大数据与决策研究

2022 年第 7 期（总第 117 期）

广西壮族自治区信息中心
广西壮族自治区大数据研究院　　2022 年 4 月 21 日

运用隐私计算技术破解数据共享开放困局的思考

数据作为数字经济时代的核心生产要素，正改变全球经济社会发展模式。面对数据要素市场优化配置形势，如何化解数据共享开放中存在的发展和安全、效率和风险矛盾，最大化释放数据要素价值，是当前亟待解决的重要课题。利用隐私计算技术，在保证数据安全前提下，实现数据可用不可见，正成为突破困局的新思路新模式。对此，本文阐述隐私计算概念、作用和各地发展现状，结合我区现阶段存在不足，提出对策建议。

一、背景

当前，各地在数据共享开放过程中，普遍存在确权困难、流动不畅、质量差异、资源有限，以及数据安全等问题，导致数据共享开放效能有待提升。要发挥数据核心生产要素对其他要素效率倍增作用，形成推动经济高质量发展的新动能，应探索技术赋能，联通信息孤岛，加快数据流动。隐私计算技术作为其中有效实践路径之一，正吸引各方关注，成为数据技术新赛道。

二、隐私计算概念、内涵和作用

（一）概念和内涵

隐私计算是指提供方、管理方和使用方在数据采集、存储、处理、使用和销毁等全生命周期，为将所有权、管理权和使用权分离，进行描述、度量、评价和融合等操作而建立的可计算模型与公理化系统。隐私计算是涵盖众多学科的交叉融合技术，目前主要分为：多方安全计算，其核心思想是设计特殊的加密算法和协议，基于密码学原理，实现在无可信第三方的情况下，在多个参与方输入的加密数据之上直接进行计算；联邦学习，其本质是分布式的机器学习，在保证数据隐私安全的基础上，实现保护终端数据的联合建模，分为横向、纵向与联邦迁移学习；可信执行环境，其核心思想是构建一个独立于操作系统而存在的可信的、隔离的机密空间，数据计算仅在该安全环境内进行，通过依赖可信硬件来保障其安全。

（二）主要作用

1. 助力数据要素市场配置

隐私计算有效破解数据要素价值盘活过程中的确权难、成本高、质量低、规模小，推动数据资源化、资产化和价值化，助力数据要素市场优化配置，赋能数字经济融合发展。一是维护数据资产权属。隐私计算可将数据所有权、管理权和使用权分离，调动多方主体积极性，加快数据汇聚、交易和流通。二是保障数据交换、使用价值。隐私计算能够不交换原数据而输出数据蕴含的知识，解决因抽取、清洗、转换导致数据价值稀释，促进数据要素市场化。三是赋能数据要素市场产业升级。隐私计算激发上下游产业链协作动能，带动全链条关联产业，提供数据清洗、供需撮合、法律咨询、价值评估等新业态新模式。

2. 有效防范隐私数据泄露

隐私计算技术间的融合应用，实现对等网络无可信第三方的联合建模，防止中间梯度信息泄露，提升隐私数据或模型安全等级，增强防范数据泄露风险能力，减轻多方主体顾虑。与区块链等其他领域技术的融合应用，可防止操作和处理记录被篡改，构建多边信任关系，解决数据共享参与者身份及数据可信问题，验证隐私数据保护合规性，提供闭环安全和隐私服务。

3. 促进数据安全合规协作

隐私计算推动多方主体数据安全合规协作，将数据价值

从消费侧向生产侧延伸，全链条最大化释放数据红利。一是消除多方主体间信任鸿沟，化解数据安全合规协作风险，减少数据保护成本，降低数据泄露风险，提高数据可用性，满足跨系统的业务形态；二是建立数据复制、传输等安全合规管理范式，履行数据保护责任和义务，切实保护关键信息、商业秘密，维护多方主体相关权益；三是兼顾发展和安全，平衡效率和风险，打破固有的数据保护束缚，消除数据壁垒和信息孤岛，创新全新的数据协同模式，拓展深化数据融合应用，最大化释放数据要素红利。

三、国内隐私计算发展现状

（一）国家层面

随着《中华人民共和国网络安全法》、《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》施行，我国网络安全与数据保护领域基本法律框架形成。为加快要素市场配置改革，国家、部委陆续出台《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》《要素市场化配置综合改革试点总体方案》《全国一体化大数据中心协同创新体系算力枢纽实施方案》《“十四五”大数据产业发展规划》等政策、规划，提出探索“原始数据不出域、数据可用不可见”交易范式，加强隐私计算等技术研发，构建数据可信流通环境，分级分类、分步有序推动数据融合应用。

（二）各省市层面

北京、上海、广东等省市围绕数据要素市场化，积极布局隐私计算，强化数字基础设施，打破数据资源壁垒，激发数据资源价值。**北京市**重点突破隐私计算等薄弱环节，建设隐私计算基础平台，打通“数道”“链道”，形成多域协同、自主可控、安全隐私的可信智能计算基础环境。**上海市**创新融合零信任等技术，构建良好生态，与长三角区域其他省共推隐私计算等技术应用。**广东省**构建包含隐私保护计算在内的新型数据基础设施三大枢纽，探索通过结合多方计算等技术，解决数据共享中的隐私保护问题。**山东省**搭建集数据建模、隐私计算、数据分析与可视化于一体的若干服务中台，推动开展多方计算等安全技术攻关。**浙江省**应用隐私计算等技术，推动数据所有权和使用权分离。**甘肃省**探索运用多方安全计算等新技术。

（三）行业层面

数据管理、医疗健康、金融保险等行业纷纷开展隐私计算应用试点。北京市运用隐私计算技术，提升数据管理效率效能，促进数据安全有序流动。上海市和厦门市建立健康医疗大数据应用开放平台，打通健康医疗数据孤岛，为医养健康、医疗保障等提供决策支持。由锘崴科技建设隐私计算平台，共享跨国多中心罕见疾病数据，开展新突发传染病实时监测和早期预警。浦发银行等多家金融保险机构打造异构隐私计算平台，构建风控联合模型、精准营销建模和信贷数据

分析体系，联合完成用户精准画像。

综合来看，各省市和行业主要做法：一是强化顶层设计，指明发展方向。各地依托自身资源禀赋，围绕数字要素市场配置，出台法律文件、规划纲要或行动方案，统筹顶层设计，明确总体思路，以完善“数据要素市场结构”为方向，以“数据不出域”“可用不可见”为重点，抢占新赛道，构建培育新生态，推动数字化转型。二是夯实基础平台，强化支撑能力。围绕数据集聚、运营和交易等环节，打造多域协同、自主可控、安全隐私的可信智能计算基础环境，构建数据流通共性设施平台，打通数据要素流动安全通道，夯实新型数据基础设施。三是推动数据共享，打破信息孤岛。探索隐私计算与区块链技术结合，解决数据共享中的隐私保护问题，推进政府、医疗、金融等领域数据要素赋能，建立健全数据安全治理体系，强化数据安全监管，确保数据交互安全、使用合规、范围可控。

四、我区隐私计算发展存在不足

我区数据要素市场化发展已取得显著成效，但在推动隐私计算技术研究应用，助力数据要素市场化配置方面，与其他地区相比，还有不小差距。

（一）前瞻性布局有待明朗。目前，我区尚未开展隐私计算顶层设计研究，出台相关法律法规、政策文件。缺乏数据要素资源配置标准规范、技术体系、监管规则以及相关发展产业布局指导，不利于推动数据要素市场进一步开放。

（二）抢占新赛道创新动能较弱。产业基础和发展环境相对薄弱，前沿技术研发门槛高、技术产品研发与应用需求结合不够紧密、资金支持有限等因素，导致隐私计算技术的核心理论、芯片模组、关键算法等创新能力较弱，创新成果无法支撑数据要素资源配置。2020年，我区计算机、通信和其他电子设备制造业规模以上工业企业研究与试验发展（R&D）经费5.47亿元，投入强度0.46%，低于全区0.32个百分点[1]。截止2022年3月28日，全国隐私计算领域专利总数1770件，我区仅有4件[2]。

（三）人才短缺瓶颈制约明显。从内部看，我区在全国有影响力的行业龙头企业不多，专注技术创新的科研机构较少，高校短时间难以培育适用人才。从外部看，我区长期存在对发达地区人才吸引力不高，高层次人才引进困难，人才流失严重等情况，导致隐私计算技术研究智力支撑力度不足。

五、对策建议

以助力数据共享开放和深度融合应用为目的，以隐私计算技术创新为引领，以供给侧结构性改革为动力，推进数据要素市场优化配置，加快数据资源流通，释放数据要素价值，为数字广西建设奠定坚实基础。

（一）做好顶层设计明确发展方向

做好顶层设计和统筹规划。尽快出台相关政策文件，明

[1] 数据来源：广西统计局网站 http://tjj.gxzf.gov.cn/tjsj/jdfx/qq/t10276165.shtml
[2] 数据来源：中国专利专利之星检索系统 https://www.patentstar.com.cn/Search/Index

确隐私计算技术应用条件、应用范围，鼓励融合创新，统筹产业布局，以新动能、新方向、新特征开启数据要素市场化配置新征程。

平衡技术应用与数据安全。既要为数据要素市场化配置预留空间，加快试点应用规模化推广，加强数据安全保护，加强监管以防止技术滥用，又要在技术推广应用与数据安全保护中找到最佳平衡点。

（二）培育数据要素市场完善产业发展环境

加快数据要素市场供给侧改革，加快数据分级分类，开展政企数据对接试点应用；制定关键共性技术标准和管理规范，建立数据质量管理体系，提高数据治理水平；约束数据要素流动各环节，建立健全数据权益、交易流通、跨境传输和安全保护等基础性制度规范，明确数据主体、数据控制方、数据使用方权利义务，保护数据主体权益。健全数据市场定价机制，激发数据流转活力，规范多方主体责任义务。

重点选择培育一批以科技创新和模式创新为支撑，成长性良好或进入高成长期的企业，集中数据、技术、资金、市场、人才等要素供给予以积极支持。以园区和基地为载体，开展针对性的招商引资和孵化培育，强化资金、技术、人才、项目和企业等产业要素导入和集聚，推动形成产业集群。

推动区块链、人工智能等隐私计算关联产业融合创新，找准融合路径，提出融合措施，坚持示范引领、典型带动，推进项目化、实物化，打造分行业、分领域高水平深度融合

典型示范项目，形成可复制、可推广的融合技术、可信产品和服务模式，带动技术更新、模式创新和产品供给革新，拓展发展新空间。

（三）加大关键技术研究，加速应用场景落地

抢抓新技术发展新赛道，统筹前沿技术前瞻新布局，强化关键技术创新突破，力争掌握核心技术新主导。

加速关键技术研发，补齐关键技术短板。构建隐私计算数据共享平台等新型基础设施，夯实数据要素市场化底座支撑；以提升计算性能和安全可靠为突破口，不断迭代密码技术和算法协议，开展隐私计算的算法、通信和硬件加速优化；以国产化替代相关产业为基础，重点研发可信计算环境与国产化硬件适配等关键技术和产品；以多路径融合、异构平台对接、海量数据支撑、数据合规遵从为方向，探索基于联邦学习的深度学习模型研究。加快隐私计算分支技术间、与区块链等其他领域技术融合。

深化融合应用加速应用场景落地。扩大技术、产品和服务供给能力，加快隐私计算应用场景推广，拓展跨领域、跨行业融合应用的广度和深度，支持高层次、高水平应用示范，进一步打通行业数据孤岛，鼓励和扶持新业态、新模式。

（四）加强人才引进培育，厚植人才资源优势

建立健全关键技术创新人才机制体制。加快制定人才发展专项规划，建立以隐私计算等前沿技术需求为导向的人才引培机制。打造产业优势、创新生态系统、提供多方面保障

性条件吸引人才，不断优化人才资源结构。加强对人才队伍建设的统筹协调和组织保障，确保人才供应链稳定。

强化产学研协作培养高层次人才。整合各类要素、融合更多优势资源，建立产学研联合培养机制，通过产学研紧密合作、联合攻关、协同培养，引进和培养高层次人才。

打造平台载体吸引人才聚集。深入实施人才强桂等战略，依托东博会、重大研发任务和人才基地平台等载体平台，持续开展“东盟杰青”和“港澳台英才聚桂”等计划，支持重点实验室和创新平台建设；加强与国内顶尖企业合作，持续引进领军企业机构。

发挥高校企业人才培养主体作用。激发企业抢占新赛道的意愿与动力，建立人才选拔培养体系和人才开发投入体系。鼓励高校在专业设置、师资培养、招生规模等方面倾斜，推动产教融合、校企合作人才培养机制，推进教育模式、内容与数据要素资源市场化需求对接，加强人才培养目标设计。

（执笔人：覃炜革）

编辑部地址：南宁市体强路 18 号广西信息中心 1412 号房
联系电话：0771-6113592
电子邮箱：dsjyjs@gxi.gov.cn
网址：http://gxxxzx.gxzf.gov.cn/

扫描二维码获取
更多决策参考信息