我国政府开放数据风险研究热点与趋势分析*

申笑宇[1]，罗书怡[1]，胡文袁[2]，贾新露[3]
（1. 重庆邮电大学　经济管理学院，重庆　400065；2. 数字重庆大数据应用发展有限公司，重庆　401121；
3. 西部数据交易有限公司，重庆　400020）

摘　要：数据作为生产要素的地位不断凸显，数据安全重要性也逐步增加，学界对政府开放数据风险的关注度正不断提升。研究借助 CiteSpace 对中国知网（CNKI）数据库相关文献进行可视化分析，梳理出政府开放数据风险研究的热点和趋势。研究发现，该领域的文献数量相对有限，但总体呈上升趋势。研究主题聚焦于风险理论和风险评估与治理，尤其侧重隐私风险的研究。研究逐步从理论扩展到实践治理，技术手段治理是当前的研究热点，未来可能持续发展。本研究为学界了解政府开放数据风险研究领域的问题提供了一定的帮助，对深化领域研究具有一定意义。

关键词：政府开放数据；数据风险；趋势分析；可视化
中图分类号：G353；G203　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.05.009
引用格式：申笑宇，罗书怡，胡文袁，等. 我国政府开放数据风险研究热点与趋势分析［J］. 网络安全与数据治理，2024，43(5)：61-68.

Research hotspots and trends analysis of government open data risk in China

Shen Xiaoyu[1], Luo Shuyi[1], Hu Wenyuan[2], Jia Xinlu[3]
(1. School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing 400065, China;
2. Digital Chongqing Co., Ltd., Chongqing 401121, China; 3. Western Data Exchange Co., Ltd., Chongqing 400020, China)

Abstract: The status of data as a factor of production continues to be highlighted, emphasizing the criticality of ensuring data security. And academic circles are increasingly paying attention to the risks of government open data. This study leveraged CiteSpace and examined related articles sourced from the China National Knowledge Infrastructure (CNKI) database, elucidating the hotspots and trends in research on risks related to government open data. Findings indicate that while the literature in this field is relatively limited, it exhibits an overall upward trend. Research themes center on risk theory and the assessment and governance of risks, with a particular emphasis on the investigation of privacy risks. The research is gradually transitioning from theoretical exploration to practical governance, with technological governance emerging as the current research hotspot, poised for sustained development in the future. This study contributes to the scholarly understanding of issues in the domain of research on risks associated with open government data, offering valuable insights for furthering research in this field.

Key words: open government data; data risk; trend analysis; visualization

0　引言

2015 年国务院发布《促进大数据发展行动纲要》，提出“加快政府数据开放共享，推动资源整合，提升治理能力”。自此，各省市纷纷开始实施政府数据开放行动。截至 2022 年底，全国已有 208 个省级和城市地方政府上线了数据开放平台。在大力推进数据开放进程以释放政府数据价值的同时，数据开放风险问题值得我们关注。2023 年，印度新冠肺炎疫苗情报网（Co-WIN）疑似发生严重的数据泄露事件，导致印度公民的详细信息遭到泄露。类似政府开放数据平台的数据泄露事件不仅导致了个人隐私泄露的风险，还可能对国家安全和社会安定造成重大影响。根据 IBM 发布的《数据泄露成本报告》显示，2023 年全球数据泄露的平均成本达 445 万美元，与 2020 年相比，三年期间增加了 15.3% 的平均成本，创下历史新高。可见如何在实现政府开放数据价值的同时有效管理和规避风险，已成为当前研究和政策制定的

*基金项目：国家社会科学基金规划项目（23BGL273）

重要议题。目前有学者借助知识图谱工具对中国政府开放数据的研究进行可视化分析[1]，也有学者专注于政府开放数据中的隐私风险[2]。然而，隐私风险只是政府开放数据所面临的诸多风险之一，开放数据的风险还涉及治理、经济、法律、数据特征、元数据、访问获取、技能等多方面的风险[3]。为全面把握政府开放数据的潜在风险，本文拟借助 CiteSpace 工具，对政府开放数据风险领域的现有研究进行可视化分析，梳理出该领域的基本情况、研究热点及未来研究趋势，为未来的研究提供参考。

1　研究方法和数据采集

1.1　研究方法

本文借助 CiteSpace 软件（版本 6.2.R4，64 bit），对收集到的论文进行文献计量和可视化分析。在使用 CiteSpace 进行分析时，需对相关参数进行设置。具体参数设置如下：时间切片设置 2017－2023 年，切片平均年数选择 1 年，即以 1 年为分割点，阈值设置 TopN = 50（即是每个时间片中出现频率数排名前 50 的关键词），节点类型和网络剪裁根据绘制图谱类型选择，其他参数默认预定设置。

1.2　数据采集

以中国知网（CNKI）数据库为检索库，以北大核心、CSSCI、CSCD 的来源期刊为检索范围，采用“篇关摘 =（开放政府数据 + 政府数据开放 + 政府开放数据 + 政府数据 + 政务数据）* 风险”进行高级精确检索，时间范围选择 2012－2023 年，共检索到 134 篇文献，检索时间为 2023 年 8 月 25 日。为进一步提高检索范围与结果的准确性，通过查看标题、作者、关键词和摘要等方法进行人工筛选检查，删除综述、笔谈纪要等以及与主题明显不相关的文献，共获取有效文献 97 篇，筛选后的首篇文献从 2017 年开始。将上述有效文献以 Refworks 数据格式导入 CiteSpace，经数据转换和去重清洗之后有 93 篇文献，以此作为本文研究对象。

2012 年上海市上线了我国第一个政府数据开放平台，我国开始推进政府开放数据的研究。因此，选择 2012 年作为检索起始时间。

2　基本情况分析

2.1　发文量统计分析

发文量对研究主题的受关注程度和学术研究趋势具有一定帮助。政府开放数据风险相关研究成果数量的时间分布图（如图 1 所示）。由图可知该研究领域的年发文量总体呈上升趋势，2017 年以前，年均发文量不足 5 篇，占总发文量的 5.37%；2018－2020 年发文量呈缓慢上升趋势，此阶段年均发文量不超过 10 篇，占总发文量 27.96%，表明研究热点正在形成但还未深入，研究主题有待进一步发掘；2021－2023 年为波动增长期，发文量在 2021 年迅速增加达到峰值，2022 年发文量较 2021 年有所下滑，但总体年均发文量超 20 篇，占总发文量 66.67%。从发文量来看，该领域的总体发文量不多，还存在很大的探索空间，预计在未来一段时间内研究还会不断深化。

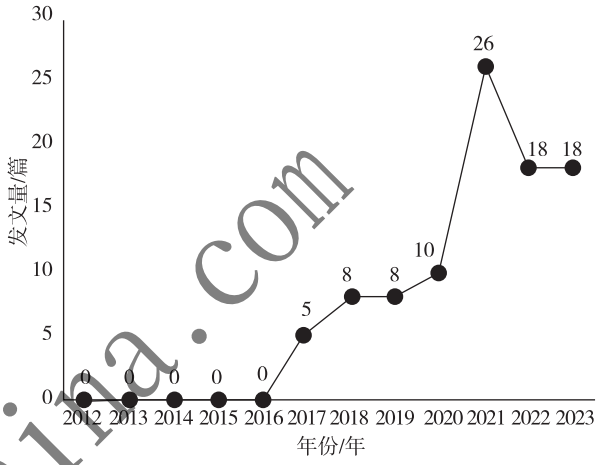

图 1　政府开放数据风险研究的发文量统计图

2.2　作者共现网络分析

作者共现网络分析有助于了解该领域发文量较高的研究者及他们之间合作的紧密程度。利用软件绘制作者共现网络图谱，其中节点类型选择作者，无网络剪裁，其他参数设置不变，得到节点数 133 个，连接线 117 条，密度为 0.013 3 的图谱（如图 2 所示）。

图 2 中节点对应发文作者，节点和标签字体越大，表明该作者的发文量越多。节点连线表示作者间的合作关系，由图 2 可知作者之间合作发文的趋势较为明显。此外，本研究将发文量在 3 篇及以上的作者认定为该领域的高发文量作者，分别是：陈美（14 篇）、梁乙凯（7 篇）、夏义堃（5 篇）、郝文强（4 篇）、陈朝兵（4 篇）、代佳欣（3 篇）、宋烁（3 篇）、曹惠民（3 篇）、臧国全（3 篇），共 9 位，占比 6.77%，高产作者的数量不多。

2.3　机构分布网络分析

机构分布分析可以帮助了解在该领域中的高产机构及其合作趋势。本研究将发文量在 3 篇及以上的机构认为该领域的高发文量机构。根据高发文量机构统计结果（如表 1 所示）可知，共有 17 家（占比 27.42%）单位发文量在 3 篇及以上。发文量大于 5 篇的单位分别是：中南财经政法大学（10 篇），复旦大学（8 篇），山东财经大学（7 篇），武汉大学（6 篇）。

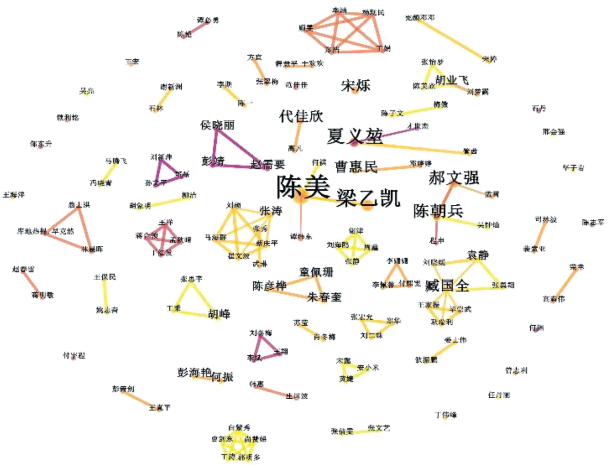

图 2　政府开放数据风险研究的作者共现网络图

表 1　高发文量机构统计（发文量≥3）

序号	发文量	机构
1	10	中南财经政法大学
2	8	复旦大学
3	7	山东财经大学
4	6	武汉大学
5	4	清华大学
6	4	中国社会科学院
7	4	西南财经大学
8	4	湘潭大学
9	4	湖北工业大学
10	4	郑州大学
11	4	西南交通大学
12	3	郑州市数据科学研究中心
13	3	中国矿业大学
14	3	北京大学
15	3	西北大学
16	3	北京科技大学
17	3	中山大学

3　研究热点分析

3.1　关键词共现

研究利用 CiteSpace 软件提取文献关键词信息并进行共现可视化分析，节点类型（NodeTypes）选择关键词（Keyword），网络剪裁（Pruning）选择寻径（Pathfinder），其他参数设置不变，得到节点数 202 个，连接线 360 条，网络密度 0.017 7 的共现图谱（如图 3 所示）。关键词共现是指两个及以上数量的关键词在同一篇文献中出现的现象，共现图谱中节点圆圈大小反映该关键词出现频次高低，圆圈面积越大，则关键词出现的频次越高；连线代表关键词间的共现关系，连接线越多、密度越大，关键词间的联系也越强。节点从内到外的颜色表示从早期到现在的发文时间，部分节点外圈颜色为紫色，说明该关键词中心性高（中心度 > 0.1）。利用 CiteSpace 软件中的“Nodes – Compute Nodes Centrality”功能计算关键词中心度，并按照关键词出现频次和中介中心性大小降序对关键词进行排列，结果如表 2 所示。

结合图 3 和表 2 可知，频次最高的关键词有：政府开放数据、数据安全、隐私风险、数据开放、数据治理等，是该领域研究的热点和重点。中介中心性高的关键词有：数据开放、数据安全、政府开放数据、数据开放风险、数据共享等。

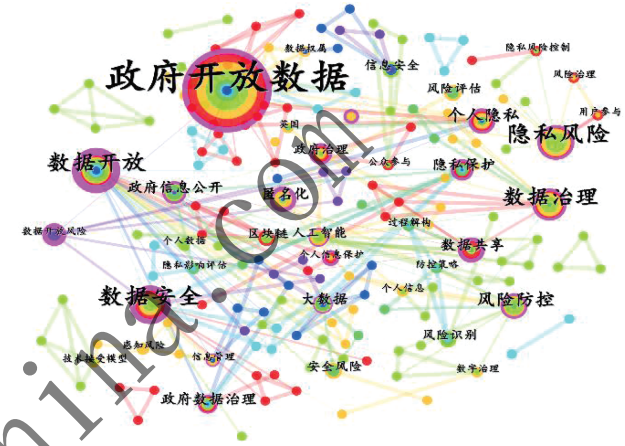

图 3　政府开放数据风险研究关键词共现图谱

表 2　政府开放数据风险研究的高频和高中介中心性关键词统计（前 20 位）

高频次关键词			高中介中心性关键词		
序号	关键词	频次	序号	关键词	中介中心性
1	政府开放数据	69	1	数据开放	1
2	数据安全	13	2	数据安全	0.73
3	隐私风险	13	3	政府开放数据	0.63
4	数据开放	11	4	数据开放风险	0.62
5	数据治理	10	5	数据共享	0.42
6	风险防控	6	6	匿名化	0.42
7	个人隐私	5	7	个人隐私	0.37
8	大数据	4	8	隐私保护	0.34
9	隐私保护	4	9	风险防控	0.29
10	数据共享	4	10	数据治理	0.28
11	政府信息公开	4	11	政府信息公开	0.28
12	匿名化	4	12	政府治理	0.24
13	政府数据治理	4	13	荷兰	0.22
14	区块链	3	14	隐私风险	0.21
15	风险评估	3	15	个人信息保护	0.21
16	风险识别	3	16	政府数据治理	0.16
17	安全风险	3	17	信息管理	0.14
18	人工智能	3	18	大数据	0.12
19	信息安全	3	19	人工智能	0.11
20	政府治理	3	20	感知风险	0.09

3.2 关键词聚类

通过 CiteSpace 生成聚类视图（如图 4 所示），并导出关键词聚类表（如表 3 所示）。图 4 中，聚类编号越小，聚类的体积越大，其次聚类图谱中的模块值（Q 值）和平均轮廓值（S 值）两个指标可以作为评判图谱绘制效果的一个依据。一般而言，Q 值一般在［0，1）区间内，$Q>0.3$ 就意味着划分出来的社团结构是显著的，当 S 值在 0.7 时，聚类是高效率令人信服的[4]。图 4 显示总体聚类效果良好，社团结构显著。

由图 4 和表 3 可知，共有“#0 政府开放数据”“#1 隐私影响评估”“#2 风险控制”“#3 数据治理”“#4 人工智能”“#5 数据开放”“#6 隐私风险”“#7 区块链”“#8 公务员”“#9 技术风险”“#10 隐私计量”11 个聚类。

图 4 政府开放数据风险研究关键词聚类图谱

表 3 政府开放数据风险研究的关键词聚类信息表

聚类号	节点数	轮廓值	平均年份	核心关键词
#0	40	1	2021	数据权属；政府开放数据；政府数据开放；数据开放；数据治理
#1	22	0.948	2019	数据安全；隐私保护；数据开放风险；隐私影响评估；对策分析
#2	18	0.845	2020	风险控制；过程解构；韩国；治理工具；数字治理
#3	17	0.982	2020	数据治理；公共卫生危机；数据价值；协同体系；疫情防控
#4	15	0.992	2021	人工智能；政府大数据；安全治理；数据风险防控；治理变革
#5	14	0.97	2019	数据开放；政府数据治理；信息治理；挑战；协同治理
#6	14	0.899	2021	隐私风险；政府开放数据；用户参与；风险治理；新西兰
#7	13	0.892	2022	区块链；跨界面交互；界面治理；全过程阳光；数字水印
#8	11	0.939	2020	公务员；计划行为理论；推动意愿；技术接受模型；政府数据开放
#9	11	0.883	2019	大数据；技术风险；刑法规制；治理法；法益衡量
#10	10	1	2021	个人隐私；数据隐私；隐私计量；国际经贸条约；国际经贸合作

3.3 研究热点分析

结合高频及高中心性关键词（如表 3 所示）与聚类标识词（如图 4 所示）进行归纳，可以看出关键词和聚类标识词含有相似词，为进一步总结出学界的研究热点，对政府开放数据风险研究的主题进行归纳整理，可以分为风险理论研究和风险治理研究两个层面，其中风险理论研究包含研究对象和风险类型的研究。“政府开放数据（聚类#0）”“数据开放（聚类#5）”与本文研究对象相关；而“隐私风险（聚类#6）”“公务员（聚类#8）”“技术风险（聚类#9）”与风险的类型相关，合并为风险类型。

风险治理研究包含风险评估和治理手段两个主题，将“隐私影响评估（聚类#1）”“隐私计量（聚类#10）”合并成风险评估；“风险控制（聚类#2）”“数据治理（聚类#3）”“人工智能（聚类#4）”“区块链（聚类#7）”合并成治理手段。

表 4 政府开放数据风险研究主题合并结果

研究主题	聚类合并	聚类标识词
风险理论研究	研究对象	#0 政府开放数据 #5 数据开放
	风险类型	#6 隐私风险 #8 公务员 #9 技术风险
风险治理研究	风险评估	#1 隐私影响评估 #10 隐私计量
	治理手段	#2 风险控制 #3 数据治理 #4 人工智能 #7 区块链

3.3.1 风险理论研究

政府开放数据风险的理论研究聚焦于风险内涵和分

类等内容，此研究是进行其他研究的基础和前提。

风险内涵研究。政府开放数据的风险可以理解为政府主动向公众开放数据的过程中可能引发的各种不确定性和潜在威胁，这种不确定性可能导致数据泄露、数据篡改等不同类型的风险，从而对个人、组织、社会甚至国家的利益造成损害[5]。

风险类型研究。为深入理解政府开放数据风险的内涵和风险特点。学术界基于不同的视角和理论对政府开放数据可能引发的风险类别形成了较成系统的研究。有学者基于宏观视角，认为政府开放数据涉及国家安全、政治、行政、隐私、社会和经济方面的风险[6]。由于宏观视角着重于全局性的分析，只能从大范围对政府开放数据的风险进行把控，为更细致深入分析政府开放数据的安全风险，学界从数据生命周期理论出发，进行微观视角的数据风险分析，关注政府开放数据的各个具体阶段的风险。由于学界对公共数据生命周期尚未达成一致意见，故研究也因此产生不同的观点，有学者分析了数据预处理、开放、维护 3 阶段中可能存在的安全和隐私问题[7]。还有学者在分析数据收集、存储和公开利用的常见环节的基础上，对数据安全事故发生后的阶段也进行了分析[8]。但从风险类型的聚类词来看，学界对“#6 隐私风险”“#8 公务员”“#9 技术风险”中分别代表的隐私、人员、技术方面风险的关注度较高，并针对此进行了更为细致的分析。隐私风险方面，有学者从生命周期的动态维度分析了采集处理、存储发布以及开发利用三个阶段中的隐私风险类型、成因及应对策略[9]。人员风险方面，现有研究从公职人员的视角进行切入，认为公职人员的感知责任风险会影响政府数据的开放[10]；技术风险方面，有学者对平台安全风险进行研究[11]。此外，学界意识到技术的发展应用，可能会让政府开放数据在个人隐私、社会安全、经济安全、政府管理等领域的风险进一步加大[12]。比如区块链技术的应用可能会因其本身存在的技术缺陷导致新型数据安全风险[13]。

风险识别研究。学界还从风险识别角度，对风险的影响因素及其形成机制进行研究，丰富了风险理论的研究，旨在建立一个通用的识别框架，以帮助对风险进行系统性的识别和评估。部分学者借助国际经验，构建理论分析框架，有助于更好地识别潜在风险。比如有学者基于加拿大的经验，考虑数据开放的隐私风险水平、开放程度和影响因素三个维度，构建数据开放和隐私保护的平衡框架[14]。也有学者对数据生命周期的各个阶段进行风险影响因素识别研究，比如从动态视角将政府数据开放解构为筹备、实施和完善等阶段，分析了各阶段的风险因素[15]。或从机制原理及运行逻辑出发，构建政府数据开放隐私风险识别机制框架[16]。机制研究为风险识别提供了认知体系，有助于制定相应的风险管理策略。同时，具体风险点识别研究也至关重要，能更加准确地把握风险的本质和影响。有学者分析了城市开放数据中可能导致个人隐私泄露风险的潜在威胁点[17]。还有学者则是将隐私泄露的风险点分为政府部门、公众、数据本身及保密审查标准 4 个层面来识别[18]。

3.3.2 风险治理与对策维度研究

基于风险识别结果，进一步探讨政府数据开放风险评估与治理等相关议题。

风险评估方面。学者通过搭建指标体系对风险进行计量研究，以测量和比较不同风险的大小和影响。有学者以政府数据隐私相关的文本为研究对象，搭建隐私计量模型，对客观视角的隐私值进行计量[19]。有学者搭建隐私风险识别的指标体系，从法律、技术、管理三个维度分析，并运用 Dematel 方法对隐私风险控制影响因素进行分析识别[20]。还有学者针对政府开放数据质量进行研究，结合国际标准和我国需求，构建了突发事件下政府数据开放质量评估体系和指标体系，对政府数据开放质量进行定量评估[21]。

风险治理方面。大量文献研究国际上政府开放数据风险的治理经验，以便为我国政府开放数据风险治理提供参考[22-24]。还有学者从技术视角出发，提出将人工智能、区块链、数字水印、匿名化技术等技术融入政府数据开放风险治理过程，以期更好地达成政府数据开放风险管控目的。比如在人工智能技术背景下，强化风险防控，实现政府数据治理[25]。学者考察了政府数据开放共享的现实问题，评估区块链技术与政府数据开放共享的匹配度，探索实现区块链技术在治理领域融合的可能性[26]。学者认为可以结合区块链与数字水印技术，搭建政府开放数据风险的管控体系[27]。

根据研究热点的结果分析，从政府开放数据风险理论的研究文献来看，学者从风险类型分析这一更宏观和概念层面，扩展到了风险识别机制这一更具体和操作层面的研究，总的来说已经初步形成一个比较系统的框架。从政府开放数据风险治理的现有文献来看，研究还较为分散，虽然已有一些研究从不同角度探讨了政府开放数据风险治理，但尚未形成一个综合性的治理框架，缺乏将各个方面综合考虑的研究。此外虽然学者提出了将新技术如人工智能、区块链和数字水印纳入治理过程的建议，但研究还停留在治理的理论层面，还未详细探讨这些技术的实际可行性，实施的成本以及实施难度。

综合分析政府开放数据风险领域的文献可以看出，

不论是风险理论还是风险治理层面，主要研究文献都侧重于隐私风险视角，说明学术界目前聚焦于该领域关键风险的研究和治理，这也与聚类标识词：“#1 隐私影响评估”“#6 隐私风险”“#10 隐私计量”中反复出现的“隐私”一词的情况正好相符。

4 研究趋势分析

4.1 关键词时区图谱

聚类视图侧重于不同研究领域的知识结构，时间线视图侧重于勾画聚类之间的关系和某个聚类中文献的历史跨度，时区视图是另一种侧重于从时间维度上来表示知识演进的视图，它可以清晰地展示出文献的更新和相互影响[4]。

在工具栏图表上选择时间线视图，得到图 5。图谱从上到下指聚类按大小递减，而从左到右表示时间由远到近。每个聚类都有相对应的一条直线，直线上的节点表示该聚类所涵盖的主要研究内容。此外节点代表相对应的年份出现的关键词，不同的节点之间的连线表示不同的关键词之间的发展承接关系。

4.2 关键词突现

某一时段突现的关键词，可以反映该时段内的研究前沿。通过制作重点关键词的突现图谱，可直观了解到所示时间段内研究热点的变化。在控制面板中的突变选择视图，得到图 6。突发强度是指关键词在一定时间段内的出现频次突然增长的强度，数值越大表明其出现频次越高。在 2017 – 2023 年的研究中，排名前 15 的突现关键词为：数据开放、信息安全、大数据、隐私保护、政府数据治理、过程解构、隐私影响评估、防控策略、风险识别、隐私风险、风险防控、人工智能、技术接受模型、个人信息、数字治理。

4.3 研究演进趋势

结合时间线图谱和重点关键词突现图，可将研究热点演进趋势划分为如下两个阶段。

（1）第一阶段：2017 – 2020 年，研究政府开放数据风险理论，这一阶段的突现关键词有：风险识别、防控策略、隐私影响评估等。

根据我国数据开放的进程可以看出，早期的关注点主要集中在如何加速政府数据的共享开放进程上，对于政府开放数据的潜在风险研究尚未明确。随着相关政策的实施，数据开放程度的不断加大，各类数据安全问题开始逐步显现，学界也开始对数据开放可能带来的风险点进行研究，对政府开放数据风险的研究进入探索阶段。

（2）第二阶段：2021 – 2023 年，研究政府开放数据风险评估治理，这一阶段的突现关键词有：人工智能、技术接受模型、个人信息、数字治理。

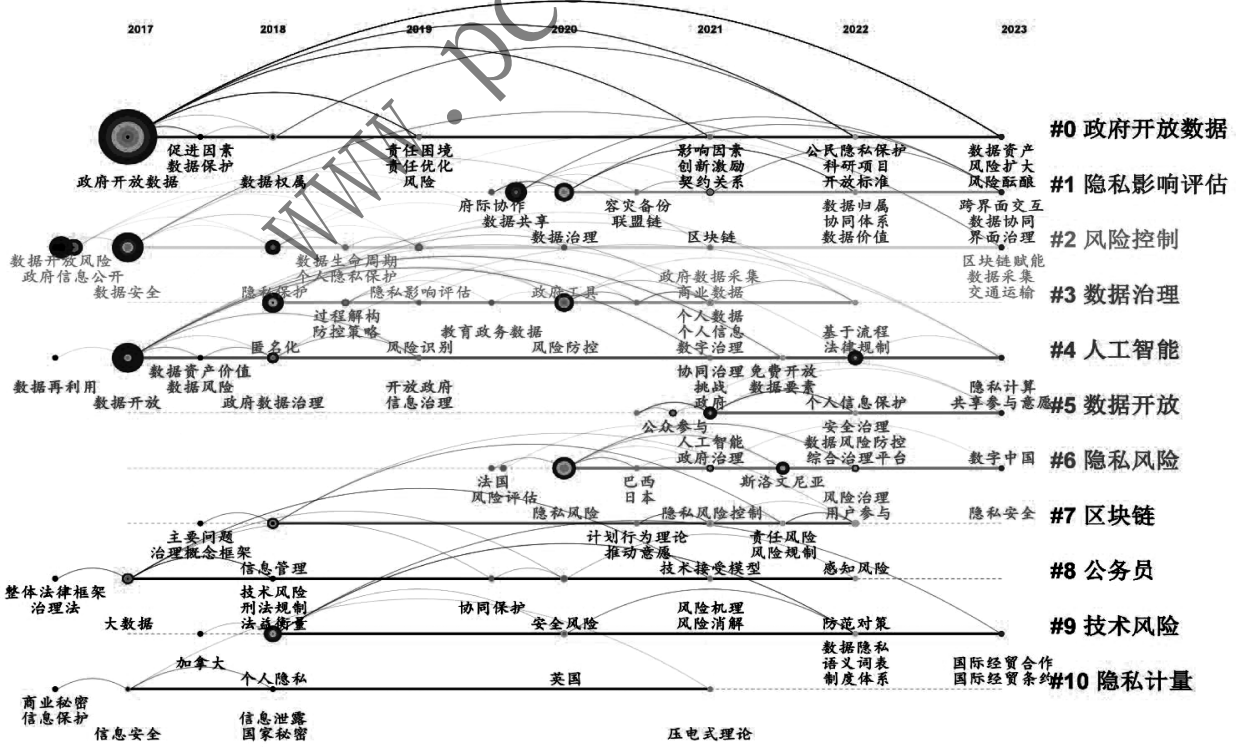

图 5 政府开放数据风险研究时间线视图

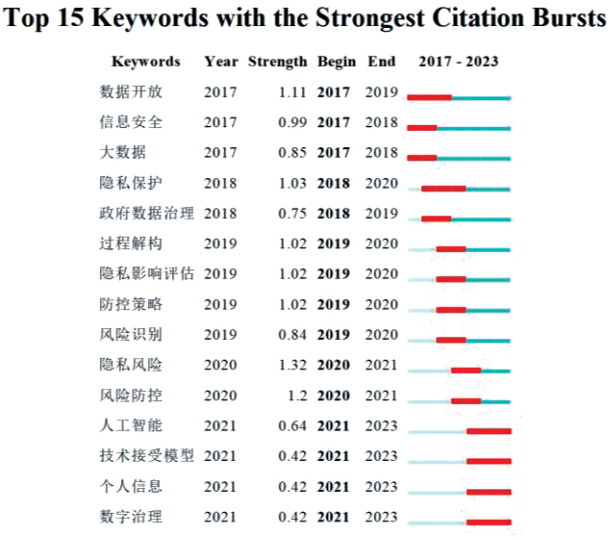

图 6　政府开放数据风险研究突现词图谱

数据作为生产要素的地位不断凸显，保障数据安全重要性也逐步增加，加上我国保障数据安全的法律体系逐渐完善，对政府数据开放风险的关注度也不断提升。从顶层法律来看，2021 年相继出台《中华人民共和国个人信息保护法》及《中华人民共和国数据安全法》，均强调了对可能引发风险的数据应依法予以保密，采取相应措施应对数据安全风险，体现了国家对数据安全风险的重视，为防范数据安全风险提供了法律保障。从行政法规和地方性法规来看，2021 年国务院办公厅关于印发的《要素市场化配置综合改革试点总体方案》中强调“运用技术手段构建数据安全风险防控体系”。各省市相继发布的数据条例中，也不同程度地提到数据安全事件的处理措施，比如浙江省提到存在安全风险的开放数据，应当立即中止开放，并在消除安全风险后开放。学界对政府开放数据潜在风险的关切程度不断增加，从理论研究过渡到政府开放数据风险治理的研究。这意味着从技术角度出发，结合人工智能、区块链、数字水印、匿名化技术等新兴技术，对政府开放数据风险进行治理的主题将会是未来研究的热点和趋势。

5　结论

对 2017 – 2023 年发表的 93 篇政府开放数据风险领域文献进行分析发现，该领域的总体文献数量有限，整体呈上升趋势，机构合作趋势不明显，作者间的合作比较紧密。研究主题主要聚焦于风险理论和风险评估治理两个层面，且大量文献基于隐私风险视角进行研究分析，其中不乏有国际经验研究，隐私风险作为政府开放数据风险领域的关键风险是目前研究的热点话题。研究进程从风险理论研究进展到风险治理研究，意味着学界对该领域认知逐渐深化。早期以明晰政府开放数据风险的概念内涵和类型为主的质性研究。而人工智能等新兴技术的引入，引发了来源更为多样、程度更为深刻的安全风险。比如可能导致数据处理和共享开放的不透明性，使政策监管变得更加困难等。继而该领域风险治理的研究将逐渐向技术手段和解决方案的创新转移。基于上述研究发现，提出几点未来的研究建议。

5.1　探索多维度风险

探索不同类型的政府开放数据风险。政府开放数据风险不再局限于个人隐私风险问题，还可能导致国家机密泄露、公共利益损害和商业机密侵害等方面的风险。学者对政府开放数据涉及的商业机密泄露风险[28]、公共安全风险[29]和国家安全风险[30]的研究还较少见。2022 年，中共中央国务院出台《关于构建数据基础制度更好发挥数据要素作用的意见》，也提出要在保护个人隐私和确保公共安全的前提下，加大数据开放和使用范围。未来研究可以拓展对公共安全、国家安全风险等角度的研究。

探索多维度的政府开放数据风险。不同风险可能存在交叉和协同效应，学界尚未将个人隐私、公共安全和国家安全三个维度的风险结合起来研究，未来可以深入研究三者之间的相互影响机制。探索多维度的风险评估框架，同时评估多个维度的风险，以更全面地管理政府开放数据风险。

5.2　新兴技术与风险治理研究

新兴技术如何治理政府开放数据风险。技术是促进风险治理的有利手段，目前已有学者对此进行探讨，但尚不完善，未来可持续探索如何利用创新技术加强风险治理的研究。此外，还缺乏充分的实际案例分析，验证提出的理论和技术实践中可行性，可以从数据安全厂商的一些应用案例和实践治理方案等方面进行拓展分析。

新兴技术对政府开放数据风险的影响。在探讨如何利用新兴技术改变政府数据开放的风险面貌的同时，需要考虑技术本身可能导致的数据安全、隐私问题和技术滥用等风险。深入研究人工智能、区块链、物联网、隐私计算等新兴技术如何影响政府开放数据风险，引发了该领域哪些新风险等视角进行深入研究。

新兴技术下的政府开放数据法律研究。技术可能导致数据处理的不透明性，使政策监管变得更加困难。政府需要增强政策监管的穿透性，制定新的法律法规来适应新技术，实现数据开放的同时保护隐私和安全，确保数据资源开发利用权利的公正公平。

参考文献

[1] 顾琳，王贵海. 基于文献计量与知识图谱的我国政府开放数据研究 [J]. 图书馆工作与研究，2022 (1)：79 – 86.

[2] 陈朝兵，郝文强. 国内外政府数据开放中的个人隐私保护研究述评［J］. 图书情报工作，2020，64（8）：141－150.
[3] MARTIN S，FOULONNEAU M，TURKI S，et al. Risk analysis to overcome barriers to open data［J］. Electronic Journal of e－Government，2013，11（1）：348－359.
[4] 陈悦，陈超美，刘则渊，等. CiteSpace 知识图谱的方法论功能［J］. 科学学研究，2015，33（2）：242－253.
[5] 才世杰，夏义堃. 试论政府数据开放风险的识别与防范［J］. 图书与情报，2017（4）：104－112，121.
[6] 夏义堃. 论政府数据开放风险与风险管理［J］. 情报学报，2017，36（1）：18－27.
[7] 丁红发，孟秋晴，王祥，等. 面向数据生命周期的政府数据开放的数据安全与隐私保护对策分析［J］. 情报杂志，2019，38（7）：151－159.
[8] 梅傲，陈子文. 政府数据开放中的数据安全隐忧及其纾解［J］. 情报杂志，2023，42（5）：76－85.
[9] 吴钟灿. 政府数据开放中的隐私风险：类型、成因与治理策略［J］. 贵州省党校学报，2021（5）：38－48.
[10] 李斯，陈一. 政府数据开放的感知责任风险及规制研究［J］. 中国图书馆学报，2022，48（6）：97－112.
[11] 完颜邓邓，宋婷. 我国地方政府数据开放平台的安全风险测评［J］. 图书馆论坛，2022，42（2）：119－128.
[12] 庄国波，韩惠. 5G 时代政府数据开放共享的安全风险及防范［J］. 理论探讨，2020，（5）：48－54.
[13] 李轩. 区块链赋能政府数据开放的风险及其规制［J/OL］. 北京航空航天大学学报（社会科学版），1－9［2023－11－15］.
[14] 邹东升. 政府开放数据和个人隐私保护：加拿大的例证［J］. 中国行政管理，2018（6）：75－82.
[15] 代佳欣. 政府数据开放风险识别——基于“过程”的分析框架［J］. 现代情报，2020，40（4）：111－119.
[16] 郝文强. 政府数据开放隐私风险识别机制研究［J］. 电子政务，2021（3）：103－111.
[17] 陈美. 城市政府开放数据的隐私风险及其技术控制策略［J］. 图书馆建设，2018（8）：16－21，27.
[18] 赵需要，彭靖. 政府数据开放中个人隐私的泄露风险与保护［J］. 信息安全研究，2016，2（9）：792－801.
[19] 臧国全，王家振，毕崇武，等. 政府数据中敏感数据识别与隐私计量研究［J］. 图书情报工作，2022，66（15）：66－75.
[20] 陈美，何祺. 开放政府数据的隐私风险关键影响因素识别［J］. 图书情报工作，2023，67（8）：40－49.
[21] 翁士洪，林晨晖，早克然·库地热提. 突发事件政府数据开放质量评估研究：新冠病毒疫情的全国样本实证分析［J］. 电子政务，2020（5）：2－13.
[22] 陈美. 政府开放数据的隐私风险评估与防控：英国的经验［J］. 中国行政管理，2020（5）：153－159.
[23] 陈美. 政府开放数据的隐私风险评估与防控：法国的经验［J］. 情报资料工作，2020，41（2）：99－105.
[24] 陈美，谭纬东. 政府开放数据的隐私风险评估与防控：新西兰的经验［J］. 情报理论与实践，2020，43（5）：110－114，90.
[25] 何振，彭海艳. 人工智能背景下政府数据治理新挑战、新特征与新路径［J］. 湘潭大学学报（哲学社会科学版），2021，45（6）：82－88.
[26] 张翠梅，方宜. 区块链架构下政府数据开放共享治理研究［J］. 南通大学学报（社会科学版），2021，37（6）：60－70.
[27] 张怡梦，陈美欣，胡业飞. 技术赋能下的政府数据开放风险管控体系设计［J］. 情报杂志，2023，42（4）：178－185.
[28] 赵需要，侯晓丽，彭靖. 政府数据开放中商业秘密的泄露风险与保护策略［J］. 情报理论与实践，2017，40（7）：11－16.
[29] 姚志奋，王保民. 政府数据开放的公共安全悖论及其法治策应［J］. 中国科技论坛，2023（8）：139－149.
[30] 侯晓丽，彭靖，赵需要. 政府数据开放中国家秘密的泄露风险与保护策略［J］. 情报理论与实践，2018，41（7）：53－59.

（收稿日期：2023－11－16）

作者简介：

申笑宇（1988－），通信作者，女，博士，副教授，主要研究方向：开放数据安全与治理。E-mail：shenxy@ cqupt. edu. cn。

罗书怡（1997－），女，硕士，主要研究方向：开放数据安全与治理。

胡文袁（1995－），男，本科，主要研究方向：公共数据开放利用。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部