数据流通安全治理模式及实现：基于共创共治视角

文英姿[1]，江金菁[1]，杨红[1]，陈军[1,2]，何海兵[1]，曹礼峰[3]
1. 苏州数据资产运营有限公司，江苏 苏州 215131；
2. 苏州大数据交易所，江苏 苏州 215131；
3. 苏州市数据局，江苏 苏州 215031

摘要
数据跨域流通对安全治理提出了新挑战。识别了数据流通多主体，分析了流通安全治理挑战，提出以价值共创驱动数据流通，以安全共治保障数据流通安全，形成让数据“供得出，流得动、用得好、保安全”的“物理空间，技术支撑、制度安排和生态运营”四位一体数据要素可持续发展的长效安全治理模式。结合苏州落地实践，分析了多主体共创共治的具体路径和生态循环机制，为数据流通的安全治理实践提供参考。

关键词
数据要素；跨域流通；安全风险；治理模式；价值共创；安全共治

中图分类号：TP302 文献标志码：A doi:10.11959/j.issn.2096-0271.2024067

Data circulation security governance model and implementation: from the perspective of co-creation and co-governance

WEN Yingzi[1], JIANG Jinjing[1], YANG Hong[1], CHEN Jun[1,2], HE Haibing[1], CAO Lifeng[3]
1. Suzhou Data Asset Operation Co. , Ltd. , Suzhou 215131, China
2. Suzhou Big Data Exchange, Suzhou 215131, China
3. Suzhou Data Bureau, Suzhou 215031, China

Abstract
Cross-domain data circulation has brought new challenges to security governance. Multiple participants of data circulation were identified, challenges of circulation security governance were analyzed. Under the principles of promoting data circulation through value co-creation, ensuring data circulation security through security co-governance, a long-term security governance model oriented to ensure data can be high-supplied, smooth-circulated, well-used, and safe-guaranteed was proposed, which involved physical space, technical support, institutional arrangements and ecological operation. Based on the practice in Suzhou, the specific path and ecological cycle mechanism of value co-creation and security co-governance were analyzed, which provides reference to implementation of data circulation security governance.

Key words
data factor, cross-domain data circulation, security risk, governance model, value co-creation, security co-governance

0 引言

2022年，中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”），提出“建立数据来源可确认、使用范围可界定、流通过程可追溯、安全风险可防范的数据可信流通体系”“培育数据要素流通和交易服务生态”“把安全贯穿数据治理全过程，构建政府、企业、社会多方协同的治理模式”。各地政府高度重视，相继出台政策法规，设立数据交易场所，开展数据要素市场化流通探索。在实践探索中，数据要素流通指不同主体、不同场景、不同域、不同网络环境间进行数据交换的行为[1]，实质体现为数据的跨域流通，表现为跨空间、跨管辖、跨信任[2]。面对数据生产、加工、使用环境虚拟化、模糊化、碎片化等特征，传统“政府+市场”治理模式出现失灵[3]，如何让数据稳定、高效、安全流通，释放更多价值成为数据要素市场化面临的主要问题和关键挑战。笔者识别了6类数据主体，分析了数据流通安全治理的风险和挑战，基于“共创共治”视角，设计了包含“物理空间、技术支撑、制度安排、生态运营”在内的四位一体的数据流通安全治理新模式，提出了完善数据价值共创生态和安全共治生态，从生态运营逻辑增强数据流通安全治理生态系统多主体正向黏性，形成可持续的运营闭环，推动数据要素增值、复用，实现数据要素价值的放大、叠加、倍增。最后，本文分析了该模式在苏州医保场景中的落地实践，为数据流通安全治理模式落地、赋能地方产业和社会民生提供了一个可借鉴方案。

1 数据流通安全治理现状

1.1 数据流通多主体参与

数据主体是指参与数据要素市场化流通且具有相关职责与权利的组织或个人。王衍之等[4]按照供给、加工、需求，将数据要素市场参与主体总结为数据生产商、数据服务商和数据服务需求商，数据生产商提供数据要素，数据服务商进行数据要素整合、加工形成数据产品或服务，最终提交给数据服务需求商。苏宇等[5]提出数据持有者、提供者、消费者、使用者、中介机构、监管机构等，在共同空间实现跨领域数据互操作及流通。由于数据要素具有可复制性，为避免数据滥用，保障数据主体权益，需引入监管方。李凤华等[6]认为数据流通涉及数据提供方、中间服务方、数据使用方、监测方等主体。为保障数据安全并推动主体互信，需引入数据运营方，推动数据提供方和数据使用方的供需对接，形成由数据提供方、使用方、运营方、监管方4类主体组成的数据要素市场化流通生态系统[7]。综上，本文基于已有研究对数据流通多主体的探讨，将数据主体分为数据持有方、提供方、开发方、运营方、使用方和监管方等。数据持有方将数据授权给数据提供方。开发方将原始数据开发成数据产品或服务。运营方负责数据需求调研，实现数据供需场景化匹配，并根据实际情况联合成立大数据重点实验室、行

业联合体等，共同开展应用场景挖掘和数据产品开发。数据使用方是对数据产品或服务具有使用需求的主体，数据监管方是负责全流程监管责任的主体。

1.2 数据流通全过程安全

数据流通安全应采用全过程治理策略。邓巍伟等[8]依据数据在医疗场景中的流通行为特点，提出涵盖数据采集、传输、存储、使用、提供&公开、销毁等主要阶段差异化的数据安全管控策略。王文娟[9]提出制定流通事前合规计划，提升流通事中监管实效，构建流通事后惩治机制。对数据流通过程的划分，黄超等[10]认为流通前包括数据采集和预处理等活动，流通中进行数据开发、发布联合建模等活动，流通后开展数据审计、合约落实监督等活动。尹绮等[11]基于数据生产到完成全过程，提出数据流通应包括生产、治理与维护、合规审查、登记与评估、议价与沟通、签约与交付等核心环节。综上，笔者基于流通过程中的数据特点、主体参与和业务场景的差异，将数据流通安全过程分为数据汇聚治理安全、流通入网安全、授权开发安全、授权使用安全、终止与销毁安全等主要环节。

1.3 数据流通安全治理挑战

（1）主体间信任有待提升

多主体差异化的利益诉求产生冲突，数据供给和需求缺乏有效对接机制，供需双方存在双边模糊性及信息不对称问题[12]，数据提供方无法确认其他数据主体如何使用、是否会滥用所提供的数据[13]。数据采集、汇聚、加工、流通等各环节可能存在的数据泄露、数据滥用等安全风险及数据流通过程中可能产生的负外部性[14]均加深了数据供给方对数据安全和隐私的顾虑[15]，多元主体之间信任关系基础薄弱导致多元主体间缺乏长效的协同机制，数据流通往往是一次性、小规模且影响有限的[12]，难以充分发挥各数据主体的优势和潜力，阻碍数据高质量供给，不利于数据要素价值的放大、叠加和倍增。

（2）技术保障有待创新

相较于单域数据流通的场景，数据跨域流通时可能被留存，变相用于其他未授权场景[16]。多方参与可能存在恶意推理攻击、恶意镜像、非法流出等风险。支撑数据要素安全、稳定流通的完整技术体系和安全、可信的流通环境并未完全建立，数据流通全生命周期管理机制和数据全流程追溯技术能力有限。同时，大规模跨域数据的调度和寻址对关键技术的要求日益提高，部分传统安全防护技术难以应对当前数据跨域流通的安全风险。比如，去标识化数据再聚合后的标识信息存在暴露风险[17]，数据匿名化和加密技术的有效性难以被保证[18]，数据匿名化可能存在再识别风险[19]等。此种情况下，传统数据安全机制和技术面临巨大挑战[20]，业界需要新型数据安全机制和技术应对跨域数据流通复杂、多元的安全风险。

（3）制度障碍有待突破

数据流通交易形成了“政策–发展规划–国家标准–法律法规”的框架[21]，但仍然面临诸多制度障碍，如权责利不清晰、标准规范不统一、安全监管机制不健全等。首先，现有数据产权相关法律制度尚不健全，“数据二十条”创新提出数据资源持有权、数据加工使用权和数据产品经营权“三权分置”的数据产权制度框架，但权属界定模糊，权利边界划定不清，责任划分不明确，导致数据流通过程中的数据权益的转移路径和机制不清晰。其次，数据流

通各环节标准缺乏统一共识[22]，跨域部门、系统之间数据接口、数据格式、数据语义、数据模型、访问机制、安全和隐私保护要求等标准不同，不利于跨域数据的互操作和统一查询，阻碍了数据跨域的大规模流通。最后，数据安全监管体制机制长时间缺位，导致主体行为缺乏有效的约束，不利于数据全生命周期安全监管、溯源和审计。

（4）数据要素市场化流通动力不足

与传统要素市场相比，数据要素市场仍处于培育期，面临较多的市场机制障碍，如应用场景日益增长的数据需求与高质量数据供给不足之间出现矛盾。据测算，2023年我国数据产量超32 ZB，但场内多数挂牌数据产品没有被交易，难以实现预期经济利益流入[23]，市场化配置效率偏低，数据供需匹配均值仅为0.41[24]。另外，市场参与者激励机制不足。现有收益分配的不规范、价格无序、激励与利益补偿机制不完善，加上数据开发成本及合规成本日益增加，数据主体参与数据开发利用的主动性和积极性进一步减弱，难以形成稳定、可持续、高效率的数据供应链。

综上，笔者尝试构建长效且可持续的数据流通安全治理模式，通过价值共创实现市场激励，完善数据安全政策标准，促进数据流通；同时，在传统数据安全措施基础上，创新空中开发、分域匿名化等关键技术方案，保障数据处理的可追溯性和可验证性。

2 数据流通可持续发展的长效安全治理模式

2.1 核心原则

（1）“运营—生态”价值共创

价值共创是指主体间进行资源整合与服务交换，建立服务生态系统的活动[25]。各数据主体通过数据流通实现主体间的资源互换、能力互补，形成“运营—生态”的价值共创生态。在该生态系统中，各数据主体以一致的价值主张达成价值共识，形成合作意愿；以资源和能力的共享互补实现多主体间的深度互动，推动价值共创。在这个过程中，各主体逐渐建立稳定的正向循环机制和正反馈机制，算法模型、开发者能力等在应用场景迭代中实现修正和优化，结合应用场景需求和痛点，在获得主体授权的基础上，可对数据进行新的价值组合。同时，新开发的数据产品或服务又可作为新的数据资源供给，赋能新的应用场景，形成“数据供给—数据整合—数据开发—数据利用—数据消费—数据再供给”的正向循环和“价值发现—价值激活—价值释放—价值叠加—价值放大—价值倍增”的价值共创链条，不断挖掘数据复用的增值潜力，其价值外溢更广泛地惠及价值共创系统中各主体，实现数据红利的共享，进一步增强各主体的黏合力，最终实现可持续的运营。

（2）“技术—机制”安全共治

针对数据要素市场数据主体多元、应用场景多变等特征，及流通中安全责任主体不清、安全事故溯源难等问题，本文通过“技术—机制”协同联动，构建多方数据主体共同信任、多元控制的数据流通全过程安全治理体系，如**图1**所示。其中，技术保障以数据流通平台等流通基础设施为载体，以数据匿名化、数据脱敏、数据加密、区块链、数据沙箱、多方安全计算、身份认证和访问控制技术等基础安全能力为支撑，构建空中开发、分域匿名等应用级流通安全技术。机制保障聚焦数据跨域流通各主体的安全合规核心诉求，形成体系化的数据流通全过程安全管理制度、规范与流程。

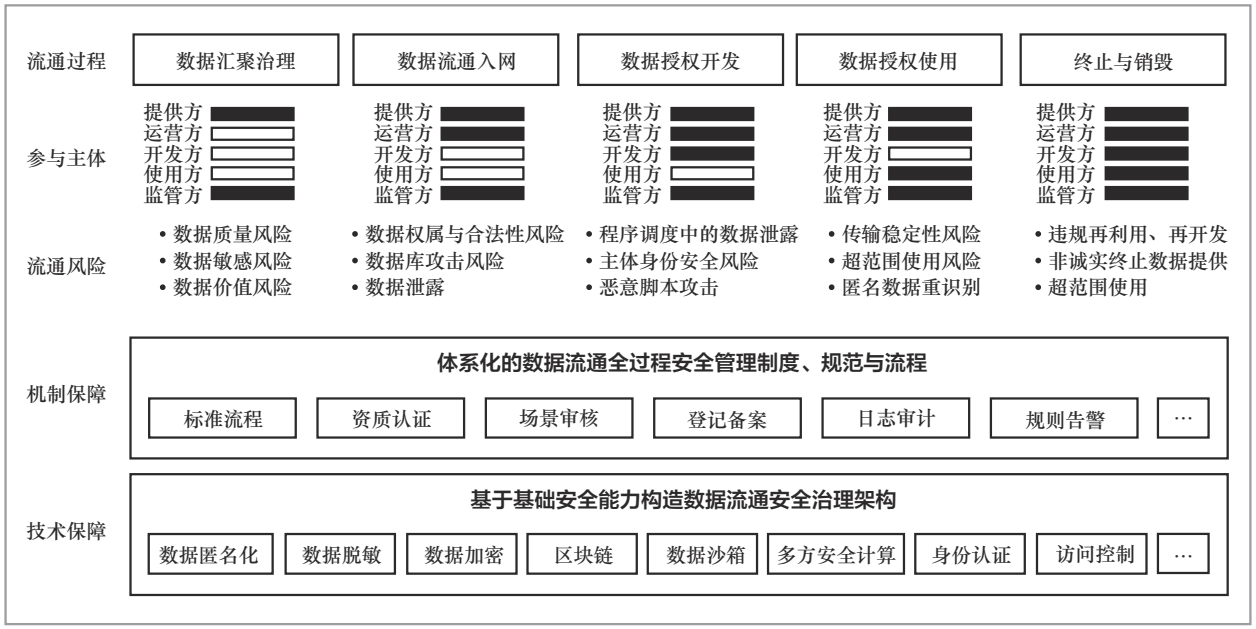

图1 数据流通全过程安全治理体系

2.2 “四位一体”模式

（1）物理空间

为实现价值共创，打造数据要素产业专业化高水平“孵化器”，与高校、科研机构等合作，聚焦应用场景核心需求和痛点，联合行业企业、第三方专业服务机构，构建起从数据资源整合到开发、应用拓展直至数据产品或服务流通、场景赋能的全链条，形成紧密的产学研合作模式和创新生态，向前贯通创新链，向后链接产业链。结合具体应用场景，为数据使用方提供定制化的数据产品或服务。依托资源、能力等整合以及政策虹吸效应，吸引各类数商汇聚，加快数据产品和服务在创新中心的孵化和转化。在创新中心生态逻辑下，打造垂直行业创新联合体，推动“数据链”“创新链”“价值链”“人才链”四链深度融合，发挥创新引领和数据资源聚集效应，持续优化价值共创。

为保障安全共治，打造数据安全屋模式，作为数据安全“缓冲区”，通过“数据不动算法动”，为高敏感数据的管理与保护提供一个全方位、多层次的安全环境，实现数据所有权和使用权分离，确保信息资产在存储、处理、传输及销毁过程中的安全性与合规性，保障“数据可用不可见”。具体包括物理与环境安全保障，以及数据分类与标签制度、强化访问控制机制、全方位加密策略、动态监控与智能审计体系、安全政策、规程与人员教育等制度安排。

• 物理与环境安全保障：确保数据中心及其他关键设施具备高标准的物理防护、环境监控及灾难恢复能力。

• 数据分类与标签制度：依据数据敏感度、价值及其对业务的影响进行分级，贴上相应标签，为差异化保护策略奠定基础。

• 强化访问控制机制：采用基于角色的访问控制（role-based access control，RBAC）、最小权限原则及双因素认证等方法，严格限制对敏感数据的访问权限，仅

授权必要人员在规定条件下进行操作。

• 全方位加密策略：实施端到端加密，包括数据静止时的存储加密与传输过程中的通信加密，确保即使数据遭遇非授权访问，其内容仍保持不可读性，有效防止信息泄露。

• 动态监控与智能审计体系：部署先进的监控工具，持续追踪数据访问行为，及时发现并响应安全威胁，确保安全策略的有效执行与持续优化。

• 安全政策、规程与人员教育：建立全面的数据安全政策与操作规程，定期开展安全意识教育与技能培训，提高操作人员对数据保护重要性的认识，构建稳固的安全文化基础。

（2）技术支撑

① 整体架构

为促进数据资源多元融合开发利用、规范数据要素流通等行为，采用组件化、分布式方法搭建贯通“数据层—支撑层—流通层—系统层—应用层—用户层”的平台，整体架构如**图2**所示。其中，数据层实现公共数据、企业数据等数据汇聚。支撑层包括网络、计算和安全设施等数据基础设施。流通层搭建数据接入引擎、计算开发引擎、要素加工引擎，实现跨域多源数据接入、加工、开发、安全治理。系统层提供数据授权、加工利用、使用计量、产品上架、流程审批、过程监管、信息公示等一站式运营服务功能，包括授权监管平台、数据流通一体机、运营服务平台、集中加工平台、数据服务商城平台、数据登记服务平台以及数据交易服务平台等。应用层主要管理数据产品，支持“数据要素×行业领域”的互联互通示范应用。

② 关键技术方案

一是空中开发。传统的数据开发模式

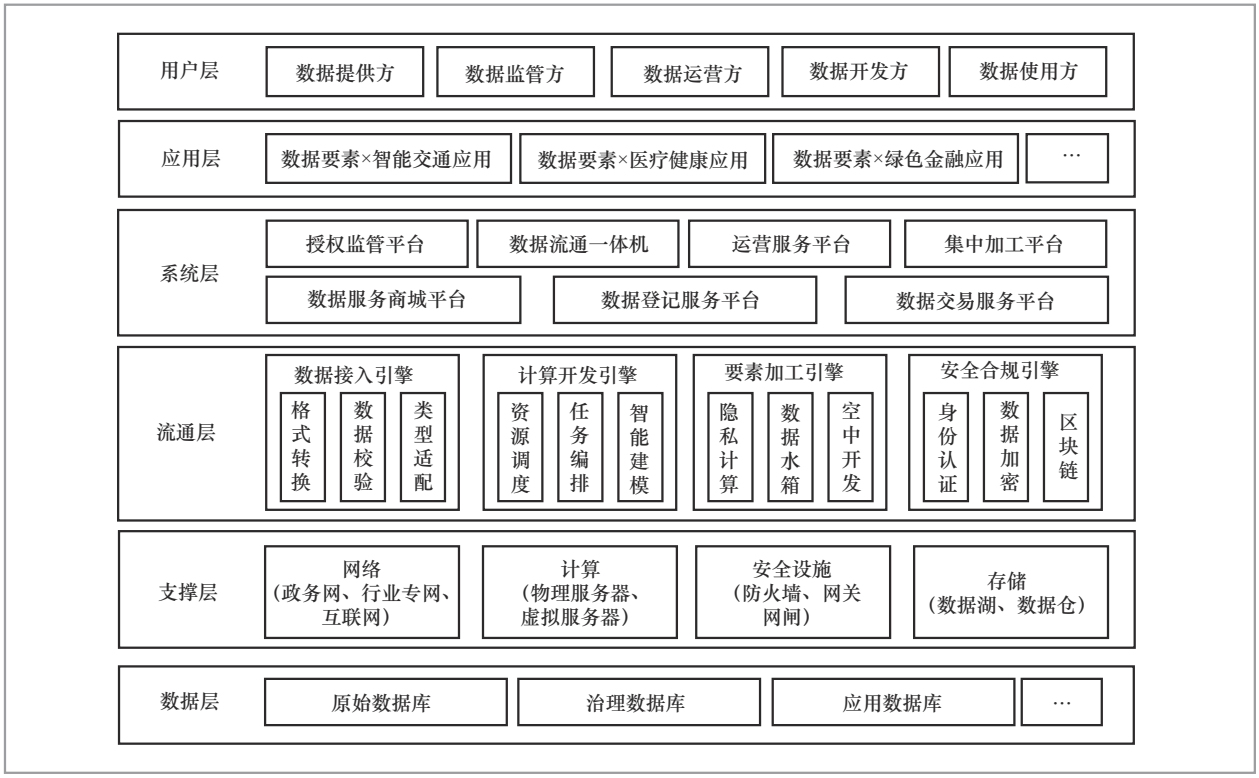

图2 平台整体架构

中，各数据主体难以形成产品开发的合力，数据提供方对数据流通安全存在顾虑，开发方需前往特定物理环境进行开发。尤其是在政务环境中，政务数据通过政务网传输，社会数据和政务数据难以在该环境中进行多元融合，且开发方需进入政府机房。针对以上问题，空中开发模式在“原始数据不出域、数据可用不可见”的原则下，分离生产环境和开发环境，贯通场景审批授权、数据加工处理、仿真数据生成、模型开发与测试、安全屋验证和产品上架等关键环节，具体如**图3**所示。其中，生产环境部署在数据提供方私域中，实现数据处理、部署验证、产品生产、调用运行。开发环境部署在运营方公域中，实现代码开发、专线访问、上架调用。在具体操作中，数据提供方经授权在生产环境中将原始数据分别利用仿真工具生成仿真数据存入样本库，利用抽样脱敏工具生成测试数据存入测试库，利用匿名化工具生成匿名化数据存入授权库，并通过镜像方式挂接至开发库。开发方在可信开发空间进行模型编码、测试、训练、评估等模型开发，并将算法包移交至安全屋。安全屋通过专线访问生产环境，利用测试库进行算法包部署验证以及模型调试、发布、运维等操作，在可信生产空间完成产品生产，发布至可信运营空间并通过授权库进行调用运行，上架至开发环境中进行应用。

二是分域匿名化。针对跨域流通中个人信息被泄露等安全风险，该方案基于场景和使用方主体划分隔离匿名域，并在各匿名共享域内采用不同的匿名化算法对个人信息主体特征进行匿名化处理，确保流通全过程的数据始终经过了匿名化，且无法直接定位到特定个人主体，增强对个人隐私信息的保护。若发生数据泄露等安全事故，数据提供方可快速锁定问题的匿名共享域，方便排查追踪，控制数据泄露范围，具体如**图4**所示。数据提供方基于xID等匿名化技术对原始数据中的敏感字段进行匿名化，生成匿名化数据存储在授权数据域。根据具体应用场景和数据使用申请，对授权数据域中具体场景所需数据资源再次匿名化处理，二次匿名化的数据被存储在匿名共享域，可供数据使用方查询。若

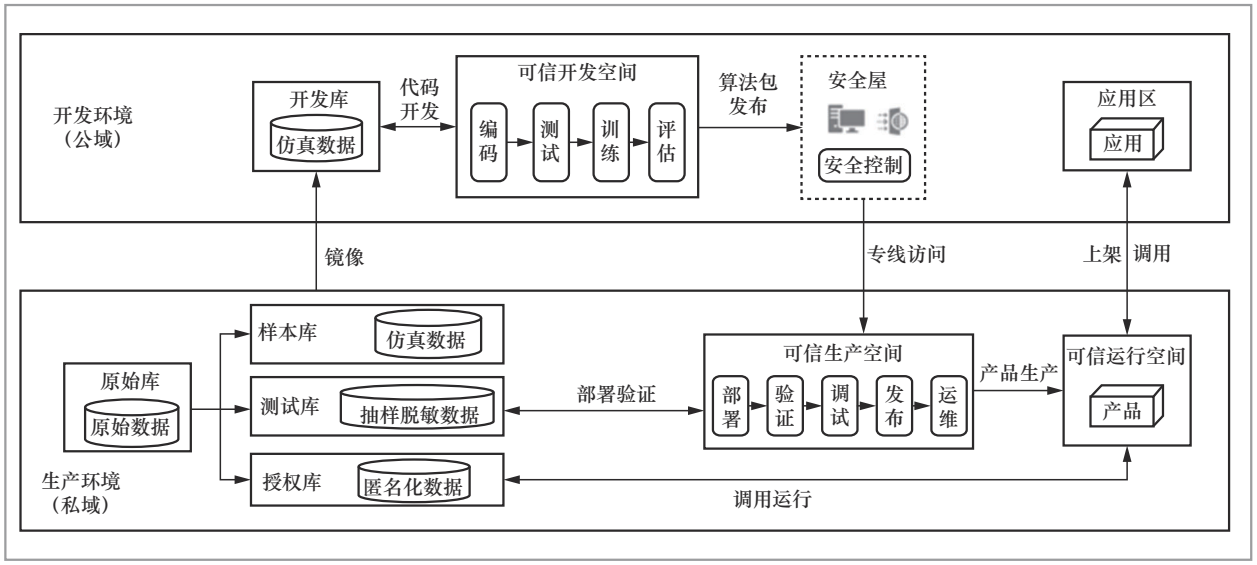

图3 空中开发技术方案

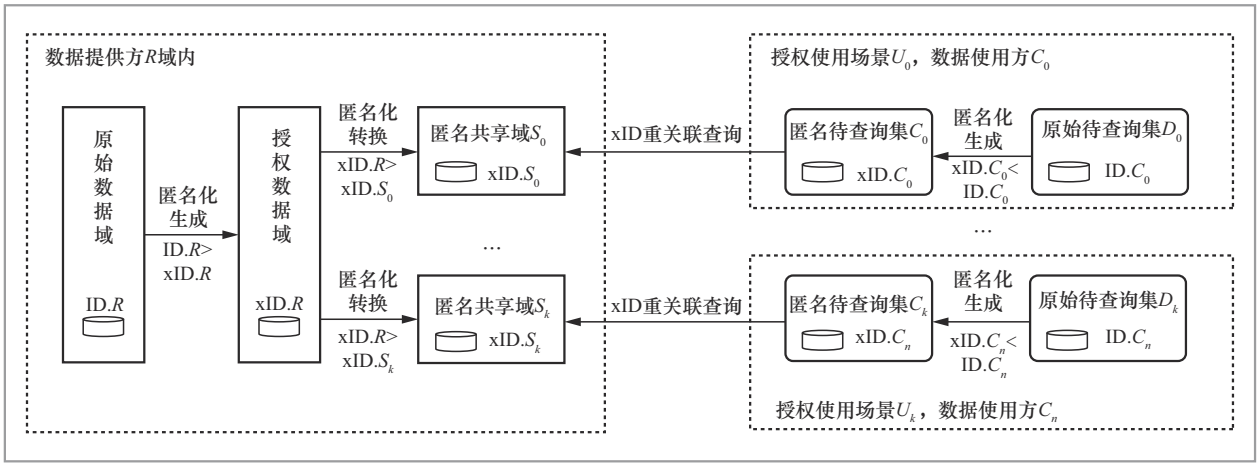

图4 分域匿名化技术方案

数据使用方发起数据查询，可通过匿名化生成后的匿名待查询集与匿名共享域中的主键字段进行重关联，获得查询结果。同时，针对不同应用场景及使用方设置不同的匿名共享域，确保各匿名共享域间无法进行匿名化后的标识重关联。

（3）制度安排

制度安排包括法律法规、标准规范、机制、合约（协议）等，是确保数据流通安全“合法合规合约”的重要依据。

- “合法”即在法律法规层面，国家拟出台数据产权、数据流通、收益分配、安全治理、数据开发利用等相关法律法规（管理办法），为数据流通安全提供坚实的法治基础。
- “合规”主要包括数据标准规范体系、开发利用规范体系、安全流通规范体系等。其中，数据标准规范体系涵盖数据的采集、存储、处理、传输、共享、撤销等，通过建立统一的数据标准规范，提高数据的质量、准确性和可靠性。开发利用规范体系关注规范开发方对数据的合法开发和利用方式，包括开发方的权限管理、开发工具的使用规范、开发过程中的合规审查等。安全流通规范体系涉及数据交换的加密传输、安全访问控制、数据交易的合法化和监管等，重点防范数据泄露和不当使用风险，保障数据的完整性和保密性。
- “合约”即在具体授权运营的应用场景，若法律法规、标准规范暂未覆盖事宜，可借由合同/合约等形式进行约定。比如，对特定场景下数据主体的权利、责任、义务做出明确规定，维系当事人之间的利益平衡，保障数据流通安全。

（4）生态运营

本文创新提出“C2M2R”生态运营模式，形成连通消费端（consumer）、制造端（manufacturer）、资源端（resource）的“应用场景牵引产品需求，产品需求驱动创新加工，供需两侧同向发力”的运营机制。以应用场景牵引产品需求，驱动数据产品开发与加工，匹配高质量数据供给。结合行业的现状和数据加工流通链条，明确不同主体在具体应用场景下的数据需求，吸引数据开发者打造数据产品或服务。强化多主体“资源—合作”关系，匹配高质量数据供给，扩大价值共创内生动力。采用“数据可用不可见”的方法接入行业和社会数据，丰富数据资源的供给途径，开发内部数据应用场景，逐步探索行业数据的外循环。

通过“价值主张—价值共识—价值共享—价值共创—价值共赢”逻辑，形成跨领域多主体参与、供需双重驱动的价值共创生态，通过数据资源、开发能力、场景应用与赋能等畅通数据供需匹配，减少因信息不对称造成的供需不匹配、市场化配置效率低下等问题的出现，提高各数据主体黏性，形成价值共创生态系统正向反馈闭环。完善数据流通计量计费能力，探索支持按条计费、收益分润、包年包月等多种灵活的计价方式，并利用区块链存证和智能合约技术，为数据流通各方提供公开、透明的收益分配机制，激励多主体参与数据流通，促进多主体间形成长期、持续、深入、长效的合作与互动机制，拓展数据合作的深度和广度，推动数据价值创造的更大化，实现多主体价值共赢。

3 苏州商业医疗保险理赔场景落地实践

本文以苏州商业医疗保险理赔为例，阐释多主体如何基于“四位一体”的数据流通安全治理模式实现价值共创与安全共治，赋能产业发展和民生服务。首先，阐述了“四位一体”模式在苏州的落地；其次，分析该场景多主体参与、数据跨域流通堵点等基本情况；最后，从场景需求和问题出发，论述了价值共创驱动数据流通、安全共治保障流通安全的解决方案。

3.1 “四位一体”模式苏州落地

（1）物理环境

苏州建设运营苏州大数据开发者创新中心，将其作为线上线下相结合的数据要素产业服务社区，汇聚数据开发者，为其提供物理空间，开发工具、数据资源、算力资源、合规审查、市场推广等数据要素创新应用一站式服务。建设数据安全屋，按照“原始数据不出域，数据可用不可见”原则，支持数据开发者安全、依法、合规对数据进行开发利用，推动公共数据、社会数据融合应用，促进数据使用价值复用。

（2）技术支撑

苏州开发建设数据要素价值共创平台，获评工业和信息化部2023年大数据产业发展示范。面向数据要素应用场景需求，以构建数据运营长效机制为目标，采用隐私计算、区块链等技术，创新空中开发、分域匿名化等技术方案，构建可信、安全、透明、便捷、可计量的数据要素流通环境，提供数据授权、加工利用、使用计量、产品上架、流程审批、过程监管、信息公示等一站式运营服务，支撑多渠道数据接入、开发、交易流通的全流程、精细化监管，推动数据要素实现内部流通使用，外部跨体系、跨行业、跨区域、跨主体的“内外双循环”。

（3）制度安排

苏州印发《苏州市数据条例》《苏州市公共数据运营工作方案》《苏州市公共数据开放三年行动计划（2023—2025年）》等法规政策。苏州大数据交易所构建覆盖交易前、中、后的全流程数据交易规则，围绕数据交易的数商入驻、产品上架、交易合约、资金结算等全流程，构建“1+7+4”数据交易规范体系。以“不审核不进场、不合规不上架、无场景不交易”为原则，根据不同数据交易类型，形成“数据供给合规→产品开发合规→产品交易合规”的数据交易合规范式，并发布数据交易合规审查指引等。

（4）生态运营

在“C2M2R”生态运营模式下，苏州大数据交易所开设金融、医疗、工业、交通、人工智能等行业交易专区，挖掘重点行业的应用场景需求，吸引数据开发者入

驻苏州大数据开发者创新中心，联合打造数据产品，并上架到专区进行流通交易。针对数据加工时的多源数据需求，互认全国数据、汇聚行业和社会数据，推动公共数据授权运营。各数据主体以价值共创为目标，形成多主体间深入合作，实现多主体可持续交互下的价值共创闭环。

3.2 场景基本情况

当前，商业医疗保险理赔流程环节烦琐、审核周期长，用户体验不佳。为打通多源数据核验通道，实现商业医疗保险“一键式”快速理赔，笔者梳理了该场景数据流通主要涉及的数据主体及核心堵点。

六大数据主体如下。

• 医院：数据持有方，通过业务系统采集业务数据。

• 医院监管单位：数据提供方，负责制定数据治理标准规范，指导并监督医疗健康数据合规使用。

• 数据运营企业：苏州数据资产运营有限公司作为运营方，负责数据供需对接等。

• 商保监管单位：数据开发方，前期基于样本数据开发快保核赔产品，后期基于匿名数据调用数据产品并将结果返回给商业保险公司。

• 商业保险公司：数据使用方，携带保险消费者的授权及查询入参发起查询申请，获得查询结果后为保险消费者提供赔偿服务。

• 保险消费者：是医疗健康数据的数据主体，也是商业医疗保险理赔的服务主体。

两大核心堵点：一方面，多主体参与下权责利交织，供给侧数据流通动力不足，市场供需不匹配；另一方面，该场景涉及大量非标准异构数据，此类数据不面向流通，直接使用存在困难。

3.3 场景解决方案

（1）价值共创：多种形式的收益分配和激励机制

多主体以实现商业医疗保险“一键式”快速理赔为价值共识，并以各方资源、能力形成不同主体间复杂的“资源-合作”“辅助-支撑”“互补-依赖”“补充-竞合”关系，强化多边主体依赖关系，扩大价值共创的内生动力。为进一步激发供给侧流通动力，笔者团队创新设计现金与非现金形式相结合的收益分配方案，并设立数据风险准备金。其中，现金收益分为数据产品收益和数据收益。数据产品收益由商保监管单位直接向商业保险公司收取。数据收益由数据运营公司作为拨付主体，按多方拟定合约分配机制进行收益流转。监管方负责过程中的监管核算。非现金收益主要表现为技术服务反哺、监管考核指标等。另外，数据风险准备金由运营方按比例将部分收益以风险准备金的形式存入数据风险账户，可用于购买保险或留存，以应对潜在的数据意外风险赔偿风险。

（2）安全共治：“技术—机制”安全保障

表1梳理了场景中各数据流通过程涉及的安全问题及其解决方案。

• 数据汇聚治理阶段，源头数据标准不一，原始库中个人敏感数据未被脱敏、未被加密，无法面向流通对外使用。对此，使用数据融合治理工具、xID匿名化工具等面向流通场景进行流通前数据治理。

• 数据流通入网阶段，通过数据登记标准指南厘清数据权属，使用分域匿名化等技术分离流通数据与其他数据，并对该区域内数据库中的敏感数据进行加密。

• 数据授权开发阶段，使用空中开发技术规避可能存在的数据泄露风险。开发前期，使用样本仿真工具构造样本数据，

表1 商保理赔场景下数据流通全过程“技术—机制”安全治理

流通过程	安全风险	技术保障	机制保障
数据汇聚治理	数据底账不清	数据资产管理（数据扫描）	—
	数据标准、模型、分类分级及安全保护要求不同	数据融合治理（实体对齐、模式匹配）；数据分类分级	医疗健康数据治理标准；数据分类分级管理指南
	个人健康数据等高敏感隐私数据	匿名化（xID）；数据脱敏	最小必要；合规评审；特权访问管理
数据流通入网	原始数据被绕开系统访问管控	敏感字段加密；分域匿名存储	数据存储安全管理规范
	数据权属不清	—	数据资产登记规范指南
数据授权开发	原始数据泄露	数据仿真增量；空中开发	数据安全屋；优先仿真数据开发；外部人员数据安全管理规范及保密协议
数据授权使用	数据传输脆弱性（弱口令等）	传输加密；安全传输通道等	数据传输安全管理规范
	缺乏数据安全边界防护及数据泄漏检测	API安全防护；API安全检测	数据接口安全管理规范；数据泄露安全风险补偿机制
	无法跟踪、监测数据使用方及使用场景	分域匿名化；区块链（智能合约、链上存证）	数据授权使用合约；以模型或核验等方式对外服务
	个人信息单独授权同意成本高	分域匿名化	企业及个人数据授权管理规范
	跨域主体间互不信任	可信身份认证；区块链	可信第三方；全程日志审计
	网络防护暴露面、被攻击风险增加	API防护网关；WAF（web application firewall）；IP白名单	数据安全威胁情报共享机制
	数据泄露时无法快速准确定位	数据水印溯源;分域匿名化等	数据风险补偿机制
	场景合规评估风险	—	数据使用场景安全评估机制
数据终止与销毁	超范围使用及再开发等	区块链；日志审计等	数据资产登记规范指南
	违约提前终止数据提供	区块链（智能合约）	数据授权使用协议中明确数据服务内容

并引导开发方优先使用样本数据进行开发，后期基于数据安全屋策略，在受控物理环境中通过安全通道访问匿名化的真实数据进行测试部署。

• 数据授权使用阶段，已有平台无法监控数据使用场景与使用主体，难以控制流通数据的超范围使用，安全控制措施薄弱，且存在接口安全机制不完备、数据加工过程缺乏有效的隐私保护机制和安全计算方法、数据可能被恶意镜像等安全风险。为此，笔者团队设计以数据沙箱、区块链、安全计算协议为核心的可信数据流通基础设施，使用API安全网关、安全传输通道等能力支撑数据传输。

• 数据终止与销毁阶段，为及时应对流通完成后潜在的数据泄露与超范围使用等安全风险，使用数据水印、数据访问控制、智能合约等技术进行智能阻断与实时安全风险态势感知监控。

（3）跨域数据流通的实现

经个人授权同意后，场景所需医疗数据信息通过跨域流通，实现商业医疗保险“一键式”快速理赔，具体如**图5**所示，主要涉及卫生专网、政务外网及商保专网3个数据流通域，以及两次信任域内跨主体流通、两次跨信任域流通。

• 卫生专网域内，各医院业务系统数据资源汇聚到本地的前置机（或数据库）中，按流通治理标准进行标准化治理后汇聚至卫健委数据中心。

• 从卫生专网到政务外网，数据运营公司作为该场景数据的授权运营方，将经过匿名化处理的脱敏数据接入数据流通交易平台进行匿名托管。

• 从政务外网到商保专网，商保监管单位根据业务场景需要向数据运营公司申请使用相关数据开发数据产品，在政务外网域内利用数据流通交易平台中的样本数据开发数据产品，并将最终产品接入数据产品服务平台。

• 商保专网域内，商业保险公司以接口的形式携带商保消费者授权发起查询。

3.4 场景落地成效

开发商业医疗保险“一键式快赔”数据产品，实现“数据多跑路，群众少跑腿，商保更普惠”。据不完全统计，该数据产品的流通应用，已成功帮助保险公司办结超800件理赔案件，赔付总额超25万元，赔付平均时长从原来的1.27天缩短至0.71天，至少缩短44%。同时，该场景中价值共创生态和安全共治生态各主体间形成稳定、正向互动机制，为后续健康险等数据产品开发的深入合作和可持续运营提供基础。

4 结束语

数据作为新的生产要素，具有易复制、排他性、非竞争性等特征，与传统生产要素相适应的治理规则难以适应数据要素市场化建设，给数据流通安全治理带来新的挑战。本文通过聚焦“数据要素可持续流通长效安全治理”，深入研究了数据流通安全治理面临的困难和挑战，建立了包含“物理空间、技术支撑、制度安排、生态运营”在内的全新治理模式；结合苏州商业医疗保险理赔应用场景，分析了价值共创生态和安全共治生态融合，共同推动数据跨域流通，促进数据要素价值创造与价值实现，赋能社会民生的具体路径。本文从应用场景需求出发，以生态运营为推进思路，完善流通规则，通过合约/协议约定各

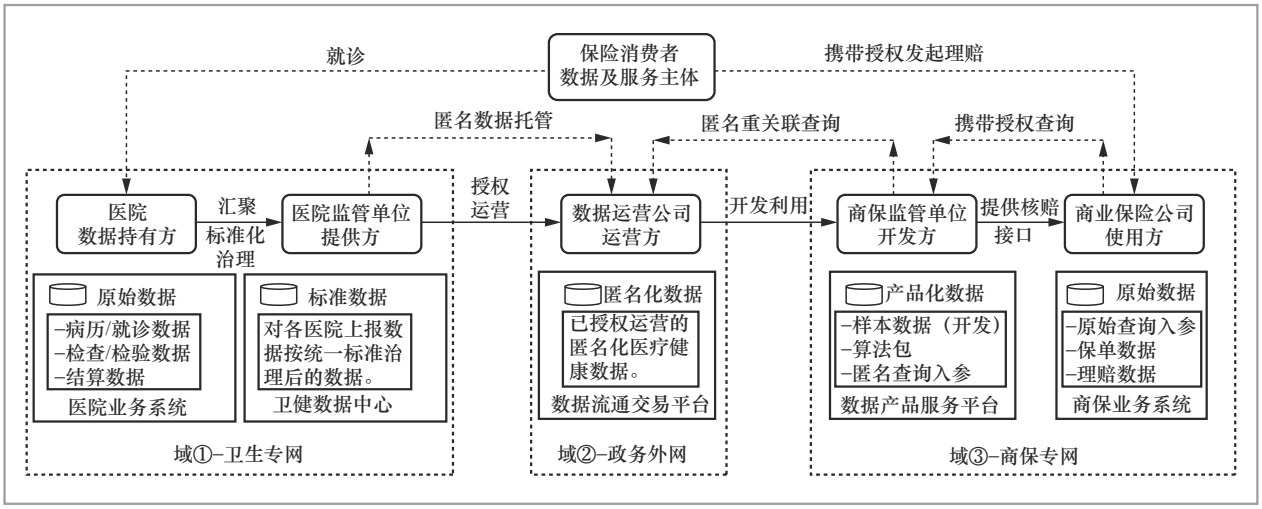

图5 商保理赔场景下数据跨域流通

方主体权责利，设计收益分配方案和激励机制激活数据供给侧动力，让数据“供得出”；基于平台搭建的可信安全流通环境以及运营方创新中心、安全屋等载体，实现数据多次跨域流通，让数据“流得动”；聚焦解决场景需求痛点、难点，让数据“用得好”；建立健全“技术—机制”多维数据流通安全治理体系，为数据“保安全”。

下一步，笔者将探索如何营造好价值共创生态和安全治理生态，丰富应用场景，推动关键技术体系落地，实现数据要素价值释放和安全治理协同发展。

参考文献：

[1] 姜琪, 孙超臣, 倪硕. 数据要素市场化进程中的数据流通与价值创造: 基于上海数据交易所的案例研究[J]. 金融教育研究, 2024, 37(3): 3-10.
JIANG Q, SUN C C, NI S. Data circulation and value creation in the process of data factor marketisation—a case study based on Shanghai data exchange[J]. Research of Finance and Education, 2024, 37(3): 3-10.

[2] 杜小勇, 李彤, 卢卫, 等. 跨域数据管理[J]. 计算机科学, 2024, 51(1): 4-12.
DU X Y, LI T, LU W, et al. Cross-domain data management[J]. Computer Science, 2024, 51(1): 4-12.

[3] 黄朝椿. 论基于供给侧的数据要素市场建设[J]. 中国科学院院刊, 2022, 37(10): 1402-1409.
HUANG C C. On building data market based on supply side[J]. Bulletin of Chinese Academy of Sciences, 2022, 37(10): 1402-1409.

[4] 王衍之, 黄静思, 王剑晓, 等. 数据要素流通与收益分配机制研究: 以风电场景融合气象数据为例[J]. 管理评论, 2024, 36(6): 30-41.
WANG Y Z, HUANG J S, WANG J X, et al. Research on the circulation and revenue sharing mechanisms of data elements: an example of integrating meteorological data in wind power scenarios[J]. Management Review, 2024, 36(6): 30-41.

[5] 苏宇, 卢怡. 数据要素可信交易流通: 共同数据空间的制度塑成[J]. 电子政务, 2021.
SU Y, LU Y. Trusted transaction and circulation of data elements: the formation of a common data space[J]. E-Government, 2024.

[6] 李凤华, 李晖, 牛犇, 等. 数据要素流通与安全的研究范畴与未来发展趋势[J]. 通信学报, 2024, 45(5): 1-11.
LI F H, LI H, NIU B, et al. Research category and future development trend of data elements circulation and security [J]. Journal on Communications, 2024, 45(5): 1-11.

[7] 张会平, 赵溱, 马太平, 等. 我国数据要素市场化流通的两种模式与生态系统构建[J]. 信息资源管理学报, 2023, 13(6): 29-42.
ZHANG H P, ZHAO Q, MA T P, et al. Two modes and ecological system construction of data element market circulation in China[J]. Journal of Information Resources Management, 2023, 13(6): 29-42.

[8] 邓巍伟, 关林宝, 张超, 等. 新形势下医疗数据安全体系的研究[J]. 网络安全技术与应用, 2024(6): 76-78.
DENG W W, GUAN L B, ZHANG C, et al. Research on medical data security system under the new situation[J]. Network Security Technology & Application, 2024(6): 76-78.

[9] 王文娟. 数据流通风险的识别与全流程治理路径[J]. 南昌大学学报(人文社会科学版), 2024, 55(3): 88-98.
WANG W J. Identification of data circulation risks and full process governance paths[J]. Journal of Nanchang University (Humanities and Social Sciences), 2024, 55(3): 88-98.

[10] 黄超, 贾宇航, 李克鹏, 等. 浅谈企业数据流通风险管理框架的构建[J]. 信息通信技术与政策, 2024(4): 47-55.
HUANG C, JIA Y H, LI K P, et al. Discussion on the construction of a management framework for enterprise data circulation risk[J]. Information and Communications Technology and Policy,

2024(4): 47-55.
[11] 尹绮, 王成. 数据要素化背景下医院医疗健康数据流通研究[J]. 中国卫生信息管理杂志, 2024, 21(3): 342-348.
YIN Q, WANG C. A study of hospital healthcare data circulation in the context of data factorization[J]. Chinese Journal of Health Informatics and Management, 2024, 21(3): 342-348.
[12] 杨艳, 林凌. 数据要素高质量供给: 内涵解析、困境挑战与规制设计[J]. 电子政务, 2024(7).
YANG Y, LIN L. High-quality supply of data elements: connotation analysis, dilemma challenges and regulatory design [J]. E-Government, 2024(7).
[13] LOMOTEY R K, KUMI S, DETERS R. Data trusts as a service: providing a platform for multi - party data sharing [J]. International Journal of Information Management Data Insights, 2022, 2(1): 100075.
[14] ACEMOGLU D, MAKHDOUMI A, MALEKIAN A, et al. Too much data: prices and inefficiencies in data markets[J]. American Economic Journal: Microeconomics, 2022, 14(4): 218-256.
[15] 黄京磊, 李金璞, 汤珂. 数据信托: 可信的数据流通模式[J]. 大数据, 2023, 9(2): 67-78.
HUANG J L, LI J P, TANG K. Data trust: a trustworthy data transaction model[J]. Big Data Research, 2023, 9 (2): 67-78.
[16] 张纪林, 顾小卫, 张亦钊, 等. 跨域数据授权运营研究及应用[J]. 大数据, 2023, 9(4): 83-97.
ZHANG J L, GU X W, ZHANG Y Z, et al. Research and application of cross-domain data authorization and operation [J]. Big Data Research, 2023, 9(4): 83-97.
[17] 周梓馨, 张功萱, 寇小勇, 等. 一种基于自注意力机制的深度学习侧信道攻击方法[J]. 信息安全研究, 2022, 8(8): 812-824.
ZHOU Z X, ZHANG G X, KOU X Y, et al. A deep learning side channel attack method based on self-attention mechanism[J]. Journal of Information Security Research, 2022, 8(8): 812-824.
[18] 施敏, 杨海军. 大语言模型数据隐私保护的难点与探索[J]. 大数据, 2024, 10(5): 168-176.
SHI M, YANG H J. Difficulties and explorations in data privacy protection for large language models[J]. Big Data Research, 2024, 10(5): 168-176.
[19] 张艳, 王璐瑶. 政府数据开放场景下匿名化数据的再识别风险防范[J]. 电子政务, 2024(5): 64-76.
ZHANG Y, WANG L Y. Re-identification risk prevention of anonymous data in the scene of government data opening[J]. E-Government, 2024(5): 64-76.
[20] 潘颖, 元昌安, 李文敬, 等. 一种支持更新操作的数据空间访问控制方法[J]. 电子与信息学报, 2016, 38(8): 1935-1941.
PAN Y, YUAN C A, LI W J, et al. Access control method for supporting update operations in dataspace[J]. Journal of Electronics & Information Technology, 2016, 38(8): 1935-1941.
[21] 文英姿, 曲杨, 张旭东, 等. 数据交易相关法规比较研究[J]. 大数据, 2022, 8(3): 66-77.
WEN Y Z, QU Y, ZHANG X D, et al. Comparative study on laws and regulations related to data transaction[J]. Big Data Research, 2022, 8(3): 66-77.
[22] 闫树, 卿苏德, 魏凯. 区块链在数据流通中的应用[J]. 大数据, 2018, 4(1): 3-12.
YAN S, QING S D, WEI K. Application of blockchain in data circulation[J]. Big Data Research, 2018, 4(1): 3-12.
[23] 文英姿, 吴维娜. 数据产品的资产性分析[J]. 大数据, 2024, 10(2): 43-53.
WEN Y Z, WU W N. Asset analysis on data product[J]. Big Data Research, 2024, 10(2): 43-53.
[24] 清华大学计算社会科学与国家治理实验室,中国电子信息行业联合会数据治理专业委员会. 中国地方数据发展报告(2023年)[R]. 2023.
Laboratory of Computational Social Science and State Governance, Tsinghua University, Data governance committee of china electronic information industry federation. Report on the development of local data in China (2023)[R]. 2023.
[25] LUSCH R F, VARGO S L. Service-dominant logic: premises, perspectives, possibilities[M]. Cambridge: Cambridge University Press, 2014.

作者简介

文英姿（1994– ），女，苏州数据资产运营有限公司研究员，主要研究方向为数据要素流通利用、数据资产、数字经济等。

江金菁（1999– ），女，苏州数据资产运营有限公司数据产品经理，主要研究方向为数据要素流通、人工智能等。

杨红（1997– ），女，苏州数据资产运营有限公司解决方案经理，主要研究方向为数据要素流通、数据安全等。

陈军（1975– ），男，苏州大数据交易所总经理，主要研究方向为数据要素流通、数据治理、数据资产运营、产业数字化等。

何海兵（1984– ），男，苏州数据资产运营有限公司技术总监，主要研究方向为数据基础设施、数据安全治理、大数据处理平台、隐私计算等。

曹礼峰（1989– ），男，苏州市数据局数据资源处四级主任科员，主要研究方向为数据基础制度、数据要素流通、公共数据开发利用等。

收稿日期: 2023-08-13

通信作者: 文英姿,yingzi_wen_ecnu@163.com