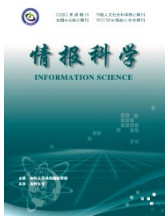

情报科学
Information Science
ISSN 1007-7634,CN 22-1264/G2

《情报科学》网络首发论文

题目：人工智能时代公共空间数据个人信息保护机制研究
作者：张玫瑰，张琪梦
网络首发日期：2024-12-18
引用格式：张玫瑰，张琪梦. 人工智能时代公共空间数据个人信息保护机制研究[J/OL]. 情报科学. https://link.cnki.net/urlid/22.1264.G2.20241218.1436.012

[

人工智能时代公共空间数据个人信息保护机制研究

张玫瑰[1] 张琪梦[2*]

（1.郑州大学 法学院，河南 郑州 450001；
2.中南财经政法大学 涉外法治研究院，湖北 武汉 430073）

摘要：【目的/意义】本文旨在构建一套适用于人工智能时代的公共空间数据个人信息保护机制，针对现有个人信息保护中法律法规不完善、技术手段不足以及公众隐私保护意识薄弱等问题提出解决方案。【方法/过程】本文采用多种研究方法，通过结合“蔚来汽车用户信息泄露事件”和“平安人寿泄露事件”等典型案例、对比中国《个人信息保护法》和欧盟《通用数据保护条例》（GDPR）的框架，基于隐私保护和数据安全理论，系统论述了人工智能时代公共空间数据中个人信息保护的特征事实，分析了其发展现状及存在的问题。【结果/结论】本文提出的四层保护机制框架在法律法规完善、技术手段应用及公众参与等方面具有普遍适用性和独特优势，并提出相应的政策建议与优化措施，以实现个人信息的有效保护。【创新/局限】本文在提出系统化保护机制的同时，结合了实际案例和国际对比分析，为未来的实证研究和机制优化提供了理论支持与实践指导。

关键词：人工智能；公共空间数据；个人信息；平台数据；保护机制

0 引言

人工智能时代的到来使得公共空间数据的收集、处理和利用变得更加普遍和复杂。公共空间数据是通过各种传感器、摄像头和智能设备在公共场所采集的，包括个人行为、活动轨迹和社交互动等信息。这些数据在提升公共服务效率、推动技术进步和促进社会发展的过程中起到了至关重要的作用。然而，伴随着“蔚来汽车用户信息遭窃”“平安人寿泄露 4 万条公民信息”等数据泄露、信息滥用和隐私侵权事件不断涌现，个人信息的隐私保护问题日益突出，引发了广泛的社会关注和担忧[1]。特别是在人工智能时代，数据的处理和分析能力大幅提升，使得隐私保护面临更为复杂的技术挑战和法律困境[2]。因此，如何在促进公共数据

* 作者简介：张玫瑰(1971-），女，河南孟州人，博士，教授，主要从事经济法、网络与信息法、智能司法研究。张琪梦（2000- ），女，河南登封人，硕士，研究助理，主要从事经济法、国际经济法研究。
本文系国家社会科学基金一般项目“司法裁判中人工智能的应用限度及规制问题研究 ”(项目编号 23BFX123)的前期成果之一。

开放和利用的同时，确保个人信息的安全，已成为亟待解决的重要课题。

为应对这一挑战，国家和地方政府相继出台了一系列法律法规，如《个人信息保护法》《数据安全法》等，旨在规范个人信息的收集、存储、处理和传输，保护个人隐私权和数据安全。但现有的法律法规和技术手段在实际应用中仍面临诸多问题和局限，亟需进一步完善和提升。本研究通过全面分析人工智能时代公共空间数据个人信息保护的特征事实，厘清当前个人信息保护的现状及存在的问题，从主体治理层、本体治理层、环境治理层和机制运行层四个层面构建人工智能时代公共空间数据个人信息保护机制。本研究旨在为人工智能时代公共空间数据个人信息保护提供理论支持和实践指导，通过构建完善的保护机制，推动数据的安全利用和数字经济的健康发展，为公众提供一个更加安全和可信的数字生活环境，也为国家安全体系和能力的现代化建设提供了重要的参考和借鉴。

1 人工智能时代公共空间数据个人信息保护的特征事实

1.1 公共空间数据的定义与范围

在人工智能迅猛发展的时代，公共空间数据的收集与利用变得越来越普遍[3]。基于法律和技术的角度而言，公共空间数据指的是那些在公共场所、通过公共设施或由第三方机构通过公开渠道合法收集的数据，这些数据既可以包含个人信息，也可以是群体行为的反映。此外，公共空间数据不仅仅限于传统的公共场所，还可以通过传感器网络、智能设备等新兴技术获取。因此，公共空间数据的范畴在现代技术背景下发生了扩展，不再局限于物理空间，而是涵盖了数字环境中的行为痕迹。与传统的个人数据相比，公共空间数据具有广泛性、实时性和多样性等特点。具体来说，公共空间数据包括以下几种类型（图 1）：第一，行为轨迹数据。通过监控摄像头、移动设备等获取的个人在公共空间中的移动轨迹。这些数据常用于城市管理、交通规划等领域。第二，使用记录数据。记录个人使用公共设施（如公共交通、公共厕所等）的情况，这类数据帮助城市管理者优化公共资源配置。第三，网络活动数据。在使用公共网络（如公共 Wi-Fi）时产生的上网记录，包括个人在网上的行为、访问的网站和使用的应用等，特别是个人在公共社交平台上发布的公开信息、评论和互动，反映社会舆情和公众的意见动态。第四，公共服务数据。在使用公共服务（如医院、学校、图书馆等）时产生的个人信息，对提升公共服务质量具有重要参考价值。此外，随着智能设备和传感器的

普及（如无人机、智能摄像头、物联网设备），数据收集变得更加便捷和广泛，进一步丰富了公共空间数据的来源和类型。

图 1 公共空间数据类型

Figure 1 Public space data types

公共空间数据的收集与利用日益广泛，其广泛性、实时性和多样性使其在多个领域具有重要应用价值。新兴技术手段的应用也使得数据收集更加便捷和多样化，进一步丰富了公共空间数据的来源和类型，推动了公共空间数据在社会管理和服务中的广泛应用。

1.2 个人信息在公共空间数据中的特征

公共空间数据中的个人信息具有广泛性与多样性、实时性与动态性、关联性与可识别性、集体性与共享性、持久性与可追溯性、高度敏感性和技术依赖性等独特特征（图 2）。虽然这些特征增强了公共数据的应用价值，但这些特征也带来了复杂的法律与伦理挑战[4]，隐私问题和数据滥用风险随之增加。首先，公共空间数据来源广泛，包括监控摄像头、公共交通系统、社交媒体平台和公共 Wi-Fi 等渠道，且数据形式多样，涵盖文字、图像、视频和音频等多种类型。其次，这些数据具有显著的实时性和动态性，能够即时采集和传输个人行为和状态的变化。此外，尽管公共空间数据中的个人信息常经过匿名化处理，但通过数据关联分析，仍可能重新识别个体，从而增加隐私泄露的风险。公共空间数据不仅反映个体行为，还揭示群体行为和社会动态，具有集体性与共享性，在城市管理和公共服务

中应用广泛。然而，这些数据往往长期存在并可追溯，使个人隐私面临更大的侵扰风险。更重要的是，这些数据可能包含个人行为习惯、健康状况和经济活动等高度敏感的隐私内容，一旦泄露，可能对个体造成严重的负面影响。最后，公共空间数据的采集、存储、处理和分析高度依赖于大数据、人工智能和物联网等先进技术，虽然这些技术提高了数据处理的效率和智能化程度，但也带来了技术滥用和数据泄露的风险。

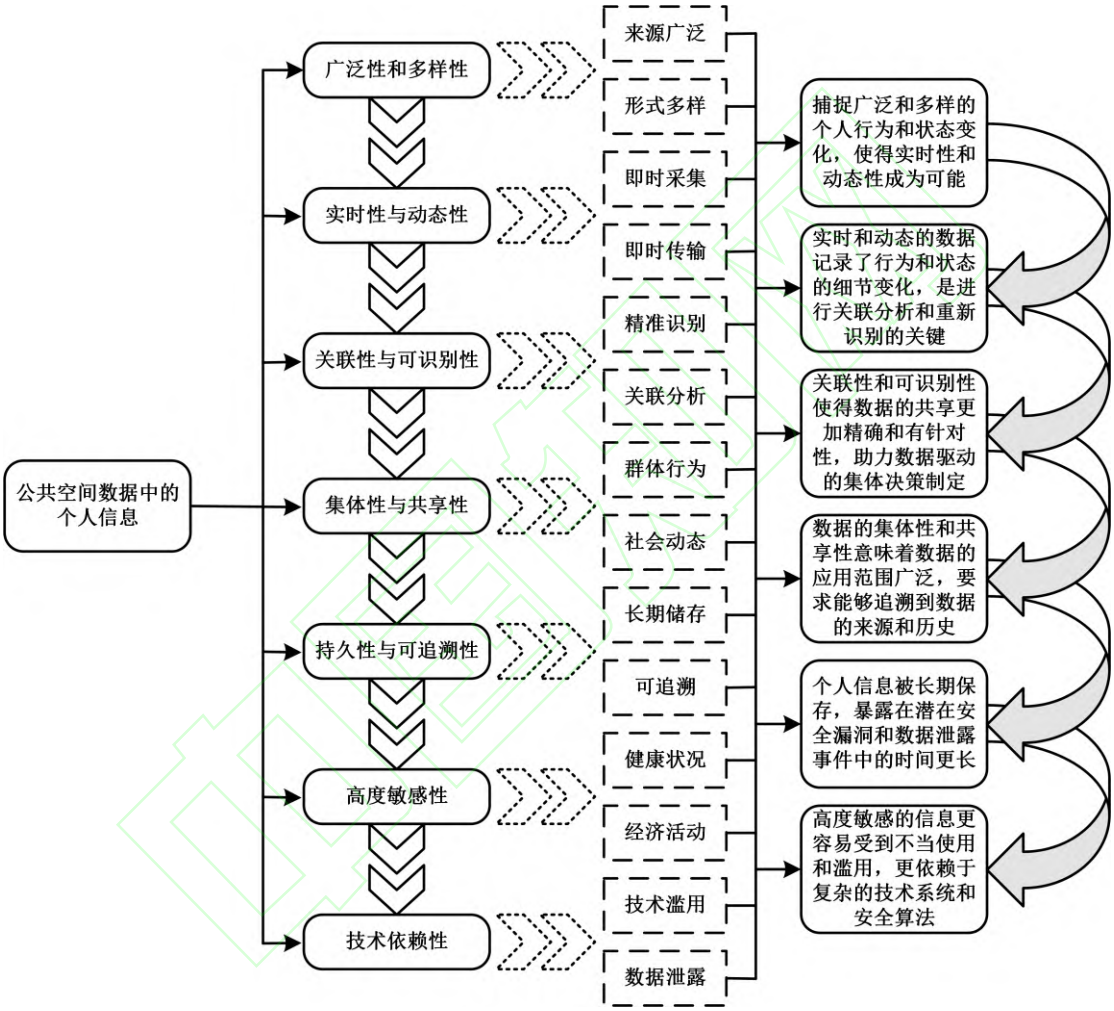

图 2 个人信息在公共空间数据中的特征

Figure 2 Characterization of personal information in public spatial data

1.3 人工智能时代的数据信息与个人隐私

数据信息的广泛应用极大地推动了社会进步和经济发展，但随着公共空间数据的广泛采集与利用，个人隐私问题愈发凸显[5]。首先，现有的隐私保护法律框架，如《个人信息保护法》和《数据安全法》，虽在一定程度上为隐私提供了法律保障，但其覆盖范围与深度尚未完全跟上技术发展的步伐。人工智能依赖于大

数据分析，数据来源广泛，涵盖个人位置信息、行为轨迹、消费记录等。这种全方位覆盖的数据采集使得个人隐私面临更大的暴露风险[6]。其次，人工智能算法能够高效、精准地分析海量数据，从中挖掘出深层次的信息和关联，尽管这在提升服务质量和用户体验方面具有重要作用，但也显著增加了个人隐私泄露的风险。此外，数据共享与跨域应用在提高公共服务效率的同时，也增加了隐私风险和保护难度。不同机构和平台之间的数据共享，虽然促进了信息的整合与利用，但也意味着更多的隐私风险。数据一旦被多个主体掌握，隐私保护的难度将显著增加。与此同时，数据滥用现象普遍存在，黑客攻击和数据泄露事件频发，导致大量个人信息落入不法分子之手，造成严重的隐私侵害和经济损失。

现有的隐私保护技术在面对复杂的数据分析和关联挖掘时效果有限，人工智能算法的“黑箱”特性使得数据处理过程缺乏透明性，难以有效监控和审计[7]。尽管现行的法律法规已为数据隐私保护奠定了基础，但由于技术发展速度极快，法律法规往往处于滞后状态。此外，新技术的不断涌现进一步增加了隐私保护的难度，尤其在数据跨境流动日益频繁的背景下，国家间的数据保护立法差异使得个人隐私保护面临更多的挑战[8]。

2 人工智能时代公共空间数据个人信息保护现状及存在问题

2.1 公共空间数据个人信息保护现状

2.1.1 法律法规现状

随着公共空间数据的广泛应用，国家和地方政府相继出台了一系列法律法规，构成了个人信息保护的坚实法律基础。首先，《中华人民共和国个人信息保护法》明确了个人信息处理的基本原则和具体要求，强调了对个人信息主体权利的保护，并详细规范了个人信息的收集、存储、使用和处理等环节，确保这些活动的合法性、正当性和必要性[9]。此外，《中华人民共和国数据安全法》对数据安全管理提出了全面的要求，涵盖了数据收集、存储、处理、传输、提供和公开等方面，明确了各项数据安全保护措施，并对违法行为规定了相应的处罚措施[10]。这一法律框架的建立，有助于全面提升数据安全管理水平，保障个人信息安全。地方政府也积极响应，出台了地方性数据条例，进一步细化和落实国家法律，对地方政府和企业的个人信息保护提出了具体要求。这些地方性法规不仅补充了国家法律的不足，还针对地方实际情况进行了具体规定，确保个人信息保护政策在地方层

面得到有效执行[11]。在国际合作方面，我国积极参考和借鉴欧盟《通用数据保护条例》（GDPR）等国际标准，推动个人信息保护立法的国际化进程。通过参与国际合作，我国致力于提升个人信息保护水平，与国际社会接轨，共同应对个人信息保护的全球性挑战[12]。

2.1.2 技术手段现状

公共空间数据的个人信息保护依赖于多种先进技术的应用，以确保数据处理的安全性和透明度，减少隐私风险[13]。首先，数据加密和匿名化技术通过对敏感信息进行加密处理或匿名化处理，有效减少了数据泄露和隐私侵害的风险[14]。这些技术确保即使数据被获取，也难以重新识别个人，从而实现“去连结性”。其次，区块链技术的去中心化、不可篡改和可追溯特性，被广泛应用于公共数据管理和个人信息保护中。区块链技术不仅确保数据在传输和存储过程中不被篡改，还通过智能合约实现自动化的数据管理，提升数据处理的透明度和安全性[15]。再次，大数据和人工智能技术在公共空间数据的收集、分析和利用中发挥着重要作用。这些技术能够快速处理和分析海量数据，挖掘潜在价值信息。然而，大数据技术的不当应用可能会侵害个人信息自决权和隐私权，因此需要谨慎处理。此外，隐私计算技术，如联邦学习和多方安全计算，是保护个人信息隐私的新兴方法。通过在数据不出境的前提下进行计算，这些技术实现了数据利用和隐私保护的双赢，可以在不泄露具体数据内容的情况下完成数据的联合分析和建模[16]。最后，算法透明性和公平性是保护个人信息的重要手段。通过透明化处理算法，确保数据处理过程和结果可解释，减少因算法黑箱带来的隐私风险。同时，确保算法的公平性，避免在数据处理过程中对不同群体造成歧视和不公平对待[17]。

2.1.3 社会公众意识现状

随着社会公众对公共空间数据个人信息保护意识的逐步提升，法律法规的普及和宣传使公众对个人信息保护的重要性有了更深刻地认识，越来越多的人开始关注自己的个人信息安全，并主动了解和行使自己的隐私权利。然而，尽管公众的隐私保护意识有所增强，但在实际生活中，许多人在使用移动应用、社交媒体和电子商务平台时，仍然忽视隐私设置和权限管理，导致个人信息泄露的风险增加[18]。这表明在公众意识和实际行为之间仍存在显著的认知差距和行为偏差。更重要的是，尽管当前的公共空间数据个人信息保护法律法规体系逐步完善，技术

手段也在不断进步，社会公众的隐私保护意识正在提高，但在法律执行、技术应用和公众行为等方面仍存在诸多问题和挑战。

2.2 公共空间数据个人信息保护存在的问题

2.2.1 数据收集与处理中的隐私风险

公共空间数据的收集与处理伴随着诸多隐私风险，首当其冲的便是数据的收集过度。许多公共空间数据的收集存在过度化倾向，超出必要范围的信息收集导致个人隐私泄露的风险增加。例如，一些智能设备和应用程序在收集数据时，并未明确告知用户其具体用途和收集范围，导致用户隐私权受到侵害[19]。其次，数据处理不透明，过程缺乏透明度，使得用户无法了解其个人信息如何被使用和存储。一些企业和机构在数据处理过程中未能遵循最小化原则，导致个人信息被滥用[20]。最后，由于数据管理不善或安全措施不足，数据泄露事件时有发生。这些事件不仅导致个人信息的泄露，还可能带来经济损失和社会信任的降低[21]。

2.2.2 法律法规的不完善

尽管我国已经出台了一系列法律法规以保护个人信息，但仍存在一些不完善之处。第一，法律执行力度不足。现有法律法规在执行过程中存在力度不足的问题。一些企业和机构未能严格遵守法律规定，导致个人信息保护不到位。例如，尽管《个人信息保护法》明确了对个人信息处理的要求，但在实际操作中，法律执行效果不尽如人意[22]。第二，立法细节不够全面。现有法律法规在某些细节上仍有不足。例如，对一些新兴技术的监管尚未跟上技术发展的速度，导致法律存在滞后性。此外，对数据跨境流动和国际合作的法律规定也不够明确，影响了个人信息保护的全面性和有效性。第三，地方性法规与国家法律的衔接不足。尽管各地出台了地方性数据条例，但这些条例与国家法律的衔接仍存在问题，导致地方在执行过程中存在不一致性和混乱。

2.2.3 技术手段的局限性

在个人信息保护的技术手段方面，人工智能技术在处理数据时，往往采用复杂的算法，这些算法的运行过程和结果难以解释，导致算法透明性不足，且若算法自动抓取或爬取的数据涉及个人信息，则直接构成对该数据主体隐私权的侵害[23]。这种“黑箱”操作方式增加了个人信息被滥用的风险[24]。此外，虽然区块链技术具有不可篡改和可追溯的优点，但其与个人信息保护的新式权利（如更正权、

被遗忘权）存在冲突，使得区块链技术在个人信息保护中的应用受到限制。最后，隐私计算技术虽有助于实现数据的安全利用，但其在实际应用中仍面临技术复杂度高、计算成本大等问题，难以大规模推广[25]。

2.2.4 公众隐私保护意识的不足

公众对个人信息保护的意识虽有提升，但总体上仍显不足。首先，公众的隐私保护意识薄弱。尽管公众对个人信息保护的认知有所增强，但在具体行动上仍然不足。例如，许多人在使用移动应用和互联网服务时，往往忽视隐私设置和权限管理，导致个人信息泄露风险增加[26]。其次，教育和宣传力度不够。个人信息保护的教育和宣传力度仍显不足，导致公众对隐私权和相关法律法规的认知不全面。尤其在青少年和老年人群体中，隐私保护意识较为薄弱[27]。参与度和维权意识低：公众在面对个人信息泄露和侵权时，往往缺乏主动维权的意识和能力。一些人对如何保护个人信息、如何维权等方面的信息了解不足，导致个人信息保护效果不佳[28]。

3 人工智能时代公共空间数据个人信息保护机制的建构

构建全面、系统的公共空间数据和个人信息保护机制，是应对隐私保护挑战、实现数据安全、提升公众信任、应对技术挑战和推动数字经济健康发展的重要保障。在人工智能时代，公共空间数据个人信息保护机制的四层框架不仅具有普遍适用性，而且通过综合的法律、技术、公众参与和操作执行四大治理维度，形成了动态、可持续、系统化的独特优势。具体来说，主体治理层确保法律法规的制定和政策的科学性与权威性，本体治理层通过前沿技术手段（如数据加密、访问控制等）提升数据处理的安全性，环境治理层强调公众意识和参与的重要性，而机制运行层则通过反馈机制和评估体系，确保所有保护措施能在动态变化的环境下有效执行。这一综合框架不仅是对传统隐私保护体系的延伸与扩展，更通过技术与社会协同治理，展示了其在应对人工智能时代特定挑战上的独特性和优越性（图 3）。

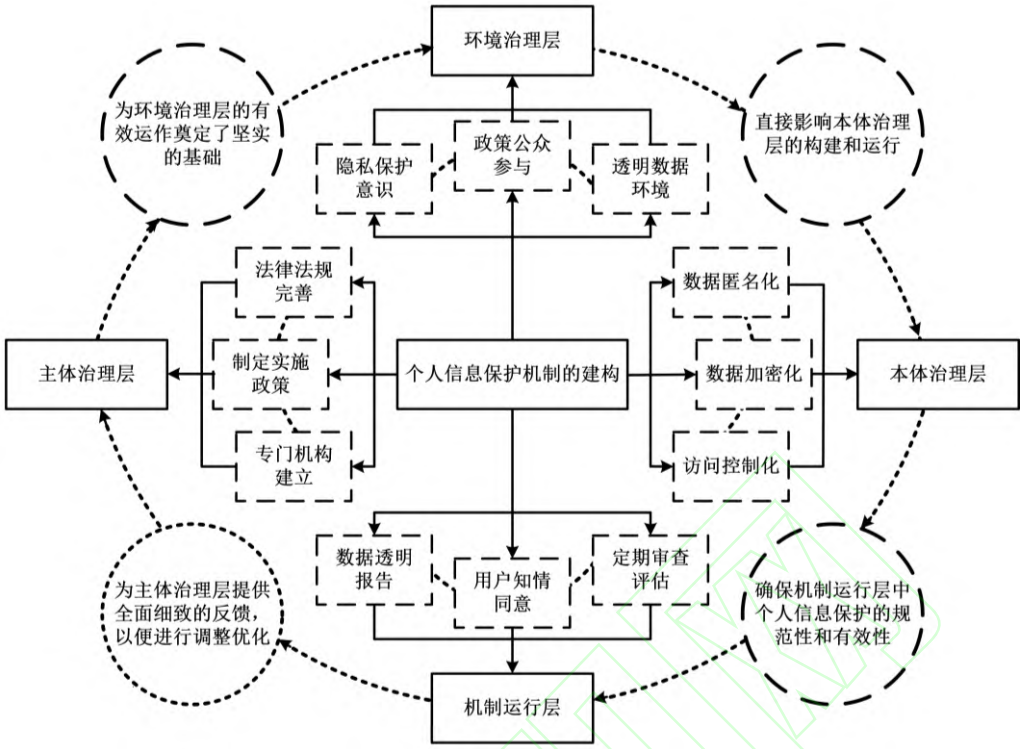

图 3 人工智能时代公共空间数据个人信息保护的机制模型

Figure 3 Mechanism model for personal information protection of public spatial data in the era of artificial intelligence

3.1 主体治理层

在人工智能时代，建立有效的公共空间数据个人信息保护机制，需要在主体治理层进行全面的规划和实施。相比传统治理框架，主体治理层在的独特性主要体现在法律法规与新兴技术的匹配性，以及跨部门合作机制的创新性上。作为公共空间数据个人信息保护机制的核心基础，主体治理层包括法律法规的完善、政策的制定与实施以及专门机构的建立。

3.1.1 法律法规的完善

完善的法律法规是公共空间数据个人信息保护的基石。首先，在完善公共空间数据个人信息保护的法律法规时，参考国际标准尤为重要。以欧盟的《通用数据保护条例》（GDPR）为例，该法律框架自 2018 年生效，统一了欧盟成员国在数据收集、处理、存储等方面的标准，并且通过严厉的罚款和跨境管辖权，确保企业对合规性给予高度重视[29]。GDPR 赋予数据主体广泛的权利，如访问权、删除权和数据可携权，同时对数据跨境传输和敏感信息处理进行了严格的控制。这为中国的《个人信息保护法》提供了借鉴。与 GDPR 类似，中国的《个人信息保护法》构建了完整的个人信息保护框架，确保在数据收集、存储、处理和传输等

环节的合法性，并且对涉及跨境传输和敏感数据处理的要求也非常严格。两者的异同之处在于，GDPR 赋予个人数据更多的跨平台携带权，而中国法律则在国家安全和跨境数据管理方面更加关注。因此，在完善公共空间数据个人信息保护的法律法规时，应借鉴 GDPR 的成功经验，尤其是在数据主体权利、跨境传输和高额罚款等方面，确保数据保护法律的适用性和国际化。同时，结合中国的实际情况，加强对国家安全和敏感数据的监管力度，从而构建更为完善的法律体系，增强其执行力和适应性。其次，随着技术的快速发展，现有法律可能无法全面覆盖所有新兴技术。因此，针对生成式人工智能和区块链技术带来的新挑战，需要制定专门的法律条款，确保在使用这些技术时个人信息得到充分保护。此外，完善的法律框架还需要强有力的执行和监督机制。通过增加对违法行为的处罚力度，可以确保法律的权威性和有效性。建立定期审查和更新机制，以确保法律能够及时应对快速变化的技术环境，进一步增强法律的执行力和适应性。

综上所述，完善的法律法规是公共空间数据个人信息保护的基石。通过细化法律条款、更新法律以覆盖新技术，并加强法律的执行和监督机制，可以确保在技术快速发展的环境中有效保护个人信息。

3.1.2 政策制定与实施

在法律框架的指导下，制定和实施具体的隐私保护政策是实现个人信息保护的关键步骤[30]。首先，政府和相关机构应制定详细的隐私保护政策，涵盖数据收集、使用、存储、共享和销毁等各个环节。具体来说，应规定公共数据开放平台必须采用数据加密和匿名化技术，以确保数据在传输和存储过程中的安全。其次，建立政策实施的监督与评估机制至关重要。这可以通过定期评估政策实施效果，及时发现和解决问题，不断优化隐私保护措施来实现。例如，可以通过第三方评估机构对企业和机构的数据保护措施进行评估，确保其符合政策要求，增强政策的执行力和有效性。此外，促进公众参与和教育也是不可或缺的一部分。在制定政策时，应广泛听取公众意见，增强政策的科学性和可行性。同时，通过教育和宣传增强公众的隐私保护意识，指导公众正确使用各种数据服务和技术，增强其自我保护能力。

综上所述，在法律框架指导下，制定和实施具体的隐私保护政策，建立监督与评估机制，并促进公众参与和教育，是实现个人信息保护的关键步骤。这些措

施不仅能够确保数据安全，还能增强公众的隐私保护意识，增强社会对个人信息保护的整体能力。

3.1.3 专门机构的建立

为了确保公共空间数据个人信息保护机制的有效实施，必须在国家和地方层面设立专门的管理和监督机构。首先，在国家层面设立独立的个人信息保护机构是必要的[31]。该机构将负责制定和实施个人信息保护政策、监督法律执行、处理投诉和纠纷等工作。其独立性和权威性将确保能够公正地履行职责，维护个人信息保护的严肃性和有效性。其次，各省市也应设立相应的地方个人信息保护机构。这些地方保护机构将与国家级机构保持紧密合作，确保国家法律法规和政策在地方层面得到有效实施。地方机构的设立可以针对本地的具体情况，提供更为细致和贴近实际的个人信息保护措施，从而增强法律法规的执行力和覆盖面。此外，个人信息保护涉及多个部门和领域，需要加强跨部门合作与协调。为此，可以建立跨部门的数据保护工作组或委员会，定期召开协调会议，确保各部门在个人信息保护方面的政策和措施能够统一协调、相互支持。这种跨部门的合作机制将有助于解决部门之间的信息壁垒，提升整体保护效果。

综上所述，通过完善法律法规、制定和实施具体政策以及建立专门的管理和监督机构，可以构建起强有力的主体治理层。这不仅能够有效保护个人隐私，还能增强公众信任，促进数据的合法合规使用，推动数字经济的健康发展。建立独立权威的国家级机构、设置地方保护机构以及加强跨部门合作，都是实现这一目标的重要步骤。

3.2 本体治理层

在构建公共空间数据个人信息保护机制时，本体治理层的建设至关重要，其最大的优势在于对最新隐私保护技术的整合与优化。本体治理层主要涵盖技术手段的应用，包括数据匿名化技术、数据加密技术以及访问控制技术[32]。

3.2.1 数据匿名化技术

数据匿名化技术是一种重要的个人信息保护手段，通过多种技术手段使个人数据无法识别特定个体，从而保护隐私[33]。具体实现方式包括数据泛化、数据扰动和数据交换。数据泛化技术将精确的数据转换为一个范围值或类别，以降低数据的精确度；数据扰动技术通过添加噪声等方式改变原始数据，从而隐藏真实信

息;数据交换技术则通过交换数据中的某些部分,打乱原始关联,增加识别难度。

匿名化技术广泛应用于数据共享和开放平台，在这些场景中，通过对数据进行匿名化处理，可以在不泄露个人隐私的前提下，实现数据的共享和利用，支持大数据分析和研究。然而，匿名化技术也面临一些挑战，尤其是在数据关联和挖掘过程中,可能会通过其他信息重新识别出个人。因此,为了提高隐私保护效果，匿名化处理需要与其他隐私保护措施相结合，如差分隐私技术，通过增加随机噪声来保护数据隐私，进一步增强数据匿名化的保护效果。

综上所述，数据匿名化技术是保护个人隐私的重要手段，通过多种技术实现并广泛应用于数据共享场景。但为了应对重新识别的挑战，需结合其他隐私保护措施，如差分隐私技术，确保数据匿名化的保护效果。这些综合措施共同构建了一个更为安全的数据保护机制，有助于实现数据共享和隐私保护的双重目标。

3.2.2 数据加密技术

数据加密技术是保护个人信息安全的重要手段,通过加密处理使数据在传输和存储过程中不可读，从而防止未经授权的访问。常用的数据加密算法包括对称加密和非对称加密。对称加密算法如 AES 速度快，适合大数据量的加密处理；非对称加密算法如 RSA 安全性高，适用于密钥交换和数字签名。

数据加密技术广泛应用于数据传输和存储的各个环节。例如，在公共空间数据的传输过程中，通过加密技术可以防止数据在网络传输过程中被截获和窃取，从而保护个人隐私和信息安全。然而，加密技术的有效性高度依赖于密钥的安全管理。为确保密钥的安全性，需要建立完善的密钥管理机制，包括密钥的生成、分发、存储、使用和销毁等环节，确保密钥在整个生命周期中的安全。

综上所述，数据加密技术是保护个人信息安全的重要手段，通过加密处理防止未经授权的访问。但其有效性需要依赖完善的密钥管理机制,确保密钥的生成、分发、存储、使用和销毁安全。这些措施共同构建了一个可靠的安全体系，确保个人信息在传输和存储过程中的安全性。

3.2.3 访问控制技术

访问控制技术是确保数据仅被授权用户访问的重要手段,通过定义和管理用户权限，实现对数据访问的有效控制。常见的访问控制模型包括自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC）。自主访问控制

允许数据所有者自行定义访问权限，强制访问控制由系统根据预定义策略强制执行，而基于角色的访问控制则根据用户的角色分配权限，确保不同用户在信息系统和数据平台中的访问权限得以有效管理和限制。

访问控制技术广泛应用于各类信息系统和数据平台。例如，在公共数据开放平台中，通过访问控制技术可以限制不同用户对数据的访问权限，确保只有授权用户才能访问和操作特定数据。随着数据使用场景的变化，访问权限可能需要动态调整。通过引入动态访问控制技术，可以根据实时情况自动调整用户的访问权限，确保数据的安全性和灵活性。

综上所述，通过应用数据匿名化技术、数据加密技术和访问控制技术，可以在本体治理层构建起强有力的个人信息保护机制。这些技术手段不仅能有效保护个人隐私，还能确保数据在传输、存储和使用过程中的安全性，从而为公共空间数据的合法合规使用提供有力保障[34]。这些措施的实施将进一步推动人工智能时代公共空间数据的安全利用，促进数字经济的健康发展。

3.3 环境治理层

在构建公共空间数据个人信息保护机制时，环境治理层通过强调公众参与和透明化建设，构建了独特的社会共治模式。环境治理层包括提升公众隐私保护意识、促进公众参与政策制定以及构建透明的数据使用环境。

3.3.1 提升公众隐私保护意识

提升公众隐私保护意识是实现有效个人信息保护的基础[35]。首先，通过教育和培训，政府和相关机构应在学校教育、社区讲座和在线课程等形式上，广泛开展隐私保护的知识普及活动。这将帮助不同年龄段的人群深入理解个人信息保护的重要性和相关法律法规，从而增强整体的隐私保护意识。其次，利用各种媒体平台进行广泛的宣传活动，也是增强公众隐私保护意识的重要手段。通过电视、广播、报纸、社交媒体等途径，持续宣传隐私保护知识和技能，帮助公众了解如何在日常生活中保护个人信息，形成全社会共同关注和重视隐私保护的氛围。此外，向公众提供便捷的隐私保护工具，如隐私设置指南、加密软件、隐私浏览器等，能够帮助公众在使用互联网和智能设备时更好地保护自己的个人信息。这些工具的推广和使用，将极大增强公众在信息社会中的自我保护能力。

综上所述，提升公众隐私保护意识是实现有效个人信息保护的基础。通过教

育培训、宣传活动和提供隐私保护工具，可以增强公众对隐私保护的认识和能力，从而更好地参与和配合相关保护机制，确保个人信息在数字时代得到全面的保护。

3.3.2 促进公众参与政策制定

公众的参与对于制定科学、合理的隐私保护政策至关重要。首先，通过广泛征集公众对隐私保护政策的意见和建议，可以确保政策更具针对性和可操作性。例如，可以通过公开听证会、在线调查问卷、意见征集平台等方式，收集公众对隐私保护的需求和建议。这种广泛的意见征集过程能够反映出公众对隐私保护的真实关注和实际需求，为政策制定提供有力的支持。其次，建立公众参与隐私保护政策制定的长效机制，确保公众能够持续、有效地参与到政策制定过程中，是关键的一步。例如，设立隐私保护咨询委员会，邀请公众代表、专家学者和行业代表共同参与政策讨论和制定。这种长效机制能够保证公众意见在政策制定的各个阶段得到充分表达和考虑，从而提高政策的科学性和合理性。此外，在政策制定过程中，保持信息透明也是增强公众信任的重要手段。及时向公众公布政策草案、意见征集结果和政策修订情况，让公众了解政策制定的全过程，可以极大增强政策的透明度和公众的信任感。透明的政策制定过程不仅有助于提高政策的接受度，也能增强公众对隐私保护政策的信心和支持。

综上所述，公众参与对于制定科学、合理的隐私保护政策至关重要。通过广泛征集意见、建立长效参与机制和保持政策透明化，可以确保隐私保护政策更具针对性和可操作性，增强公众信任，从而实现更为有效的个人信息保护。

3.3.3 构建透明的数据使用环境

构建透明的数据使用环境是实现个人信息保护的重要措施。首先，数据处理透明化是关键一步，要求公开数据收集、存储、处理和使用的全过程。在数据收集时，必须明确告知用户数据的目的、范围和使用方式，这样可以让用户清楚了解自己的数据将如何被使用，从而增加信任感。其次，建立数据使用反馈机制也是不可或缺的。通过数据使用报告和公众监督平台等形式，允许公众对数据使用情况进行监督和反馈。这不仅提高了数据使用的透明度，还能让公众有机会对数据处理提出意见和建议，进一步增强公众的信任。此外，定期审计和公开报告是确保数据使用合法合规的重要手段。通过独立第三方审计，定期对数据处理活动进行全面审查，并将审计结果向公众公开，可以确保数据处理活动符合法律法规

和政策要求。这种公开透明的审计机制，能够有效提升公众对数据使用的信任。

综上所述，构建透明的数据使用环境是实现个人信息保护的重要措施。通过数据处理透明化、建立反馈机制和定期审计与公开报告，可以增强公众对数据使用的信任，促进数据的合法合规使用，推动人工智能时代公共空间数据个人信息保护的全面发展。这些措施不仅能够有效保护个人信息，还能推动社会的和谐与进步。

3.4 机制运行层

在构建公共空间数据个人信息保护机制的过程中，机制运行层不仅是个人信息保护框架中的执行环节，还通过创新的反馈与评估机制，确保其持续优化和与时俱进的优越性。机制运行层包括数据透明度报告、用户知情同意以及定期审查与评估。

3.4.1 数据透明度报告

数据透明度报告是确保数据处理过程透明化的重要手段。首先，透明度报告应详细列出数据收集的类型、数量、用途、存储方式以及共享对象等信息。此外，还应包括数据保护措施、数据泄露事件及其应对措施等内容，确保公众能够全面了解数据处理的全过程。这种详尽的报告内容能够帮助公众清晰地了解数据是如何被收集和使用的，从而增强信任感。以蔚来汽车用户信息泄露事件为例，该事件暴露了企业在数据处理和传输过程中的透明度缺失问题。由于数据泄露前未向公众发布任何相关透明度报告，用户无法了解自己的数据如何被收集、存储和使用，且无法掌握数据处理的安全状况。这直接导致事件发生后，公众对企业的信任大幅下降。其次，透明度报告应至少每半年或每年定期发布。通过定期更新报告，向公众展示数据保护工作的新进展和改进措施，保持信息的及时性和透明度。定期发布不仅展示了对数据保护工作的持续关注，还能让公众看到实际的改进措施，从而进一步增强信任和参与度。此外，透明度报告应采用易于理解的形式，如图表和数据可视化，帮助公众更好地理解报告内容。结合平安人寿信息泄露事件可以看出，虽然公司可能具备一定的内部信息披露流程，但没有采取有效的透明化和易于理解的形式向用户解释其信息处理过程，造成了公众的普遍不信任。透明度报告应通过官方网站、社交媒体等多渠道发布，确保公众能够方便地获取和查阅。这样，不仅可以提高透明度，还能通过图表和数据可视化的方式，使复

杂的技术和数据处理流程更为直观，增加公众的理解度。

综上所述，数据透明度报告是确保数据处理过程透明化的重要手段。通过详细的报告内容、定期发布和采用易于理解的形式，可以增强公众的信任和参与度，促进数据的透明使用和保护。这不仅有助于提升数据处理的合法性和合规性，还能推动数据治理工作的全面发展。同时，结合上述实际案例不难看出，透明度报告的规范和发布频率对于维护企业信誉、减少数据泄露风险、增强公众信任有着不可忽视的作用。

3.4.2 用户知情同意

用户知情同意是个人信息保护的重要原则，旨在确保用户在数据收集和使用过程中拥有知情权和选择权[36]。首先，数据处理者应在数据收集时，清晰地告知用户数据收集的目的、范围、使用方式、存储期限以及共享情况。告知内容应简明扼要，避免使用专业术语，确保用户能够理解这些信息，从而做出明智的决策。其次，同意机制必须明确并得到用户的主动确认。例如，通过勾选同意框或点击确认按钮等方式来获得用户同意，确保用户是在充分知情的情况下自愿同意数据收集和使用。隐含同意或默认勾选的方式应被严格禁止，以防止用户在不知情的情况下被迫同意。此外，用户应有权随时撤回对数据收集和使用的同意，撤回过程应设计得简便易行。数据处理者在收到撤回请求后，应迅速采取行动，停止相关数据处理活动，并及时删除用户的数据。这不仅保障了用户的选择权，还增强了用户对数据处理者的信任。

综上所述，用户知情同意是个人信息保护的重要原则。通过清晰告知信息、明确的同意机制和简便的撤回流程，可以确保用户在数据收集和使用过程中拥有充分的知情权和选择权，从而有效保护个人信息。

3.4.3 定期审查与评估

定期审查与评估是确保个人信息保护机制有效运行的重要环节。首先，数据处理机构应定期对其个人信息保护措施进行内部审查，检查数据处理活动的合规性和有效性。这包括对数据收集、存储、使用和销毁等环节进行全面检查，确保所有操作符合相关法律法规和政策要求。其次，聘请独立的第三方机构进行外部评估，以确保评估的客观性和公正性。外部评估应包括对数据安全措施、用户隐私保护措施和数据处理流程等方面的全面检查，确保数据处理活动的透明性和可

信性。根据审查和评估结果，及时采取改进措施，修订和完善个人信息保护政策和操作流程。例如，针对发现的问题，调整数据处理方式，增强数据安全措施，增强员工隐私保护意识等。这些改进措施可以确保个人信息保护机制持续优化和有效运行。

综上所述，定期审查与评估是确保个人信息保护机制有效运行的重要环节。通过内部审查、外部评估和改进措施，可以确保个人信息保护的合规性和有效性，增强公众对数据处理和使用的信任，促进数据的合法合规使用，推动人工智能时代公共空间数据个人信息保护的全面发展。这些努力将进一步确保个人信息在数字时代得到有效保护，推动社会的和谐与进步。

4 结语

在人工智能迅猛发展的时代，公共空间数据的广泛应用带来了前所未有的机遇和挑战。本文系统分析了人工智能时代公共空间数据个人信息保护的特点，对当前个人信息保护现状的深入分析，揭示了在法律法规、技术手段和公众意识等方面存在的问题，并进一步提出了从主体治理、本体治理、环境治理和机制运行四个层面构建的个人信息保护机制。在主体治理层面，强调完善法律法规、制定实施政策及建立专门机构的重要性，以确保法律的权威性和政策的科学性、可行性；在本体治理层面，通过应用数据匿名化、数据加密和访问控制技术，提高数据处理的安全性和隐私保护水平；在环境治理层面，提升公众隐私保护意识、促进公众参与政策制定及构建透明的数据使用环境，增强公众信任和社会参与度；在机制运行层面，通过数据透明度报告、用户知情同意以及定期审查与评估，确保保护措施的有效落实和持续改进。

总之，构建全面、系统的公共空间数据个人信息保护机制，是应对隐私保护挑战、实现数据安全、提升公众信任、应对技术挑战和推动数字经济健康发展的重要保障。未来研究和实践应继续深化和完善这些机制，以确保个人信息在人工智能时代得到充分保护，推动社会和谐与进步，并支持国家安全体系和能力的现代化建设。这些努力不仅能有效保护个人隐私，还能促进数据的合法合规使用，推动数字经济的健康发展，为公众提供一个更加安全和可信的数字生活环境。

Personal Information Protection Mechanism for Public Space Data in the Age of Artificial Intelligence

ZHANG Meigui[1] ZHANG Qimeng[2]

(1. Law School, Zhengzhou University, Zhengzhou 450001, China;

2.Institute of Foreign-related Rule of Law, Zhongnan University of Economics and Law, Wuhan 430073, China)

Abstract: 【Purpose/significance】 This paper tries to construct a personal information protection mechanism for public space data applicable in the era of artificial intelligence, aiming to cope with the problems of imperfect laws and regulations, insufficient technical means, and weak public awareness of privacy protection in the existing personal information protection. 【Method/process】 Combining the relevant theoretical methods of privacy protection, data security and technical ethics, this paper systematically analyzes the characteristics, features and dimensions of personal information in public space data in the era of artificial intelligence, and proposes a specific and scientific protection mechanism. 【Result/conclusion】 Based on the current situation and challenges in the protection of personal information in public space data, this paper proposes a comprehensive protection mechanism framed by subject governance, ontology governance, environment governance and mechanism operation, and puts forward corresponding suggestions and countermeasures for the effective protection of personal information. 【Innovation/limitation】 The construction of personal information protection mechanism for public space data is a concrete practice of combining technology and ethics, and future research can be verified and improved by combining data from specific fields.

Keywords: artificial intelligence; public space data; personal information; platform data; protection mechanisms

参考文献：

[1] 周瑞珏.数据泄露风险治理中网络安全保险的介入路径[J].北方法学,2024,18(2):76-90.

[2] 陈光,郭军.大语言模型时代的人工智能：技术内涵、行业应用与挑战[J].北京邮电大学学报,2024,47(4):20-28.

[3] TENE O, POLONETSKY J. Big data for all: Privacy and user control in the age of analytics[J]. Nw. J. Tech. & Intell. Prop., 2012, 11: 239-273.

[4] VAN DER SLOOT B. Privacy as human flourishing: Could a shift towards virtue

ethics strengthen privacy protection in the age of Big Data[J]. J. Intell. Prop. Info. Tech. & Elec. Com. L., 2014, 5: 230-244.
[5] EDWARDS L, VEALE M. Slave to the algorithm? Why a'right to an explanation'is probably not the remedy you are looking for[J]. Duke L. & Tech. Rev., 2017, 16: 18-84.
[6] 丁晓蔚,苏新宁.基于区块链可信大数据人工智能的金融安全情报分析[J].情报学报,2019,38(12):1297-1309.
[7] 李晓楠.大数据技术下个人公平征信监管的数据治理维度[J].大连理工大学学报(社会科学版),2023,44(2):65-74..
[8] ZUBOFF S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, edn[M].New York:Public Affairs,2019.
[9] 洪丹娜. 个人信息权利在我国宪法权利体系中的定位[J]. 法学杂志, 2024, 45(3): 87-105.
[10] 李姝卉. 数字时代隐私权保护的立法因应[J]. 法学, 2024,(3): 17-31.
[11] 许娟. 地方数据立法中的个人信息产权保护——基于 23 个省(区、市)现行地方性数据条例的考察[J]. 求索, 2024(3): 152-162.
[12] 王旭,刘斌斌,薛宇菲.我国个人信息保护政策法律文本量化评价研究——基于 PMC 指数模型和中欧法律对比分析[J/OL].重庆大学学报(社会科学版),1-18[2024-10-11].https://knshtbprolcnkihtbprolnet-p.libvpn.zuel.edu.cn/kcms/detail/50.1023.C.20240612.1559.002.html.
[13] VAN DER SLOOT B. Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data[J]. J. Intell. Prop. Info. Tech. & Elec. Com. L., 2014, 5: 230-244.
[14] 薛悟娟. 大数据时代个人信息的运作模式、理论困境及保护路径[J]. 中国海商法研究, 2024, 35(2): 103-112.
[15] 童云峰.区块链技术和个人信息权利之冲突与消融[J]. 东北大学学报(社会科学版), 2024, 26(1): 108-116,150.
[16] 周毅, 郭朗睿.公共数据开放中隐性安全风险的内涵、表现及其生成逻辑[J]. 情报资料工作, 2024, 45(3): 70-77.
[17] 孟凡骞, 王仲羊.个人信息保护视域下 ChatGPT 的法律风险及其治理[J]. 传媒, 2024(3): 51-54.
[18] 吴烨, 公保端知. 数字时代个人信息保护的中国方案[J]. 智库理论与实践, 2023, 8(5): 109-117.
[19] 斜晓东. 风险与控制：论生成式人工智能应用的个人信息保护[J]. 政法论丛, 2023(4): 59-68.
[20] 陈禹衡. 生成式人工智能中个人信息保护的全流程合规体系构建[J]. 华东政法大学学报, 2024, 27(2): 37-51.
[21] 蒋国银, 蔡兴顺, 杨三, 等.公共价值视角下资源禀赋与政府规制对平台数据隐私保护水平的影响——基于多案例的实证分析[J]. 电子政务, 2024,(8):81-96.（补充年、卷、期、页码）
[22] 齐延平, 田奥妮. 司法数字公开中个人信息隐私保护的“整体—责任”模式[J]. 中国法律评论, 2024(4):102-113.
[23] 张玫瑰.司法裁判中人工智能应用的限度及规制[J].政法论丛, 2023(5):128-138.
[24] 孟凡骞, 王仲羊. 个人信息保护视域下ChatGPT的法律风险及其治理[J]. 传媒, 2024(3): 51-54.

[25] 任保平, 刘洁. 建立完善中国特色的数据市场定价机制[J]. 当代经济研究, 2024(7): 51-59.
[26] 李雷. 论数字时代个人信息保护与利用平衡的展开路径[J]. 行政法学研究, 2024(1): 111-122.
[27] 苏君华, 杜念. 国外公共数据资源开放共享中的隐私风险控制研究综述[J]. 现代情报, 2024,44(3): 164-177.
[28] 丁晓东. 隐私权保护与个人信息保护关系的法理——兼论《民法典》与《个人信息保护法》的适用[J]. 法商研究, 2023, 40 (6): 61-74.
[29] WACHTER S, MITTELSTADT B, FLORIDI L. Why a right to explanation of automated decision-making does not exist in the general data protection regulation[J]. International data privacy law, 2017, 7(2): 76-99.
[30] 杨巧云,张彦菲,李欣,等.政府开放数据个人隐私保护政策保障——基于 10 个国家政策实践的内容分析[J].图书情报工作,2024,68(11):56-71.
[31] 徐孝娟,赵泽瑞,贾海洋,等.国外数字人文众包个人信息保护研究及启示——以网站运营者“隐私政策”为视角[J].现代情报,2023,43(2):168-177.
[32] 高颖,杜娟.大数据时代数据匿名化的法律规制[J].情报理论与实践,2021,44(10):50-56.
[33]MAHANAN, WARANYA, W. ART CHAOVALITWONGSE, and JUGGAPONG NATWICHAI. Data privacy preservation algorithm with k-anonymity[J]. World Wide Web, 2021, 24(5): 1551-1561.
[34] 陈美,梁乙凯.开放政府数据隐私风险控制中个人数据匿名化研究[J].图书馆学研究,2021(11):66-71.
[35] ACQUISTI A, BRANDIMARTE L, LOEWENSTEIN G. Privacy and human behavior in the age of information[J]. Science, 2015, 347(6221): 509-514.
[36] 梅傲,柯晨亮.数据共享与数据财产化[J].四川师范大学学报(社会科学版),2024,51(2):59-67,200-201.