

国外微观数据价值挖掘实践及对我国的启示

——基于隐私计算技术视角^{*}

董波^{1,2}, 高金莎^{1,2}, 方丹^{1,2}

(1. 之江实验室发展战略与合作中心, 浙江 杭州 311121;
2. 浙江省哲学社会科学实验室—之江实验室智能社会治理实验室, 浙江 杭州 311121)

摘要: 微观数据价值挖掘对赋能经济社会发展具有重要意义, 以统计局为代表的国家有关部门也在积极推动微观数据的开发应用。而随着数据隐私安全重要性的不断凸显, 隐私计算技术成为了有效平衡微观数据开发应用和安全保护的重要途径。围绕政策支撑、技术赋能、多主体合作、法律保障等方面详细梳理了国外关于隐私计算技术赋能微观数据应用的重要举措, 为我国政府进一步开展微观数据开发应用工作提供有益参考。

关键词: 微观数据; 隐私计算技术; 价值挖掘

中图分类号: G203; D63

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2025.12.008

引用格式: 董波, 高金莎, 方丹. 国外微观数据价值挖掘实践及对我国的启示——基于隐私计算技术视角 [J]. 网络安全与数据治理, 2025, 44(12): 55-61.

The practice of the international microdata value mining and its implications: from the perspective of privacy computing technology

Dong Bo^{1,2}, Gao Jinsha^{1,2}, Fang Dan^{1,2}

(1. Development Strategy and Cooperation Center, Zhejiang Laboratory, Hangzhou 311121, China;
2. Zhejiang Labs for Philosophy and Social Sciences—Laboratory for Intelligent Society and
Governance in Zhejiang Laboratory, Hangzhou 311121, China)

Abstract: The value mining of microdata plays a significant role in empowering socioeconomic development. Relevant national authorities, represented by statistical bureaus, are actively promoting the development and application of microdata. With the growing importance of data privacy and security, privacy computing technology has emerged as an effective approach to balance the development and application of microdata with security protection. This study comprehensively reviews international initiatives regarding the application of privacy computing technology in microdata, focusing on policy support, technological empowerment, multi-stakeholder collaboration, and legal safeguards, aiming to provide valuable references for the Chinese government to further advance the development and application of microdata.

Key words: microdata; privacy computing technology; value mining

0 引言

2018 年我国提出:“要建立健全大数据辅助科学决策和社会治理的机制, 推进政府管理和社会治理模式创新。”微观数据包含丰富的企业、住户等个体数据, 背后潜藏着经济社会的发展趋势, 对政府宏观调控、开展深层次学术研究等都具有重大意义。挖掘微观数据价值,

赋能经济社会发展具有重要战略意义。但长期以来, 受限于数据安全、个人隐私保护、制度不完善等因素, 我国的微观数据价值并未得到充分挖掘和释放。

近年来, 随着数据要素市场持续健全和深化, 数据开放共享的需求持续攀升, 数据安全和隐私保护的重要性愈发凸显。隐私计算技术通过有效平衡数据流通与隐私安全成为解决数据有效流通难题的关键途径。

而从国际上看, 欧美等发达国家和地区已经纷纷利

^{*} 基金项目: 全国统计科学研究项目重点项目 (2023LZ005)

用隐私计算技术赋能微观数据开发。但技术使用的同时需要法律、政策、组织等多方面要素的合力支撑,才能最大化技术应用效能。因此在利用隐私计算技术赋能微观数据价值挖掘的过程中,欧盟国家也制定了相应的法律和标准,明确组织机构和开发流程。

本文通过系统分析和总结欧美国家和地区在微观数据价值挖掘过程中所采取的隐私计算技术应用、政策和法律制定、多主体合作等方面的举措,为我国进一步开展微观数据开发应用工作提供有益参考。

1 理论综述

1.1 微观数据的内涵

数据按照层次和观察角度可以分为微观数据和宏观数据,其中微观数据是指在特定调查背景下,针对最小调查单元进行数据采集与记录而得的结果^[1]。如人口普查微观数据、住户收支与生活状况调查微观数据,均属此类。微观数据着重于细微层面,精准呈现个体的特征、行为表现以及动态变化。鉴于微观数据涉及个体隐私信息,其收集、处理和使用均受到相关法律法规的严格保护,以确保数据主体的合法权益不受侵害。

对于微观数据范畴,国家层面已经明确了相应的范围。根据数据生成来源主体不同,微观数据可进一步分为政府微观数据、企业微观数据与个人微观数据^[1]。其中,政府微观数据主要通过普查体系(涵盖全面调查、抽样调查、重点调查及典型调查)、行政记录系统以及卫星遥感监测、网络爬取等新型数据采集技术获取,覆盖企业运营、居民生活等社会主体的信息。企业微观数据特指商业机构在经营过程中形成的个体级交易流水、消费轨迹、行为特征等运营数据集合,具有显著的商业智能价值。个人微观数据则是指通过智能终端设备、社交平台、商业服务系统及公共政务数据库等多渠道,以数字化或实体介质形式记载的个体生物特征、位置轨迹、消费偏好、社交关系等具有身份识别性的个人信息资产。但在实践运用中,个人虽然产生数据却较少加工利用数据,而企业在日常运营过程中会收集个人数据,类似地政府也会因履职需要依法依规收集企业和个人产生的数据,因此三类数据在以具体数据集呈现时存在一定交叉。如人口普查数据是政府收集、加工的个人数据;手机运营商数据是企业所收集的个人移动端产生的数据。

1.2 微观数据价值挖掘的作用

微观数据既是微观行业的指向标,又是调控、规范宏观经济的重要基础,运用好海量微观数据有利于进一步促进我国经济理性、平稳发展。

具体而言,一是有助于决策主体科学制定和评估政

策。决策部门可利用微观数据构建多维度政策仿真模型,对各类施政方案进行动态推演与效果预测,例如利用贫困人口数据评估扶贫效果^[2]、利用人口普查数据评估营养改善计划效果^[3]、利用企业数据评估科技政策^[4]等。通过量化分析不同政策选项的潜在经济成本、社会效益及长期影响,结合多元利益主体的诉求评估,为科学决策提供精准依据。也可以构建量化指标与质性分析相结合的评估框架,建立政策弹性系数矩阵和效果传导图谱,实现政策实施的全周期监测与多维效能评价。或是引入动态权重调节机制和偏差修正模型,可显著提升评估结果的靶向性与预测效度,精准刻画政策干预的真实影响路径,最终形成政策实施的动态反馈机制。

二是有助于专家学者开展深度研究。专家学者可以利用微观数据设计多变量实证模型,开展多维度研究,例如有学者基于人口普查数据和地方落户政策来分析户籍制度改革与城市人口老龄化、经济发展程度、产业比重、教育水平之间的关系^[5]。微观数据可以提供更小调查单元的细节信息,学者可以通过可重复性检验、稳健性测试、反事实推断等方法论工具在微观层面开展系统性验证与拓展,这一过程不仅能够实现研究结论的稳健性评估,还可深化研究维度,从而推动学术共识的形成与理论边界的拓展,产出具有更高信效度的研究成果。例如有学者以家庭为分析单元,突破了传统的经济、社会、文化等宏观因素的影响,研究家庭收入对个体生育意愿的影响^[6]。

三是有助于政府部门提升数据质量。在用户使用微观数据的过程中,可以结合专业知识储备,对政府的数据分类标准、指标口径的界定逻辑、调查方法的设计原理以及数据采集的实施流程提出调查方案优化建议,包括但不限于抽样设计改进、问卷效度提升、数据处理流程优化等,从而推动有关部门实现数据调查方法的迭代升级与数据产品的持续优化。如有学者关注宏观数据和微观数据之间感受的差异性,如宏观数据好转,但微观数据表现却偏低迷,发现国民经济核算方法存在加总和统计偏差^[7],PPI(工业生产者出厂价格指数)和CPI(居民消费价格指数)统计制度和核算方法存在覆盖面问题与重复计算等问题^[8]。

1.3 隐私计算技术赋能数据开放的理论概述

隐私计算技术是指在保证数据提供方不泄漏原始数据的前提下,对数据进行分析计算的一系列信息技术。隐私计算涵盖了数据所有者、收集者、发布者和使用者在整个数据生命周期中的所有计算操作,包括数据生成、感知、发布和传播,到数据存储、处理、使用和销毁^[9]。主流的隐私计算技术包括基于密码学的安全多方计算、

基于硬件的可信执行环境、基于人工智能的联邦学习、基于噪声的差分隐私以及同态加密等^[10]。通过对个人信息等敏感数据的加密保护和专门的通信和算法协议设计，隐私计算可以实现“原始数据不出域”，保障数据在流通与融合过程中的“可用不可见”，只实现数据价值的转移，有效解决数据流通后潜在的失控问题^[11-12]。

一是通过部署可信的硬件环境，实现数据的可控可计量。传统的政府数据以数据包或者 API 接口形式对外开放。但由于数据的“可复制性”且数据利用过程的监测环境缺乏，政府可能会丧失对数据后续流通过程的控制，最终导致数据流通至不满足申请条件的用户处，出现个人隐私信息暴露或者数据滥用问题^[12]。而隐私计算技术中的可信执行环境可以通过基于硬件芯片的安全处理器将政府无法脱敏的数据隔离在一个安全空间内，阻止任何未经许可的数据访问和修改。同时，通过硬件访问控制权，政府也可以直接查询其他主体的数据使用记录，审查各方是否以合规合法的方式开展数据开发利用工作，预判风险发生的可能性^[13]。

二是通过模型运算和算法加密，实现数据可用不可见。联邦学习作为一种分布式机器学习框架，其通过模型参数的传递替代了数据的直接共享^[14]，不同数据资源的各个节点独立训练数据并获得模型参数后，上传至中心节点进行分发，而原始数据始终保留在本地。而安全多方计算则通过设计专用的密码协议与算法，在无需可信第三方介入的情况下，实现多方参与的加密数据直接开展联合计算。在数据处理过程中，各参与方无法获取原始数据，仅通过数据切片或密文来得到计算结果^[15]。安全多方计算已经被广泛用于涉及敏感隐私的特定场景中，例如医疗联合科研中患者隐私保护、跨机构金融风险模型训练等。目前开源的安全多方计算库也越来越多，如 Google 公司推出的 TF-Encrypted，Mata 开源的 CrypTen 以及蚂蚁开源的 SPU 等。

三是在数据可控可计量、可用不可见的基础上，满足多方参与需求，扩大数据开放范围。政府数据价值挖掘不是单方面的信息供给，而是多主体参与开发利用，因此需要和社会主体形成联动，共同构建数据价值挖掘机制。然而政府数据开放过程中涉及主体多样，容易引发数据权属争议等问题，导致政府不愿或不能开放。隐私计算实现了数据可控可计量、可用不可见，即使在数据所有权不明确或存在争议的前提下，也无需担心数据被转移泄露。

2 国外实践总结

2.1 将微观数据列入高价值数据集范围

欧盟、美国等国家和地区都将微观数据纳入高价值

数据集范畴，重点推动其开放和复用，将其作为拉动数据驱动型经济增长的重要着力点，相关政策如表 1 所示。早在 2013 年，美国、英国等国家便签订了《G8 开放数据宪章》，划定了高价值数据所涉及的领域，包括统计、公司、社会流动性与福利等 14 大类^[16]。美国在 2015 年提出要将高价值数据集开放作为地方政府数据开放的主要任务，由各部门或各州自行决定高价值数据集的发布方式和发布内容，如德克萨斯、明尼苏达等州政府均将人口、教育等微观数据纳入定期开放的高价值数据集^[17]。

欧盟则是在 2019 年发布的《开放数据和公共部门信息再利用指令》中正式明确了高价值数据集的概念与范畴，包括统计、地理空间、地球观测与环境、气象、公司及公司所有权、流动性六大类^[18]，并提出要开展高价值数据集开放试点。2022 年欧盟发布《数据治理法》，并指出要利用匿名化、差异隐私等技术确保微观数据可安全地再用于研究和创新^[19]。2023 年，欧盟更是进一步要求公共部门在 16 个月内按照数据清单免费提供统计数据、公司和公司所有权在内的高价值数据集。

表 1 主要国家/地区微观数据开放的相关政策

国家/地区	政策	主要内容
八国集团	《G8 开放数据宪章》	共同推动公司、犯罪与司法……统计、社会流动性与福利、交通运输与基础设施等 14 大类高价值数据的开放
美国	各州/部门自行决定	劳工部：公共劳动力系统数据集；明尼苏达州：人口普查、教育、环境等；德克萨斯州：人口普查、犯罪统计等
欧盟	《开放数据和公共部门信息再利用指令》	高价值数据集的主题类别涵盖邮政编码、国家和地区地图（地理空间）、能源消耗和卫星图像（地球观测和环境）、仪器和天气预报的现场数据（气象）、人口和经济指标（统计数据）、商业登记和注册标识（公司和公司所有权）、道路标志和内陆水道（流动性）
	《欧洲数据战略》	高价值数据集要在整个欧盟范围内以机器可读的格式并通过标准化应用程序编程接口（API）免费提供
	《数据治理法》	例如匿名化、差异隐私……以及其他先进的隐私保护方法……成员国应支持公共部门机构充分利用这些技术……欧盟层面已有此类安全处理环境的经验，可用于统计微观数据的研究

2.2 利用隐私计算技术部署数据可信安全环境

美国等许多国家和地区已经在跨部门使用、公私部

门协作等多类场景中应用隐私计算技术推动微观数据的应用^[20]，部分案例如表2所示。

表2 国外基于隐私计算技术的微观数据应用案例

国家/地区	隐私计算技术	数据集	涉及数据类型	应用场景
美国人口普查局	差分隐私	人口普查数据	政府数据、个人数据	向公共或私营机构输出口普查数据
印度尼西亚旅游部	可信执行环境	手机运营商数据	企业数据、个人数据	通过运营商数据生成旅游统计报告
欧盟统计局	可信执行环境	手机运营商数据	企业数据、个人数据	分析居民的居住变动信息
美国波士顿	安全多方计算	人口数据和工资数据	政府数据、个人数据	定期分析波士顿地区的性别和种族工资差距
荷兰统计局	安全多方计算、 同态加密、联邦学习	医疗保健数据	政府数据、个人数据	利用医疗保健数据开发疾病风险预测模型
意大利国家统计研究所	安全多方计算	社会人口统计数据、 金融数据	政府数据、个人数据、 企业数据	社会经济分析
韩国统计局	同态加密、安全 多方计算、差分隐私	各类统计数据	政府数据	统计数据关联并面向个人、 企业、公共组织输出

美国人口普查局部署“差分隐私免披露系统”，以安全披露美国人口普查数据。大数据再识别技术的出现使得人们可以利用美国人口普查统计所公布的许多数据，特别是那些在小地理单元中收集的数据，来推断出美国各子群体的情况，这与美国法律中统计数据必须保护公民的信息和身份这一要求相悖，导致部分统计数据始终无法开放。为了解决该问题，美国人口普查局自2020年起采用差分隐私技术，通过向公民数据添加噪声，以提升数据的隐私保护和可用性，对发布结果施加约束。

印度尼西亚旅游部和欧盟统计局则是对手机运营商所掌握的用户数据进行利用，前者用于编制旅游统计报告，后者用于分析居民位置移动信息。但运营商所提供的数据中包含用户定位信息，属于机密业务和个人隐私信息，不能无条件共享。因此印尼和欧盟均设计了一个可信执行环境，将运营商的数据输入到安全沙箱中，数据的分析仅在预定义的一组算法上进行，最终输出加密后的分析结果。

也有一些高敏感数据的应用涉及多种隐私计算技术，如荷兰统计局利用医疗保健数据开发疾病风险预测模型。医疗保健数据涉及公民的就诊信息、生活方式及其他个人数据，而这些数据往往属于多个部门，因此在数据连接环节就需要保障数据安全。为此荷兰统计局利用联邦学习技术设计了一个基础平台（Vantage），在该平台上数据输入方和计算参与方均通过经批准的 Docker 镜像来运

行预定义的代码，平台会对各参与方的操作历史进行集中记录以排除潜在隐私风险。

2.3 以多主体合作治理推进数据开发利用

合作治理的模式主要可以分为政府主导型、企业主导型以及政府主导市场化运作型。政府主导型一般是指政府负责顶层设计并承担规则制定、基础设施建设等职能，包括通过创新应用竞赛、建立试点项目和数据平台等形式来深化政府数据的应用。如美国的“公民黑客日”活动，便是动员全国各地的公民、企业共同利用美国劳工部、人口普查局等政府部门的公开数据、代码来设计数字化解决方案。欧盟部分“共同数据空间”的建设也是典型代表之一，政府主导在公共管理、工业（制造业）、交通、医疗健康、能源等影响公共利益和经济发展的领域建设数据空间。根据2020年出台的《欧洲数据战略》（European Data Strategy）^[21]，由政府开展各个数据空间的战略规划及监督指导，制定数据空间标准和构建技术支撑平台，而市场主体按要求参与数据空间的运行。

企业主导型则是指由行业内部约定数据流通标准，开展数据应用，甚至包括行业企业主动开放数据给政府、其他行业企业等群体。如德国工业数据空间是由弗劳恩霍夫协会牵头，协同130多家行业企业共同推进，在建设过程中，将参与主体划分为核心参与者、中介机构、软件和服务提供者以及监管机构四大类，明确各参与者在数据治理上的权责义务^[22]。该数据空间不仅服务于政

府决策，也支持高校院所开展相关基础性研究，还应用到行业中开展工业应用场景建设。而美国三大征信机构之一的 Equifax 通过整合个人号码、收入、房产、交易、水电煤账单等公共授权数据来提供全美领先的个人征信服务^[23]。

政府主导市场化运作型则是指政府负责统筹管理并提供资金或政策上的支持，而行业企业则负责具体的架构设计、平台运营等活动，欧盟的数据中介服务模式便是典型代表。根据调研和专家评估，欧盟发现个人、企业和政府间数据流通困难的主要梗阻在于缺少信任，担忧个人隐私、商业秘密或公共利益等方面受到损害。基于此，欧盟创设了“数据中介服务”，以既不掌握数据又不是数据需求者的第三方机构或平台来为数据持有者和使用者之间建立商业关系，实现数据交换。而为了提高社会主体对数据中介的信任，欧盟提供政府背书，为数据中介发放通行于整个欧盟的通用认可标识^[24]。

2.4 构建多层次法律体系保障数据安全和高效流通

欧盟与其他国家和地区相比，尤为突出的便是法律法规制定的充分度和详细性，数据安全合规是其法律法规的牵引主线。考虑到成员国法律体系的复杂性，欧盟通过阶梯式立法逐步完善数据治理规则，其立法框架聚焦于制定清晰公平的数据获取与使用规则。其中 2019 年

修订发布的《开放数据和公共部门信息再利用指令》，明确了欧盟范围内公共数据可访问的最低法律要求，包括数据格式和数据使用费用等方面。而 2022 年推出的《高价值数据集实施法案》则进一步规定了以统计数据等微观数据为代表的高价值数据集的目录清单、复用条件、传输标准等（表 3）^[25]，如其要求数据必须在知识共享许可或同等乃至限制更少的开放许可条件下公开，以欧盟范围内认可的开放格式进行发布，且允许以 API 接口等形式批量下载等。而 2024 年 4 月 21 日，欧盟正式发布了《数据法案》（Data Act）以进一步规范欧洲范围内数据共享标准和互操作性，特别是在构建数据空间的过程中必须遵循数据在空间内部及跨空间自由流动的标准。

为强化欧盟成员国间法律适用标准的统一性，欧盟还构建了多层联动的数据治理监管体系。欧盟数据保护委员会（European Data Protection Board, EDPB）负责制定各类意见文件和决定，并解决法律执行过程中所产生的争议^[26]。而在该委员会之下，各成员国也成立了本地数据保护机构，负责具体执行数据保护相关法律，并针对欧盟层面的法案出台本国的具体操作指南，如法国国家信息与自由委员会发布《通用数据保护条例开发者指南》、爱尔兰数据保护委员会发布《个人数据泄露指南》《通用数据保护条例下的数据泄露通知使用指南》等^[27]。

表 3 欧盟高价值数据集中关于微观数据的目录清单和使用要求

类型	数据集	发布要求	数据安全要求
生产消费	工业生产者价格指数； 按活动划分的销售量； 国际货物贸易统计； 欧洲旅游情况； 消费者物价协调指数	在知识共享许可或任何同等或限制性更少的开放许可的条件下； 以公开记录的、欧盟或国际认可的、开放的、机器可读的格式，包括 CSV、XML、JSON 等；	采用适当技术方法对涉及个人数据或其他隐私数据进行处理，包括概括、汇总、匿名化、差别隐私或随机化； 建立和完善数据获取的全生命周期审计机制； 定期发布数据安全风险监管报告
国民经济	企业关键指标； 家庭关键指标	通过应用程序编程接口（API）批量下载； 应按法律所要求的更新频率进行月度、季度和年度更新，保持最新数据； 数据应在公开文档中进行描述，包括数据结构和语义； 部分数据集的元数据以结构化文件形式提供； 附加有关个人数据再利用的法律条件	
政府	政府支出； 政府收入； 政府债务		
人口	人口总数、生育率、死亡率； 贫困人口； 就业； 失业； 潜在劳动力		
公司和公司所有权	公司基本信息； 单个公司的文件和账户信息		

注：笔者根据高价值数据集实施法案中的数据集清单及使用规则整理。

与欧盟全面覆盖成员国的数据安全保护和合规发布要求不同,美国倡导政府数据的自由流动,因此其法律法规中着重于数据的质量和可利用性,兼顾数据安全。2019年1月正式发布的《开放政府数据法》中明确要求要对政府公开数据进行日常性审查,创建政府数据及时性、完整性、准确性、实用性的评估流程,还对政府数据提出了每90天更新目录的要求。同时为确保政府数据高效开放流通,在联邦层面设立首席数据官制度,由政府各部门的首席数据官负责本领域数据的全生命周期管理,包括数据格式标准化、数据开放流程、基础设施建设等方面。

而在政府数据安全监管上,美国尚未在联邦层面出台统一的强制性要求,而是由各州单行立法为主。尽管2024年2月美国拜登政府签发行政令《关于防止受关注国家访问美国人敏感个人数据和美国政府相关数据的行政命令》,但也仅限于防止敏感数据跨境流动,对美国本土访问并不作限制。

3 对我国的启示

3.1 制定微观数据开放清单和动态更新机制

参照欧盟高价值数据清单模式,综合考虑数据类型、用途和敏感程度,制定相关政策明确微观数据无条件开放或有条件开放的范围和渠道。面向不同主题的微观数据,明确元数据格式、数据获取形式和获取方应具备的资质。如涉及个人隐私但又具备高社会价值的数据,可以建立专门的申请审批流程,要求数据获取方或使用方提供合法合规的使用计划。

结合数据生产频率、社会需求变化和相应法律要求等因素,定期对微观数据进行更新。积极探索数据获取形式,除传统的接口调用、下载等方式外,也可以提供数据可视化工具和分析平台,以更直观、便捷的方式利用微观数据。

3.2 搭建基于隐私计算的数据流通平台

利用隐私计算技术搭建包含底层硬件、基础协议、算法应用的分层架构,实现微观数据全生命周期管理体系。在底层硬件层利用可信执行环境实现存储即加密,也可利用联邦学习技术将微观数据存储在各数据提供方本地,实现原始数据不出库。在基础协议层,构建复杂运算逻辑,将数据开放的合规要求代码化,将其转化为隐私计算算法组件,避免事后补救。在算法应用层,可利用联邦学习进行联合建模,以数据不动模型动的方式实现通信和聚合。

也可以隐私计算技术融合来最大化巩固数据安全防护线,如融合联邦学习和多方安全计算两种技术,可以在

多方参与本地模型运算时,加强对中间数据的安全保护;而联邦学习和可信执行环境的融合又可以支撑在密闭数据空间内开展数据计算操作。

3.3 探索权责清晰的多主体合作模式

建立常态化沟通机制,积极开展产学研等社会主体对微观数据的需求调研,吸引其参与微观数据开发共建、规则标准设计等。在明确数据共治主体的基础上,制定权责清晰的合作机制,明确数据提供者、数据加工者、数据中介、数据需求方的责任和权益,同时鼓励各社会主体发挥自身优势,如企业可提供场景和资金支持,高校院所可贡献技术和人力支撑。

创新数据应用场景,形成场景牵引价值释放的共识,挖掘能反哺政府和社会主体双方的共赢场景,如在智慧城市建设中可以采取政企合作开发产品,在民生领域可以鼓励高校院所开展人口健康分析、劳动力情况分析,为政府政策制定提供依据。在场景应用搭建上,也可实施多样化的合作模式,通过数据应用比赛、项目试点、数据产品交易等形式开展微观数据应用。

3.4 完善分层分类的法律与标准体系

在现有《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规基础上,细化微观数据在归集、分类、开放、共享、交换、使用和安全等方面的管理办法和配套条例,在有条件的情况下,也可出台专项条例。

明确隐私计算技术在微观数据开发利用过程中的数据标准、技术标准、质量标准、应用标准等全方位标准体系,使数据能够以合理的成本被完整获取。建立技术和制度并行的数据合规体系,提升现有数据监管效能,在明确技术标准的情况下,通过立法或行政命令建立数据安全风险监管、数据内部定期审计、应急响应等制度,确保各部门在微观数据价值挖掘过程中有效履责。

4 结论

微观数据为分析经济社会发展形势提供了更为精细、翔实的信息,是保障政府部门科学决策、推动经济高质量发展的重要战略资源。以国家统计局为代表的政府有关部门在微观数据价值挖掘上开展了一系列工作。但微观数据作为聚焦居民、企业等个体层面的信息,在开发利用过程中,难以避免个人隐私保护等数据安全问题,因此在微观数据开发利用过程中,有效平衡发展与安全的问题是一大挑战。本文从政策、法律、组织、技术等多个维度系统分析了欧美国家的前沿探索,总结了系列做法,以期为我国微观数据进一步扩大开放范围、安全释放数据价值提供参考。

参考文献

- [1] 领导干部统计知识问答编写组. 领导干部统计知识问答 [M]. 北京: 中国统计出版社, 2018.
- [2] 李芳华, 张阳阳, 郑新业. 精准扶贫政策效果评估——基于贫困人口微观追踪数据 [J]. 经济研究, 2020, 55 (8): 171–187.
- [3] 蔡伟贤, 沈小源, 陈淋铃. 营养改善计划的人力资本提升效应研究——基于全国人口普查微观数据 [J]. 数量经济技术经济研究, 2022, 39 (10): 150–169.
- [4] 叶初升, 李竺雯, 孙薇. 政府与市场“双轮”何以驱动中小科技企业创新? ——基于微观企业数据的“促进科技和金融结合试点”政策评估 [J]. 经济问题探索, 2022 (5): 32–46.
- [5] 张吉鹏, 陈翥. 户籍制度改革与城市落户门槛的量化分析: 1996—2024 [J]. 经济学 (季刊), 2024, 24 (6): 1781–1797.
- [6] 方建国, 杨光瑾. 家庭住产市值收入比对居民生育意愿的影响研究——基于 CFPS2018、2022 微观数据的分析 [J]. 统计与管理, 2025, 40 (1): 40–49.
- [7] 倪红福, 冀承. 宏观数据与微观感受的“温差”: 现象、成因与对策 [J]. 经济学家, 2024 (5): 87–96.
- [8] 倪红福, 吴立元, 张志达. PPI—CPI 分化“悖论”及其传导机制——基于生产链 PPI 统计指标体系的新解释 [J]. 管理世界, 2023, 39 (2): 38–89.
- [9] LI F H, LI H, NIU B, et al. Privacy computing: concept, computing framework, and future development trends [J]. Engineering, 2019, 5 (6): 1179–1192.
- [10] 李建华, 银鹰, 李思源, 等. 大数据安全与隐私计算技术综述 [J]. 网络空间安全科学学报, 2024, 2 (6): 1–15.
- [11] 韩关锋, 陈刚. 隐私计算在大数据侦查中的应用研究 [J]. 中国人民公安大学学报 (社会科学版), 2023, 39 (4): 60–69.
- [12] 李轩. 隐私计算赋能公共数据开放的逻辑进路与风险规制 [J]. 科学学研究, 2024, 42 (8): 1716–1723.
- [13] 徐伟, 赵洲. 隐私计算赋能政府数据开放: 逻辑理路、现实风险与优化路径 [J]. 情报杂志, 2025, 44 (6): 193–200.
- [14] LO S K, LU Q, WANG C, et al. A systematic literature review on federated machine learning: from a software engineering perspective [J]. ACM Computing Surveys, 2021, 54 (5): 1–39.
- [15] ZHAO C, ZHAO S, ZHAO M, et al. Secure multi-party computation: theory, practice and applications [J]. Information Sciences, 2019, 476: 357–372.
- [16] 翟军, 李晓彤, 林岩. 开放数据背景下政府高价值数据研究——数据供给的视角 [J]. 图书馆学研究, 2017 (22): 76–84, 54.
- [17] 闫志开. 政府优先开放高价值数据集多维解析 [J]. 数字图书馆论坛, 2023, 19 (4): 29–38.
- [18] European Parliament. Open data and the re-use of public sector information [EB/OL]. [2025–05–26]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L1024>.
- [19] European Parliament. Data Governance Act [EB/OL]. [2025–05–26]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868>. 2022–05–30/2025–05–06.
- [20] 官方统计隐私增强技术 (PETs) 指南 [EB/OL]. [2025–05–26]. https://www.bjca.cn/content/details_267_6732.html.
- [21] European Commission. European Data Strategy [EB/OL]. [2025–05–26]. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.
- [22] 刘丽超, 高婴劼, 王宇霞. 借鉴德国经验打造我国工业数据空间 [J]. 数字经济, 2023 (7): 2–6.
- [23] 上海数据交易所. 数据要素化的创新实践 [M]. 北京: 经济管理出版社, 2024.
- [24] 宋杰, 柯晓燕. 欧盟“数据中介”: 促进数据可信流通的关键角色 [N]. 人民邮电报, 2022–07–15.
- [25] Commission Implementing Regulation. Laying down a list of specific high-value datasets and the arrangements for their publication and re-use [EB/OL]. [2025–05–27]. https://eur-lex.europa.eu/eli/reg_impl/2023/138/oj/eng.
- [26] European Data Protection Board: task and duties [EB/OL]. [2025–05–27]. https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en.
- [27] 王冬梅, 谭睿, 魏伟, 等. 数据要素下的数据安全合规风险与对策建议 [J]. 网络安全与数据治理, 2024, 43 (12): 67–73, 87.

(收稿日期: 2025–06–23)

作者简介:

董波 (1979–), 男, 硕士, 高级经济师, 主要研究方向: 数据治理、数字政府。

高金莎 (1996–), 通信作者, 女, 硕士, 主要研究方向: 数据治理。E-mail: G1693807389@163.com。

方丹 (1994–), 女, 硕士, 主要研究方向: 公共政策。

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

www.pcachina.com