数据要素市场化面临的数据安全问题及解决方案研究

Research on Data Security Issues and Solutions Faced by Marketization of Data Elements

赵勇波[1]，智海峰[2]（1. 中电科普天科技股份有限公司，广东 广州 510310；2. 广州杰赛通信规划设计院有限公司，广东 广州 510310）

Zhao Yongbo[1], Zhi Haifeng[2] (1. Cetc Potevio Science & Technology Co., Ltd., Guangzhou 510310, China; 2. Guangzhou GCI Plan & Design Institute of Communication Engineering Co., Ltd., Guangzhou 510310, China)

摘　要：

数据作为新型生产要素，是数字经济深化发展的核心引擎。国家高度重视数据要素市场培育，发布了一系列政策法规，成立了国家数据局等。通过分析数据要素市场化的背景，数据安全相关要求，数据要素交易中存在的问题，结合数据要素市场产业链构成，提出管理+技术+运营+监管审计的闭环解决方案，以促进数据合规高效流通使用，赋能实体经济发展，供数据要素市场各环节主体在进行数据安全防护体系建设时参考。

关键词：

数据要素；数据要素市场；数据安全；数据隐私；数据安全运营

doi：10.12045/j.issn.1007-3043.2024.12.011

文章编号：1007-3043（2024）12-0066-06

中图分类号：TP391

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Data, as a new type of production factor, is the core engine for the deepening development of the digital economy. Our country attaches great importance to cultivating the data element market, has issued a series of policies and regulations, and established the National Data Bureau. By analyzing the background of data element marketization, data security requirements, and problems in data element transactions, combined with the composition of the data element market industry chain, a closed-loop solution incorporating management, technology, operation, and regulatory audit is proposed to promote the efficient and compliant circulation and use of data, and empower the development of the real economy, which provides references for various entities in the data element market when constructing a data security protection system.

Keywords：

Data elements; Data element market; Data security; Data privacy; Data security operations

引用格式：赵勇波，智海峰. 数据要素市场化中面临的数据安全问题及解决方案研究[J]. 邮电设计技术，2024（12）：66-71.

0 引言

随着“云大物移智”等新一代信息技术的快速发展，数字经济成为驱动世界各国经济发展的关键力量。数据作为数字经济深化发展的核心引擎，对提高生产效率的乘数作用不断凸显，成为最具时代特征的生产要素。切实用好数据要素，将为经济社会数字化发展带来强劲动力[1]。

自2019年党的十九届四中全会首次将数据增列为生产要素以来，中央已发布多项政策文件，旨在培育数据要素市场，以数据安全为前提，完善数据要素产权配置、完善数字治理、细化市场领域，由浅入深地建立健全数据要素市场的基础制度[2]。《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“原始数据不出域、数据可用不可见”的要求，推动数据流通交易[3]。国内各级政府部门也在进行数据要素市场化探索。其中，浙江省发布了全国首个数据运营管理办法，即《浙江省公共数据授权运营管理办法（试行）》[4]，杭州市政府也发布了《杭州市公共数据授权运营实施方案（试行）》[5]等。

2023年8月21日，财政部印发《企业数据资源相关会计处理暂行规定》，该规定自2024年1月1日起施

收稿日期：2024-11-19

行[6]。这一举措标志着国内首个关于企业数据要素会计处理规则出台，数据资源入表。将数据作为企业资产入表，此举推动了数据要素市场化建设的进程。

综上所述，近年来，我国各级政府都在大力发展数据要素市场，然而，数据安全问题已成为制约数据要素市场化的重要因素。只有统筹好发展和安全的关系，才能更好发挥数据要素的作用。

1 国内外数据安全发展情况

世界各国通过加强网络安全战略指导，来提升数字经济安全保障能力。中国发布的《网络安全法》，从网络安全支持与促进、网络运行安全、网络信息安全、监测预警与紧急处置等角度，明确了网络安全战略和治理目标，旨在促进经济社会信息化健康发展。美国发布《改善国家网络安全行政令》，通过保护联邦网络、改善美国政府与私营部门间在网络问题上的信息共享以及制定应对突发事件的响应机制，来提高国家网络安全防御能力。俄罗斯发布新版《国家安全战略》，首次加入信息安全相关章节。英国发布了《2022年国家网络空间战略》和《安全、防务、发展和外交政策综合评估报告》，将网络安全作为战略重点。日本发布了《未来三年网络安全战略纲要》，以强化网络空间安全的战略指导[7]。

网络安全工作，三分靠技术，七分靠管理。目前，国内数据要素市场化数据安全风险研究工作主要从管理制度建设和安全技术保障2个方面展开。

1.1 数据安全管理制度建设

在安全风险管理制度建设方面，国家先后出台了《数据安全法》《个人信息保护法》《数据出境安全评估办法》等多部法律法规，各级地方政府也制定了相关制度。其中，《数据安全法》作为我国数据安全方面的基础性法律，提出“维护数据安全应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力”“国家建立数据分类分级保护制度”“对数据实行分类分级保护”等要求。《数据安全法》《个人信息保护法》《数据出境安全评估办法》分别从国家重要数据保护、个人隐私和权益保护、数据主权维护角度给出了行为指引。在标准制定方面，国家发布了《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《信息安全技术 数据交易服务安全要求》（GB/T 37932-2019）、《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）等标准规范。全国信息安全标准化技术委员会秘书处发布了《网络安全标准实践指南—网络数据分类分级指引》，该指引给出了网络数据分类分级的原则、框架和方法，以指导数据处理者开展数据分类分级工作。

1.2 数据安全技术保障建设

国家标准《信息安全技术 数据交易服务安全要求》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个维度提出数据交易服务的安全要求。针对数据流通交易的访问权限控制、防篡改、可追溯、隐私安全等安全需求，目前学者们主要探索区块链、隐私计算、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的安全可控的“计算合约”，实现“用途可控可计量”。Thapa C等人提出在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[8]。

2 数据要素市场化中的数据安全问题

数据要素市场化过程主要包括供给、流通和应用三大环节。从数据要素的产生到发挥价值，又涉及众多细分环节。数据要素供给环节一般包含数据采集、整理（数据标注、数据清洗、脱敏脱密、标准化）、聚合（数据传输、存储、集合汇聚等）以及分析几个阶段。数据要素流通环节一般包括确权登记、定价交易、交付清算步骤。数据要素应用环节则聚焦于数据价值的挖掘，数据服务的丰富。在数据要素市场化过程中，所面临的数据安全问题主要有以下6个方面。

a）数据泄露。政务、企业或者个人的数据，如果涉及国家安全、公共利益和个人隐私等敏感信息，一旦泄露，可能会造成严重影响。例如政府内部人员可能因为贪污或其他原因泄露政务数据；黑客攻击可能导致重要数据的泄露；个人隐私数据被暗网售卖等。

b）数据滥用：部分企业和个人可能利用数据进行非法活动，如诈骗、侵犯隐私等。此外，一些企业可能会通过非法手段获取数据，用于不正当竞争或谋取不正当利益。

c）数据篡改。恶意攻击者可能对数据进行篡改，从而影响政府或者企业决策和公众利益。例如，攻击者可以通过篡改交通数据来制造交通拥堵，从而影响政府的决策。

d）数据误用。由于缺乏专业训练、粗心大意，数据运维人员错误使用了某个数据，造成不良结果。

e）数据非法跨境流动。企业或者个人未经国家相关部门批准将可能影响国家安全、经济发展、公共利益的数据擅自传输至国外。

f）法律法规滞后。现有的法律法规难以适应数据要素市场化带来的新型安全问题。具体而言，现有的法律法规对于数据的收集、存储、使用等方面的规定较为模糊，导致在实际执行过程中存在较大的法律风险。例如，目前法律对数据价值和产权没有明确分类和清晰界定，使得数据收集者的动机可能被隐藏。

3 解决方案建议

数据安全建设不仅是技术层面的事情，同时需要管理保障、运营保障、监管与审计保障共同发力，才能确保数据合规高效流通使用。如图1所示，应从数据安全管理、数据安全防护、数据安全运营、数据安全监管与审计4个方面研究数据安全解决方案。

3.1 数据安全管理

3.1.1 数据安全管理组织

数据安全管理需要强有力的组织机构保障。数据安全组织取决于数据要素市场产业链上不同主体的规模。例如，大型企业通常设有向首席信息官（CIO）或首席执行官（CEO）报告的首席信息安全官（CISO）或者首席数据官（CDO）。在缺失专职信息安全人员的组织中，数据安全的责任将落在数据管理者身上。在任何情形下，数据管理者都需要参与数据安全工作。

自2021年以来，我国部分城市也在试点并推广首席数据官制度。其中，广东省印发了《广东省首席数据官制度试点工作方案》等一系列文件，在全省范围内率先开展试点工作。在2023年服贸会成果发布现场，普华永道发布了《2023中国首席数据官调研》报告。该报告显示，当前中国企业首席数据官或类似管理岗的渗透率仅为1.3%，这一比例远低于全球平均水平（27%）[9]。中国数据安全管理组织保障亟需加强。

3.1.2 数据安全管理制度

数据安全管理需要切实可行的制度约束。数据要素市场各环节主体应基于自己的业务和法规要求来制定数据安全制度，且数据制度必须是审计过的。所有数据安全制度遵从行动必须协调一致的原则，以降低成本、避免工作指令混乱和不必要的本位之争。

管理与企业/政府安全相关的行为需要不同级别的制度，具体包括：

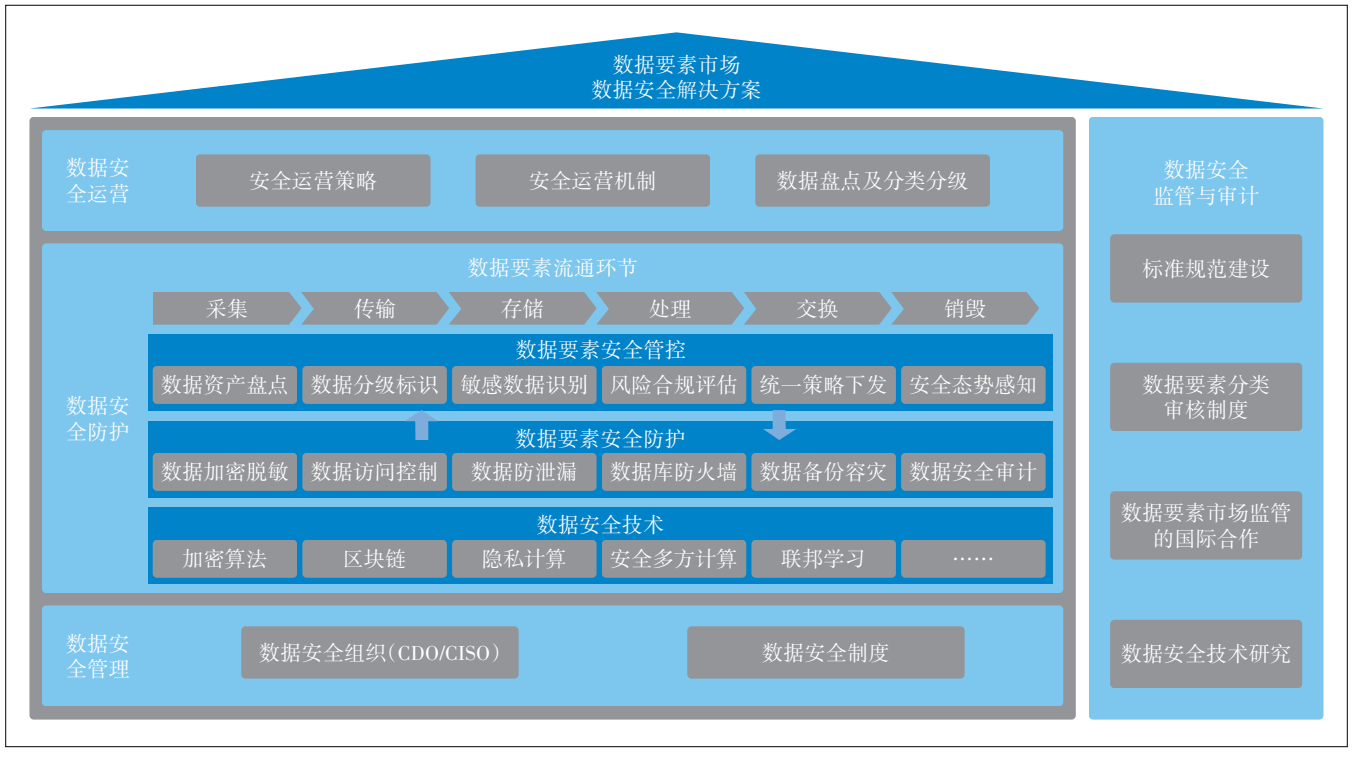

图1 数据安全解决方案框架

a）企业/政府安全制度。包括员工访问设施和其他资产的全局策略、电子邮件标准和策略、基于职位或职务的安全访问级别以及安全漏洞报告策略。

b）IT安全制度。包括目录结构标准、密码策略和身份管理框架。

c）数据安全制度。包括单个应用程序、数据库角色、用户组和信息敏感性的类别。

各主体应定期重新评估数据安全制度、过程和活动，力求在所有利益相关方的数据安全要求之间达成尽可能的平衡[10]。

3.2 数据安全防护

3.2.1 安全技术框架

数据要素产业链包括上游、中游和下游[11]。上游是指数据提供方，其提供公共数据、业务信息、个人信息的数据。中游主要包括数据交易所、数据服务商。下游是指数据需求方，包括政府、金融、教育、医疗等行业客户。

在数据供方、数据交易服务机构、数据需方传递数据时，需要采用多种安全防护手段保护数据的安全和隐私。数据要素交易安全技术框架如图2所示。

3.2.2 数据安全技术

通过应用访问控制、国密算法、可信计算、区块链、隐私计算、智能合约、联邦学习、安全多方计算等多种数据安全与隐私保护技术，企业和政府部门数据的安全性得到提高。

a）采用基于角色的访问控制（RBAC）策略对数据的访问进行权限分配和管理。建议企业和政府部门能够定义安全用户和角色。数据访问控制可根据需要在单个用户级或组织级中进行管理。小型组织可使用单个级别管理数据访问。对于大型组织，建议采用基于角色的访问控制，通过为角色组授予权限，从而为组中每个成员授予权限。角色组使得安全管理员能够按角色定义权限，并通过在适当角色组中注册用户实现权限授予。有些组织会将用户注册到多个组中，这导致用户信息（如姓名、职务和员工ID）被冗余存储在多个位置，多个版本的数据孤岛之间经常发生冲突。为避免数据完整性问题，需要对用户身份数据和角色组成员身份集中管理。

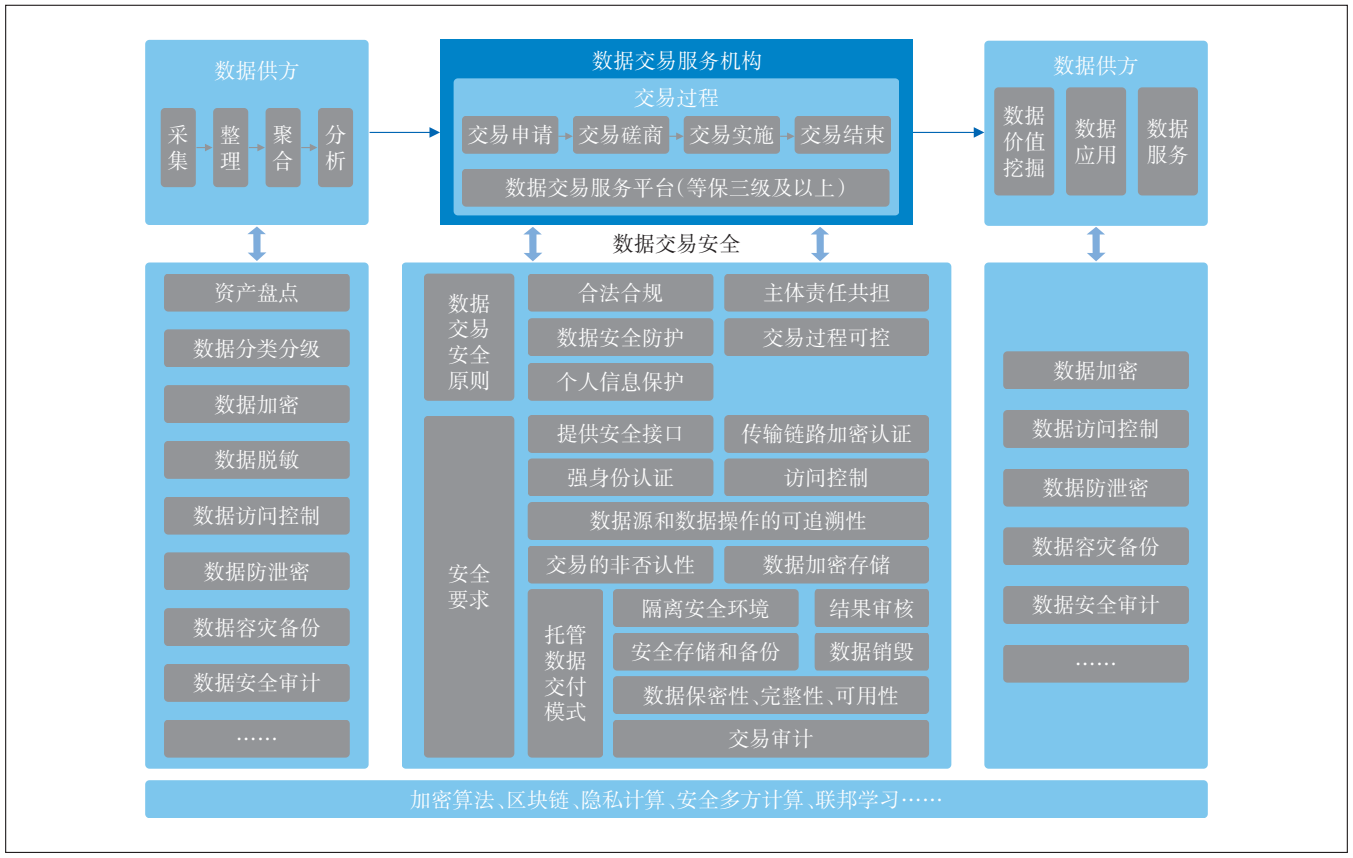

图2　数据要素交易安全技术框架

根据数据机密性、法规要求和用户功能需求，来授权各个角色和用户对数据的访问权限。例如，公共用户角色可以访问公开级别中列出的所有数据，不受任何法规约束。营销角色可以访问某些用于开展营销活动的数据，但不能访问任何受控数据或客户机密数据。

b）根据《信息安全技术 信息系统密码应用基本要求》，对数据访问、存储、传输、计算等采用国密加密算法进行加密，为身份鉴别信息、访问控制信息、相关数据、日志等提供机密性和完整性保护，为数据交易过程提供不可否任性保护等。

c）根据《信息安全技术 网络安全等级保护基本要求》，建设满足安全通用要求和大数据应用场景安全要求的数据防护体系，保障数据的完整性、保密性和可用性。

d）通过运用区块链和隐私计算等前沿技术，提升数据安全与隐私保护水平。应用区块链技术确保计算过程和数据可信；采用隐私计算实现数据可用不可见；应用联邦学习或者安全多方计算可以在不共享或者泄露数据的情况下，对多个数据源进行联合训练或者计算，保护商业机密、数据隐私和其他合规要求。另外，联邦学习、安全多方计算、区块链、可信计算等技术深入融合，并通过使用硬件加速技术，可大幅度提升数据的安全计算效率和防护水平[12]。

3.3 数据安全运营

3.3.1 数据安全运营策略

良好的数据安全运营能让数据要素市场行稳致远。参照计划-执行-检查-处理（Plan-Do-Check-Act，PDCA）模型，强化数据安全运营体系在数据安全防护的核心作用，有效上承管理制度体系，下接技术体系，落实数据流动性带来的持续、动态、闭环管理。

首先，制定数据安全规划（P），通过对组织应遵循的法律法规和行业标准进行解读，结合业务情况，输出并持续更新数据资产分类分级知识库和数据安全合规库，并进行数据资产梳理及分类分级，摸清数据资产家底，评估风险暴露面缺陷，再依照合规性要求，针对风险点设定动态分级防护策略；其次，落实全生命周期安全防护（D），依据规划制定的安全策略，面向不同级别的敏感数据对象，构建覆盖数据全生命周期节点的按需、动态防御技术能力体系；再次，开展风险监测与防护效果评估（C），实时监测数据安全运行风险，对安全事件进行响应处置，并对安全防护效果进行合规性综合评价；最后，根据风险监测和防护效果评估结果，结合业务变革，进行持续改善、优化（A），迭代驱动下一个安全规划（P）。数据安全运营策略如图3所示。

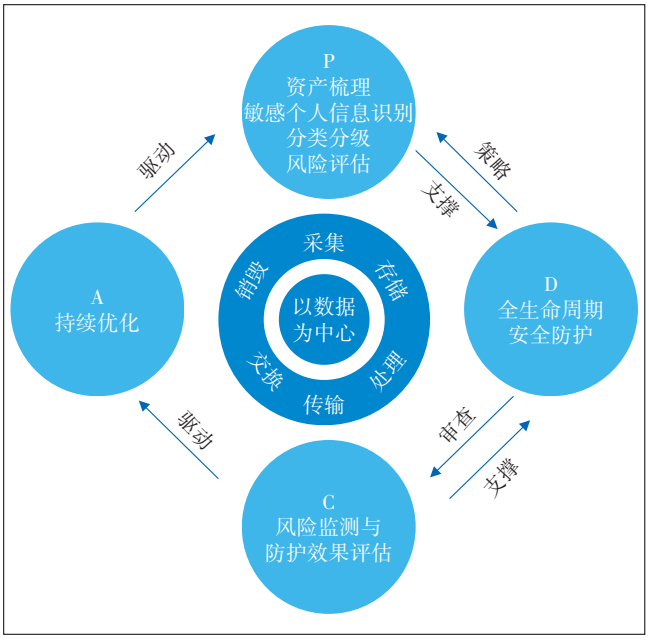

图3 数据安全运营策略

3.3.2 数据安全运营机制

成立安全运营团队，通过安全运营中心（SOC）、安全信息和事件管理系统（SIEM）构建数据安全隐患发现及处置机制、数据安全风险评估机制、数据安全突发事件应急响应机制、数据安全监控与审计机制，形成规范化、流程化、智能化运营的长效安全运营体系。

a）构建数据安全隐患发现及处置机制。通过专用工具实时监测网络运行状态，及时对数据安全隐患进行预警，并快速处置。

b）构建数据安全突发事件应急响应机制。制定数据安全专项应急预案，明确数据安全事件的应急处置流程，使得在发生安全事件时，安全事件能及时得到处置，降低其造成的损失。

c）构建数据安全风险评估机制。通过专业的风险评估服务，定期对数据采集、传输、存储、处理、交换和销毁等各个阶段进行威胁识别和风险评估，有效发现各阶段面临的数据安全风险。

d）构建数据安全监控与审计机制。在数据安全整体策略中规范数据安全监控审计策略，该机制覆盖数据生命周期各阶段的监控和审计，以实现对数据安

全风险的防控。

3.4 数据安全监管与审计

良好的数据要素市场安全审查策略能够有效提升数据要素市场的安全防护水平，切实筑牢数据要素市场安全屏障。企业和政府部门需构建一个可控、可查、可见的统一的内部数据安全闭环监管体系，从数据产生，到场景化使用，进行流向监控和精准分析，从而实现有效监管；通过对数据安全风险及业务数据场景的持续运营，梳理资产、数据、用户、权限等要素的要求，指导安全技术、管理、运营能力的体系化建设与协作。具体包括以下几个方面。

a）制定标准规范。制定数据资源产权、交易流通、跨境传输和安全保护等标准规范，推动平台经济、共享经济标准化建设，支撑数字经济发展[13]。

b）完善数据要素分类审核制度。建立重要数据脱敏机制，推动数据要素安全审查和评估制度落地，深化数据要素安全管理认证制度等[14]。

c）积极开展数据要素市场监管的国际合作。建议建立数据跨境的合法性审查机制。

d）通过支持数据安全技术研究和相关产业发展，鼓励数据安全与隐私保护技术的研发和应用推广。在数据要素市场入口处加强风险监测，采用静态和动态相结合的可信认证模式，消除安全隐患；通过可验证计算、动态加密等技术手段，并结合交易过程溯源技术，对数据要素市场交易实施全过程监管[15-16]。

4 结论

数据要素市场化是大势所趋，但随之而来的数据安全问题也不容忽视。数据安全工作需要企业与政府部门的管理人员和技术人员共同努力，在体系机制的保障下，加强数据安全防护，从而为数据要素市场化奠定安全的环境基础，最大化地发挥数据要素在促进数字经济发展中的核心引擎作用。在未来的发展中，应不断完善法律法规，加快数据安全技术的研究应用，建立有效的监管机制，提高公众安全意识，以确保数据要素市场化的健康、有序发展。

参考文献：

[1] 国务院. 国务院关于印发“十四五”数字经济发展规划的通知：国发〔2021〕29 号[EB/OL]. (2021-12-12)[2024-09-12]. https://www.gov.cn/gongbao/content/2022/content_5671108.htm.

[2] 中国信息通信研究院. 数据要素白皮书(2022年)[R/OL]. [2024-09-12]. http://www.caict.ac.cn/kxyj/qwfb/bps/202301/P020230107392254519512.pdf.

[3] 中共中央，国务院. 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[EB/OL]. (2022-12-02)[2024-09-12]. https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm.

[4] 浙江省人民政府办公厅. 浙江省人民政府办公厅关于印发浙江省公共数据授权运营管理办法(试行)的通知：浙政办发〔2023〕44号[EB/OL]. (2023-08-01)[2024-09-12]. https://www.zj.gov.cn/art/2023/8/22/art_1229017139_2487072.html.

[5] 杭州市人民政府办公厅. 杭州市人民政府办公厅关于印发杭州市公共数据授权运营实施方案(试行)的通知：杭政办函〔2023〕63号[EB/OL]. (2023-09-01)[2024-09-12]. https://www.hangzhou.gov.cn/art/2023/9/8/art_1229063382_1837127.html.

[6] 财政部. 关于印发《企业数据资源相关会计处理暂行规定》的通知：财会〔2023〕11号[EB/OL]. (2023-08-01)[2024-09-12]. https://www.gov.cn/zhengce/zhengceku/202308/content_6899395.htm.

[7] 中国信息通信研究院. 全球数字经济白皮书(2022年)[R/OL]. [2024-09-12]. http://www.caict.ac.cn/kxyj/qwfb/bps/202212/P020221207397428021671.pdf.

[8] 刘业政，宗兰芳，金斗，等. 数据要素流通使用的安全风险分析及应对策略[J]. 大数据，2023，9(2)：79-98.

[9] 新华财经. 调研报告显示：当前中国首席数据官或类似管理岗渗透率仅为1.3%远低于全球水平[EB/OL]. (2023-09-03)[2024-09-12]. https://www.cnfin.com/hg-lb/detail/20230903/3925858_1.html.

[10] DAMA 国际. DAMA 数据管理知识体系指南：原书第 2 版[M]. DAMA 中国分会翻译组，译. 北京：机械工业出版社，2020.

[11] 国家市场监督管理总局，国家标准化管理委员会. 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.

[12] 腾讯研究院. 腾讯隐私计算白皮书 2021[R/OL]. (2021-04-19)[2024-09-12].https://www.tisi.org/18351.

[13] 中共中央，国务院. 中共中央 国务院印发《国家标准化发展纲要》[EB/OL]. (2021-10-10)[2024-09-12]. https://www.gov.cn/zhengce/2021-10/10/content_5641727.htm.

[14] 陈思. 培育数据要素市场的逻辑理路、安全困境与应对策略[J]. 当代经济管理，2023，45(3)：24-31.

[15] 国家工业信息安全发展研究中心. 中国数据要素市场发展报告(2021-2022)[R/OL]. (2022-11-25)[2024-09-12]. https://dsj.guizhou.gov.cn/xwzx/gnyw/202211/t20221125_77220298.html.

[16] 陈蕾，李梦泽，薛钦源. 数据要素市场建设的现实约束与路径选择[J]. 改革，2023(1)：83-94.

作者简介：
赵勇波，高级工程师，学士，主要从事政府和企业数字化转型、网络安全等相关咨询设计工作；智海峰，工程师，学士，主要从事智慧城市、网络安全等相关咨询设计工作。