

数据跨境 可信流通及共享体系的构建与实践

Construction and Practice of Trustworthy Cross-Border Data Circulation and Sharing System

穆晓君¹, 范 琨², 马瑞涛¹, 赵 灿¹, 加雄伟¹ (1. 中国联通研究院, 北京 100048; 2. 中国联合网络通信集团有限公司, 北京 100033)

Mu Xiaojun¹, Fan Kun², Ma Ruitao¹, Zhao Can¹, Jia Xiongwei¹ (1. China Unicom Research Institute, Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China)

摘 要:

在数字时代,数据跨境流动已成为数字经济的重要组成部分。然而,当前的数据跨境制度体系仍不够完善,存在合规监管与基础措施不足、安全及隐私保护手段欠缺、数据确权与价值分配机制不明确等问题。深入探讨了当前数据跨境流通中存在的问题,提出构建数据跨境可信流通及共享服务体系,分析了A市和B市利用这一跨境服务体系开展医疗数据跨境交互的实践,并对数据跨境可信流通的趋势进行了展望。

关键词:

数据跨境;可信流通;数据共享;数据保护

doi: 10.12045/j.issn.1007-3043.2025.05.005

文章编号: 1007-3043(2025)05-0026-05

中图分类号: TN919.2

文献标识码: A

开放科学(资源服务)标识码(OSID):



Abstract:

In the digital era, cross-border data flow has become an important part of the digital economy. However, the current cross-border data regime is still imperfect, with problems such as insufficient compliance supervision and basic measures, lack of security and privacy protection means, and unclear data rights confirmation and value distribution mechanisms. It deeply explores the problems in current cross-border data circulation, proposes the construction of a trustworthy cross-border data circulation and sharing service system, analyzes the practice of medical data interaction between city A and city B using this cross-border service system, and looks forward to the trends of trustworthy cross-border data circulation.

Keywords:

Cross-border data; Trustworthy circulation; Data sharing; Data protection

引用格式: 穆晓君, 范琨, 马瑞涛, 等. 数据跨境可信流通及共享体系的构建与实践[J]. 邮电设计技术, 2025(5): 26-30.

0 引言

在经济全球化与数字技术深度融合的背景下,数据跨境^[1-2]流动已成为驱动全球经济发展与技术创新的核心要素之一。随着云计算、物联网、人工智能等技术的普及,数据作为“新型生产资料”的战略价值日益凸显,其跨境传输、访问与使用的规模和频率呈爆发式增长。根据商务部发布的《中国数字贸易发展报告 2024》^[3],高速发展的数字贸易带来了大量的跨境数据流动。中国信通院数据表明^[4], 2020—2022年,

全球数据跨境流动规模平均增速超过30%。麦肯锡研究预测,预计到2025年,全球数据流动对经济增长的贡献将达11万亿美元,凸显了数据跨境对全球经济的强劲驱动作用。

近年来,我国紧扣数据跨境流动的关键因素,搭建起数据出境“双轨并行”的制度架构。一方面,依据《个人信息保护法》^[5],确立“个人信息跨境提供制度”。该制度聚焦个人权益保护,为个人信息的跨境流动开辟了多元合法路径。另一方面,依托《数据安全法》^[6]与《网络安全法》^[7],构建起“重要数据出境安全管理制度”,以维护国家安全为核心目标,对重要数据的跨境流动提出严格的安全保障要求,为数据跨境筑牢安全

收稿日期: 2025-03-14

屏障。2024年3月,国家互联网信息办公室颁布《促进和规范数据跨境流动规定》^[8],明确了数据出境路径的适用及豁免条件,为数据跨境流动提供了更加清晰的指导,具有里程碑式的意义。虽然上述法律和规定对数据跨境流动做出原则性规定,但暂时没有形成体系化的法律规则,数据跨境制度体系有待完善。

由于各国数据监管政策与法律体系不同、隐私保护理念和标准存在差异、网络安全技术发展不均衡以及对数据主权认知存在分歧,数据跨境流通面临诸多挑战。面对这些挑战,我国不仅要进一步完善国内的数据跨境流动制度体系,还需积极推动国际规则的协调与对接,减少因规则差异带来的摩擦。同时,政府和产学研机构要加大技术创新投入,提升数据跨境流动的安全保障能力,从而充分释放数字经济的发展潜力,推动全球数字经济的可持续发展。

1 当前数据跨域流通存在的问题

数据跨境流通和价值分享是数据要素市场化配置的重要手段^[9],正受到越来越多国家和地区的重视。为保障数据跨境流通和价值分享的安全可信可靠,相关国家和地区纷纷推出系列法律法规以构建和完善数据跨境流通监管体系。然而,当前数据跨境流通面临三大突出挑战:监管机制不完善导致合规风险频发,跨域计算安全与隐私保护技术滞后加剧数据泄露风险,跨主体确权与价值分配机制缺失阻碍资源优化配置。这些问题制约着数据要素的高效流动,影响全球数字经济可持续发展。

1.1 数据跨境流通监管机制不足

当前数据跨境流通的合规性监管措施和基础措施不足主要有3个方面的原因。第一,缺少统一的数据跨境流通监控规则。各国家/地区受国家安全、人权保护、数据主权等因素影响,制定了侧重点不同、多层次的数据跨境规则,在数据跨境流通过程中,需要同时遵从数据输出地和输入地不同的监管规则,输入地与输出地的监管规则各有侧重和差异。第二,尚未建立可信的数据流通体系。为保障数据的可信流通,需要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透明可信流通体系,实现数据要素跨境流通的全过程动态管理,目前尚没有可执行的可信的数据流通体系。第三,数据跨境流通的监管环节复杂,监管能力薄弱。数据跨境流动涉及多个国家/地区的数据中心,环节多,监管复杂,同时

目前的监管设施和监管能力薄弱,需要推动数据跨境流通安全保证能力建设,构建数据跨境流通监管基础设施。因此,亟需加强数据跨境流通全程可信追溯和透明监管的水平。

1.2 数据跨域计算的安全性和隐私保护手段欠缺

当前数据跨境流通中数据跨域计算(特别是人工智能服务)的安全与隐私保护手段欠缺。随着信息技术的快速发展,数据跨境流动从单一主体演变为多元主体、从物理形式演变为数据全生命周期,产生的风险也从个人隐私保护、商业利益诉求向国家数据主权升级跃迁,这也使得数据跨域传输和计算、隐私保护、数据安全面临更大的风险和挑战,期望通过以可信执行环境(Trusted Execution Environment, TEE)^[10]、隐私计算^[11]为代表的多种技术实现数据跨域传输和计算的可信安全和隐私保护机制,并适配监管机制,提高数据安全性和隐私性。但由于技术手段不成熟,目前在技术上对数据跨域计算防护尚未有可行的技术路径,需要进一步研究高安全、高隐私保护数据跨域传输与计算技术。

1.3 数据跨主体服务确权与价值分配机制不明

当前数据跨境流通中数据跨主体服务的确权与价值分配机制不明。数据跨境流通具有数据主体多元、权利内容多样的特点,数据主体的多元性反映了数据要素跨境流通过程中价值利益的不同,需要建立适配监管机制的可度量多方隐私计算服务机制,实现数据跨主体服务确权,进行主体间的激励相容。针对数据确权和价值分配问题,可以利用区块链、隐私计算等先进技术,确立多方数据服务确权机制,建立可信多方安全计算服务环境^[12-13]。

2 数据跨境可信流通与共享体系

本文提出数据跨境可信流通及共享服务体系,旨在通过涵盖基础设施层、服务层、应用层,提供全流程的安全与监管,保障数据跨境流通与共享时的数据隐私和安全(见图1)。在构建全域的数据跨境可信流通与共享体系过程中,基础设施层需布局关键基础设施;服务层提供跨境数据可信共享的关键数据服务,包括可信隐私计算服务、基于TEE的可信数据跨境流通管理服务、数字身份服务等;应用层着重探索数据跨境流通与共享的应用领域,包括医疗、教育、交通、工业互联网等;安全及监管层则聚焦数据监管与隐私保护,提供数据跨境流通合规检测与安全保护等;从

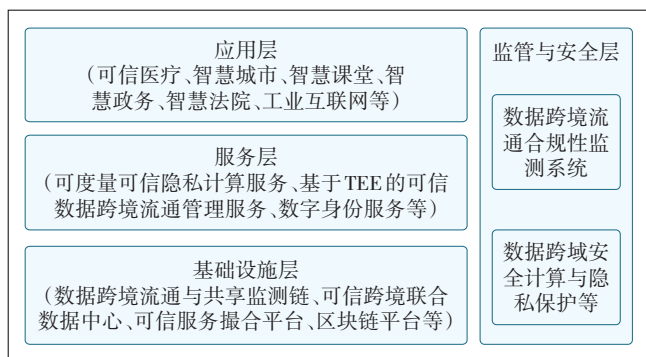


图1 数据跨境可信流通与共享体系

而打造全方位可信流通与共享体系。

a) 基础设施层。它是数据跨境可信流通与共享体系的底层支撑,提供数据跨境流通与共享监测链、可信跨境联合数据中心、可信服务管理平台、区块链平台等可信基础设施,为数据的存储、传输及管理提供物理和技术基础。这些设施确保数据能够在不同地区之间安全、稳定地流转,是整个体系运行的基石。

b) 服务层。建立在基础设施层之上,提供一系列集成的功能性服务。具体包括:可度量可信隐私计算服务,在保护数据隐私的前提下进行计算分析;基于可信执行环境(TEE)的可信数据跨境流通管理服务,保障数据在跨境过程中的安全性和合规性;数字身份服务,用于确认数据主体的身份,确保数据访问和使用的合法性。这些通用服务为数据的可信流通和共享提供了技术保障,也是此体系的核心创新点。

c) 应用层。聚焦于数据的实际应用场景,涵盖可信医疗、智慧城市、智慧课堂、智慧政务、智慧法院、工业互联网等。这些应用借助数据跨境流通与共享,全方位推动各领域的跨境交流与协同发展。本文第3章将详细解释此体系如何应用于医疗数据的可信跨境流通与共享。

d) 监管与安全层。承担着保障体系安全合规运行的重要职责。一方面,通过数据跨境安全计算与隐私保护技术,防止数据在跨境过程中被窃取、篡改;另一方面,数据跨境流通合规监测系统对数据跨境活动进行监督,确保其符合相关政策法规要求,避免出现违规风险。

3 数据跨境可信流通与共享实践

数据跨境流通与共享对于提升医疗服务质量和效率至关重要,某医疗体系在A市和B市积极开展数据跨境可信流通与共享实践,构建个人授权病历跨境

可控分享服务平台,提升个人医疗数据跨境的安全性。此平台具有个人授权病历流转、个人授权病例加密上传、个人授权病例加密展示等核心功能。通过采用授权机制,以及数据加密^[14]、数据脱敏^[15]和数据匿名化^[16]等技术,切实保障病人的隐私权益。同时,协同A市和B市的数据跨境流通合规性监测系统,严格满足数据保护法规与合规要求,从而实现合作医疗机构间个人授权病历的可信、可监测、高安全且高隐私保护的跨境流通分享。此外,借助协同数据跨境流通及共享监测链,有力确保数据在传输、计算和存储过程中的安全可靠。

如图2所示,个人病历流转系统涉及多方主体,包括A市医院、B市医院、可信跨境联合数据中心(涵盖A市与B市)以及就医者,各主体间形成紧密且有序的协作关系。具体流程如下。

步骤①,就医者提交申请病历流转的请求。

步骤②,完成个人病历隐私备案,此环节是保障患者隐私权益的基础。

步骤③,A市医院收到申请后,对授权范围内个人病历进行加密处理并上传至可信跨境联合数据中心。

步骤④,该中心依托基于TEE的可信数据服务系统,对加密病历开展病历分析、处理等操作,以满足B市医院的诊疗需求。

步骤⑤,经处理后的授权个人病历以加密形式在B市医院展示,实现跨境医疗场景下病历的有效传递。

为确保数据跨境流通的安全性与合规性,该系统引入两条关键监测服务。数据跨境流通与共享监测链以及数据跨境流通合规性监测服务(覆盖A市与B市),通过存证写入和存证读取的操作,对病历流转的全流程进行实时监测与管理。这一机制不仅保障了医疗数据在跨境传输过程中的安全,也符合相关法律法规要求,为跨境医疗服务的高效开展提供了坚实支撑。

4 数据跨境可信流通与共享体系优势

在全球化与数字化加速融合的当下,数据跨境流通与共享已成为数字经济发展的关键引擎。本文创新性地聚焦多个关键层面,涵盖监测机制、传输计算技术以及隐私计算服务机制等,旨在构建一个安全、可信且高效的跨境数据流通与共享体系。它具有如下优势。

a) 构建全链条可信溯源追踪、透明开放的数据跨

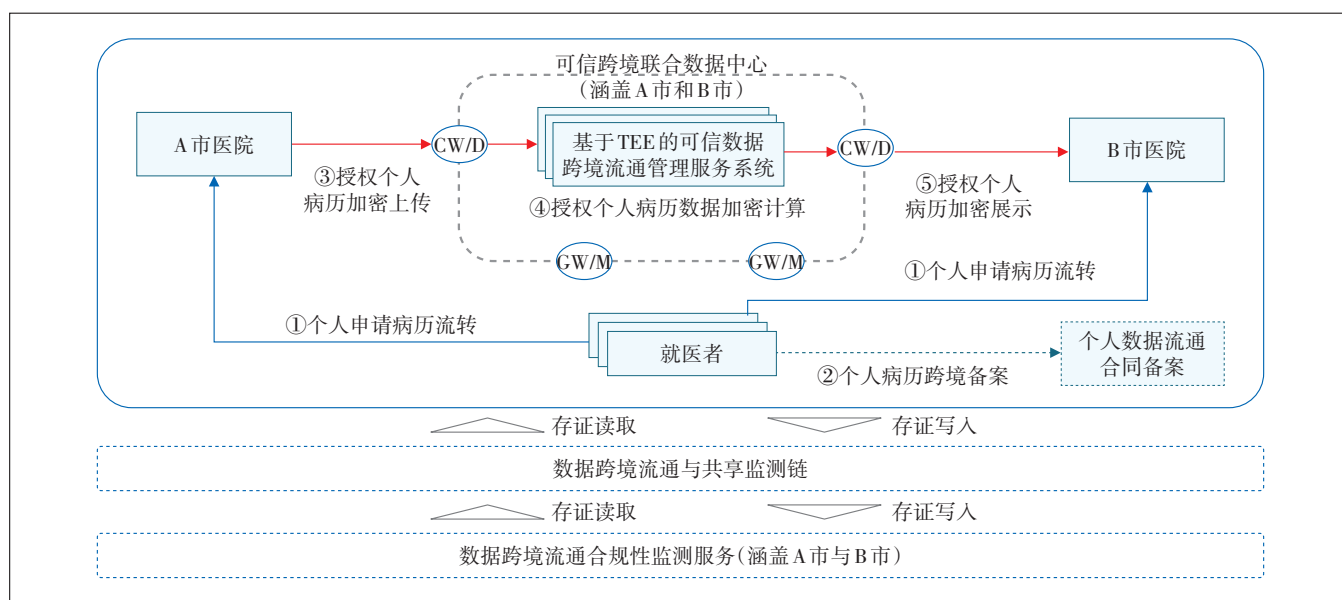


图2 数据跨境可信流通与共享实践

境流通监管机制和数据跨境流通合规性监测基础设施。构建全链条可信溯源追踪、透明开放的数据跨境流通监管机制,采用数据跨境流通合规性监测系统对跨境数据进行上链管理,以区块链不可篡改的特性保证数据流动全链条可信溯源追踪,在安全可信保障下,释放数据价值,开放数据应用。同时,在数据跨境流通合规性监测机制指导下,构建以数据跨境流通与共享监测链、可信跨境联合数据中心、可信服务撮合平台、区块链平台等为基础的数据跨境流通合规性监测基础设施。

b) 提出高安全、高隐私保护的数据跨境跨域可信传输与可信计算技术,实现端到端的个人病历跨境可信、可控、合规流转和共享。提出高安全、高隐私保护的数据跨境跨域可信传输与可信计算技术。通过在数据跨境跨域传输和计算过程中引入可信执行环境,敏感数据在可信执行环境中进行计算。本系统提供端到端的数据传输和计算加密保护机制,防止中间人攻击、数据泄露和恶意篡改的风险,确保数据传输过程的安全性和完整性,保护数据安全和数据隐私。基于TEE的可信数据跨境流通管理服务系统,能够实现硬件级安全的、隔离的、独立的可信执行环境,为敏感数据的可控跨境流通与共享提供高安全、高隐私保护和可监管的解决方案。

c) 可信可度量多方隐私计算服务机制帮助实现数据跨境服务场景下数据服务可运营、可管理、可评估。在数据跨境服务进程中,引入隐私计算^[17]、同态

加密^[18-19]等前沿技术手段,保证数据隐私安全。数据跨境服务通常涉及多个参与方,运用区块链技术完整记录各方的数据交互流程与计算操作,达成可信多方隐私计算,能够显著提升数据跨境服务场景下数据服务的可信度、安全性与可追溯性。与此同时,隐私计算服务机制对参与方所提交的有效数据、有效参数以及开展的有效计算等方面的贡献程度进行精准的可信度量。可信度量为数据服务的质量与效益提供切实有效的评估与监督,进而为后续数据跨境服务价值的可信分配奠定科学基础。

5 数据跨境可信流通与共享发展方向

5.1 加强国际合作与标准制定

在全球化的数字经济时代,数据跨境可信流通及共享体系的建设离不开国际合作与统一标准的制定。各国正在积极参与国际数据跨境流动规则的制定,共同应对数据跨境流动带来的挑战,推动建立公平、公正、合理的国际数据治理秩序。作为数字经济大国,我国拥有庞大的数据资源和活跃的数字市场,在国际数据治理中具有重要的影响力。加强国际合作与标准制定,将自身的数据保护理念、发展需求和治理经验融入到国际规则中,能够为我国数字经济企业的国际化发展创造有利的外部环境。

5.2 完善技术支撑与创新应用

鼓励加大对数据跨境可信流通关键技术的研发投入,推动技术创新和应用,提高数据流通的安全性

和效率。随着数字经济的快速发展,数据跨境流动的规模和频率不断增加,对技术的要求也越来越高。持续的技术研发和创新能够为数据跨境可信流通提供更加坚实的技术保障,促进数据的安全、高效流通。政府应充分发挥引导作用,通过制定科技政策、设立专项科研基金等方式,鼓励高校、科研机构和企业加大对区块链、加密技术、隐私计算等关键技术的研发投入。企业作为技术创新的主体,也应积极参与技术研发,加大研发投入,将技术创新与市场需求相结合,推动技术的产业化应用。

5.3 强化监管协同与风险防控

在当今数字化时代,数据跨境流动的规模和频率不断增加,涉及的领域和主体日益广泛,这对数据跨境流通的监管提出了更高的要求。传统的单一部门监管模式已难以适应新形势下的数据跨境流动监管需求,必须加强各部门之间的协同合作,形成监管合力,才能有效防范数据跨境流动中的风险,保障数据安全和隐私。各政府部门在数据跨境流通监管中承担着不同的职责,需要明确各自的定位和任务,加强协调与配合。

6 结论与展望

数据作为新型生产要素,是数字化、网络化、智能化的基础,它已快速融入生产、分配、流通、消费和社会服务管理等各个环节,深刻改变着生产方式、生活方式和社会治理方式。政府和企业也在积极探索推进跨境数据要素合法、合规、有序、可控、安全的流通共享机制,促进跨境数据价值释放。本文提出的数据跨境可信流通及共享服务体系,结合数据跨境流通合规性监测技术、可度量可信隐私计算服务技术、基于TEE的可信数据跨境流通技术,构建了高可信、高安全、高可靠的数据跨境可信流通及共享服务平台,实现数据跨境可信流动、可信共享、价值流动。未来,随着数据跨境可信流通及共享体系的不断发展和完善,数据跨境合作也将持续推动数字经济的蓬勃发展,促进新业态和新模式的兴起,为全球数字经济的高质量发展提供有力支撑。

参考文献:

- [1] 许皖秀,左晓栋.全球竞争格局下的中国特色数据跨境流动治理方案研究[J].中国工程科学,2025,27(1):111-121.
- [2] 葛平原,陈永强,郭伟豪,等.数据跨境流动规制综述[J].信息安

全研究,2025,11(2):164-172.

- [3] 新华社.中华人民共和国个人信息保护法[EB/OL]. [2024-08-26]. https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.
- [4] 新华社.中华人民共和国数据安全法[EB/OL]. [2024-08-26]. https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm.
- [5] 新华社.中华人民共和国网络安全法[EB/OL]. [2024-08-26]. https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.
- [6] 新华社.促进和规范数据跨境流动规定[EB/OL]. [2024-08-26]. https://www.gov.cn/gongbao/2024/issue_11366/202405/content_6954192.html.
- [7] 汪建.深化数据要素改革助推高质量发展[N].人民邮电,2025-03-14(1).
- [8] 李风华,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.
- [9] 中华人民共和国商务部.中国数字贸易发展报告[EB/OL]. [2024-08-26]. https://fms.mofcom.gov.cn/xxfb/art/2024/art_2af090f44fd44b16b4d281d55dd5a31c.html.
- [10] 张涵,于航,周继威,等.面向隐私计算的可信执行环境综述[J].计算机应用,2025,45(2):467-481.
- [11] SABT M,ACHEMLAL M,BOUABDALLAH A. Trusted execution environment: what it is, and what it is not[C]//2015 IEEE Trustcom/Big-DataSE/ISPA. Helsinki: IEEE, 2015: 57-64.
- [12] GOLDBREICH O. Secure multi-party computation[EB/OL]. [2024-08-26]. <https://www.wisdom.weizmann.ac.il/~oded/PSX/prot.pdf>.
- [13] ZHOU I, TOFIGH F, PICCARDI M, et al. Secure multi-party computation for machine learning: a survey[J]. IEEE Access, 2024, 12: 53881-53899.
- [14] 朱闻亚.数据加密技术在计算机网络安全中的应用价值研究[J].制造业自动化,2012,34(6):35-36.
- [15] 乔宏明,梁兔.运营商面向大数据应用的数据脱敏方法探讨[J].移动通信,2015(13):17-20,24.
- [16] 张涛.大数据时代个人信息匿名化的规制治理[J].华中科技大学学报(社会科学版),2019,33(2):76-85.
- [17] 李风华,李晖,贾焰,等.隐私计算研究范畴及发展趋势[J].通信学报,2016,37(4):1-11.
- [18] 李顺东,王道顺.基于同态加密的高效多方保密计算[J].电子学报,2013,41(4):798-803.
- [19] ACAR A, AKSU H, ULUAGAC A S, et al. A survey on homomorphic encryption schemes: theory and implementation[J]. ACM Computing Surveys(Csur), 2018, 51(4): 1-35.

作者简介:

穆晓君,毕业于澳大利亚墨尔本大学,工程师,硕士,主要研究方向为区块链、人工智能、数据要素等;范琨,高级工程师,硕士,主要从事网络规划优化、网络新技术实验、科技创新管理等工作;马瑞涛,毕业于北京邮电大学,高级工程师,硕士,主要研究方向为人工智能、算力网络等;赵灿,毕业于中国科学院大学,工程师,硕士,主要从事区块链技术、人工智能技术及相关应用研究工作;加雄伟,毕业于华中科技大学,教授级高级工程师,硕士,主要研究方向为区块链、人工智能等。