Operations Research and Fuzziology 运筹与模糊学, 2023, 13(4), 3072-3081
Published Online August 2023 in Hans. https://www.hanspub.org/journal/orf
https://doi.org/10.12677/orf.2023.134308

Hans汉斯

个人隐私数据治理研究：热点、趋势与前沿

郭江丽

贵州大学公共管理学院，贵州 贵阳

收稿日期：2023年6月15日；录用日期：2023年7月31日；发布日期：2023年8月9日

摘　要

本文以Web of Science核心合集数据库2008~2022年发表的1061篇关于个人隐私数据治理研究的文献为研究对象，运用信息可视化软件CiteSpace，主要对文献引文聚类图谱、关键词聚类图谱、时间线图谱及文献共被引突发强度进行分析，揭示个人隐私数据治理研究领域的研究热点、趋势与前沿。分析发现，其研究热点主要聚焦于数据生命周期层面，实际运用层面与具体方法与技术层面，其研究的演化趋势主要分为三个阶段，从研究前沿上看，位置隐私、接触者追踪、自我披露、记录隐私以及在线隐私代表了在个人隐私数据治理研究领域的重要方面。对此，文章给出进一步的总结和思考，以期为个人隐私数据治理领域的深入研究提供参考。

关键词

个人隐私数据，热点分析，趋势研究，前沿分析，CiteSpace

Research on Personal Privacy Data Governance: Hot Spots, Trends and Frontiers

Jiangli Guo

School of Public Administration, Guizhou University, Guiyang Guizhou

Received: Jun. 15th, 2023; accepted: Jul. 31st, 2023; published: Aug. 9th, 2023

Abstract

This paper takes 1061 articles on personal privacy data governance published in Web of Science core collection database from 2008 to 2022 as the research object, and uses information visualization software CiteSpace. This paper mainly analyzes the literature citation clustering graph, key-

文章引用: 郭江丽. 个人隐私数据治理研究: 热点、趋势与前沿[J]. 运筹与模糊学, 2023, 13(4): 3072-3081.
DOI: 10.12677/orf.2023.134308

word clustering graph, timeline graph and literature co-citation burst intensity, and reveals the research hotspots, trends and frontiers in the research field of personal privacy data governance. It is found that the research mainly focuses on the data life cycle level, the practical application level and the specific methods and technologies level, and the evolution trend of its research is mainly divided into three stages. From the research frontier, location privacy, contact tracking, self-disclosure, record privacy and online privacy represent important aspects in the research field of personal privacy data governance. In this regard, the paper gives a further summary and reflection, in order to provide a reference for the in-depth research in the field of personal privacy data governance.

Keywords

Personal Privacy Data, Hot Spot Analysis, Trend Research, Frontier Analysis, CiteSpace

1. 引言

随着大数据时代的到来以及云计算、物联网、移动通信等新一代信息技术的快速发展和应用，海量的数据正在急速地产生和流通。这些海量的数据背后蕴藏着巨大的经济与政治利益，使得个人、政府、企业等从中获益。与此同时，个人隐私数据泄露事件也频繁发生，给个人、政府、企业等带来了不同程度的影响与损失[1]。

党的二十大报告中提出要加强个人信息保护，2020 年 5 月 28 日第十三届全国人民代表大会第三次会议通过的《中华人民共和国民法典》第四编第六章也专门对隐私权和个人信息保护作了规定。2018 年 5 月 25 日，欧盟出台《通用数据保护条例》(General Data Protection Regulation)，简称“GDPR”正式生效，GDPR 的核心是更新数字时代的相关隐私条款，并确保各机构对其用户的个人数据保护，GDPR 为隐私和数据保护设定了一个新的全球标准，越来越多的国家都借鉴了 GDPR 中的一些原则和条例。由此可知，各个国家都开始重视个人隐私数据的保护，与此相关的研究也相应增多，但目前聚焦于个人隐私数据治理研究的热点、趋势与前沿的文献并不多。为此，本研究采用科学知识图谱方法，对检索到的相关文献进行多层次的研究，即利用 CiteSpace 知识图谱进行可视化分析，探测个人隐私数据治理研究领域的发展状况。通过对样本文献的研究机构、热点主题聚类等知识图谱进行分析，以期为个人隐私数据治理领域的深入研究与实践探索提供参考。

2. 数据来源与研究方法

2.1. 数据来源

本文数据来源于 WOS 数据库。高级检索模式下，选择 WOS 核心合集数据库，文献类型限定为期刊文献(Article)，语言限定为英语(English)，为保证文献来源的权威性，期刊索引范围限定为 SCI 期刊(science citation index expanded)和 SSCI 期刊(social science citation index)。以 TS = (personal privacy data OR personal privacy information)为检索条件，检索得到 4573 篇文献，然后通过阅读这些文献的题目及摘要，筛选掉与研究主题明显不相关的文献，经筛选后得到 2008 至 2022 年的 1061 篇文献。

2.2. 研究方法

本研究采用知识图谱(knowledge map)进行数据分析。知识图谱是以知识域为对象，显示科学知识的发展进程与结构关系的一种图像，用可视化的图谱揭示知识之间的联系和知识的进化规律[2]。CiteSpace是一款用于对学科文献数据进行计量与分析的信息可视化软件。通过对文献间的分析与数据可视化，可以绘制一系列的蕴含学科领域发展的知识图谱，以直观展示学科领域的研究热点、趋势前沿等。本文采用 CiteSpace 中的期刊共被引的学科分布图谱分析研究领域的学科分布情况，以研究机构共现图谱分析机构间的合作情况，以文献引文聚类图谱和关键词聚类图谱综合分析研究热点情况，以关键词时间线图谱和文献共被引突发强度排序图谱分别分析研究的演化趋势与研究前沿情况。

3. 实证分析与讨论

3.1. 文献数据计量分析

3.1.1. 论文发表数量的时间分析

样本文献发文量情况如图 1 所示，总体呈现逐年递增趋势，对其进行曲线拟合，符合指数函数，且拟合效果较好，发文量拟合曲线的 R^2 达到 0.9598。根据发文量变化趋势，结合国外个人隐私数据治理领域的实际情况，将国外对该领域的研究划分为两个阶段：第一阶段(2016 年之前)，主要围绕着开发与保护个人隐私数据相关的技术展开，文献量较少；第二阶段(2016 年之后)，2016 年 4 月 27 日，欧洲议会通过了规制个人数据或个人信息的《通用数据保护条例》，并于 2018 年 5 月 25 日正式生效，引起了学者与专家的重视，与此相关的文献量剧增。

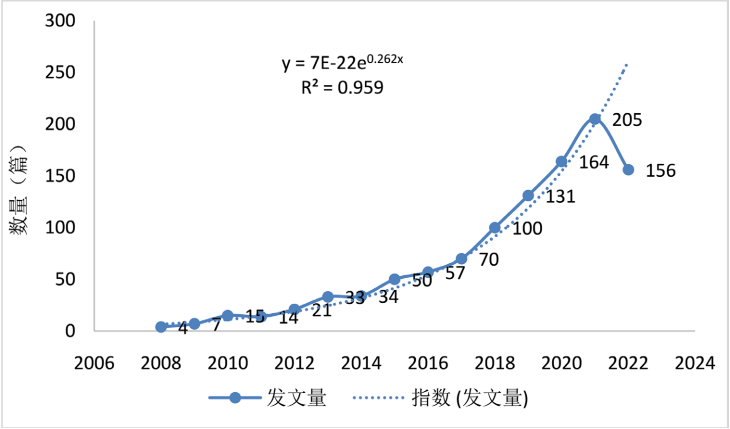

Figure 1. Change trend of the number of literature articles
图 1. 文献发文量变化趋势

3.1.2. 期刊共被引的学科聚类分析

本文通过对期刊共被引的学科进行聚类，得到图 2，以显示个人隐私数据治理研究领域的学科分布情况。根据图 2 可知，个人隐私数据治理研究领域的期刊共被引的学科聚类结果主要为信息科学与图书馆学、企业经济学、卫生保健科学与服务、计算机科学(人工智能方面)、计算机科学(理论与方法方面)、哲学、数学、计算机科学(软件工程方面)、法学、电信学、计算机科学(硬件结构方面)。总体上，关于个人隐私数据治理领域的研究具有横跨自然科学与社会科学的特征。

3.1.3. 研究机构的合作网络分析

对筛选得到的文献进行研究机构的合作网络分析，将阈值设为 7 得到图 3。图中连线代表研究机构

间的合作网络关系，节点代表机构发表论文数量的多少。其中，共现频次前 15 的机构分别是西安电子科技大学(32)、北京邮电大学(18)、广州大学(15)、南京信息工程大学(13)、悉尼科技大学(11)、武汉大学(11)、中国科学院(10)、福建师范大学(10)、卡耐基梅隆大学(10)、穆尔西亚大学(9)、罗维拉－威尔吉利大学(8)、沙特国王大学(8)、电子科技大学(8)、联邦科学与工业研究组织 CSIRO (7)、迪肯大学(7)。由此可知，在个人隐私数据治理研究领域，国内外都有比较关注该领域的研究机构，且机构间有较多的文献合作。

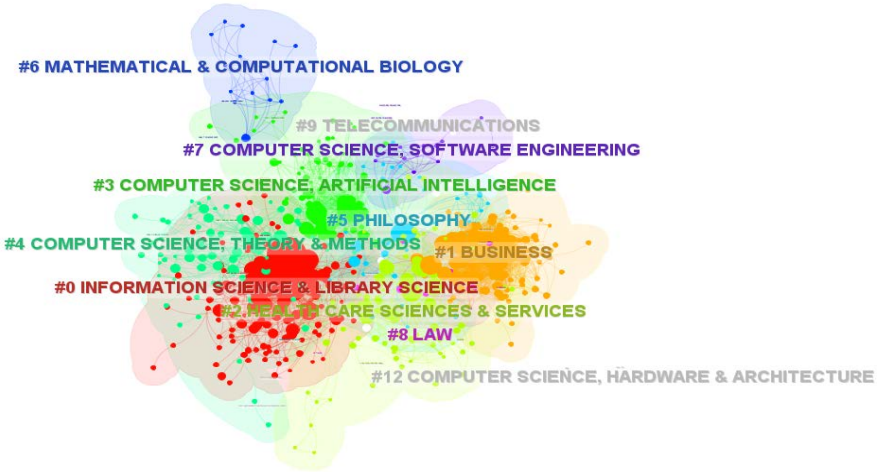

Figure 2. Subject clustering map of periodical co-citation
图 2. 期刊共被引的学科聚类图谱

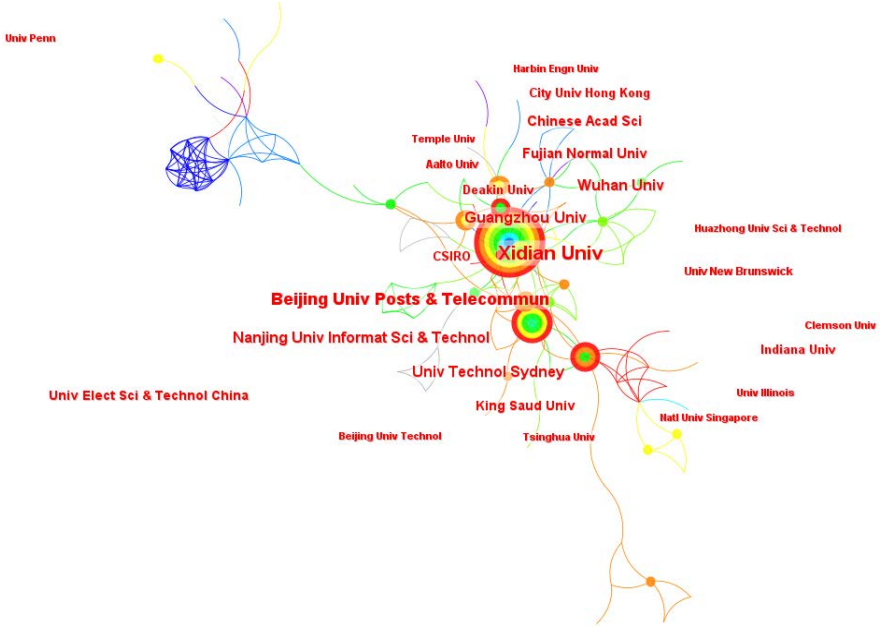

Figure 3. Co-occurrence map of research institutions
图 3. 研究机构共现图谱

3.2. 研究热点分析

研究热点是某个领域专家学者们共同关注的话题，具有很强的时代特征。确定个人隐私数据治理研究领域的研究热点，分析该领域的研究趋势，对把握该领域的发展变化具有重大意义与价值。研究热点通过

对数似然率算法(LLR)进行聚类，自动生成聚类标识词图谱，本文的聚类来源是文献的引用文献和关键词。通过对样本文献进行文献引文记录的 LLR 聚类，得到图 4。其中聚类节点的连线代表共被引情况，大小代表共被引的频次，即关联程度。其聚类标签主要包括：#0 隐私问题或隐私忧虑；#1 区块链；#2 大数据；#3 万维网；#4 云计算；#5 可搜索加密；#6 新型冠状病毒肺炎；#7 无处不在的健康数据；#8 算法；#9 众包；#11 图像隐私；#15 公共政策；#16 可用的隐私。通过对样本文献进行关键词聚类，得到图 5。其聚类标签主要包括：#0 云计算；#1 信息隐私；#2 数据共享；#3 数据保护；#4 深度学习；#5 数据隐私；#6 位置隐私；#7 差分隐私；#8 系统；#9 隐私行为；#10 移动电话；#11 隐马尔可夫模型；#12 隐私问题或隐私忧虑；#13 物联网；#14 数据挖掘中的隐私保护；#15 个人隐私。对这两类聚类所得到的结果进行比对与合并，可知，当下个人隐私数据治理研究领域内的研究热点主要聚焦于以下三个层面。

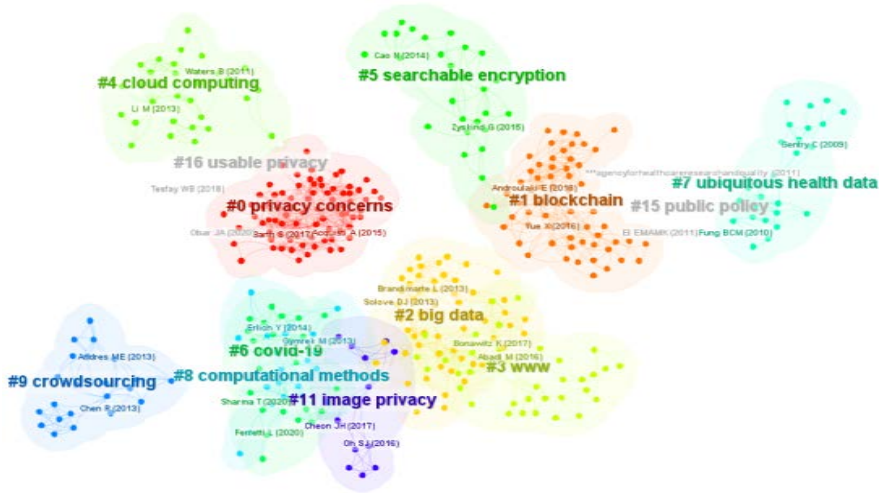

Figure 4. Literature citation cluster map
图 4. 文献引文聚类图谱

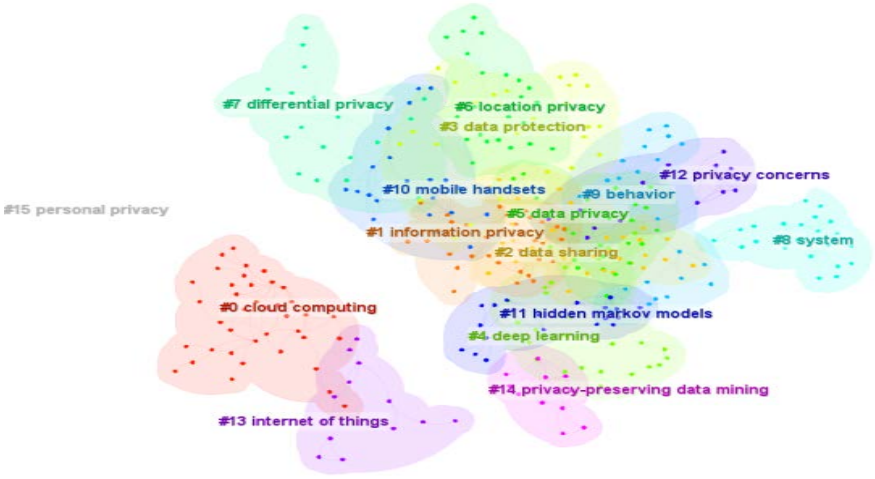

Figure 5. Keyword cluster map
图 5. 关键词聚类图谱

3.2.1. 数据生命周期层面

数据生命周期层面下的个人隐私数据治理，涉及个人隐私数据的采集、存储、处理、传输、交换、

销毁阶段的数据保护与数据共享等。在数据采集方面，Soohyung Kim 与 Yon Dohn Chung [3]学者提出了一种用于隐私保护数据收集的新协议，设计了一种协作方法来收集分布式个人数据，从而达到在不侵犯隐私的情况下收集个人数据的目的；在数据存储方面，Yashothara Shanmugarasa，Hye-young Paik [4]等学者讨论了个人数据存储(PDS)——以用户为中心的数据存储或处理环境，用于实施隐私感知的智能家居数据存储，以协助用户做出数据共享决策，以避免意外的隐私事故；在数据处理与传输方面，Lalitha Sankar，Wade Trappe [5]等学者讨论了数据处理与传输过程中的隐私保护，并通过信号处理方法来解决隐私问题；在数据交换方面，Jason I. Pallant，Jessica L.Pallant [6]聚焦于消费者何时以及如何愿意与零售商交换数据，同时利用社会交换理论和隐私演算来研究消费者与零售商交换数据的意愿差异；在数据销毁方面，Young Ki Kim，Saeed Ullah [7]等提出了一种基于强化学习的数据自毁方案，以实现数据安全管理。

3.2.2. 实际运用层面

实际运用层面下的个人隐私数据治理，涉及在线隐私、位置隐私、医疗卫生数据隐私等。在线隐私方面主要聚焦于两个方面：一是为在线社交网络开发的隐私保护解决方案，例如匿名化、屏蔽、加密和假名化等，以保护用户的隐私[8]；二是在线隐私悖论，即用户声称非常关心他们的隐私，但他们几乎没有采取任何实际行动来保护他们的个人数据，用户态度与其实际行为之间存在差异[9]，Gajendra Liyanaarachchi [10]采访了代表 13 个国家的 30 名千禧一代，使用扎根的理论方法探讨了民族文化对在线零售背景下信息披露态度的影响，同时提出了一个新的框架，即隐私悖论金字塔，通过民族文化的视角来管理隐私悖论。Byoungsoo Kim [11]等学者从隐私悖论的角度探讨了用户在社交网站中披露行为的形成机制，研究发现，对个人信息的感知控制在增强对社交网站(SNS)提供商的信任、用户披露个人信息的意图以及披露行为方面发挥着重要作用，此外，对个人信息的感知控制减轻了隐私问题的程度。位置隐私方面主要聚焦于基于位置的服务(LBS)中的位置隐私以及与保护位置隐私方面的技术这两块。Dan Yin [12]等研究了移动数据密度分布的隐私保护问题。其设计了一种与在原始数据中添加噪声以保护隐私不同的生成对抗网络(GAN)来训练生成器和鉴别器以生成隐私保护的数据的方法，对两个真实世界的移动数据集进行了广泛的实验，结果表明，该方法在数据效用和攻击误差方面均优于差分隐私方法。医疗卫生数据隐私方面，主要聚焦于电子健康记录(EHR)、个人健康信息(PHI)以及公共安全与个人隐私以及围绕它们所展开的防止数据泄露的技术方法这几个层面。Na Young Ahn，Jun Eun Park [13]等以韩国的案例，探讨了在 COVID-19 期间平衡个人隐私和公共安全的相关问题与如何实施个人同意程序和大数据的适当使用，同时他们研究了原始数据、去标识化数据和加密数据的使用模式，为其它国家在平衡个人隐私和公共安全方面提供了借鉴。

3.2.3. 具体方法与技术层面

具体方法与技术层面的个人隐私数据治理，涉及差分隐私、深度学习、隐马尔可夫模型、匿名化、区块链、可搜索加密、算法、众包等。这些技术与方法其研究的重心主要聚集在技术与方法本身，或是技术与方法的改进以及技术与方法的配套使用上，从而达到防止个人隐私数据泄露或被滥用的目的。而在众多的技术与方法中，研究者使用频次最高的是差分隐私与匿名化技术。差分隐私旨在为敏感数据的计算功能过程提供保证，并具有许多功能，使其成为量化隐私的具有吸引力的方法，其通过确保过程是随机的，并承诺以下内容来保证隐私：如果数据库中任何记录(对应于单个个体)的参与不会对任何结果的概率产生太大影响，则算法是微分私有的[14]。Anand D. Sarwate [15]等重点介绍了对连续数据进行操作的差分私有统计方法和算法，同时他们讨论了分类程序、降维技术和信号处理技术。在匿名化技术方面，比较流行的是 K 匿名化技术，K 匿名化技术允许发布包含个人信息的数据库，同时确保一定程度的个人隐私。Aristides Gionis [16]等研究了泛化的概念，并提出了三种信息理论措施，用于捕获匿名化过程中丢失的信息量。

3.3. 研究趋势与前沿分析

3.3.1. 研究趋势分析

为了更好地观察到每个时期内个人隐私数据治理研究领域的演化趋势，本文将样本文献的关键词聚类结果按照时间线图显示，得到图 6。可以将个人隐私数据治理研究领域的演化路径分为几个重要的时间段：1) 2008~2013 年，大部分学者的研究重心放在个人隐私数据保护的技术、模型上，如差分隐私、匿名化等。其中比较典型的研究包括 Jinhyung Kim，Choonsik Park [17]等学者所讨论的隐私保护方面的防泄漏系统(DLP system)，Sara Motahari，Sotirios G. Ziavras [18]等研究者提出的一种基于信息熵的用户匿名水平现实估计和利用基本信息熵属性的复杂性降低方法以解决在线隐私保护问题；2) 2014~2019 年，这一阶段，较之前一阶段，研究重心更加聚焦于某个具体场域下的隐私数据保护，如智能电表中的隐私保护、在线隐私等。相关的研究包括 Dongyoung Koo，Youngjoo Shin [19]等学者提出的智能电网系统中存在个人信息推断的可能性，单个智能电表测量的使用信息的隐私性受到威胁，并由此提出智能电网系统中多源智能电表的隐私保护聚合与认证方案，以保护用户隐私，以及 Moritz Büchi [20]等研究者解释了互联网用户使用结构方程建模在线保护其隐私的自助活动，其提出一般的互联网技能是解释用户隐私行为的关键，这些技能使用户能够降低隐私丢失的风险，同时从越来越依赖于个人数据披露的在线活动中获得好处；3) 2020~2022 年，这一阶段，由于全球疫情肆虐，以此相关的位置隐私，医疗健康卫生方面的隐私以及开发相关的隐私保护技术等引起学者们的高度关注，与此相关的研究也急剧增加。比如 Tyler M Yasaka [21]等学者致力于开发一种有效的接触者追踪智能手机应用程序，他们建议使用人际互动的匿名图来进行一种新颖形式的接触者追踪，并开发了一个概念验证智能手机应用程序来实现这种方法，从而达到不收集位置信息或其他个人数据，尊重用户隐私的目的。Sheikh Mohammad Idrees [22]等研究者主张采用基于区块链的去中心化网络来处理与可用的接触者追踪应用程序，以期实现该应用程序在不影响性能和效率的情况下为用户提供保护隐私的接触者追踪。

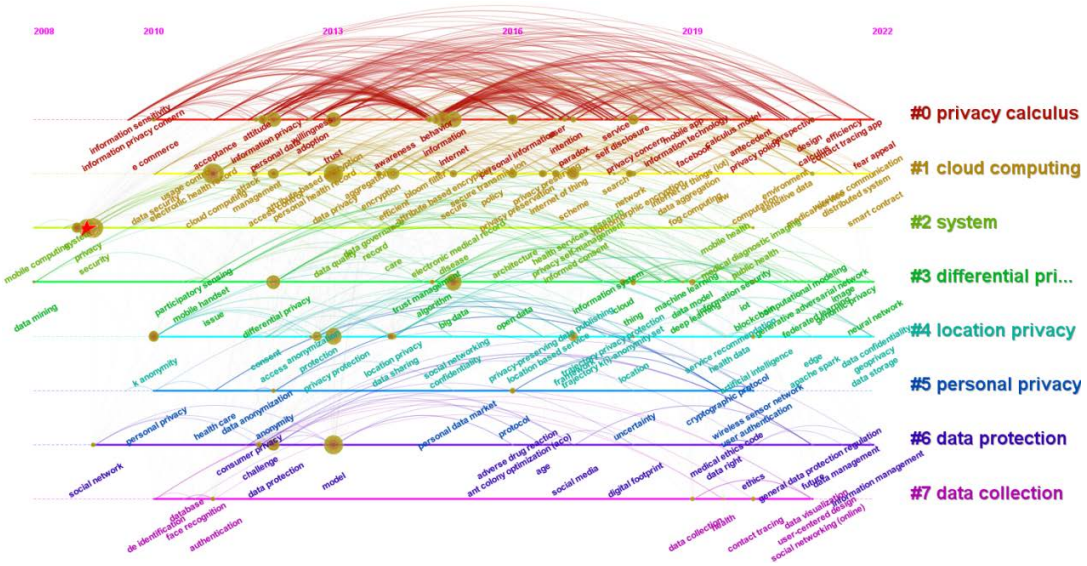

Figure 6. Timeline map
图 6. 时间线图谱

3.3.2. 研究前沿分析

研究前沿指某一领域内最具发展潜力、最先进的研究主题或方向。本文研究前沿的分析主要是通过文献

共被引突发强度进行，从而识别发展新趋势及研究主题的突变。样本文献的共被引突发强度排序情况如表1所示，对表1进行解读与分析。首先从突发强度与时间维度来解读与分析。从突发强度上看，排名前六的分别是location privacy、trust、record、online、access、system。由此可知，位置隐私、记录隐私(包括PHR个人健康记录、搜索浏览数据记录、行车数据记录等)以及在线隐私代表了在个人隐私数据治理研究领域的重要方面。同时，信任是影响个人隐私数据披露的一个重要因素。此外，数据的访问获取，围绕隐私保护所开发的系统方法及技术也是个人隐私数据治理研究领域专家学者比较关注的方面。从突发持续的时间维度来看，突发持续时间排名前三的分别是data mining、location privacy、internet user，说明在数据挖掘、位置隐私及互联网用户的隐私方面，引起了该领域专家学者持续的关注。同时，着眼于最新的突发持续时间，可以发现，contact tracing、self disclosure、health，其突发持续时间都在2020年至2022年，说明最新的研究前沿就聚焦于接触者追踪、自我披露、健康方面。联系当下实际，这一时间段主要是围绕疫情下的个人隐私数据治理研究所展开，其中涉及个人位置移动数据隐私、健康记录数据隐私、隐私披露等诸多方面。

Table 1. The ranking of burst intensity of co-cited literature
表1. 文献共被引突发强度排序

关键词	年份	强度	起始年	结束年	2008~2022年
data mining	2008	2.38	2008	2015	
Electronichealthrecord	2008	2.92	2011	2013	
cloud computing	2008	2.3	2011	2014	
consent	2008	2.14	2012	2015	
trust	2008	4.36	2013	2016	
system	2008	3.18	2013	2015	
internet user	2008	2.03	2013	2017	
location privacy	2008	4.37	2014	2019	
record	2008	4.11	2014	2016	
model	2008	1.95	2014	2016	
online	2008	3.39	2015	2018	
big data	2008	2.92	2015	2017	
risk	2008	2.88	2015	2017	
access	2008	3.36	2016	2018	
behavior	2008	2.87	2017	2019	
anonymization	2008	2.3	2017	2018	
contact tracing	2008	2.65	2020	2022	
self disclosure	2008	2.27	2020	2022	
health	2008	2.21	2020	2022	

4. 结论与展望

人们在享受海量数据给生产与生活带来巨大便利的同时，也面临着数据泄露或滥用所带来的风险与

挑战[23]。对个人隐私数据治理领域进行文献计量研究与知识图谱研究，有利于把握该领域的前沿热点问题，同时为应对数据泄露或滥用所带来的风险与挑战提供理论与方法上的指导，以使数据的使用更好造福于人。

4.1. 研究结论

本文通过 Web of Science 数据库，借助信息可视化软件 CiteSpace，对有关个人隐私数据治理研究领域的文献进行科学计量分析，从发文规模、学科分布、机构合作、热点、趋势前沿这几个维度来看，具体结论如下：

从发文规模上看，个人隐私数据治理领域的文献逐年递增，且从 2016 年之后，增速加快。学科分布方面，该领域研究主要分布在计算机科学方面，社会科学方面也涉及，但所占比重较小。从机构合作上看，在个人隐私数据治理研究领域，国内外研究机构都比较关注该领域，国内的科研机构间分布较紧密，国外的研究机构间分布相对松散，国内外的研究机构间合作较少。

从研究热点上看，当下个人隐私数据治理研究领域内的研究热点主要聚焦于以下三个层面：一是数据生命周期层面，该层面下的个人隐私数据治理，涉及个人隐私数据的采集、存储、处理、传输、交换、销毁阶段的数据保护与数据共享等；二是实际运用层面，该层面下的个人隐私数据治理，涉及在线隐私、位置隐私、医疗卫生数据隐私等；三是具体方法与技术层面，涉及差分隐私、深度学习、隐马尔可夫模型、匿名化、区块链、可搜索加密、算法、众包等，其重心主要聚集在技术与方法本身，或是技术与方法的改进以及技术与方法的配套使用上。

从研究趋势上看，其演化趋势分为三个阶段：2008~2013 年，研究重心放在个人隐私数据保护的技术、模型上；2014~2019 年，研究重心更加聚焦于某个具体场域下的隐私数据保护，如智能电表中的隐私保护等；2020~2022 年，位置隐私，医疗健康卫生方面的隐私以及开发相关的隐私保护技术等获得高度关注。从研究前沿上看，接触者追踪、自我披露、位置隐私、记录隐私(包括 PHR 个人健康记录、搜索浏览数据记录、行车数据记录等)以及在线隐私代表了在个人隐私数据治理研究领域的重要方面。

4.2. 未来展望

对个人隐私数据治理领域的相关文献进行梳理与分析，是为了回应现实诉求，以更好保护个人隐私数据。基于上述文献计量与知识图谱分析，本文提出以下几点展望：

第一，加强机构间的交流与合作。当前个人隐私数据治理领域，国内外的研究机构间合作较少。未来应鼓励国内外学者加强交流与合作，同时要鼓励大学、企业、政府等主体间开展跨机构合作交流，统筹研究资源，形成多个研究网络与研究核心。

第二，加强学科间的交流与学习。现有的个人隐私数据治理领域，多聚焦于计算机科学，侧重技术与方法的开发方面，学科视角相对单一。未来应多借鉴心理学、管理学等学科的研究思路与研究方法，以此探究影响人们披露个人隐私数据的内在动因以及多元主体参与个人隐私数据治理方面的深层次问题。以加强学科的思想交流与碰撞，促进理论创新，为更好地解决现实中遇到的个人隐私数据相关的问题提供指导。

第三，鼓励多元主体参与个人隐私数据治理。当前的研究主要聚焦于在线隐私、位置隐私等以及开发相关的技术方面，治理主体方面，也主要关注政府、企业、消费者等单个主体在个人隐私数据治理方面的活动，但个人隐私数据泄露等问题涉及众多的利益相关者，仅依靠单一主体无法实现有效治理。因此，未来的研究应鼓励多元主体参与到个人隐私数据治理中来。

参考文献

[1] 刘雅辉, 张铁赢, 靳小龙, 程学旗. 大数据时代的个人隐私保护[J]. 计算机研究与发展, 2015, 52(1): 229-247.

[2] 李杰, 陈超美. CiteSpace: 科技文本挖掘及可视化[M]. 第 2 版. 北京: 首都经济贸易大学出版社, 2017.

[3] Kim, S. and Chung, Y.D. (2017) An Anonymization Protocol for Continuous and Dynamic Privacy-Preserving Data Collection. *Future Generation Computer Systems*, **93**, 1065-1073.

[4] Shanmugarasa, Y., Paik, H., Kanhere, S.S., *et al*. (2022) Automated Privacy Preferences for Smart Home Data Sharing Using Personal Data Stores. *IEEE Security & Privacy*, **20**, 12-22. https://doi.org/10.1109/MSEC.2021.3106056

[5] Sankar, L., Trappe, W., Ramchandran, K., *et al*. (2013) The Role of Signal Processing in Meeting Privacy Challenges: An Overview. *IEEE Signal Processing Magazine*, **30**, 95-106. https://doi.org/10.1109/MSP.2013.2264541

[6] Pallant, J.I., Pallant, J.L., Sands, S.J., Ferraro, C.R. and Afifi, E. (2022) When and How Consumers Are Willing to Exchange Data with Retailers: An Exploratory Segmentation. *Journal of Retailing and Consumer Services*, **64**, Article ID: 102774. https://doi.org/10.1016/j.jretconser.2021.102774

[7] Kim, Y.K., Ullah, S., Kwon, K., Jang, Y., Lee, J. and Hong, C.S. (2018) Reinforcement Learning Based Data Self-Destruction Scheme for Secured Data Management. *Symmetry*, **10**, Article No. 136. https://doi.org/10.3390/sym10050136

[8] Majeed, A., Khan, S. and Hwang, S.O. (2022) A Comprehensive Analysis of Privacy-Preserving Solutions Developed for Online Social Networks. *Electronics*, **11**, Article No. 1931. https://doi.org/10.3390/electronics11131931

[9] Barth, S. and de Jong, M.D.T. (2017) The Privacy Paradox—Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review. *Telematics and Informatics*, **34**, 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

[10] Liyanaarachchi, G. (2021) Managing Privacy Paradox through National Culture: Reshaping Online Retailing Strategy. *Journal of Retailing and Consumer Services*, **60**, Article ID: 102500. https://doi.org/10.1016/j.jretconser.2021.102500

[11] Kim, B. and Kim, D. (2020) Understanding the Key Antecedents of Users' Disclosing Behaviors on Social Networking Sites: The Privacy Paradox. *Sustainability*, **12**, Article No. 5163. https://doi.org/10.3390/su12125163

[12] Yin, D. and Yang, Q. (2018) GANs Based Density Distribution Privacy-Preservation on Mobility Data. *Security and Communication Networks*, **2018**, Article ID: 9203076. https://doi.org/10.1155/2018/9203076

[13] Ahn, N.Y., Park, J.E., Lee, D.H. and Hong, P.C. (2020) Balancing Personal Privacy and Public Safety during COVID-19: The Case of South Korea. *IEEE Access*, **8**, 171325-171333. https://doi.org/10.1109/ACCESS.2020.3025971

[14] Ganta, S.R., Kasiviswanathan, S.P. and Smith, A. (2008) Composition Attacks and Auxiliary Information in Data Privacy. *The* 14*th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Las Vegas, 24-27 August 2008, 265-273.

[15] Sarwate, A.D. and Chaudhuri, K. (2013) Signal Processing and Machine Learning with Differential Privacy: Algorithms and Challenges for Continuous Data. *IEEE Signal Processing Magazine*, **30**, 86-94. https://doi.org/10.1109/MSP.2013.2259911

[16] Gionis, A. and Tassa, T. (2009) k-Anonymization with Minimal Loss of Information. *IEEE Transactions on Knowledge and Data Engineering*, **21**, 206-219. https://doi.org/10.1109/TKDE.2008.129

[17] Kim, J., Park, C., Hwang, J. and Kim, H.-J. (2013) Privacy Level Indicating Data Leakage Prevention System. *KSII Transactions on Internet and Information Systems* (*TIIS*), **7**, 558-575. https://doi.org/10.3837/tiis.2013.03.009

[18] Motahari, S., Ziavras, S.G. and Jones, Q. (2010) Online Anonymity Protection in Computer-Mediated Communication. *IEEE Transactions on Information Forensics and Security*, **5**, 570-580. https://doi.org/10.1109/TIFS.2010.2051261

[19] Koo, D., Shin, Y. and Hur, J. (2017) Privacy-Preserving Aggregation and Authentication of Multi-Source Smart Meters in a Smart Grid System. *Applied Sciences*, **7**, Article No. 1007. https://doi.org/10.3390/app7101007

[20] Büchi, M., Just, N. and Latzer, M. (2016) Caring Is Not Enough: The Importance of Internet Skills for Online Privacy Protection. *Information, Communication & Society*, **20**, 1261-1278. https://doi.org/10.1080/1369118X.2016.1229001

[21] Yasaka, T.M., Lehrich, B.M. and Sahyouni, R. (2020) Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App. *JMIR mHealth and uHealth*, **8**, e18936. https://doi.org/10.2196/18936

[22] Idrees, S.M., Nowostawski, M. and Jameel, R. (2021) Blockchain-Based Digital Contact Tracing Apps for COVID-19 Pandemic Management: Issues, Challenges, Solutions, and Future Directions. *JMIR Medical Informatics*, **9**, e25245. https://doi.org/10.2196/25245

[23] 金元浦. 大数据时代个人隐私数据泄露的调研与分析报告[J]. 清华大学学报(哲学社会科学版), 2021, 36(1): 191-201+206.