

政务可信数据空间的构建路径研究

侯玉国

上海市大数据中心三分中心, 上海 200051

摘要

聚焦政务数据流通领域, 分析了当前存在的“不敢享”“用不深”等核心问题。研究认为, 构建政务可信数据空间是破解政务数据流通瓶颈的关键路径, 作为全国可信数据空间体系的重要组成部分, 该空间能够为数据要素流通提供涵盖规则、技术、治理的三重保障。针对大模型训练、行业模型微调等人工智能应用对数据安全与系统支撑提出的新要求, 提出以数据分级治理为基础、以融合隐私计算与区块链技术为重点、面向AI任务的构建路径, 旨在推动政务数据实现合规高效流通, 为全国一体化数据要素市场建设及智能化治理能力提升提供参考依据。

关键词

可信数据空间; 政务数据共享; 隐私计算; 区块链; 人工智能

中图分类号: TP3

文献标志码: A

doi: 10.11959/j.issn.2096-0271.2026019

Research on the construction path of government trusted data space

Hou Yuguo

Third Branch Center, Shanghai Municipal Big Data Center, Shanghai 200051, China

Abstract

Focusing on the field of government data sharing, this paper analyzes the core problems such as "dare not share" and "not deeply utilized" that currently exist. The research holds that building a trusted government data space is the key path to breaking the bottleneck of government data circulation. As an important part of the national trusted data space system, this space can provide triple guarantees covering rules, technology, and governance for the circulation of data elements. In response to the new requirements for data security and system support put forward by artificial intelligence applications such as large model training and industry model fine-tuning, a construction path based on data hierarchical governance, integrating privacy computing and blockchain technology, and oriented towards AI tasks is proposed, aiming to promote the compliant and efficient circulation of government data and provide a reference basis for the construction of a national integrated data element market and the improvement of intelligent governance capabilities.

Key words

trusted data space, government data sharing, privacy computing, blockchain, artificial intelligence

0 引言

数据要素作为新型生产要素，是推动新质生产力发展的核心驱动力^[1]。然而，其规模化流通仍面临制度、技术与市场等多重瓶颈，制约了价值释放^[2]。可信数据空间作为新型流通设施，致力于解决身份互认、安全流通与使用控制等关键难题^[3]。2024年11月，国家数据局印发《可信数据空间发展行动计划（2024—2028年）》（以下简称《行动计划》），明确提出开展可信数据空间培育推广行动，培育五大类可信数据空间，以加速构建全国一体化数据市场。

在政务领域，我国已初步建成纵向贯通、横向联动的数据共享体系。国家层面，公安部、人力资源和社会保障部、教育部等部门构建的基础数据库，为跨省通办和全国性政务服务提供了关键支撑；地方层面，上海、浙江、江苏等地依托各自省级一体化平台，构建了省内数据共享机制，实现了高频数据的高效协同；长三角、珠三角等区域则通过区域平台，推动实现跨域业务联动与数据互通。但同时也应该看到，在推动政务数据要素化与市场化配置的过程中，“不敢享”的安全信任困境与“用不深”的技术应用瓶颈依然突出，这反映出传统数据共享模式难以满足敏感数据在深度应用场景下的安全与合规要求^[4-5]。

在此背景下，本文立足政务数据共享的发展现状与面临挑战，结合上海市的实践探索，旨在将国家可信数据空间的顶层设计与现有政务数据共享基础相衔接，构建适用于政务领域的可信数据空间体系，为国家数据空间体系建设提供政务行业实践范例。

1 政务数据共享的发展现状与问题分析

1.1 现有成就：“线一面”格局初步形成

经过国家“十三五”和“十四五”规划期间的持续建设，我国政务数据共享体系已实现从分散建设到集约整合、从无序交换到有序治理的重大转变。具体而言，其核心成就是初步构建了国家、省、市、县纵向贯通，各委办局横向连接的公共数据共享与开发利用体系^[4]，形成了“线一面”结合的可信数据空间雏形。

（1）“线”：国家级纵向数据空间

国家层面，各部委依托国家政务服务平台，纵向汇集本系统内的全国数据，构建全国统一的资源目录，建成多个关键领域的基础数据库，形成强有力的纵向数据枢纽，已成为支撑跨省通办、全国性政务服务的核心数据资源，提升了政务服务的规范性和效率。例如，公安部的人口基础信息为跨省身份核验提供了重要支持；教育部的国家学历学位认证信息有效促进了人才流动并加强了学历真实性核验能力；人力资源和社会保障部构建的全国统一社保服务平台支撑了跨省社保业务协同办理等。

（2）“面”：省级和区域级横向数据空间

在“面”的层面，各地已从平台建设阶段进入业务场景驱动的深度应用阶段，形成以省级平台为枢纽的横向数据共享与协同能力^[6]。上海以“一网通办”“一网统管”为牵引，依托全市统一公共数据平台汇聚超2000亿条数据，接口调用超480亿次，为超大城市全域治理提供坚实支撑^[7]；浙江以“一本账管理”和“一站式共享”

体系赋能“最多跑一次”改革，实现了服务理念重塑^[8]；江苏则通过高效共享交换体系（日均3.32亿条次），展现出数据规模化运营的巨大潜力^[9]。更重要的是，“面”的范畴已延伸至区域协同层面，长三角通过构建跨省共享底座与场景授权机制实现数据实时流动，累计交换超8亿次^[10]，已初步构建起一个服务于区域一体化的数据空间雏形。

1.2 核心问题：安全担忧与共享深度的矛盾

尽管建设成就显著，当前政务数据流通仍面临两大核心矛盾，制约其向更深层次发展。

（1）“不敢享”的安全信任困境

数据能够以远低于生产成本的代价进行复制，且能够被其他主体同时获取，加之数据源头难以追溯，确权工作推进困难，为数据要素这一新型生产要素的管理和治理带来新挑战^[11]。

数据提供方肩负数据安全责任，在对数据需求缺乏充分论证、数据使用去向不明确的情况下，出于合规与安全考虑，对共享或开放敏感数据存在“不敢”的顾虑^[12]。现有数据共享机制普遍缺乏细粒度的数据管控能力，无法实现对数据流通全生命周期的有效监控与审计，还存在数据二次共享问题，因此数据提供方对数据一旦共享后可能面临的滥用、泄露、权责不清等问题存在严重担忧^[5]。

（2）“用不深”的技术应用瓶颈

当前，各地政务服务应用（如“一网通办”“最多跑一次”“只报一次”“不见面审批”等）主要基于接口调用实现数据共享与业务协同，有效支撑了行政审批和便民服务工作。然而，政务数据的价值尚未被充分利用，基础数据库数据与其他业

务数据的深度结合能力未能充分体现，缺少通过智能化辅助决策、预测分析等手段提升政府科学决策能力的实践探索^[13]。在城市治理、宏观决策、预警分析等需要大规模数据融合、建模、深度挖掘与复杂分析的场景中，政务数据应用仍缺乏安全可靠的技术体系与应用环境支撑。一方面，由于此类应用往往涉及大量敏感数据，数据提供方出于安全与合规考虑，普遍存在“不敢共享”的顾虑；另一方面，现有技术平台在支持跨域数据“可用不可见”、联合建模与可信计算等方面仍存在明显不足，制约了政务数据在高层次决策与智能化治理中的价值释放^[14]。

上述问题的本质是现有治理模式与技术架构无法满足数据要素化对高等级信任保障和复杂应用支撑的双重要求。当前政务数据建设的重点任务已从打通数据共享渠道转向提升数据质量、保障数据安全、释放数据价值等更深层次的挑战^[15]。

2 政务可信数据空间的构建路径

为解决上述问题，构建以共识规则为基础、以技术为支撑、以治理为保障的系统性解决方案至关重要，国家层面倡导的可信数据空间，正是实现这一目标的关键路径。尤其值得注意的是，随着人工智能技术的迅猛发展，政务数据在支撑大模型训练、行业模型微调等智能任务方面的需求日益迫切，这对数据流通的安全性与系统支撑能力提出了新的更高要求。国家数据局在《行动计划》中明确指出，可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的

重要载体。

政务可信数据空间在现有政务数据共享体系基础上，引入可信数据空间的先进理念和技术体系，实现从“数据互通”向“价值互信”的升级。其充分继承现有数据资源目录、交换体系、管理制度等基础设施，针对包括AI训练在内的复杂数据应用场景，同时通过隐私计算、区块链等新技术建立更完善的安全信任保障体系，既是国家可信数据空间体系在政务领域的具体实践，也是其核心组成部分和重要应用标杆^[16]。结合上海实践，本文提出政务可信数据空间的5个重点构建路径。

2.1 实施数据分级治理,构建分类施策的流通体系

应基于《中华人民共和国数据安全法》及国家标准，对政务数据进行分类分级管理，建立与之匹配的分层治理体系并纳入差异化管理框架，实现“数据分类、技术分级、安全分区”的有机统一^[14,16-17]。具体而言，可根据数据敏感度和使用场景，将政务数据治理划分为以下3个层次。

(1) 原始数据域内计算层

此层包含最原始、最敏感的政务数据（如含个人身份证号、详细住址、电话号码的原始记录），其核心治理原则是“原始数据不出域”。该层数据不直接用于共享流通，而是仅作为基础资源用于支持隐私计算（联邦学习、安全多方计算（secure multi-party computation, SMPC））、数据沙箱（可信执行环境（trusted execution environment, TEE））、密态计算等先进计算范式。在此模式下，可以完成计算任务并返回计算结果，但原始数据永不移动，从根本上杜绝数据泄露风险。

(2) 脱敏标签化编目层

此层是当前政务数据共享体系中的核

心支撑层，通过对原始数据进行脱敏处理（如泛化、遮蔽），附加业务、质量、安全等多维标签，形成高质量、可共享的数据产品。以上海为例，其在数据安全分级与差异化脱敏基础上，基于各委办局的共性需求，对原始数据开展关联整合与深度加工，形成“推荐数据目录”，并构建自然人、法人等主题数据库，显著提升了政务数据的可发现性、可用性与易用性，为政务数据资源的高效利用奠定了坚实基础。

(3) 融合化数字产品层

此层是数据价值增值和创新层，其核心产出是基于融合数据开发，用于宏观分析、产业规划和社会治理的模型与数字产品^[16]。在此层面，可积极探索数据授权运营机制，在安全合规的框架下推动数据要素价值释放^[18]。该模式在赋能经济发展方面已显现巨大潜力，上海普惠金融应用为典型成功案例：市大数据中心并非简单开放原始数据，而是融合8个部门的300多项高价值数据，开发出用于企业信用评估的数据产品与风控模型；商业银行在“数据可用不可见”的授权模式下调用上述产品与服务，有效提升了中小微企业信贷的精准度和覆盖面^[19]。

2.2 深化隐私计算应用,打造“可用不可见”的安全底座

国家信息中心《基于区块链和区块链服务网络（BSN）的可信数据空间建设指引》（以下简称《指引》）和《行动计划》均将隐私计算、数据沙箱等列为构建可信数据空间的核心支柱与信任基石。

(1) 深化隐私计算应用

在跨部门、跨区域及跨行业数据融合场景中，应深化联邦学习、安全多方计算等隐私计算技术的落地应用。这些技术通过构建“数据不出域、价值可流动”的新

型基础设施，为跨主体数据融合与协同计算提供了“可用不可见、可控可计量”的安全保障能力，从根本上缓解数据提供方“不敢共享”的顾虑，推动政务数据从“有序共享”迈向“可信融合”和“价值释放”的新阶段^[15, 20]。

（2）建设数据沙箱环境

针对必须使用原始数据的高敏感计算任务，可部署基于TEE的数据沙箱^[21]。数据提供方将加密数据传入沙箱，计算任务在硬件级加密环境中执行，全程可监测、可审计，确保计算逻辑合规且原始数据不被泄露，实现数据“可用不可见”^[16]。

（3）探索密态计算全流程

推动数据在存储、传输及计算全流程保持密态。依托同态加密等密码学技术实现密文状态下的数据处理与分析，最终仅授权方可解密计算结果，最大限度降低数据处理过程中的数据暴露风险^[21]。

依托上述技术架构，政务可信数据空间能够在严守“原始数据不出域”红线的前提下，为跨部门数据协同场景提供切实可行的落地通道。在此基础上，针对大模型训练、行业模型微调等复杂AI任务的特殊需求，还需要构建更精细化的技术支撑体系，具体分析见2.5节。此外，也需要关注安全问题，针对联邦学习中可能出现的模型窃取、成员推断等隐私推断攻击，需结合差分隐私、梯度裁剪等AI加固技术，在模型协同训练时注入可控噪声，有效平衡隐私保护与模型可用性，增强AI任务的安全性^[20]。

以上海市虹口区“公共就业服务能力提升”项目为例，该项目可清晰体现不泄露原始数据前提下的跨部门数据协同计算实践。人力资源和社会保障部门持有就业、参保数据，公安部门拥有人口基本信息，双方需开展关联分析，但原始数据（如详

细的个人身份信息、参保明细）不能直接交换。项目借助蚂蚁集团发起并开源的隐私计算框架SecretFlow的安全协作查询语言SCQL，数据所有者通过列控制列表（column control list, CCL）机制对数据使用进行细粒度授权，例如限定公安部门的居民身份证号仅能用于与人社数据的关联拼接，且关联后立即进行脱敏处理；人力资源和社会保障部门的个人缴费明细仅允许在加密状态下进行聚合计算（如求平均值），不允许导出明细。SCQL引擎接收到一条虹口区参保人员情况分析查询请求后，会将其转换为一个明密文混合的执行图，通过安全多方计算等技术在分布式环境下协同执行，最终输出授权范围内的统计结果，全程不接触双方原始敏感数据，将“数据不动价值动”的安全合规目标从理念转化为现实。

2.3 依托区块链技术，构建面向智能时代的可信治理机制

信任的建立不仅源于技术控制，更源于透明的规则和可验证的机制。国家信息中心《指引》明确指出，区块链是构建分布式可信数据空间的基础技术底座，通过不易篡改特性，为数据提供了确权机制，对数据的使用进行追踪和记录，为数据的贡献者提供合理的利益分配。

（1）数据确权与存证

利用区块链的不易篡改特性，将数据资源的哈希值、数据目录、授权策略、使用规则等关键信息上链存证，为数据资源提供事实上的“确权”凭证，明确数据的来源、归属和版本，有效解决权属纠纷^[22]。在大模型时代，数据价值更多体现在其对模型训练的支撑贡献上，应在链上精准记录该数据在模型训练、微调过程中对模型性能提升的实际贡献（如梯度方向

一致性、损失下降幅度、特征重要性权重等指标)。

(2) 全生命周期溯源

将数据申请、授权、访问、使用、销毁等全流程行为记录在区块链上,使每一次数据调用成为透明可审计的“交易”。这不仅为数据提供方提供清晰的“数据使用画像”,增强其数据共享意愿,也为监管方提供全链条、可追溯的监管能力。

(3) 创新利益分配机制

构建可持续的政务数据要素化生态,其核心在于创新数据要素利益分配机制。

其一,应依托区块链技术构建数据从目录编制到流通利用的全流程可信环境。以上海为例,其通过将部门职责、业务系统与数据目录上链存证,建立了完整的元数据治理体系,并实现了数据申请与使用流程的全链上记录,形成了可追溯、不可抵赖的数据流通日志,为合规审计与监管提供了强大支撑^[12]。

其二,在全流程可信环境基础上,进一步探索数据要素的利益分配机制。可基于智能合约,根据数据使用次数、价值贡献、权重占比等指标,在授权运营场景中实现结算与分配的自动化。在政府部门间,亦可探索将链上记录的数据贡献、模型贡献作为财政记账或经费分配的参考依据,从而建立可持续的正向激励机制^[15,14]。

2.4 纳入特殊部门节点,构建“点一线一面”立体生态

一个完整的政务可信数据空间生态,还必须将掌管高敏感数据的部门纳入体系并作为政务可信数据空间中的特殊“点”节点。这类部门往往受法律法规或行业政策的严格约束,同时也是高价值政务数据的重要需求方。其并非孤立于体系之外的“数据孤岛”,而应以更高安全等级接入政

务可信数据空间网络,在不移动原始数据的前提下参与数据流通和联合计算^[14]。这一模式不仅能推动此类部门从被动的“数据保管者”转变为主动的“价值开放者”,也能在保障数据安全的前提下充分释放高敏感数据的价值潜能。通过科学的分级治理,结合隐私计算等关键技术,“点”“线”“面”三者协同,共同构成了一个既安全隔离又有机联动的政务可信数据空间有机体。

2.5 构建面向AI任务的支撑体系

政务可信数据空间的核心价值之一在于为AI驱动的政务智能化治理提供安全合规的数据基础^[3]。基于前文所述隐私计算安全框架,在“原始数据不出域”原则下,为满足大模型训练、行业模型微调等任务对网络、算力、算法的特殊需求,政务可信数据空间必须在现有数据分级治理框架基础上,构建一套与之匹配的精细化技术支撑体系。

(1) 网络

不同数据层级和应用场景对网络的要求存在显著差异,需构建分级、弹性的网络支撑架构;通过通信协议标准化、梯度稀疏化等机制,可在不对现有政务网络进行颠覆性改造的前提下,优先在“原始数据域内计算层”支撑跨部门的协同训练任务。

“原始数据域内计算层”主要支撑联邦学习等任务,其核心是模型参数与梯度的高频同步。政务专网需为参与联合建模的各部门节点建立低延迟、高带宽的加密通信隧道;为缓解带宽压力,需集成通信压缩、异步调度等优化机制^[23]。目前主流隐私计算框架(如SecretFlow、FATE)均已内嵌对这些机制的支持。

“脱敏标签化编目层”的数据沙箱环境

要求网络能够支持研究人员安全、流畅地进行远程操作，这需要构建安全、高速的远程访问体系，确保计算指令和加密结果的可靠传输。

“融合化数字产品层”提供模型即服务（model as a service, MaaS），要求网络具备高可用性和高并发能力，需通过应用程序接口（application programming interface, API）网关与服务网格技术，为模型服务调用提供负载均衡、流量治理和安全防护。

（2）算力

AI任务的算力需求需根据数据存储位置进行分布式部署，实现资源利用效率最大化。依托统一的算力调度平台（如SecretFlow采用的Kuscia架构），可以实现对分散边缘算力与集中中心算力池的统一管理与动态调度。

在“原始数据域内计算层”，各委办局（数据持有方）在本地部署满足联邦学习训练需求的算力设施（如GPU/NPU计算节点），构成分布式训练的算力基础，这些边缘节点需具备独立完成本地模型训练任务的能力。

在“脱敏标签化编目层”，省、市级大数据中心集中建设高性能GPU算力池，主要服务于数据沙箱环境中的高性能模型微调与复杂数据分析任务，通过算力虚拟化技术实现资源的弹性分配与集约化使用。

“融合化数字产品层”的模型推理服务算力主要由服务提供方（如大数据中心、数据授权运营方）承担，对使用者完全透明，实现了算力的即取即用。

（3）算法

算法层面是平衡模型性能、训练效率与隐私安全的关键，需针对不同层级的数据形态进行算法创新，使政务部门以较低的技术门槛启动在隐私保护前提下的联合

建模。

“原始数据域内计算层”需采用联邦学习与安全多方计算或差分隐私等技术融合的框架，在确保原始数据不离域的前提下进行协同建模。为应对政务网络的不稳定性，算法需兼容异步通信模式。

“脱敏标签化编目层”的算法需适配在TEE等受控环境中执行，并充分利用高质量的脱敏数据进行高效的参数高效微调（parameter-efficient fine-tuning, PEFT），快速完成领域模型的场景化适配。

“融合化数字产品层”产出的标准化模型API，其算法已封装为开箱即用的服务，重点在于服务的稳定性、兼容性和模型版本的持续管理。

政务可信数据空间的5个构建路径：从数据分级治理奠定流通基础，到隐私计算筑牢安全底座，再到区块链技术构建可信治理机制，继而通过纳入特殊节点拓展生态广度，最终构建面向AI任务的精细化支撑体系——共同构成了一套层层递进的实施框架。上述方案的有效性已得到初步实践验证，以上海的探索为例，其在政务数据治理体系基础上构建的城市级可信数据空间，作为国家首批试点，已生动展现出政务可信数据空间的赋能效应：该平台在试运行期间已吸引近300家企业入驻，开发数据产品超300个，累计数据调用量达数亿次^[24]。这充分证明，政务可信数据空间能够为城市级和行业级可信数据空间提供高质量的数据基础和丰富的产品供给，有助于加速推动全国一体化数据要素市场建设。

3 结束语

本文针对政务数据流通中“不敢享”

和“用不深”的核心挑战，提出构建政务可信数据空间的系统性解决方案，其核心在于通过规则、技术与治理的协同作用，实现从“数据互通”到“价值互信”的升级。该方案回应了人工智能时代大模型训练、行业模型微调等复杂任务对数据安全保障与高效计算提出的新需求，通过构建分级治理框架与相应技术支撑体系，为AI驱动的政务智能化应用奠定了安全可信的数据基础。展望未来，政务可信数据空间的建设应以现有政务数据共享体系为基础，重点推动隐私计算、区块链等技术的规模化落地，持续优化面向AI任务的网络、算力与算法支撑能力。建议各地在普惠金融、城市治理、民生服务等重点领域开展深度试点，推动政务数据从“共享”向“赋能”跃升；通过持续创新构建安全高效的数据要素流通体系，为数字经济高质量发展注入新动能。

参考文献：

[1] 王海杰,王开阳.数据要素驱动新质生产力发展的机制、挑战与应对措施[J].中国流通经济,2025,39(1):3-13.
Wang H J, Wang K Y. The mechanism and challenges in data elements driving the development of new quality productive forces and the countermeasures[J]. China Business and Market, 2025, 39 (1): 3-13.

[2] 莫梓嘉,赵晨.融合区块链和联邦学习技术的数据资产流通交易方案研究[J].大数据,2025,11(5):185-196.
Mo Z J, Zhao C. Research on data asset circulation and trading scheme integrating blockchain and federated learning technologies[J]. Big Data Research, 2025, 11(5): 185-196.

[3] 杨云龙,张亮,杨旭蕾.可信数据空间助力数据要素高效流通[J].邮电设计技术,2024(2):57-61.
Yang Y L, Zhang L, Yang X L. Trusted data space helps efficient circulation of data elements[J]. Designing Techniques of Posts and Telecommunications, 2024 (2): 57-61.

[4] 郭真,白喆,郭中梅,等.“十四五”时期数字政府研究与思考[J].邮电设计技术,2022(5):82-87.
Guo Z, Bai Z, Guo Z M, et al. Research and thinking on digital government in the “14th five year plan” period[J]. Designing Techniques of Posts and Telecommunications, 2022(5): 82-87.

[5] 易兰丽,赵丽丽,魏娜.机理与路径:区块链技术如何赋能政务服务“跨省通办”[J].电子政务,2025(2):45-56.
Yi L L, Zhao L L, Wei N. Mechanism and Path: How does blockchain technology empowers government services to “run across provinces” [J]. E-Government, 2025(2): 45-56.

[6] 孟凡,杨群力,高阳.决策驱动型省级政务大数据治理技术架构及实现[J].大数据,2024,10(2):140-151.
Meng F, Yang Q L, Gao Y. Technical architecture and implementation of decision-driven provincial government big data governance[J]. Big Data Research, 2024, 10(2): 140-151.

[7] 中国政府网.政务数据共享迈入法治化新阶段 上海“两张网”释放数字治理新效能[EB].2025.
Chinese Government Network. Government data sharing enters a legalized new stage: Shanghai’s “two networks” release new efficiency in digital governance[EB]. 2025.

[8] 中国政府网.全面贯彻落实条例 谱写数字政府建设新篇章[EB].2025.
Chinese Government Network. Fully

- implement the regulations to compose a new chapter in digital government construction[EB]. 2025.
- [9] 中国政府网.《江苏省数据条例》4月1日正式实施 推动数据“试验田”变要素“新高地”[EB]. 2025.
Chinese Government Network. Jiangsu Provincial Data Regulations officially implemented on April 1st: promoting data "test fields" to become factor "highlands"[EB]. 2025.
- [10] 新华网.长三角一体化|推动数据流通畅行 长三角建成跨省政务数据共享底座[EB]. 2023.
Xinhua News Network. Yangtze River Delta integration: facilitating smooth data circulation, the Yangtze River Delta completes a cross-provincial government data sharing base[EB]. 2023.
- [11] 中国信息通信研究院.数据价值化与数据要素市场发展报告(2024)[R]. 2024.
China Academy of Information and Communications Technology. Report on Data Valorization and Data Element Market Development (2024)[R]. 2024.
- [12] 人民政协网.天津市政协委员呼吁——进一步完善数据安全标准要求[EB].2025.
CPPCC Network. Tianjin CPPCC members call for further improving data security standards[EB]. 2025.
- [13] 邱玉婷, 万文佳. 江苏政务数据共享现状及对策研究[J]. 江南论坛, 2021(3): 13-15.
Qiu Y T, Wan W J. On status quo of and countermeasures for government affairs data sharing of Jiangsu[J]. Jiangnan Forum, 2021(3): 13-15.
- [14] 李林, 任伏虎, 王宇奇, 等. 基于实数融合的可信数据空间构建[J]. 大数据, 2026, 12(4): 24-44.
Li L, Ren F H, Wang Y Q, et al. Construction of trusted data space based on real number fusion[J]. Big Data Research, 2026, 12(4): 24-44.
- [15] 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.
Xu W, Zhao Z. Privacy computing empowers government data openness: logical mechanism, risk concerns and path innovation[J]. Journal of Intelligence, 2025, 44(6): 193-200.
- [16] 李帅峥, 张敏, 史翔, 等. 城市可信数据空间技术探索与建设路径[J]. 通信世界, 2025(13): 27-30.
Li S Z, Zhang M, Shi X, et al. Exploration and construction path of urban trusted data space technology[J]. Communications World, 2025(13): 27-30.
- [17] 商希雪, 韩海庭. 数据分类分级治理规范的体系化建构[J]. 电子政务, 2022(10): 75-87.
Shang X X, Han H T. Systematic construction of data classification and classification governance norms[J]. E-Government, 2022(10): 75-87.
- [18] 吕正英, 王浩然, 贺一舟, 等. 基于地方政府政策文本的公共数据授权运营模式对比分析[J]. 大数据, 2025, 11(6): 2-17.
Lyu Z Y, Wang H R, He Y Z, et al. Comparative analysis of public data authorized operation models based on local government policy texts[J]. Big Data Research, 2025, 11(6): 2-17.
- [19] 中国政府网. 上海: 大数据普惠金融应用上线[EB]. 2019.
Chinese Government Network. Shanghai: big data inclusive finance application launched[EB]. 2019.
- [20] 刘立伟, 傅超豪, 孙泽堃, 等. 数据要素流通全流程隐私关键技术: 现状、挑战与展望 [J]. 软件学报, 2026, 37(1): 301-325.
Liu L W, Fu C H, Sun Z K, et al. Privacy key technologies in whole stages of data circulation: current situation, challenges, and prospects[J]. Journal of Software, 2026, 37(1): 301-325.
- [21] 拾以娟, 周丹平, 范磊, 等. 基于可信执行环境的安全多方计算协议[J]. 信息安全,

2025, 25(9): 1439-1446.

Shi Y J, Zhou D P, Fan L, et al. Secure multi-party computation protocol based on trusted execution environment[J]. Netinfo Security, 2025, 25(9): 1439-1446.

[22] 王娟娟. 区块链助力数字政府可信建设[J]. 中国电信业, 2022(2): 45-47.

Wang J J. Blockchain helps the credible construction of digital government[J]. China Telecommunications Trade, 2022 (2): 45-47.

[23] 李程, 袁勇, 郑志勇, 等. 基于区块链的联邦学习: 模型、方法与应用[J]. 自动化学报, 2024, 50(6): 1059-1085.

Li C, Yuan Y, Zheng Z Y, et al. Blockchain-enabled federated learning: models, methods and applications[J]. Acta Automatica Sinica, 2024, 50(6): 1059-1085.

[24] 解放日报. 上海城市可信数据空间试运行已有近300家企业加入形成数据产品超300个[EB]. 2025.

Jiefang Daily. Shanghai urban trusted data space put into trial operation: nearly 300 enterprises joined, forming over 300 data products[EB]. 2025.

作者简介



侯玉国（1972-），男，上海市大数据中心三分中心副高级工程师，主要研究方向为软件工程、电子政务、大数据治理、数据安全等。

录用日期: 2026-01-23