数据要素流通使用的安全风险分析及应对策略

刘业政[1,2]，宗兰芳[1]，金斗[1]，袁昆[1,2]
1. 合肥工业大学管理学院，安徽 合肥 230009；
2. 大数据流通与交易技术国家工程实验室，上海 201203

摘要
系统地分析了数据要素流通使用过程中存在的安全风险问题，在总结国内外数据交易制度与规范、理论与技术的基础上，构建了事前-事中-事后全链路数据要素流通使用安全风险应对策略，提出了管理与技术相互协同的数据要素流通使用安全可信体系建设方案，为实现“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”的可信可控数据交易提供借鉴，促进数据交易市场平稳持续发展。

关键词
数据要素流通；数据要素使用；安全风险分析；安全风险管理；安全风险技术

中图分类号：F49，TP309 文献标志码：A doi：10.11959/j.issn.2096-0271.2023021

Security risk analysis and countermeasures in the circulation and use of data factors

LIU Yezheng[1,2], ZONG Lanfang[1], JIN Dou[1], YUAN Kun[1,2]
1. School of Management, Hefei University of Technology, Hefei 230009, China
2. National Engineering Laboratory for Big Data Distribution and Exchange Technologies, Shanghai 200436, China

Abstract
The security risks existing in the process of circulation and use of data factors were analyzed systematically. On the basis of summarizing the statue of researches, practices and relevant national standards and norms of data circulation at home and abroad, a countermeasure before, during and after the whole process of circulation and use of data factors for the security risks was proposed, and amanagement and technology synergistic solution to construct a secure and trusted system for circulation and use of data factors was presented. It provided reference for the realizing trusted, controllable data trading that “data sources can be confirmed, scope of use can be defined, circulation process can be traced, and security risks can be prevented”, and promoted the stable and sustainable development of data trading market.

Key words
circulation of data factors, use of data factors, security risk analysis, security risk management, security risk technology

0 引言

数据作为数字经济新型生产要素，是数字化、网络化、智能化的基础[1]。数据要素流通使用有助于促进数据融合和资源整合，激活数据潜能，做强做优做大数字经济。然而，数据要素流通使用环境复杂，涉及多方主体、多个环节，同时数据产品具有极易复制、非排他性、难追溯等特征[2]，均使数据流通使用面临安全风险、隐私泄漏挑战等问题。这不仅威胁国家数据安全，也不利于企业和个人数字权益的保护，严重阻碍数据要素流通使用市场化配置。国家出台了一系列政策文件，统筹推进数据要素安全可信、集约高效的流通使用。2022年12月2日，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》明确指出，数据安全是数据要素流通交易的底线和红线，是开展数据流通交易的首要条件，要求统筹发展和安全，贯彻总体国家安全观，强化数据安全保障体系建设，将安全贯穿数据供给、流通、使用全过程[1]。同时，《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）等多部国家法律法规相继出台，对数据要素流通使用过程中的数据安全与隐私保护作出了相关规定。为了保障数据安全可信、集约高效的流通使用，识别数据要素流通使用全过程中的安全风险管理需求，构建有效的安全风险管理应对策略，成为学术界和产业界关注的热点问题。

目前数据要素流通使用的安全风险管理研究主要从管理制度建设和安全技术保障两方面独立展开：一方面通过法规、制度、标准的制定明确数据交易安全风险需求及保障要求，另一方面通过技术手段解决数据交易安全风险管控问题。在安全风险管理制度建设方面，国家先后出台《数据安全法》《个人信息保护法》等多部法律法规，各级地方政府也制定相关制度，例如《上海市数据交易场所管理实施办法（征求意见稿）》《天津市数据交易管理暂行办法》。另外，国家标准《信息安全技术–数据交易服务安全要求》[3]从数据交易参与方安全、交易对象安全和数据交易过程安全3个角度规范数据交易中的安全风险管理需求。学者重点关注数据分级分类、数据脱敏、数据存储、交易主体资质审核与交易流程安全审计等机制问题。在安全风险应对技术方面，围绕数据流通交易的访问权限控制、防篡改、可追溯等安全需求，目前学者主要探索区块链、联邦学习、数字水印、数据加密等技术在数据流通交易市场的应用。凡航等人[4]以去中心化、多方监督的技术思路，将多方安全计算与区块链智能合约结合，提出了一种数据流通使用安全可控的“计算合约”，实现“用途可控可计量”。Thapa C等人[5]提出区块链中可以用同态加密、零知识证明等技术对隐私数据进行加密以达到保护隐私数据的目的。

总体来看，数据要素流通使用安全风险的研究工作既包含数据流通全流程的管理机制设计，将数据交易安全风险管理从交易对象扩展到交易主体和交易流程，又包含支撑数据要素流通使用的安全技术与算法模型。但结合数据流通使用实践经验来看，当前国内数据交易服务机构存在应用场景多元不确定、技术架构单一不灵活、技术与场景不适配等问题，导致数据要素安全可信流通使用的安全风险需求内涵不清晰、应对策略不明确。另外，管理制度建设与安全技术研究相割裂，特别是数据要素合规可信流通交易中技术和管理作用的边界尚不清晰，技术与管理未形成合力。

本文总体结构框架如**图1**所示，系统分

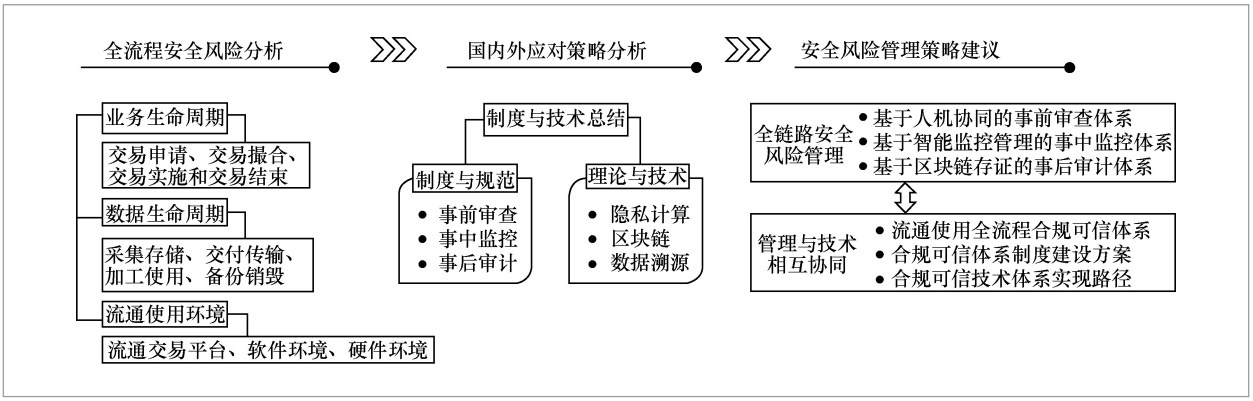

图1 本文总体结构框架

析了数据要素流通使用过程中存在的安全风险问题，在总结国内外数据交易安全风险管理制度与规范、理论与技术的基础上，提出了管理与技术相互协同的数据流通使用全链路安全风险管理策略，为保障数据要素市场公平高效与安全有序提供借鉴。

1 数据要素流通使用的安全风险分析

相比普通商品，数据要素具有固定成本高、边际成本低、产权不清、来源多样、结构多变等特征，在流通使用过程中涉及的范围更广泛、主体更多元、过程更复杂。因此，数据要素相比普通商品流通交易更加困难，数据要素价值释放过程中存在更多安全风险。基于国内外相关研究，从业务生命周期、数据生命周期、流通使用环境3个视角系统、全面地分析数据要素流通使用的安全风险，为构建数据要素流通使用安全可信体系奠定需求基础。

1.1 业务生命周期视角的安全风险分析

业务生命周期指数据要素流通使用的全过程，本文根据参考文献[3]将数据要素业务生命周期划分为交易申请、交易撮合、交易实施和交易结束4个阶段。

交易申请阶段的安全风险可归纳为交易主体资质安全风险、数据准入安全风险和产品质量风险。数据要素流通使用过程涉及供方、需方、交易服务机构等多方主体，主体资质直接关系到数据来源和流通使用的合法合规性[6]，肖建华等人[7]认为不同交易主体应有不同的资质审核要求。对于法人主体，交易平台需要审核其法人信息、营业执照、税务信息等；对于个人主体，交易平台需要审核其身份信息、交易目的、数据使用范围等，确保数据交易参与主体不存在法律、法规禁止或限制的任何情形[8]。数据是流通与使用的标的物，如果不合规的数据流入市场有可能严重影响个人隐私安全、商业安全和国家安全[8-10]，数据准入安全风险需重点关注数据产品是否包括禁止交易数据、未授权的个人数据、商业机密数据等。参与流通使用的数据要素除需满足准入的安全要求外，还要考虑数据质量风险[10-12]。若因审核不严而上线伪造或错误的数据，可能导致基于数据的分析结果无效，给需方造成巨大损失[12]。

交易撮合阶段主要存在供需匹配风险、交易公平风险和交易透明风险。在供需匹配上，数据市场中充斥着大量的数据，面对丰富的、不同规模、不同重点的数据供

给，如何找到最满足需求的数据非常困难，匹配在时间和质量上能否契合成为供需匹配的最大风险[13-14]。在交易公平性上，由于大多数的数据流通使用通过既充当交易的组织者又充当裁判的数据交易平台进行，如果交易平台与买方或卖方合谋，交易的公平性将难以保证[10,15]，此外，由于数据产品边际成本接近零，因此卖家具备了实施价格歧视的更大弹性[16-17]。在交易透明性上，供方往往面临着数据如何出售、哪些数据更有价值的挑战，需方无法获得数据的透明访问权限，无法了解原始数据的真实性[18-19]，供需双方在支付细节、上市、数据发现和存储等方面缺乏透明度保证[20]。

交易实施阶段的安全风险主要体现在权限分配、定价和交易清结算方面。在数据交易中，交易的不仅是数据本身，更是与之相关的各项权限，数据产品交割后所有参与者主张的排他性权限能否得到保障，关系到数据要素流通交易能否顺利进行[21]。数据作为一类特殊产品，相较于传统商品，在成本及消费单位、聚合性、消费方式、再利用和转售上存在巨大的差异[22]，导致在定价原则和方法上的不同考虑。版本控制成为设计和定价数据要素的常用机制[23]，不同版本的价格可以与不同客户群体的价值相关联。这对数据要素的定价提出了一系列新要求，其中包括公平性[24]、无套利[25]、真实性[26]、隐私保护[27]、计算效率[28]等。与此同时，数据要素定价还面临着与传统市场类似的操纵风险，即恶意打压或哄抬价格等。在交易清结算时，供需双方均可能面临交易违约风险，需方付款后收到数据的真实性、时效性和完整性是否与供方声称的一致，供方是否会因为需方发生拒不交付、抵赖等行为而无法得到约定的款项[29-31]。

交易结束阶段主要存在违规使用、转卖、再识别等安全风险。在交易结束阶段，安全风险主要来自需方。数据交付给需方后，可能出现不诚实的数据需方没有按照约定而是超范围地使用数据，侵犯供方的合法权益，甚至威胁多方安全，以及需方将其购买的数据产品进行二次流转、转卖等风险[22,32-33]。尽管在数据交易前，已对涉及用户身份信息的数据进行清洗、加密、匿名化等操作，但是随着公开资料的不断增多和互联网信息技术的不断发展，经过匿名化处理的数据有可能被再次识别[34]。

1.2 数据生命周期视角的安全风险分析

数据生命周期指数据从产生或获取到销毁的全过程。按照数据要素流通使用的相关操作流程，将数据生命周期划分为采集存储、交付传输、加工使用、备份销毁4个阶段。

采集存储的安全风险主要有采集安全风险、侵权风险和存储安全风险。数据采集的质量标准会影响整个链路的数据质量，原始数据的真实性、完整性、可靠性直接关系到后续的数据挖掘和分析工作[35]。如果采集的原始数据无法反映客观真实的情况，在此基础上的模型预测结果就会出现偏差，影响数据产品的可用性[36]。数据采集时还需要严格遵守用户知情同意和最小必要等相关法律原则，但在实际中不少智能设备厂商和App公司为了精准营销，得到更准确的用户画像，而过度收集用户个人信息，甚至“监听”用户的智能设备，使用户在网络空间变为透明人，严重侵犯了个人知情权、隐私权等[37]。数据一般存储在云端或分布式文件系统中，云端直接加密会带来巨大计算开销，提高密钥管理风险，而分布式存储中一个节点或多个节点遭受攻击，可能直接影响计算结果[34]。

交付传输的安全风险主要源自网络

硬件风险和外部攻击风险。数据在长距离网络传输过程中，面临网络不稳定导致的数据包丢失风险、网络带宽不足导致的传输时效风险，特别是面临大规模数据传输时网络硬件风险将更加突出[29,36,38]。数据在多路径中快速集群和转发，容易遭受病毒植入和攻击，大规模数据的汇集与传输会降低外部攻击成本，提高单次攻击的收益，从而引起黑客的攻击。用户与服务器间共享和生成密钥是数据传输中的重要风险点，社会工程已经成为外部攻击和窃取数据的一种重要手段[11,36,39]。

加工使用的安全风险突出表现在隐私泄露风险、安全攻击风险和数据滥用风险。从原始数据得到可流通交易的脱敏数据、模型化数据，必须借助大数据技术进行脱敏、分析、测试等加工操作[40]，但大数据技术在学习训练过程中面临两类隐私泄露风险，即非授权用户直接获取数据的隐私泄露风险和攻击者通过一定方式推断数据集中敏感信息的隐私泄露风险[41-42]。数据在加工使用时，容易遭受来自多方的攻击，如伪造数据或修改数据、攻击模型参数、恶意攻击服务器等[43-44]。由于数据要素的使用用途和用量难以监控和衡量，受利益驱动，在数据使用过程中可能出现超权限使用现象，甚至滋生出非法数据交易产业链，对个人隐私、国家安全造成严重危害[26,45-46]。

备份销毁的安全风险有备份审计安全风险和销毁安全风险。数据流通交易结束后需要生成相关交易日志并进行备份，但备份过程可能存在未经授权擅自更改或删除、异机备份等情况，无法为交易过程的查询、分析、审计和争议仲裁等提供可靠依据[47]。数据销毁安全是指在监管业务和服务涉及的系统及设备中清除数据时，通过建立针对数据的删除、销毁、净化机制，防止数据被恢复而采取的一系列防控措施。不及时、不彻底的销毁给内部人员和黑客提供可乘之机，可能产生数据泄露、个人信息被重新识别、数据二次转售等恶性影响[45]，特别是当数据存储在云端时，云服务商可能拒绝按照用户的删除指令销毁数据，而是恶意保留数据，从而使数据面临被泄露的风险[33]。

1.3 流通使用环境视角的安全风险分析

流通使用环境是指数据要素在流通使用的整个业务生命周期中所涉及的环境，具体而言，可分为流通交易平台、软件环境、硬件环境3个部分。数据要素流通使用过程中，从交易申请到交易结束的全过程都在流通交易平台中完成，检测、脱敏、挖掘等各个具体操作都依赖流通交易平台的大环境实现。同时，数据要素的汇集整理、建模分析等计算操作是依靠软件环境的相关算法实现的，而软件中算法的运行需要硬件基础设施提供算力资源才能完成。

流通交易平台的安全风险主要表现在访问控制能力、环境应变能力、运行能力和内容交换控制能力。访问控制能力是指有益用户都应能访问系统，而有害用户都应被拒绝，体现了平台的可扩展性和安全性[48]。环境应变能力是指平台对内外部变化应具有的灵活性和可靠性，一方面体现了平台可以在不同的环境下运行，另一方面体现了平台内部结构的相对稳定性[48]。运行能力是指平台有效实现数据要素流通利用的性能，有用性体现了平台的事务处理能力，易用性是指实现业务功能时占用最小系统资源的能力从而保证系统的运行性能，如访问速度快、操作方便等[48-49]。内容交换控制能力是指平台的连通性和隐私性，要求既能够保障正常内容的交换，又能保护隐私内容[48,50]。

软件环境的安全风险体现在系统软件

风险和应用软件风险。数据要素流通使用过程中需要各类系统软件和应用软件的支撑，这些软件存在各种各样的漏洞，甚至隐含着恶意代码，而检测此类软件中存在的恶意代码非常困难，给数据要素流通使用带来了巨大的潜在风险[35]。算法是数据要素流通应用中的一类特殊应用程序。随着各类深度学习模型、协同学习模型的应用，算法的计算逻辑、交互逻辑日益复杂和多样化，使得算法结果的可解释性难以使人满意，算法自身的安全性也难以控制[51]。此外很多算法的设计基于某种安全假设，如假设多个参与方之间均遵守指定规则及协议流程且不存在同谋等，这额外增加了一种安全假设风险，即当算法的安全假设不能被满足时，算法结果可能会难以预料[52]。

硬件环境安全风险指数据存储、运行等需要的关键信息基础设施安全风险，主要分为计算机物理安全和计算机网络安全。计算机物理安全风险包括计算机的异常损毁、被盗、非法使用等[53]；计算机网络安全风险包括对计算机网络设备、计算机网络系统、数据库等的攻击行为[35]。此外，供应和搭建硬件环境的厂商是否可信任、是否曾发生未经允许自动读取设备信息和产品质量不合格事件、设备是否存在故障、传输是否存在延迟、是否存在硬件木马等都是与硬件环境相关的安全风险[36]。如果硬件设备易遭受攻击、频频出现故障，将严重影响数据要素相关产业的健康发展。

2 国内外数据要素流通使用安全风险应对策略分析

数字经济逐渐进入高质量发展时期，数据要素市场对数据安全愈加重视。数据要素在入场前的合规审查、流通使用过程中的用途用量控制、流通使用后的争议解决等问题，对数据要素的安全治理和安全保护提出更高要求。因此，从“事前审查→事中监控→事后审计”的视角，对国内外现有数据要素安全风险应对策略的制度与政策、理论与技术两个方面进行梳理总结。目前国内外相关工作主要集中在制度与规范建设和理论与技术保障两个方面：一方面通过政策、制度、标准制定明确数据流通使用安全风险管理要求，另一方面通过理论与技术手段解决数据流通使用安全风险管控问题。

2.1 制度与规范建设视角的应对策略分析

近年来，我国数据要素市场发展态势十分迅猛，市场规模迅速扩大。《中国数据要素市场发展报告（2021—2022）》[54]表明，2021年我国数据要素市场规模达815亿元，预计“十四五”期间市场规模复合增速将超过25%。为了防范数据要素市场安全风险事件，国家出台一系列政策文件和规章制度统筹数据要素安全风险管理。2021年3月发布的《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》中明确提出，要培育规范的数据交易平台和市场主体，发展数据资产评估、登记结算、交易撮合、争议仲裁等市场运营体系。2021年11月，工业和信息化部发布的《“十四五”大数据产业发展规划》中不仅再次提到了有关数据要素市场建设的内容，还围绕加快培育数据要素市场、发挥大数据特性优势、夯实产业发展基础、构建稳定高效产业链、打造繁荣有序产业生态、筑牢数据安全保障防线6个方面提出了重点任务。2022年12月2日，《中国中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》强调完善数据全流程合规与监管规则体系，从全流程治理与创新

监管机制等方面入手，提出底线可守的数据要素安全治理制度。

事前审查是数据要素流通使用安全风险管控的前提，主要是指市场或市场管理者在交易前对数据交易市场的参与者和数据产品依照相关的法律法规进行审查，实现数据“上市有审核，采买有资质”。在国家层面，《数据安全法》明确规定了数据交易服务机构应审核交易双方的身份、交易数据内容、数据安全风险，并留存审核、交易记录。在地方层面，天津市出台了《天津市数据交易管理暂行办法》，其中第二章和第三章分别对数据交易主体和交易数据提出一系列明确要求。在行业内部，通过制订措施保证数据来源合规可信、数据质量安全可控，如贵阳大数据交易所发布的数据交易规则体系包含《数据交易合规性审查指南》《数据交易安全评估指南》《数据商准入及运行管理指南》等，以保障数据要素流通使用过程中交易主体、交易对象可信可控。但数据分级分类管理、数据确权授权等方面的法律制度有待进一步完善。如袁康等人[55]认为，《数据安全法》虽然明确提出国家将对数据实行分级分类保护，但仅做出了一般性规定，缺乏详细的分级分类体系和相关的实施细则，不同区域、不同部门不统一的程序标准容易导致数据准入与监管产生冲突。王建东等人[56]指出虽然在立法层面《数据安全法》和《个人信息保护法》解决了数据国家主权和人格权的问题，但是数据的财产权问题尚未在法律层面有明确定义，其中数据要素的可复制性、不确定性等独特特征是数据产权制度体系建立的难点，对参与交易的数据源的审查带来了操作上的困难。

事中监控是数据要素流通使用安全风险管控的基础，目的是对数据使用的用途、用量加以控制，约束交易主体行为，监督交易订单合规履行。《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》提出要建立合规高效的数据要素流通和交易制度，完善数据全流程合规和监管规则体系，建设规范的数据交易市场。各地方政府已陆续出台相关政策，促进数据要素安全可信流通。北京市发布《北京市数字经济促进条例》，要求完善数据分级分类、安全风险评估和安全保障措施，建立数据治理和合规运营制度，结合应用场景对匿名化、去标识化技术进行安全评估，开展数据安全方面的标准认证。上海市出台《上海市数据条例》，支持数据交易服务机构有序发展，要求数据交易服务机构建立规范透明、安全可控、可追溯的数据交易服务环境，制订交易服务流程、内部管理制度，并采取有效措施保护数据安全。贵阳大数据交易所发布的《数据交易合规性审查指南》也要求对交易合同内容、交付方式进行合规审查，同时还提供了《数据产品成本评估指引1.0》《数据产品交易价格评估指引1.0》《数据资产价值评估指引1.0》，为数据交易提供价值评估和价格依据。但在定价机制、数据交易立法上还存在明显的欠缺。目前不同数据交易平台的价格机制不透明，如某平台“省级业务平台数据服务”标价351.56万元/次，而“算力资源服务（云计算服务）”标价0.01元/次。因此，需要完善、统一数据流通定价规则[57]，规范数据消费单位和消费方式，防止定价过于随意。在立法方面，有关数据要素流通使用的规定散落在《中华人民共和国民法典》、《个人信息保护法》、《数据安全法》、《中华人民共和国网络安全法》（以下简称《网络安全法》）、《中华人民共和国反垄断法》、《中华人民共和国反不正当竞争法》中[58]，还没有一部关于数据要素流通交易的专门法律。相比之下，美国2014年就通过了《数据经纪商问责制和透明度法案》，2019年通过了《2019年数据经纪商法案》，要求数据经纪商明确数

据来源和类型，使用、保存和分发数据的方式，允许消费者访问和修改数据的范围，消费者退出数据销售或共享的方式等[59]。

事后审计是数据要素流通使用安全风险管控的关键，目的是解决交易后的争议问题。《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》中就数据要素市场的信用体系，提出需要配套建设交易仲裁机制，对数据交易主体的信用进行管理和评价，在数据要素市场形成诚信、互信、可信的交易生态。在企业内部，北京国际大数据交易所发布《北京数据交易服务指南》，推行数据交易保护义务衍生的原则，就交易中规定的使用范围和禁止用途进行保障，并设立数据要素产权知识保护体系，建立买卖双方争议解决机制。贵阳大数据交易所发布的《数据交易合规性审查指南》也包括交易后对场景应用、新增衍生数据产品进行合规审查。但在数据泄露通知制度、数据监管权限方面还需要持续完善。虽然《网络安全法》给出了数据泄露通知制度的相关要求，但是需要向用户告知的特定情形、告知用户的时限和方式、数据泄露的补救和惩戒措施、制度适用的主体范围等制度要素没有做出明确规定，缺乏一定的可操作性[60]。在我国，数据监管由网信部统筹，行业各部门分别监管，但实践中各数据监管部门、纠纷仲裁机构权责划分不明确、责任互相推诿的问题屡见不鲜[61]，应完善数据监管、纠纷仲裁相关制度，明确相关权力与职责，形成行业自律与政府监管双重安全保障。

2.2 理论与技术视角的应对策略分析

2.2.1 事前审查

在参与者资格审核方面，通常使用身份认证与控制技术保障交易主体的资质安全，确保数据供方和需方提供的身份信息真实可靠。传统的身份认证主要有基于标记识别的身份认证、基于生物特征的身份认证和基于密钥的身份认证等方式，但存在着密码泄露、伪造生物特征等风险[51]。近年来，区块链技术开始应用于身份认证领域，区块链具有去中心化、不可篡改的优势，可为主体资质安全提供技术支撑。例如，Dixit A等人[20]在物联网数据市场，利用区块链、分散标识符（decentralized identifier，DID）进行主体验证，其中每个主体持有一个独特的DID，通过在客户端验证DID，确保平台上的交易主体身份得到认定。在权限访问控制上，杜自然等人[50]提出了TID-MOP安全体系框架，从技术保障方面实施数据交易申请的安全管控，通过集中监控运维和访问权限管理重点关注交易主体合规资质的评估。

在审核数据要素的合法性、合规性、真实性上，去标识化技术、敏感数据探测技术、完整性技术为数据产品的安全准入提供了技术保障。去标识化技术通过对原始数据进行去标识化处理，降低数据集中的信息与信息主体的关联程度，主要包括数据统计技术、抑制技术、匿名化技术、假名化技术、泛化技术、随机化技术等[62]，不同的去标识化技术具有不同的特点，数据供方可以根据不同交易数据的特点、保密级别，选择合适的数据去标识化技术，从而确保数据产品可以进入数据要素市场。针对数据产品中包含敏感信息的问题，何文竹等人[63]提出了一种面向结构化数据集的敏感属性自动化识别与分级算法，利用信息熵定义了属性敏感度，通过对任意结构化数据集的敏感属性进行识别和敏感度量化，实现敏感属性的分级分类。刘金[64]通过分析敏感数据流转的生命周期，结合数据特征技术，建立了一套敏感数据识别体

系，从而加强对敏感数据的管控力度，降低敏感数据进入市场的风险。数据完整性技术一方面可以保障参与交易的数据质量，另一方面可以保障数据不被恶意篡改[65]，其中密码学技术和数据副本策略是两种传统的数据完整性技术。密码学技术利用消息认证码和哈希树等生成数据签名信息，防止数据被伪造；数据副本策略则是通过损失存储空间来保障数据完整性。实践中，一般综合利用两种方法确保数据质量安全。Nasonov D等人[66]针对企业数据要素的流通交易，提出了一种新颖的基于区块链的数据要素完整性验证技术。

2.2.2 事中监控

区块链技术和隐私计算技术体系是保障数据流通使用过程中计算环境安全、算法安全和数据隐私的有力手段[61]，也是监控交易撮合可信的可行技术。

例如，在监控交易撮合可信方面，Tan W T等人[67]提出了一种考虑信用管理的基于区块链的分布式交易机制，只有用户的信用评分不低于阈值时，才允许其参与分布式交易。Gupta P等人[68]提出了一个新的区块链框架TrailChain，该框架使用水印生成可信交易跟踪，通过建立检测市场内和市场间任何未经授权的数据转售的机制，实现对跨越多个分散市场的数据所有权的溯源跟踪。

在保障计算环境安全方面，可信执行环境（trusted execution environment，TEE）可将敏感计算与其他进程（包括操作系统、BIOS和hypervisor）隔离开来，通过芯片等硬件技术与上层软件协同对数据进行保护，同时保留与系统运行环境之间的算力共享，主要代表性产品有Intel的SGX、ARM的TrustZone等[4]。基于可信执行环境和区块链技术，Dai W Q等人[69]构建了一种新的数据交易生态系统，其中数据代理和需方都无法访问供方的原始数据，只能访问所需的分析结果，安全执行环境起着保护数据处理、源数据和分析结果的作用。

在算法安全及隐私保护方面，取得了丰富的研究成果。例如，Thapa C等人[5]提出区块链可以采用同态加密、零知识证明等技术对隐私数据进行加密以达到保护隐私数据的目的。Zheng K N等人[70]针对供应链金融信用体系中的征信数据隐私保护问题，提出了一种基于区块链的共享交易信息访问控制和管理模型，通过共识机制，实现了共享数据链的访问控制和可追溯性管理。Zhang J L等人[71]提出了一种基于移动边缘计算的联邦学习框架FedMEC，将模型划分技术和差分隐私技术集成在一起，防止局部模型参数的隐私泄露。郑婷一等人[72]提出了一个由监管体系、核心技术和模式创新三部分组成的保障平台数据与算法安全的技术生态体系架构。

2.2.3 事后审计

事后审计主要包括交易信用审计和交易安全审计。交易信用审计主要对是否存在侵权和违规行为进行认定、追责，并建立一种有效的信用评价机制。例如，Tan W T等人[67]利用区块链可溯源、抗抵赖等技术特性，提出参与者向智能合约支付一定数量的押金作为对潜在违约者的惩罚和对被违约者的补偿，在规定期限后，由智能合约根据合约履行情况执行交易结算，并根据参与者本次的表现自动刷新其信用评分。Tang H Y等人[73]利用边合约机制，建立了一种基于区块链技术的交易纠纷仲裁机制，不仅可以解决交易双方的合同争议问题，还能验证、追溯交易数据的完整性和价值。Dellarocas C[74]提出了一种信誉

机制设计方案，以鼓励供方尽可能多地降低机会主义，防止交易对需方没有价值的数据产品。

区块链技术的应用不仅能保障每笔交易的记录安全，还为交易安全审计提供了便利。例如，Fan K F等人[75]设计了一个基于区块链的云数据审计方案，提出了一个分散的审计框架消除对第三方审计者的依赖，在保障数据审计稳定性、安全性和可追溯性的同时，还能更好地协助用户验证云数据的完整性。

本文简要汇总了国内外数据要素流通交易使用安全风险及主要应对策略，具体见表1。

3 管理与技术相互协同的数据要素流通使用的安全风险应对策略

数据基础制度建设工作的不断推进和完善，对数据要素安全、可信、合规的流通使用提出了更高要求。应对数据流通使用安全风险，构建全流程合规可信体系，三分靠技术，七分靠管理[76]。管理以制度法规为基础，以流程、反馈、监督为保障，以人为核心，技术是高效落实制度法规的手段，是实现有效管理的支持系统或工具，技术的有效发挥依赖管理规章制度的完备。基于此，首先针对数据要素流通使用事前、事中、事后3个不同阶段，设计相应的安全风险应对策略，进而提出管理与技术相互协同的数据要素流通使用安全可信体系构建方案，通过规范数据供给、流通、应用全过程的一体化安全保障机制和各参与主体的安全责任，促进数据要素安全有序流通使用。

3.1 事前-事中-事后全链路数据要素流通使用安全风险应对策略

图2展示了本文提出的事前、事中、事后全链路数据要素流通使用安全风险应对策略框架，从数据要素流通使用全过程视角，针对事前、事中、事后3个不同阶段，分别制订事前审查体系、事中监控体系和事后审计体系，规范数据安全有序流通使用。

3.1.1 基于人机协同的事前审查体系

事前审查的目的是期望在交易申请阶段能够确保参与交易的主体可信、数据可信、合约可信等。交易主体审查旨在审查数据流通使用主体资质的安全风险和合规性，构建交易主体账户注册登记流程，设计面向账户登记信息真实性的机器审核与人工复核配套验证方案，保证交易平台、流通交易过程中的经手方以及机构或个人等市场主体信息可追溯，实现交易主体可信。交易数据和算法审查即检验采集存储的数据要素安全风险，包括数据完整性、真实性、可交易性，数据获取渠道的合法性，以及数据是否对个人信息进行去标识化处理，保障数据的可交易以及合法合

表1 数据要素流通交易使用安全风险及主要应对策略

应对策略	交易申请	交易撮合	交易实施	交易结束
政策、制度	交易主体资质审核、数据产品合规性审查	交易合同审核	交易环境安全风险评估、算法安全风险评估、交易服务管理制度	登记结算、争议仲裁
理论、技术	身份认证技术、数据去标识化技术、敏感数据探测技术、数据完整性技术	区块链智能合约、分布式交易机制	P2P网络技术、区块链、智能合约、安全多方计算、差分隐私、可信执行环境、联邦学习	分布式交易机制、云数据审计、边合同机制

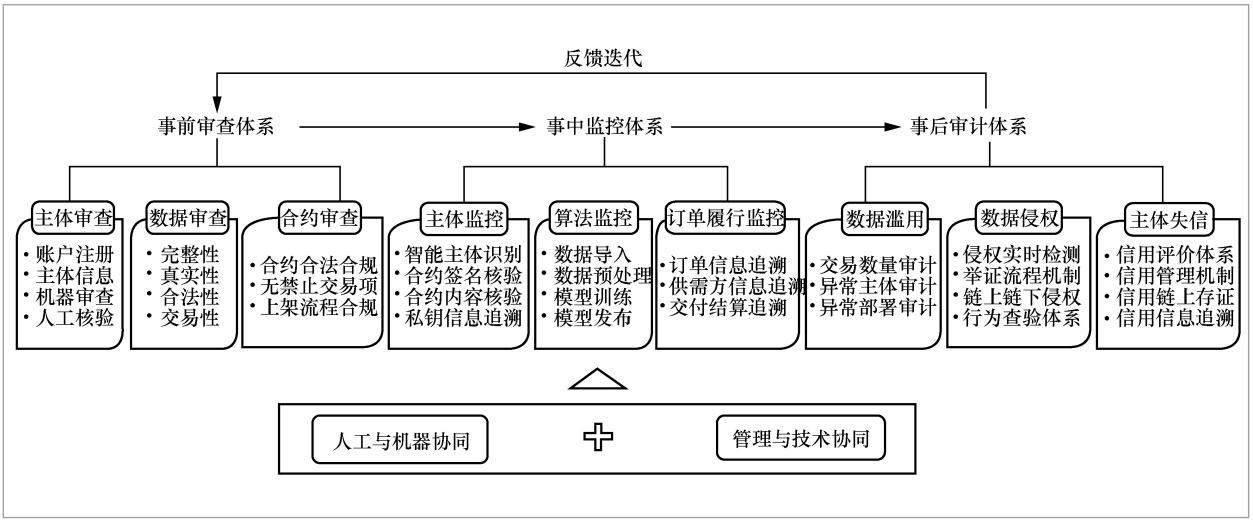

图 2 事前－事中－事后全链路数据要素流通使用安全风险应对策略框架

规。交易合约审查目的在于审查数据要素的使用场景、数据质量、数据价值、可定价要求和数据更新能力，需要面向不同应用场景制订禁止交易数据目录，建立数据产品上架交易标准规范，构建规范化的交易合约上架流程和合规审查流程，实现交易合约可信。

3.1.2 基于智能监控管理的事中监控体系

事中监控的目的是保障数据要素流通交易在磋商阶段和实施阶段安全可信，包括交易主体监控管理、合约磋商监控管理、算法行为监控管理和订单履行监控管理。交易主体监控管理聚焦交易主体识别管理，通过设计基于智能识别技术的交易主体身份与合约核验机制，确保合约双方的签名信息、合约内容的哈希值信息、私钥管理信息等合约信息的可追溯，实现数据使用者可控。合约磋商监控管理基于公平交易原则、供需匹配效率最大化原则，通过设计具有隐私保护的自动匹配技术和智能合约技术，保障交易双方的合约符合市场预期和国家相关政策法规。算法行为监控管理通过构建模型算法评估体系，设计算法行为监控方案，确保数据导入、数据预处理、模型训练、结果发布等流程规范可信、使用过程可追溯、资源消耗可度量，实现数据用途、用量与合约一致[67]，保障数据加工使用安全风险可控。订单履行监控管理建立数据传输接口备案制度，动态监控交易主体履约行为，包括感知监控数据流转、验证数据完整性和一致性、资金流审核，保证订单完全履行，实现对订单信息、供需方及交易平台信息、交付结算信息等履约过程产生的数据信息的可追溯。

3.1.3 基于区块链存证的事后审计体系

事后审计旨在防止数据在交易结束后可能面临的安全风险，主要集中在防止数据滥用、防止数据侵权和防止主体失信3个方面。在防止数据滥用方面，设计基于数据链上存储信息的交易审计机制[72]，以交易结束后链上存储的合约信息和交易信息为基础，构建智能交易审计核验指标测算

体系，设计链上资源滥用情况的监控和识别方案。制订数据销毁审查机制，杜绝数据产品倒卖风险，保证交易数量、异常交易用户、异常合约部署、数据销毁过程等审计信息可追溯。在防止数据侵权方面，制订数据交易侵权行为的举证流程机制，基于数据侵权行为链上链下线索搜寻，构建数据侵权的链上链下查验体系，保证对侵权行为信息来源的可追溯。在防止主体失信方面，建立数据交易结束后链上存储信息的信用管理机制，构建基于数据市场主体的信用评价指标体系，设计市场主体交易行为信用评价的链上存证方案，保证对数据供方、数据需方、交易平台等数据市场主体信用等级信息的可追溯。

3.2 管理与技术相互协同的数据要素流通使用安全可信体系

支持数据要素安全有序流通使用需要构建一个全流程合规可信体系，其建设过程是一个复杂的系统工程，实现路径有赖于管理制度与技术支撑的相互保障和综合作用。图3展示了本文提出的管理与技术相互协同的数据要素流通使用合规可信体系及实现路径。图3中，①表示交易申请阶段参与主体注册及对应的管理机制、技术支撑，②表示交易撮合阶段，③表示交易实施阶段，④表示交易结束阶段及各自对应的管理机制和技术支撑。

3.2.1 管理制度与技术支撑相互协同的数据要素流通使用全流程合规可信体系

管理制度与技术支撑相互协同的数据要素流通使用全流程合规可信体系包括合规可信制度体系、合规可信技术体系及管理制度与支撑技术协同方案。数据要素可信流通使用制度体系包括事前审查制度、事中监控制度、事后审计制度等。技术体系包括数据交易系统技术、区块链系统技术、跨隐私平台的联邦学习

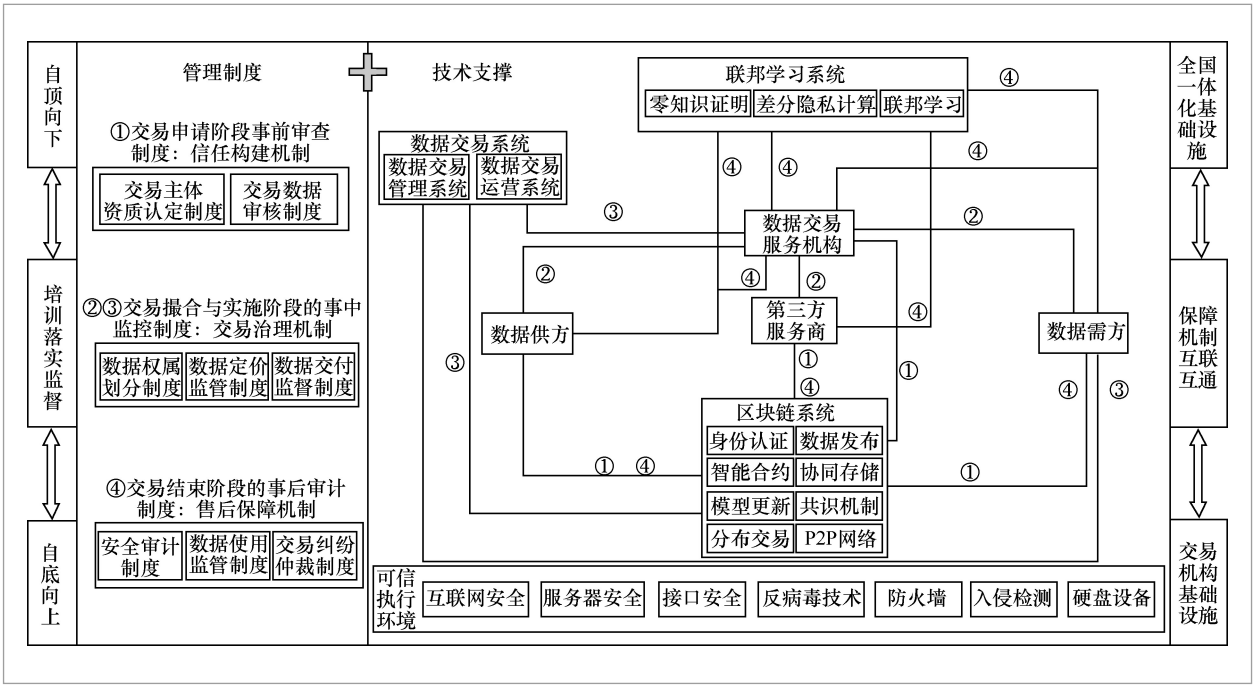

图 3 管理与技术相互协同的数据要素流通使用合规可信体系及实现路径

系统技术及可信执行环境技术等。图3中标记的①~④展示了数据要素流通使用不同阶段的管理制度和技术支撑的协同方案。

在数据流通使用的事前审查阶段，制订针对交易主体、交易数据和交易合约的审查制度，应对参与主体和数据采集安全风险。在技术上采用“机器审查+人工核验”的方式保证审查流程合规可信，即对于资质信息、数据质量、交易条目等标准信息，如企业法人信息、营业执照、数据规模与量级、禁止交易数据清单等，采用基于机器学习算法进行自动审查与人工抽验的方法。对于交易目的、数据来源等主观性较大的数据属性，采用人工核验方法。在数据流通使用的事中监控阶段，针对流通使用涉及的平台系统及软硬件、数据、云、网、端等环节制订安全保障制度，构建交易主体监控管理体系、算法行为监控管理体系和订单履行监控管理体系。在技术上设计基于智能算法支撑的保障体系，如基于智能识别技术的参与主体身份认证，保证参与主体可信；基于标识技术的数据权限管理方法，实现交付数据访问可控；面向数据用量异常检测的自动感知技术，监控数据合规加工使用；基于区块链技术的数据流通使用过程信息存证，保证数据流通使用全过程可追溯。在数据流通使用的事后审计阶段，制订数据滥用审计制度、数据侵权审计制度、主体失信审计制度，旨在确保数据流通使用全过程合规、争议可裁决、权益可保障。在技术上设计基于区块链存证信息的再审计体系，对数据流通使用全过程进行安全审计；基于数据标识和关联技术的数据追踪体系，对数据二次流通、转卖等侵权行为进行查验取证；融合交易主体信用评估制度体系与区块链可追溯技术，构建数据信用综合评估服务，推动数据流通市场公正可信发展。

3.2.2 数据要素流通使用全流程合规可信体系建设方案

数据要素流通使用全流程合规可信制度体系既包括指导全国一体化实施数据要素流通使用的宏观基础制度，又包括地方政府指导本地区实施数据要素流通使用的中观制度，同时还有数据要素交易机构实施数据要素流通使用的微观制度。在国家和地方层级的宏观制度、中观制度建设方案上，采用“自顶向下”的思路构建数据要素流通交易全流程合规可信基础制度体系。在地方和交易机构的微观制度、中观制度建设方案上，采用“自底向上”的思路，构建数据要素流通交易全流程合规可信运营制度体系。在安全可信制度的实施保障上，制订数据要素流通使用全流程合规可信制度体系培训政策、落实保障政策及制度执行的监管政策，保障数据要素流通交易全流程合规可信制度有效落地。

数据要素流通使用全流程合规可信技术体系既包括国家支撑数据要素流通交易的全国一体化基础设施，又包括各类数据交易机构支持数据要素可信可控可计量流通交易的基础设施。在全国一体化基础设施建设上，基于“东数西算”等国家基础实施建设战略，厘清全国一体化数据中心、算力中心、算法中心、安全中心等安全可信基础设施与流通环境的建设需求，提出相应的建设方案，为数据要素流通使用提供安全可信流通环境、共性公共服务、绿色高效的算力保障[77]在数据交易机构基础设施建设上，构建面向集合运算、联合建模及风险防控等功能的隐私协同计算平台，设计面向交易主体互信、数据登记互联、失信名单互通的跨链协同交易平台，为数据要素安全可信流通使用提供安全可信技术保障。在安全可信技术建设保障与互联互通上，建议

国家开展相关技术攻关、基础理论探索等重点工程项目与专项行为计划立项工作，以重点工程项目与专项行动计划为牵引，建立国家、地方政府与交易机构共同投资建设的协同机制以及各类基础设施互联互通机制，建立安全可信、集约高效的全国一体化数据要素流通使用环境。

4 总结与展望

近年来，数据要素市场培育与数据要素流通使用安全风险管理问题受到社会各界的广泛关注。从数据要素流通使用全过程出发，从业务生命周期、数据生命周期、流通使用环境3个视角系统、全面地分析数据要素流通使用全过程的安全风险，在梳理和总结国内外相关数据要素流通使用安全风险应对策略的制度与规范、理论与技术的基础上，给出了事前-事中-事后全链路数据要素流通使用安全风险应对策略，提出了管理与技术相互协同的数据要素流通使用安全可信体系及其实施路径，为实现“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”的可信可控数据流通交易提供借鉴，促进数据市场安全有序、平稳持续发展。

随着数字经济发展进入新时期，未来数据要素流通使用安全风险管理策略研究可从以下两方面继续开展。

- 面向不同应用场景下数据要素流通使用机制的安全风险管理策略。数据要素产品可分为原始数据、脱敏数据、模型化数据、AI数据服务等，来源或服务于政府、商业、金融、医疗、环境、个人等不同应用场景，分为数据资源持有权、数据加工使用权和数据产品经营权3种权属。数据要素流通使用则是数据权属在不同交易主体之间的有序流动。不同的数据产品、不同的应用场景、不同的权属交换对安全风险的要求并不相同。例如，数据资源持有权的转移涉及对数据支配权或控制权的转移，其交易全过程对安全风险的要求最严格，必须有健全的法律保护和技术支撑。未来应更加关注不同应用场景下数据要素流通使用机制的安全风险管理策略，有利于细化数据要素流通使用安全风险应对策略的适用性、可操作性、可扩展性，进一步提升和完善数据要素流通使用的安全治理制度。
- 面向安全可信、集约高效的全国数据要素统一市场的安全风险管理策略。当前数据要素流通使用的安全风险分析和管理主要针对数据交易平台和交易所，尚未上升到全国数据要素统一市场的安全风险管理。随着数据基础制度建设的不断推进和完善，为了充分释放数据要素潜能，构建全国一体化数据要素流通交易框架和保障技术体系越来越得到更多人的关注。其中，研究全国一体化安全可信的基础设施建设需求，研究基于私有链、联盟链、公有链相互协同的超链方案和跨隐私计算平台的安全可信技术方案是需要重点突破的方向。

参考文献:

[1] 中共中央 国务院. 关于构建数据基础制度更好发挥数据要素作用的意见[Z]. 2022.
The CPC Central Committee and the State Council. Opinions on the construction of data fundamental institutions for better promoting the data factor value[Z]. 2022.

[2] 刘金钊，汪寿阳. 数据要素市场化配置的困境与对策探究[J]. 中国科学院院刊，2022，37(10)：1435-1444.
LIU J Z，WANG S Y. Dilemmas and suggestions on market-based data allocation[J]. Bulletin of Chinese Academy of Sciences，2022，37(10)：1435-1444.

[3] 全国信息安全标准化技术委员会. 信息安全技术–数据交易服务安全要求: GB/T 37932–2019[S]. 北京: 中国标准出版社, 2019.
National Information Security Standardization Technical Committee. Information security technology–security requirements for data transaction service: GB/T 37932–2019[S]. Beijing: Standards Press of China, 2019.

[4] 凡航, 徐葳, 王倩雯, 等. 多方安全计算框架下的智能合约方法研究[J]. 信息安全研究, 2022, 8(10): 956–963.
FAN H, XU W, WANG Q W, et al. Research on smart contract method in the framework of secure multi–party computation[J]. Journal of Information Security Research, 2022, 8(10): 956–963.

[5] THAPA C, CAMTEPE S. Precision health data: requirements, challenges and existing techniques for data security and privacy[J]. Computers in Biology and Medicine, 2021, 129.

[6] HUTCHINGS A, HOLT T J. The online stolen data market: disruption and intervention approaches[J]. Global Crime, 2017, 18(1): 11–30.

[7] 肖建华, 柴芳墨. 论数据权利与交易规制[J]. 中国高校社会科学, 2019(1): 83–93, 157.
XIAO J H, CHAI F M. An analysis of data rights and transaction regulation[J]. Social Sciences in Chinese Higher Education Institutions, 2019(1): 83–93, 157.

[8] WANG R, TSAI W T, HE J, et al. A distributed digital asset–trading platform based on permissioned blockchains[C]// Proceedings of International Conference on Smart Blockchain. Cham: Springer, 2018: 55–65.

[9] SPIEKERMANN S, ACQUISTI A, BÖHME R, et al. The challenges of personal data markets and privacy[J]. Electronic Markets, 2015, 25(2): 161–167.

[10] KOUTROUMPIS P, LEIPONEN A, THOMAS L D W. Markets for data[J]. Industrial and Corporate Change, 2020, 29(3): 645–660.

[11] GUPTA N K, ROHIL M K. Big data security challenges and preventive solutions[J]. Data Management, Analytics and Innovation, 2019, 1042: 285–299.

[12] CHOI T M, LUO S Y. Data quality challenges for sustainable fashion supply chain operations in emerging markets: roles of blockchain, government sponsors and environment taxes[J]. Transportation Research Part E: Logistics and Transportation Review, 2019, 131: 139–152.

[13] MARTINS D M L, VOSSEN G, MALESZKA M. Supporting online data purchase by preference recommendation[C]// Proceedings of 2018 IEEE International Conference on Systems, Man, and Cybernetics. Piscataway: IEEE Press, 2019: 3703–3708.

[14] STAHL F, SCHOMM F, VOSSEN G. Data marketplaces: an emerging species[J]. Frontiers in Artificial Intelligence and Applications, 2014, 270, 145–158.

[15] COLMAN A, CHOWDHURY M J M, BARUWAL CHHETRI M. Towards a trusted marketplace for wearable data[C]//Proceedings of 2019 IEEE 5th International Conference on Collaboration and Internet Computing. Piscataway: IEEE Press, 2020: 314–321.

[16] 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.

[17] BERGEMANN D, BONATTI A, SMOLIN A. The design and price of information[J]. American Economic Review, 2018, 108(1): 1–48.

[18] FERNANDEZ R C, SUBRAMANIAM P,

FRANKLIN M J. Data market platforms: trading data assets to solve data problems[J]. Proceedings of the VLDB Endowment, 2020, 13(12): 1933-1947.

[19] OH H, PARK S, LEE G M, et al. Personal data trading scheme for data brokers in IoT data marketplaces[J]. IEEE Access, 2019, 7: 40120-40132.

[20] DIXIT A, SINGH A, RAHULAMATHAVAN Y, et al. FAST DATA: a fair, secure, and trusted decentralized IIoT data marketplace enabled by blockchain[J]. IEEE Internet of Things Journal, 2023, 10(4): 2934-2944.

[21] YU B B, ZHAO H J. Research on the construction of big data trading platform in China[C]//Proceedings of the 4th International Conference on Intelligent Information Technology. [S.l.:s.n.], 2019.

[22] GOLDFARB A, TUCKER C. Digital economics[J]. Journal of Economic Literature, 2019, 57(1): 3-43.

[23] SHAPIRO C, VARIAN H R. Versioning: the smart way to sell information[J]. Harvard Business Review, 1998, 76(6): 106-114.

[24] AGARWAL A, DAHLEH M, SARKAR T. A marketplace for data: an algorithmic solution[C]//Proceedings of 2019 ACM Conference on Economics and Computation. New York: ACM Press, 2019: 701-726.

[25] LI C, LI D Y, MIKLAU G, et al. A theory of pricing private data[J]. ACM Transactions on Database Systems, 2012, 39(4).

[26] CAI H, ZHU Y, LI J, et al. Double auction for a data trading market with preferences and conflicts of interest[J]. The Computer Journal, 2019, 62(10): 1490-1504.

[27] ACQUISTI A, TAYLOR C, WAGMAN L. The economics of privacy[J]. Journal of Economic Literature, 2016, 54(2): 442-492.

[28] BALAZINSKA M, HOWE B, SUCIU D. Data markets in the cloud: an opportunity for the database community[J]. Proceedings of the VLDB Endowment, 2011, 4(12): 1482-1485.

[29] ZHENG S L, PAN L X, HU D H, et al. A blockchain-based trading platform for big data[C]//Proceedings of 2020 IEEE Conference on Computer Communications Workshops. Piscataway: IEEE Press, 2020: 991-996.

[30] SU G X, YANG W Y, LUO Z D, et al. BDTF: a blockchain-based data trading framework with trusted execution environment[C]//Proceedings of 2020 16th International Conference on Mobility, Sensing and Networking. Piscataway: IEEE Press, 2021: 92-97.

[31] PEI J. A survey on data pricing: from economics to data science[J]. IEEE Transactions on Knowledge and Data Engineering, 2022, 34(10): 4586-4608.

[32] 何培育, 王潇睿. 我国大数据交易平台的现实困境及对策研究[J]. 现代情报, 2017, 37(8): 98-105, 153.
HE P Y, WANG X R. Predicament and countermeasure research about big data trading platform in China[J]. Journal of Modern Information, 2017, 37(8): 98-105, 153.

[33] DUCH-BROWN N, MARTENS B, MUELLER-LANGER F. The economics of ownership, access and trade in digital data[J]. SSRN Electronic Journal, 2017, 54.

[34] LV D L, ZHU S B, XU H Z, et al. A review of big data security and privacy protection technology[C]//Proceedings of 2018 IEEE 18th International Conference on Communication Technology. Piscataway: IEEE Press, 2019: 1082-1091.

[35] KOURID A, CHIKHI S. A comparative study of recent advances in big data for security and privacy[C]//Proceedings of Networking Communication and Data

Knowledge Engineering. Singapore: Springer, 2018: 249–259.

[36] GOEL P, PATEL R, GARG D, et al. A review on big data: privacy and security challenges[C]//Proceedings of 2021 3rd International Conference on Signal Processing and Communication. Piscataway: IEEE Press, 2021: 705–709.

[37] WIERINGA J, KANNAN P K, MA X, et al. Data analytics in a privacy-concerned world[J]. Journal of Business Research, 2021, 122: 915–925.

[38] MILOSLAVSKAYA N, MAKHMUDOVA A. Survey of big data information security[C]//Proceedings of 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops. Piscataway: IEEE Press, 2016: 133–138.

[39] ZHANG Q. Research on quantitative analysis of security of network risk based on big data[C]//Proceedings of 2019 International Conference on Robots & Intelligent System. Piscataway: IEEE Press, 2019: 159–162.

[40] YIN L H, FENG J Y, XUN H, et al. A privacy-preserving federated learning for multiparty data sharing in social IoTs[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(3): 2706–2718.

[41] HOLT T J, LAMPKE E. Exploring stolen data markets online: products and market forces[J]. Criminal Justice Studies, 2010, 23(1): 33–50.

[42] ZHOU H K, GU M D. Protection method of network data privacy security issues based on blockchain technology[C]//Proceedings of International Conference on Applications and Techniques in Cyber Security and Intelligence. Cham: Springer, 2021: 526–533.

[43] 顾育豪, 白跃彬. 联邦学习模型安全与隐私研究进展[J]. 软件学报, 2022: 已录用.
GU Y H, BAI Y B. Survey on security and privacy of federated learning models[J]. Journal of Software, 2022: accepted.

[44] SUN G, CONG Y, DONG J H, et al. Data poisoning attacks on federated machine learning[J]. IEEE Internet of Things Journal, 2022, 9(13): 11365–11375.

[45] 李树栋, 贾焰, 吴晓波, 等. 从全生命周期管理角度看大数据安全技术研究[J]. 大数据, 2017, 3(5): 3–19.
LI S D, JIA Y, WU X B, et al. Techniques of big data security from the perspective of life cycle management[J]. Big Data Research, 2017, 3(5): 3–19.

[46] MATTIOLI M. Disclosing big data[J]. Minnesota Law Review, 2014, 99(2): 535–583.

[47] WANG P. Research on security and privacy protection of database[J]. Applied Mechanics and Materials, 2014: 5873–5876.

[48] WHITWORTH B, FJERMESTAD J, MAHINDA E. The web of system performance[J]. Communications of the ACM, 2006, 49: 92–99.

[49] DAVIS F D. Perceived usefulness, perceived ease of use, and user acceptance of information technology[J]. MIS Quarterly, 1989, 13(3): 319–340.

[50] 杜自然, 窦悦, 易成岐, 等. TID-MOP: 面向数据交易所场景下的安全管控综合框架[J]. 数据分析与知识发现, 2022, 6(1): 13–21.
DU Z R, DOU Y, YI C Q, et al. TID-MOP: the comprehensive framework of security management and control in the scenario of data exchange[J]. Data Analysis and Knowledge Discovery, 2022, 6(1): 13–21.

[51] HAO M, LI H W, LUO X Z, et al. Efficient and privacy-enhanced federated learning for industrial artificial intelligence[J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6532–6542.

[52] 艾瑞咨询. 2022年中国隐私计算行业研究报告[R]. 2022.
iResearch. 2022 China privacy computing industry research report[R]. 2022.

[53] FUJIMOTO D, MIYACHI R, MATSUMOTO T. A threat of malicious hardware using on-chip voltmeter[C]//Proceedings of 2017 Asia-Pacific International Symposium on Electromagnetic Compatibility. Piscataway: IEEE Press, 2017: 96-98.

[54] 国家工业信息安全发展研究中心，北京大学光华管理学院，苏州工业园区管理委员会，等. 中国数据要素市场发展报告(2021—2022)[R]. 2022.
The National Industrial Information Security Development Research Center, Guanghua School of Management, Peking University, Suzhou Industrial Park Administrative Committee, et al. China data factor market development report (2021—2022)[R]. 2022.

[55] 袁康，鄢浩宇. 数据分类分级保护的逻辑厘定与制度构建：以重要数据识别和管控为中心[J]. 中国科技论坛，2022(7)：167-177.
YUAN K, YAN H Y. The logic elucidation and system construction of categorical and hierarchical data protection-centering on the recognition and protection of important data[J]. Forum on Science and Technology in China, 2022(7): 167-177.

[56] 王建冬，于施洋，黄倩倩. 数据要素基础理论与制度体系总体设计探究[J]. 电子政务，2022(2)：2-11.
WANG J D, YU S Y, HUANG Q Q. Research on the basic theory of data elements and the overall design of institutional system[J]. E-Government, 2022(2): 2-11.

[57] 黄倩倩，王建冬，陈东，等. 超大规模数据要素市场体系下数据价格生成机制研究[J]. 电子政务，2022(2)：21-30.
HUANG Q Q, WANG J D, CHEN D, et al. Research on data price generation mechanism under the ultra-large-scale data factor market system[J]. E-Government, 2022(2): 21-30.

[58] 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.

[59] 王丽颖，王花蕾. 美国数据经纪商监管制度对我国数据服务业发展的启示[J]. 信息安全与通信保密，2022，20(3)：10-18.
WANG L Y, WANG H L. Enlightenments of American data brokers supervision mechanism to China data service industry[J]. Information Security and Communications Privacy, 2022, 20(3): 10-18.

[60] 曾铮，王磊. 数据要素市场基础性制度：突出问题与构建思路[J]. 宏观经济研究，2021(3)：85-101.
ZENG Z, WANG L. The fundamental institutions of the data factor market: main obstacles and the ways to remove[J]. Macroeconomics, 2021(3): 85-101.

[61] 鄢浩宇. 数据要素市场培育的制度需求与法治保障[J]. 中国矿业大学学报(社会科学版)，2023：已录用.
YAN H Y. System construction and legal governance for the cultivation of the data element market[J]. Journal of China University of Mining & Technology (Social Sciences), 2023: accepted.

[62] 谢安明，金涛，周涛. 个人信息去标识化框架及标准化[J]. 大数据，2017，3(5)：20-29.
XIE A M, JIN T, ZHOU T. Personal information de-identification architecture and standardization[J]. Big Data Research, 2017, 3(5): 20-29.

[63] 何文竹，彭长根，王毛妮，等. 面向结构化数据集的敏感属性识别与分级算法[J]. 计算机应用研究，2020，37(10)：3077-3082.
HE W Z, PENG C G, WANG M N, et al. Sensitive attribute recognition and classification algorithm for structure dataset[J]. Application Research of

Computers, 2020, 37(10): 3077–3082.

[64] 刘金. 基于数据特征的敏感数据识别方法[J]. 信息通信, 2016, 29(2): 240–241.
LIU J. Sensitive data identification method based on data characteristics[J]. Information & Communications, 2016, 29(2): 240–241.

[65] 王利朋, 关志, 李青山, 等. 区块链数据安全服务综述[J]. 软件学报, 2023, 34(1): 1–32.
WANG L P, GUAN Z, LI Q S, et al. Survey on blockchain-based security services[J]. Journal of Software, 2023, 34(1): 1–32.

[66] NASONOV D, VISHERATIN A A, BOUKHANOVSKY A. Blockchain-based transaction integrity in distributed big data marketplace[C]//Proceedings of 2018 18th International Conference on Computational Science, New York: ACM Press, 2018: 569–577.

[67] TAN W T, LI L, ZHOU Z Q, et al. Blockchain-based distributed power transaction mechanism considering credit management[J]. Energy Reports, 2022, 8: 565–572.

[68] GUPTA P, DEDEOGLU V, KANHERE S S, et al. TrailChain: traceability of data ownership across blockchain-enabled multiple marketplaces[J]. Journal of Network and Computer Applications, 2022, 203.

[69] DAI W Q, DAI C K, CHOO K K R, et al. SDTE: a secure blockchain-based data trading ecosystem[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 725–737.

[70] ZHENG K N, ZHENG L J, GAUTHIER J, et al. Blockchain technology for enterprise credit information sharing in supply chain finance[J]. Journal of Innovation & Knowledge, 2022, 7(4).

[71] ZHANG J L, ZHAO Y C, WANG J Y, et al. FedMEC: improving efficiency of differentially private federated learning via mobile edge computing[J]. Mobile Networks and Applications, 2020, 25(6): 2421–2433.

[72] 郑婷一, 庞亮, 靳小龙. 平台经济中的数据与算法安全[J]. 大数据, 2022, 8(4): 56–66.
ZHENG T Y, PANG L, JIN X L. Data and algorithm security in platform economy[J]. Big Data Research, 2022, 8(4): 56–66.

[73] TANG H Y, QIAO Y N, YANG F, et al. dMOBAs: a data marketplace on blockchain with arbitration using side-contracts mechanism[J]. Computer Communications, 2022, 193: 10–22.

[74] DELLAROCAS C. Reputation mechanism design in online trading environments with pure moral hazard[J]. Information Systems Research, 2005, 16(2): 209–230.

[75] FAN K F, LI F, YU H Y, et al. A blockchain-based flexible data auditing scheme for the cloud service[J]. Chinese Journal of Electronics, 2021, 30(6): 1159–1166.

[76] 杜平. 加强基础制度体系建设加快构建全国一体化数据交易市场体系[J]. 数据, 2022(8): 49–51.
DU P. Strengthen the construction of basic system and accelerate the construction of national integrated data trading market system[J]. Data, 2022(8): 49–51.

[77] 国家发展改革委, 中央网信办, 工业和信息化部, 等. 关于印发《全国一体化大数据中心协同创新体系算力枢纽实施方案》的通知[Z]. 2021.
National Development and Reform Commission, Office of the Central Cyberspace Affairs Commission, Ministry of Industry and Information Technology, et al. Guiding opinions on accelerating the construction of a national integrated big data center collaborative innovation system[Z]. 2021.

作者简介

刘业政（1965- ），男，博士，合肥工业大学管理学院教授，主要研究方向为电子商务与网络空间管理、大数据开发及应用。

宗兰芳（1998- ），女，合肥工业大学管理学院硕士生，主要研究方向为个性化推荐系统、不公平定价算法等。

金斗（1997- ），女，合肥工业大学管理学院硕士生，主要研究方向为电子商务、车货匹配等。

袁昆（1991- ），男，博士，合肥工业大学管理学院讲师，主要研究方向为商务智能与大数据分析、社交网络分析和个性化推荐系统等。

收稿日期： 2023-02-08
通信作者： 袁昆，yuankun@hfut.edu.cn
基金项目： 国家自然科学基金资助项目（No.72241427，No.72271084）
Foundation Items: The National Natural Science Foundation of China (No.72241427, No.72271084)