个人数据安全保护政策落实情况的检查义务。在法律责任模块，要明确档案部门保护用户个人数据的义务及惩处措施。档案行业应以《档案法》为基础，结合档案服务业务的需求，制定有关档案用户个人数据保护的行业规章，平衡好档案精准服务与用户数据的安全保障。此外，档案行业从业者要加强配套工具的开发，编制《档案数据分类分级指南》《档案数据影响评估模板》等配套材料进行补充。

6.2. 加强用户个人数据政策的颁布落实

关于档案本身所包含的用户个人数据，可以借鉴负面清单制度与分级制度进行限制性开放。档案开放的负面清单制度就是将部分用户的敏感数据列入不开放清单，在自然人死亡前永不开放。分级开放就是按个人数据的敏感程度进行划分，对私人化程度高的数据限制开放，对具有社会性的个人数据，采取数据开放模式，强调信息利用的同时予以最低限度保护。另外可对使用者进行分级，以此来保护档案中的用户个人数据。

关于档案用户的个人数据安全，政府可以出台对档案数据平台的监管政策，并设立专门的数据管理机构，统筹规划、组织协调，制定与数据保护法律相配套的监督管理制度，加强对用户个人数据处理、使用等环节的监管力度，避免出现滥用数据、泄露数据等情况。此外，政府还应加强对档案数据存储设施的建设和管理，确保数据的安全存储和加密传输，并及时进行备份和恢复，以应对意外事件。政府可增加档案馆的经费，落实档案馆的扶助政策，为其技术引进提供资金支持。

6.3. 提高公众的数据安全素养

提高公众的数据安全素养首先要建立社会性数据伦理，即用正确的价值观引领所有人尊重他人的数据隐私，用道德为个人数据安全上道保险，从源头上减少用户个人数据安全风险。当档案工作人员的道德水准有所提升，其职业素养与数据保密意识就会有所提高，用户数据的安全风险就会降低。在档案馆

的工作培训中也应增加维护用户数据安全的相关内容，强调保护用户个人数据安全的重要性。但道德仅能约束有道德之人，档案用户提高自身数据安全意识与技能是必不可少的。档案用户要筑牢个人数据安全防线。首先，档案用户应该积极学习相关法律条款，认真从数据泄露事件中吸取经验教训，分析审视自身在数据安全保护方面的疏漏，是否每一次都仔细阅读隐私声明，是否从正规渠道获取档案资源，并根据相关维权案例，学习如何利用法律武器维护个人数据权益。其次，用户要加强对个人数据安全风险的感知。让用户在使用档案服务平台提供的资源时，就意识到可能会遭遇到的数据泄露、篡改或滥用等潜在损失。公众的数据安全素养的提升需要从宣传部门到档案部门的努力。宣传部门加强数据安全教育力度，增强对数据安全法等相关法律的法制宣讲，努力抓牢官方媒体的宣传阵地，培养公民的数据安全意识和信息保护观念，在全社会形成良好的隐私保护氛围。档案馆可在用户教育模块增加数据安全保护课程，通过讲座和海报宣传，线上线下相结合落实好用户个人数据安全风险教育，如联合社区开展“档案数据安全科普周”活动。

7. 结语

档案的开放力度增大势必会给档案中的用户个人数据带来安全风险。档案的大量开放也极大地激起了用户的利用需求。且随着技术的发展与档案馆服务意识的提升，档案用户的个人数据也在不断被采集、处理、利用。在此背景下，用户个人数据保护与精准化、高质量的用户服务产生了矛盾。数据安全事件频发也使公众将视线聚焦于个人数据的保护。当今的用户个人数据安全现状不太乐观，法律规章有所缺失、隐私政策未成体系、公众意识有待提升。期待随着技术的进步、法律的修缮和政策的落实，在用户个人数据领域形成以数据道德为保障、法律政策为支撑的保护体系。古语云“居安思危，思则有备，备则无患”，提前识别用户个人数据安全风险，形成良好的应对体系，才能维护好公众对档案馆的信任感，在大数据革命的风口浪尖乘风破浪[16]。

参考文献

[1] 王英玮, 褚英东.《国家档案馆档案开放办法》的时代意义、内容评析和实施建议[J]. 北京档案, 2022(11): 18-24.
[2] 何凡.《个人信息保护法》在档案开放利用中的适用与局限探析[J]. 档案与建设, 2022, 5(5): 12-15.
[3] 薛玉洁.《民法典》时代档案隐私权保护的困境与建议[J]. 中国档案, 2022(12): 74-76.
[4] 王玉珏, 吴一诺, 凌敏菡.《数据安全法》与《档案法》协调研究[J]. 图书情报工作, 2021, 65(22): 24-34.
[5] 苗运卫. 档案利用场景中个人信息的分类保护研究[J]. 档案学研究, 2022(5): 51-58.
[6] 聂云霞, 黄文琼. 数字档案用户个人信息保护的现实困境与解决思路[J]. 档案学研究, 2019(1): 75-79.
[7] 孙大东, 张欢笑. 我国档案网站隐私政策调查研究[J]. 档案管理, 2018(6): 65-68.
[8] 支凤稳, 徐鼐彦, 姚妩媚. 国内外档案网站隐私政策比较研究[J]. 浙江档案, 2019(12): 29-31.
[9] 周林兴, 徐承来. 信息安全视域下国内档案网站隐私政策合规性研究[J]. 档案学研究, 2022(1): 85-91.
[10] 周林兴, 徐承来, 周丽. 用户画像视域下档案用户隐私问题研究[J]. 档案学研究, 2020(2): 58-64.
[11] 肖秋会, 张博闻. 档案开放负面清单制度构建: 逻辑与框架[J]. 档案学研究, 2022(4): 66-73.
[12] 马海群. 档案数据开放的发展路径及政策框架构建研究[J]. 档案学通讯, 2017(3): 50-56.
[13] 张东华, 尹泷杰. 数据伦理视域下档案数据开放规范发展探析[J]. 档案与建设, 2022, 5(3): 21-24.
[14] 聂云霞, 牟胜男. 数字档案用户隐私风险与防控策略[J]. 档案与建设, 2020, 3(7): 15-19.
[15] 肖秋会, 李珍. 大数据环境下档案信息安全保障体系研究[J]. 中国档案, 2018(4): 76-79.
[16] Richards, N.M. and King, J.H. (2014) Big Data Ethics. *Wake Forest Law Review*, **49**, 393.