

数据流通安全标准化研究

王威^{1,2}, 袁煜琳^{3,4,5}, 于晶^{3,4,5}, 楼莉^{1,2}

1. 北京软件产品质量检测检验中心有限公司, 北京 100193;
2. 国家应用软件产品质量检验检测中心, 北京 100193;
3. 中国科学院信息工程研究所, 北京 100085;
4. 中国科学院大学网络空间安全学院, 北京 100049;
5. 网络空间安全防御重点实验室, 北京 100085

摘要

为确保数据安全高效地流通、推动数字经济健康发展, 关注于数据流通安全领域的标准化研究, 基于国内外数据流通安全的发展历程与标准化现状, 分析了国内数据流通安全标准需求。围绕基础标准、通用要求、技术标准、管理标准、产品与服务以及保障能力构建了数据流通安全标准体系框架, 分别从细化法律设计、加强技术研发、扩大人才培养、推广标准应用、加强国际合作等方面给出了数据流通安全标准化工作建议。

关键词

数据流通安全; 数据标准; 标准体系

中图分类号: TP302

文献标志码: A

doi: 10.11959/j.issn.2096-0271.2024071

Research on data circulation security standardization

WANG Wei^{1,2}, YUAN Yulin^{3,4,5}, YU Jing^{3,4,5}, LOU Li^{1,2}

1. Beijing Software Testing & QA Center Co., Ltd., Beijing 100193, China
2. National Application Software Testing Labs, Beijing 100193, China
3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
4. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
5. Key Laboratory of Cyberspace Security Defense, Beijing 100085, China

Abstract

To ensure the security and efficiency of data circulation and promote the healthy development of the digital economy, the article focuses on the standardization of data circulation security. Based on the development of data circulation security both domestically and internationally, as well as the current state of standardization, the requirements of data circulation security standards is analyzed. A data circulation security standard system framework is constructed, centered around foundational standards, general requirements, technical standards, management standards, products and services, and assurance capabilities. The article offers suggestions on data circulation security standardization, including refining legal design, strengthening technology research and development, expanding talent training, promoting standard application, and strengthening international cooperation.

Key words

data circulation security, data standard, standard system

0 引言

数据是发展数字经济的重要资源，也是国家战略资源和全球竞争的关键资源。我国作为全球数据生产和应用大国，数据规模持续增长，数据资源在工业、农业、服务业等各行各业的流通和应用也越来越频繁^[1]。随着数据汇聚、融合、流动与应用等场景的大幅增加，国家数据、企业数据和个人数据等在流通过程中面临着被非法获取和滥用的风险。如果不能保障数据在流通过程中的安全，数据流通越活跃，越会带来可预见和不可预见的各类风险隐患，甚至影响国家的安全与发展，也会导致数据供方“不愿、不敢、不想”让数据流通起来，制约数字经济的发展。

数据流通安全作为打通数据链路、促进数据价值释放的关键措施，主要包括3个方面：一是数据本身的安全，即数据采集、传输、存储、处理、交换、销毁等流通全过程的安全；二是数据流通活动的安全，即数据提供方、数据使用方、平台管理方、第三方服务提供方等各类市场主体在数据开放、共享和交易等流通活动中的行为安全可控、可追溯；三是数据流通设施的安全，即数据处理活动涉及的网络、平台和物理设施的安全，防止数据基础设施上承载的海量数据丢失、泄露、被篡改。

目前，数据流通安全相关的研究主要从分析数据流通中的安全问题、技术发展应用、产业实践等方面开展。在数据流通中面临的安全问题和风险挑战方面，基于对数据交易中存在权利义务责任不清晰、技术保障能力待提升、安全标准体系和安全监测机制待完善等安全问题的分析，高亚

楠^[2]从权责确定、技术保障和安全检测3个方面构建了数据交易流通安全保障框架；针对数据要素流通过程中面临的数据可信交易与安全交付等问题，李风华等^[3]提出了理论、产品、标准和管理法规一体推动的应对策略，构建安全保障支撑技术体系；以数据流通交易市场和流通交易流程的角度，陈华等^[4]探讨数据交易流通中面临的安全问题，提出协同治理的建议。在数据流通安全技术方面，基于区块链、隐私计算等单一或综合技术，季姝等^[5]利用区块链和隐私计算技术，构建了数据要素的跨域安全流通框架；钟子岳等^[6]探讨了基于区块链实现数据可信流通的技术要点，使其支持更加完备、高效的数据溯源需求；何安珣等^[7]分析了隐私计算在数据流通过程中数据“可用不可见”、使用“可控可计量”、数据“可算不可识”方面发挥的作用。在数据流通安全的产业实践方面，刘文懋等^[8]结合行业实践案例场景化分析了隐私计算、机密计算等新技术在推动数据流通安全中的应用。在数据流通标准安全体系方面，付少雄等^[9]从数据流通中元数据标准、数据分类分级标准构建数据流通与安全的保障体系。

研究者在数据流通安全方面的深入探讨和研究，为数据流通安全标准化研究奠定了基础。通过标准化工作，能够为数据市场化与流通交易等提供框架和准则，是确保其安全和流通效率的关键。目前，国内外已经发布了数据安全相关的若干标准并开展了应用实践，但针对数据流通安全的标准化研究仍然相对滞后，标准制定工作也相对零散。鉴于数据流通体量逐渐增大、安全性需求不断提高，现有以数据开放、共享、交易等立场进行数据流通安全研究在数据流通的实用性等方面存在不够充分的特点，缺少以数据流通安全需求为

导向，更灵活、全面、准确和详尽的标准体系框架。

本文对国内外数据流通安全发展情况、政策法规发布和标准化现状进行充分调研，在此基础上分析数据流通安全标准化工作需求，构建数据流通安全标准化体系，提出数据流通安全标准化建议，以期指导数据流通安全的实践。本文研究成果可为建设数据流通安全标准化与健全数据安全保障体系提供借鉴，助力安全可控的数据流通市场建设，服务于我国数字经济发展战略。

1 数据流通安全发展情况

1.1 国内数据流通安全发展情况

我国在数据流通安全方面已经开展了众多工作，包括优化战略布局、完善法律法规与政策标准制定、技术与产业创新发展，以及关键人才培养。其具体内容如下。

宏观数据战略方面，2020年发布的《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》正式将数据定义为第五生产要素。2022年发布的《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》提出构建数据基础制度体系，推动数据要素市场化配置，优化数据基础设施布局，加强国际合作与交流，重点推进关键领域与行业发展等。2023年发布的《“数据要素×”三年行动计划（2024—2026年）》强调优化数据流通环境，打造安全可信流通环境，加强数据安全保障^[10]。

政策法规方面，数据流通安全领域涉及的数据要素制度体系、公共数据开放、数据交易、数据安全和数据跨境流通等相关要求分散在国家安全法、网络安全法、

数据安全法等国家政策和法律法规文件中，通过明确数据处理的规则、责任主体、法律责任等，为数据安全的监管和执法提供了依据，为数据流通安全提供了法律保障。同时，各省市也在数据要素制度体系、公共数据开发开放^[3]、数据交易与跨境流通以及数据安全体系等多个方面取得了显著成效，多项地方政策法规提出了加强数据流通安全的具体措施和要求^[3]，包括建立健全数据流通利用安全治理机制、提升数据安全保障能力等。

数据安全保护能力技术发展方面，为确保数据在流通过程中免受非法获取、篡改、泄露或滥用^[11]，技术的发展和應用正从单一技术手段逐步向综合解决方案转变。随着安全需求的增加和数字化转型的加速，前沿技术也逐步发展和应用，差分隐私技术逐渐被应用于大规模数据分析和政府统计中，以保证数据实用性^[12]；同态加密^[13]和多方安全计算^[14]技术被运用在云计算、医疗和金融等数据的共享和处理过程中；区块链技术从比特币开始，逐步扩展至金融、供应链、物联网等多个行业^[6]。这些技术的频繁突破和应用进一步提升了数据安全保护能力。

产业实践和人才体系建设方面，产业从数据流通安全产业内部扩大到外部关联行业，形成了包含安全产品供应商、技术服务提供商、数据交易平台^[15]、专业咨询服务公司等多环节的完整产业链生态系统，通过合作模式创新，建立了协同高效、安全有序的数据要素流通体系^[16]。随着产业不断拓展，风险投资基金、私募股权等力量显著增加了对数据流通安全领域企业的资金支持，为初创企业的茁壮成长和成熟企业的市场拓展提供了坚实的资金后盾。同时，通过积极参与国际交流与合作，主动融入全球产业链，提升技术水平、管理

理念和自身竞争力，我国从2023年开始，逐步推动社交媒体、医疗、金融、汽车、民航五大行业重点企业完成数据出境安全评估、审批等流程，保障企业依法依规开展数据跨境流通和业务合作。此外，随着市场需求的不断扩大，数据流通安全人才体系建设也逐渐完善，从教育体系优化、专业认证强化、高端人才引进及科研平台建设等多维度，逐步打造既深谙理论又精通实践的数据安全专业队伍，为我国数字经济的健康可持续发展保驾护航。

1.2 国际数据流通安全发展情况

当今世界数据体量爆炸式增长，全球进入数字经济时代。各国都在积极部署数据战略，成立国家级数据管理部门或部署国家级数据服务平台，通过数据流通实现开放和共享，在国际数据流通中抢占数据主权，加速颁布相关政策法规，探索数据交易市场性模式，大力推动数据要素市场化配置。同时，数据流通安全的配套措施和发展也被提到了极高的层次。

在全球范围内，数据治理表现出明显的区域差异，不同国家或地区在数据跨境流动、企业合规和隐私保护上有不同的要求。制度方面，在欧盟、美国、英国、日本、韩国、加拿大、俄罗斯等区域和国家中，数据流通安全相关政策分散在一系列法律、战略、指令和条例中，包括个人数据和隐私安全、规范数据治理、规范数据跨境流通的多个方面，如欧盟的《通用数据保护条例》《非个人数据自由流动条例》《网络安全法案》《欧洲数据战略》《开放数据与公共部门信息再利用指令》《数据治理法案》《数字市场法案》和《数字服务法案》等，美国的《关于加强国家网络安全的行政命令》《敏感数据行政令》《澄清海

外合法使用数据法案》《数据隐私和保护法案（草案）》和《隐私权法案（草案）》等，英国的《国家网络安全战略2022—2030》，俄罗斯的《俄罗斯联邦国家安全战略》等。此外，随着全球化进程的不断深入，在跨境数据流通安全方面，各国通过多边或双边机制，制定了《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《数字经济伙伴关系协定》（DEPA）和《区域全面经济伙伴关系协定》（RCEP）等多个多边自由贸易协定，为跨境数据流动设定了“原则+例外”的规制框架。技术发展方面，国际数据流通安全随着技术发展和市场需求的动态更新而不断发展，例如在以数据为中心的云服务数据流通安全中，从流通和安全计算双向可追溯性框架^[17]演进到基于集成区块链、无证书加密、代理重加密等多种技术在多云环境中实现安全的数据存储和可信交易框架^[18]，而数据流动路线图的制定为国际数据流通和共享安全提供了最佳实践政策参考和指引^[19]。

综上，国内外针对数据流通与数据安全方面出台了系列法律法规，强调数据流通的必要性与数据安全的意义，但未出台专门针对数据流通安全的指导性规范，以指导数据标准与保障体系构建。为此，本文从数据流通安全标准体系建设现状和需求着手，探究标准体系建设的思路。

2 数据流通安全标准化现状和需求

2.1 国内外政策法规现状

随着数字经济的蓬勃发展，数据安全形势愈加严峻，各国都在积极构建数据安全政策法规体系。欧盟作为全球数据保护先行者，通过《通用数据保护条例》《非个

人数据自由流通条例》《数据治理法案》等严格的法律法规构建数据防护网，强调技术导向的数据共享和流动；美国秉持以商业利益为核心的策略，采取相对灵活的数据控制和数据流动策略，在全球范围内获取和控制更多的数据资源；英国建立了强有力的开放数据框架和隐私保护体系，确保数据自由流动与安全^[20]；俄罗斯强调数据的本地化存储要求，数据流动受到国家的监管和控制^[21]。由此可见，不同国家之间的数据流通法规要求存在差异，数据跨境全球流动时，需要进一步寻求并达成国际共识。

我国通过《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《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》等政策法规文件，确保数据安全、合规、有序地流动和交易，为数据规范化流通提供政策指引和立法保障。各地政府认真贯彻党中央和国务院的战略部署，开展积极的探索和实践，在数据要素制度体系、公共数据开发开放、数据交易与跨境流通以及数据安全体系等多个方面纷纷出台政策文件，并取得了显著成效。但是，针对数据流通安全领域涉及的数据要素制度体系、公共数据开放、数据交易、数据安全和数据跨境流通等的要求分散在《中华人民共和国数据安全法》等法律法规中，尚未形成专门的政策规定，还需加强数据流通体系规划研究。

2.2 国内外标准化工作现状

在全球范围内，各国积极探索数据确权、数据安全、数据跨境流转的标准化工作。通过对国内外标准化研究开展广泛调研，笔者分析和总结了数据流通安全标准

化工作中的关键成果，其中国外标准化工作包括：国际组织 ISO/IEC JTC1（国际标准化组织/国际电工委员会的第一联合技术委员会）在数据保护、数据治理等方面发布了一系列技术标准和指南，包括 ISO/IEC 29100《信息技术 安全技术 隐私框架》、ISO/IEC 19944《云计算和分布式平台 数据流、数据类别和数据使用》、ISO/IEC 38505《信息技术 数据治理》等；ITU（国际电信联盟）在网络安全、加密通信等提供了一系列框架和指导，包括 ITU-T X.1054《信息安全、网络安全和隐私保护 信息安全治理》、ITU-T X.1641《云服务客户数据安全指南》、ITU-T F.751.20《基于 DLT 的多媒体数据传输管理系统参考架构》和 ITU-T H.DLT-DCMP《基于数据流通和市场平台的分布式账本技术框架》等；IEEE（电气与电子工程师协会）提出了数据流通框架中可信数据空间、区块链和分布式记账等技术相关标准和推荐实践，包括 IEEE 3158—2024《可信数据空间系统体系结构》、IEEE P3226/D2.0《基于区块链和分布式账本技术（DLT）的可信数据流通》等。各国际组织在数据治理、数据管理和数据安全等方面各有侧重，标准框架主要根据产业发展和重点问题建立，相关国际标准和标准体系框架为数据流通安全提供了一定的指导。国内相关标准化工作如下。我国 SAC/TC260/WG8（全国网络安全标准化技术委员会/数据安全标准工作组）主要任务是研究提出数据安全和个人信息保护标准体系，开展相关标准的研究和制定，在基础通用数据安全方面，发布了 GB/T 43697—2024《信息安全技术 数据分类分级指南》、GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》等标准；在安全技术方面，发布了数据加密、数据

脱敏、隐私计算和访问控制等技术要求,例如 GB/T 32905—2016《信息安全技术 SM3 密码杂凑算法》、GB/T 38635.1—2020《信息安全技术 SM9 标识密码算法》、GB/T 42460—2023《信息安全技术 个人信息去标识化效果评估指南》和 GB/T 39205—2020《信息安全技术 轻量级鉴别与访问控制机制》等;在评估和评价方面,正在研制数据安全评价和数据流通安全风险评估方法。这些标准为数据流通安全提供基本保障。

从标准体系构建方面来看,我国在数据流通安全领域尚未建立完善的标准体系^[22],数据相关领域标准体系主要从需求导向、问题导向、产业链环节划分、产业发展等方面开展。例如,在数字商务领域,为满足技术应用、供应链管理 and 营销等方面的需求,从总体规范和关键核心推进两方面综合构建标准体系^[23],扩展现实领域;为解决顶层架构不清晰、标准体系不完善等问题,综合使用生产链环节和拓展的方式构建了标准体系框架^[24];在大数据标准领域,全国一体化大数据中心^[25]结合国家总体要求、GB/T 13016—2018《标准体系构建原则和要求》^[26]构建标准体系框架,大数据治理结合产业生态系统的新热点和重点问题提出标准体系框架^[27],数据安全和隐私保护方面,学者从数据活动出发进行标准体系构建^[28]。相关的标准体系构建为数据流通安全标准化体系框架构建提供了借鉴和参考。

2.3 数据流通安全标准化需求

当前,我国的数据流通安全标准化工作仍处于初步探索阶段,缺乏系统性的顶层规划,标准制定工作相对零散,尚未建立完善的标准体系。通过深入剖析当前数

据流通标准化领域的研究现状,笔者认为未来标准化工作主要包含以下6类需求。

- 规范数据流通安全相关术语和框架。

首先应统一行业内对数据流通安全概念、模型和框架的理解,消除交流障碍,为后续标准制定提供清晰、一致的术语基础,确保不同参与者在数据流通活动中能够准确识别安全角色、明确职责界限,以及理解数据生命周期中各阶段的安全活动。

- 推动数据流通基础设施安全建设。

应确保数据流通基础设施的安全性,为数据的采集、传输、存储、处理等关键操作提供坚固的技术支撑,防止数据泄露、被篡改和被非法访问,提升数据流通整体的安全防护能力。

- 保障数据流通生命周期的安全管理。

应确保数据在全生命周期内的安全,从数据的产生到销毁,每一个环节都应有明确的安全管理流程和措施,减少内部和外部数据安全风险,保护数据的完整性和隐私性。

- 支撑数据服务的安全管理。

应确保数据服务提供商能够提供安全可靠的服务,通过规范数据服务的安全能力、数据交易服务的安全操作,以及数据安全治理机制,增强数据服务的安全性和透明度,支持数据流通市场的健康发展。

- 数据流通产品和服务安全评估。

应建立数据流通相关安全产品和服务的评估标准和指南,确保市场上流通的安全产品和服务具有明确的安全性能指标,从而有效地保护数据在处理、传输过程中的安全,促进安全技术的健康发展和广泛应用。

- 促进数据应用的安全和持续发展。

应根据不同行业和应用场景的特定需求,制定行业数据安全标准和指南,指导各行业在数据流通和应用中采取有效的安全措施,解决数据交换和共享中的安全问题,支撑行业大数据应用的快速、安全发展。

3 数据流通安全标准化体系架构

本节通过深入分析数据流通安全标准化需求，基于三维属性空间模型，构建了数据流通安全标准体系框架，为数据要素的合规流通和安全保障提供了理论指导、实践参考和方向建议。同时，基于该体系框架，对数据流通安全标准进行分类，构建了数据流通安全标准框图，为未来的数据流通安全标准化工作提供了清晰的框架和方向。最后，对比成熟的数据安全标准体系，介绍数据流通安全标准化工作的特殊性。

3.1 构建思路

根据国家标准 GB/T 13016—2018《标准体系构建原则和要求》^[26]中的定义，体系是由相互作用和相互依赖的若干组成部分结合而成的具有特定功能的有机整体。数据流通安全标准化体系架构的构建逻辑基于三维属性空间模型，如图1所示。

三维属性包含数据要素表现形态维度、

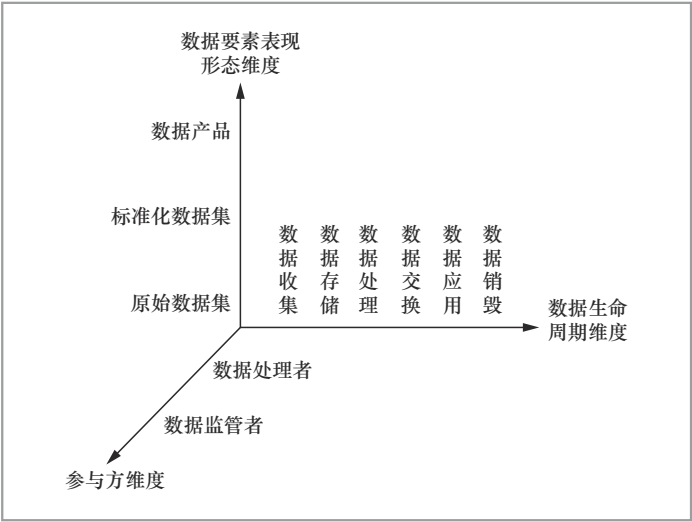


图1 标准三维空间

数据全生命周期维度以及参与方维度。数据要素表现形态维度包含原始形态的数据集、标准化后的数据集以及衍生得到的各类产品服务。数据生命周期维度围绕数据流通的收集、存储、处理、交换、应用、销毁过程进行安全防护。参与方维度从数据流通过程的参与者角度出发，对数据进行安全防护。从数据主体到其流通过程，再到参与方主体，在三者形成的三维空间中，形成“从基础到应用、从技术到管理、从规范到保障”的构建思路，从基础标准的制定到数据产品的规范要求，从数据处理的标准制定到数据监管的规范要求，将整个数据安全流通标准化体系的构建分为多个层次，从而形成一个全面的标准化体系框架。

3.2 数据流通安全标准化体系框架

数据流通安全标准化以数据保护为核心，依托安全法律法规，围绕基础标准、通用要求、技术标准、管理标准、产品与服务以及保障能力，确保数据在流通中安全可靠，从而为政府和行业主管部门的监督管理提供有力支撑。数据流通安全标准体系框架如图2所示，该框架主要包含6个部分。

- 基础标准：为整个数据安全流通框架制定统一的、规范化的术语、模型和框架，确保技术和管理操作的一致性、可靠性和合规性。
- 通用要求：从分类分级、基线要求和方法指南3个部分为数据流通提供方向性指导和规范性约束，以适用于数据在不同场景下的流通。
- 技术标准：为了数据流通全生命周期安全，确立相应的技术标准，包含基础设施安全、数据匿名化、风险监测、流通溯源、数字资产识别、数据加密、数据脱

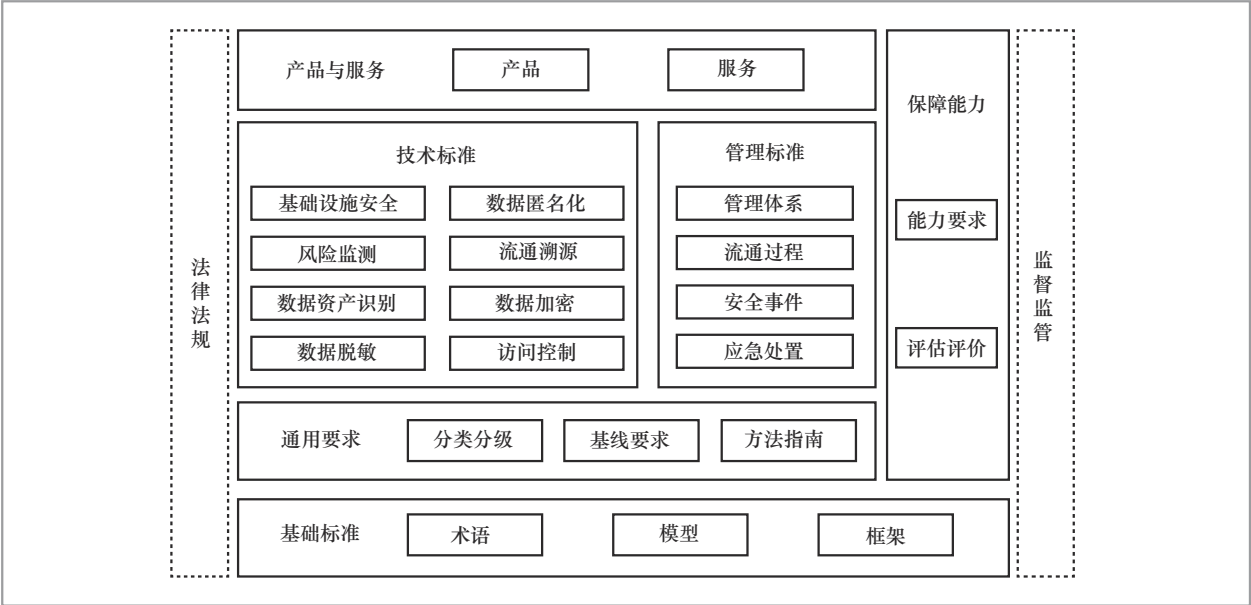


图2 数据流通安全标准体系框架

敏和访问控制等关键技术环节。

• 管理标准：为数据流通过程制定规范化的管理标准，包含应急处置、安全事件的管理、流程管理等内容，从而确保整个数据流通过程符合安全性、合规性及风险控制的要求。

• 保障能力：着重于评估和提升组织在数据安全流通方面的能力，以保障整个数据流通体系的稳定可靠。

• 产品与服务：聚焦于数据安全产品和服务的标准制定，从而保证数据安全产品和服务质量，推动产业升级。

数据流通安全体系一方面对数据进行系统的分类分级，使其能够依据数据的重要性和敏感性制定相应的保护制度，从而确保数据在流通过程中的安全性，有效降低数据泄露和滥用的风险；另一方面，在数据流通安全通用要求方面与我国的网络安全等级保护要求相衔接，确保了数据安全的规范化和法治化，这不仅增强了企业和机构在数据管理方面的合规性，也为国

家在网络安全治理中提供了可靠的基础。

3.3 数据流通安全标准体系

本节基于图2的数据流通安全标准体系框架，对标准规范进行分类，进而完善体系框架，形成图3所示的数据流通标准体系，从而为数据安全流通提供全流程支撑和保障。其中，各子分类下的标准可分为3类，黑色代表已发布标准，灰色代表在研标准，白色代表待研标准。

（1）基础标准：基础标准制定整个数据流通安全标准体系总体性、框架性和基础性的标准规范，提供术语、模型、框架3类基础标准。其中，术语类标准明确统一数据流通安全相关概念；模型类标准制定数据流通安全相关概念以及概念间关系；框架类标准提供数据流通安全内在要求、设计结构和运行建立的技术模型。

（2）通用要求：通用要求从分类分级、基线要求、方法指南三方面制定数据流通

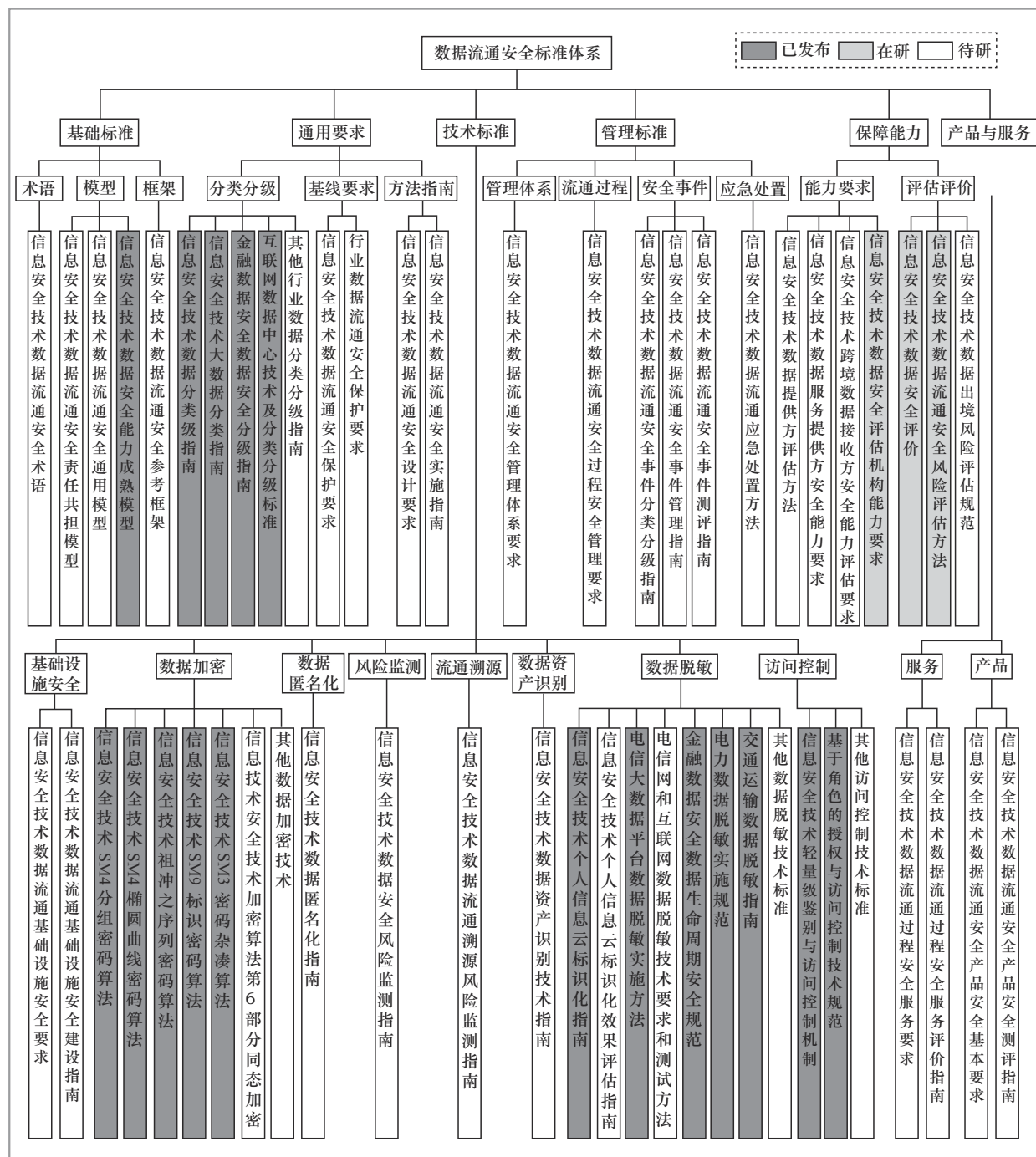


图3 数据流通安全标准体系

过程的基础操作指引。在通用要求标准制定中,除了面向一般数据的标准外,各行业可结合行业数据保护的特殊需求,制定相应的数据流通安全标准。其中,分类分

级类标准制定数据分类分级过程的基本指南；基线要求类标准制定数据流通过程中数据保护的基本要求；方法指南类标准制定数据流通安全通用技术框架，并提出具

体的实施过程和控制要求。

(3) 技术标准：技术标准是基于数据保护要求，提出的支撑数据流通基础设施安全和数据流通全生命周期安全的相关技术标准。其中，基础设施安全类标准制定数据流通基础设施的相关标准，包含安全技术要求、设计要求及测评要求等；数据加密类标准旨在制定数据加密策略和标准，包含加密算法的选择、密钥管理、加密技术应用以及合规性检查等多个方面；数据匿名化类标准旨在说明隐私技术的多种技术方法和实施步骤，在不同技术路线间建立通用的安全分级标准；风险监测类标准旨在规定对数据流通过程中的风险环节进行监控；流通溯源类标准旨在规定发生数据安全泄露事件时，对数据使用者、敏感数据、事件属性等信息建立统一的数据质量标准规则；数据资产识别类标准旨在明确数据流通全生命周期中的资产识别方法；数据脱敏类标准旨在制定统一的数据脱敏和匿名化处理标准；访问控制类标准旨在提出访问控制的要求和方法。

(4) 管理标准：管理标准与技术标准共同践行数据安全保护要求，从流通过程、安全事件等方面支撑数据可信流通，构建数据流通各环节的安全基础。其中，管理体系是一个综合性框架，规定了各组织建立、实现、维护和持续改进管理体系的要求；流通过程类标准旨在明确数据流通过程中不同环节的安全管理要求；安全事件类标准旨在明确安全事件分类分级方法，为数据流通过程中的相关方开展安全事件研判、信息通报、监测预警和应急处置等活动提供指导；应急处置类标准旨在规范不同级别风险选择控制措施，制定应急处置计划，并获得风险责任人对应急处置计划批准的过程。

(5) 保障能力：保障能力类标准旨在

明确数据流通参与方的能力要求，并规范相应的能力评估过程。其中，能力要求类标准面向数据提供方、数据服务提供方、数据接收方以及数据评估机构，规定各参与方需具备的安全能力；评估评价类标准旨在针对数据流通过程中各相关方、对象、评价管理、评价体系、评价指标、过程管理、人员管理、文档管理等提出具体要求。

(6) 产品与服务：产品和服务类标准包括数据流通安全服务安全基本要求、数据流通安全服务安全评测指南、数据流通安全产品安全基本要求和数据流通安全产品安全测评指南等。

3.4 数据流通安全标准体系和数据安全标准体系

目前，关于数据安全标准体系的研究工作已较为成熟。2020年12月，工业和信息化部印发了《电信和互联网行业数据安全标准体系建设指南》，用于规范和保障电信和互联网行业的数据安全，该标准从基础共性、关键技术、安全管理和重点领域4个方面，形成了数据安全标准体系的整体框架^[29]。随后，工业和信息化部相继颁布了工业、车联网等领域的数据安全标准体系建设指南，完善数据安全标准体系方向的相关工作。

相较于数据安全标准体系，图3的数据流通安全标准体系更加聚焦于数据在流通过程中的安全性，关注数据在流动过程中可能面临的风险，而数据安全标准体系强调的是数据在整个生命周期中的安全保障。在技术标准上，数据流通安全标准体系更加关注数据流通中的关键技术，例如，流通溯源、数据匿名化、数据脱敏和数字资产识别等，确保数据在多个平台或系统间流动时可以被有效监控、识别和追溯，而数据安全标准体系更多涉及数据的基本

保护技术，如数据加密、传输保护等，是基于全生命周期的数据安全防护。同时，在法律合规性和监管方面，数据流通安全标准体系更加关注跨主体、跨系统、跨境流通时的法律合规性，这使其监管要求更加复杂，需要应对多国、多区域法律的差异性，确保数据在不同法律框架下的合规性。

4 数据流通安全标准化工作建议

数据流通安全标准化是确保数据安全、保护隐私及维护各方权益的重要途径。在深入剖析当前该领域标准化的现状与需求后，本节旨在为未来的数据流通安全标准化工作提出一系列切实可行的建议，从而进一步优化和完善数据流通安全体系，推进标准化工作持续深入。

（1）健全数据流通安全法律法规和标准体系：法律法规是保障数据安全流通的基石，通过立法明确数据流通的边界和规则，可以有效地预防和减少数据泄露、滥用等安全事件。与此同时，应完善国家数据流通安全战略，制定配套的数据流通安全操作规范，以明确数据流通安全标准化的总体目标、基本原则、重点任务和行动指南。在数据流通过程中，确立监管机构及其职责，加大跨部门协调力度，加强信息共享和沟通协作，建立健全数据流通安全协调机制，共同应对数据流通安全挑战。

（2）加强数据流通安全核心技术标准研制：技术创新是保障数据流通安全的关键要素，加强技术研发，对于构建健康、可持续的数据要素市场，保障国家安全和公共利益，以及推动数字经济的高质量发展具有重要意义。在核心技术标准研制方面，需加大对数据流通安全的关键技术研究、产品开发和产业实施的投入，集中力

量突破技术瓶颈，加速科技成果转化，培育具有自主创新能力的优势企业。同时，根据监管要求和行业发展需求，结合技术创新方向，持续推动数据流通安全关键技术领域的标准研制工作，按照“共性先立、急用先行”的工作思路，分阶段逐步推进技术标准的制定。

（3）推广数据流通安全标准示范应用：开展数据安全标准示范应用工作，强化标准宣贯与应用推广，提高各行业数据安全意识，是数据流通安全标准落地实施的重要途径。首先，应引导企业贯彻“发展与安全并重”的原则，将数据安全融入企业发展战略与考核机制，加强数据安全工作与业务发展同谋划、同部署、同落实、同考核。其次，应鼓励行业优势单位开展数据安全标准试点示范，督促企业落实数据安全主体责任，加强数据分类分级管理、安全防护、安全评估、安全监测等工作，提升数据安全防护能力。最后，应基于数据安全标准实践情况，挑选行业数据安全标准实践优秀案例，总结经验教训，不断优化标准。

（4）建立数据流通安全标准体系研究长效机制：建立数据流通安全标准体系研究长效机制是确保数据安全与时俱进、响应技术发展和社会需求的关键策略。数据流通安全标准体系建设涉及多部门、多领域，因此需要加强政府部门、行业组织、企业、高校、科研院所之间的沟通与合作，推动形成统一、协调、高效的工作机制。同时，设立专门的数据安全标准研究机构或委员会，承担数据流通安全标准体系风险评估、框架设计、关键技术研究、标准制定、测试评估等任务，为数据流通安全标准化工作提供全方位的智力支持。为了响应技术发展和市场需求，还需密切跟踪国内外数据流通安全技术发展趋势和最佳

实践，建立数据流通安全标准体系的动态更新机制，确保标准内容及时迭代更新。

(5) 深度参与数据流通安全国际标准化工作：在数字经济全球化发展的背景下，数据跨境流动日益频繁，数据流通安全已成为全球关注的重要议题。深度参与数据流通安全国际标准化工作，应加强与世界各国、地区和国际组织的交流与合作，分享各国在数据安全和标准化方面的经验和成果，共同构建开放、合作、共赢的网络空间命运共同体。通过积极对接国际标准化组织，推动我国法律法规与标准的国际转化，在建立国际标准互认机制的同时，提升我国标准的国际影响力。此外，各国需共同构建安全可信的国际数据流通平台，制定统一的数据流通规则，以推动数据资源的跨境流动和共享。

(6) 加强数据安全流通标准人才培养：培养数据流通安全和标准化复合型人才是推进数据流通安全标准化工作的关键。一方面，通过加强数据流通安全学科建设，鼓励高校设立数据流通安全相关专业，设置科学合理的课程体系，培养具备数据安全理论知识、专业技术能力和实践经验的复合型人才；另一方面，与知名高校、科研机构、企业和标准化组织建立合作关系，加强数据流通标准宣贯培训和业内交流，提升专业技术人员的理论和实践能力。同时，积极开展国内外交流与合作，学习国际先进经验，提升专业人才的综合素质和能力。

5 结束语

随着数字经济飞速发展，数据作为生产要素的重要性已经得到广泛认可。然而，当前数据流通的相关机制设计存在滞后性，缺乏全面的数据流通相关体系去解决政府机关以及企业在实践发展中面临的现实问

题。本文针对数据在流通过程中面临的安全问题，全面总结了数据流通安全标准的现有工作，创新性地构建了一个数据流通安全标准体系，明确了标准框架、结构以及分类。同时，针对数据流通安全标准工作亟待解决的问题，从细化法律设计、加强技术研发、扩大人才培养、推广标准应用、加强国际合作等方面提出了相应建议，以构建适合我国国情的数据流通安全标准体系，从而确保数据安全合规地高效流通，促进数字经济健康发展。数据流通安全标准化工作聚焦于数据流通过程，对于加快建立数据流通安全标准体系，指导数据流通安全标准化工作开展，制/修订数据领域相关标准提供了重要指引。保障数据安全合规流通作为未来工作的重中之重，一是需要制定并不断完善数据流通安全标准体系，为数字经济的持续健康发展奠定坚实基础；二是需要政府部门、行业、高校、科研院所等携手并进，明确各自职责，形成强大的协同合力，共同推动数据流通安全标准的完善与落地；三是需要建立长效机制，围绕市场需求，从政策法规持续完善、标准体系动态更新、技术创新、人才培养等方面，构建一个灵活、高效、富有活力的数据流通安全体系。

参考文献：

[1] 王江, 姜伟, 王普. 我国数据要素交易市场发展现状与未来趋势[J]. 网络安全与数据治理, 2024, 43(7): 1-7, 25.
WANG J, JIANG W, WANG P. The current development and future trend of data trading market in China[J]. Cyber Security and Data Governance, 2024, 43 (7): 1-7, 25.

[2] 高亚楠. 数据交易流通安全保障探索与研究[J]. 信息安全研究, 2023, 9(7): 662-666.

- GAO Y N. Exploration and research on security guarantee of data transaction and circulation[J]. Journal of Information Security Research, 2023, 9(7): 662-666.
- [3] 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.
- [4] 陈华, 李庆川, 翟晨喆. 数据要素的定价流通交易及其安全治理[J]. 学术交流, 2022(4): 107-124.
- CHEN H, LI Q C, ZHAI C Z. Pricing and circulation transaction of data elements and its security management[J]. Academic Exchange, 2022(4): 107-124.
- [5] 季姝, 张金琳. 基于区块链+隐私计算的数据要素跨域安全流通体系[J]. 网络安全技术与应用, 2023(5): 65-67.
- JI S, ZHANG J L. Cross-domain secure circulation system of data elements based on blockchain and privacy computing[J]. Network Security Technology & Application, 2023(5): 65-67.
- [6] 钟子岳, 朱长昊, 李浚哲, 等. 基于区块链的数据要素可信流通技术综述[J]. 数据与计算发展前沿, 2023, 5(5): 46-62.
- ZHONG Z Y, ZHU C H, LI J Z, et al. A survey on blockchain-based trusted data elements circulation[J]. Frontiers of Data & Computing, 2023, 5(5): 46-62.
- [7] 何安珣, 李宏宇, 韦韬. 保障隐私安全 促进数据流通: 隐私计算应用技术发展趋势综述[J]. 人工智能, 2023(6): 35-42.
- HE A X, LI H Y, WEI T. Ensuring privacy security and promoting data circulation: a summary of the development trend of privacy computing application technology[J]. Artificial Intelligence View, 2023(6): 35-42.
- [8] 刘文懋, 孟楠, 汤旭. 新技术赋能数据要素安全流通[J]. 信息通信技术与政策, 2024(8): 55-61.
- LIU W M, MENG N, TANG X. New technologies empower secure circulation of data elements[J]. Information and Communications Technology and Policy, 2024(8): 55-61.
- [9] 付少雄, 孙建军. 数据流通与安全: 标准与保障体系[J]. 图书与情报, 2023(4): 20-28.
- FU S X, SUN J J. Data circulation and security: standards and assurance systems[J]. Library & Information, 2023(4): 20-28.
- [10] 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.
- LIU Y Z, ZONG L F, JIN D, et al. Security risk analysis and countermeasures in the circulation and use of data factors [J]. Big Data Research, 2023, 9(2): 79-98.
- [11] 张苑, 王波. 畅通企业数据利用路径释放数据要素价值[J]. 新经济导刊, 2024(8): 53-57.
- ZHANG Y, WANG B. Unblocking enterprise data utilization pathways to release data element value[J]. New Economy Weekly, 2024(8): 53-57.
- [12] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends® in Theoretical Computer Science, 2013, 9(3/4): 211-407.
- [13] YI X, PAULET R, BERTINO E. Homomorphic encryption[M]//SpringerBriefs in Computer Science. Cham: Springer International Publishing, 2014: 27-46.
- [14] YAO A C C. How to generate and exchange secrets[C]//Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS 1986). Piscataway: IEEE Press, 1986: 162-167.
- [15] 汪晓梅, 黄科满, 邵瑞江. 支撑数据要素流通的数据交易平台的关键技术设计与实践[J]. 新型工业化, 2023, 13(11): 40-50.

- WANG X M, HUANG K M, SHAO R J. Design and practice of key technology of data trading platform supporting the circulation of data elements[J]. The Journal of New Industrialization, 2023, 13(11): 40–50.
- [16] 窦悦, 易成岐, 黄倩倩, 等. 打造面向全国统一数据要素市场体系的国家数据要素流通共性基础设施平台: 构建国家“数联网”根服务体系的技术路径与若干思考[J]. 数据分析与知识发现, 2022, 6(1): 2–12.
- DOU Y, YI C Q, HUANG Q Q, et al. Constructing a common data circulation infrastructure platform for the national unified data factor market: technical path and policy thinking of constructing the national “data networking” root service system[J]. Data Analysis and Knowledge Discovery, 2022, 6(1): 2–12.
- [17] LIANG K T, MIYAJI A, SU C H. Secure and traceable framework for data circulation[M]//LIU J K, STEINFELD R. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016: 376–388.
- [18] ZHANG K M, WANG X W, QIU L, et al. JCDC: a blockchain-based framework for secure data storage and circulation in JointCloud[J]. Future Generation Computer Systems, 2025, 162: 107486.
- [19] The World Economic Forum. A roadmap for crossborder data flows: future-proofing readiness and cooperation in the new data economy[R]. 2020.
- [20] 刘川意, 颜亮, 吴德林, 等. 全球数据生产要素可信流通政策与实践[J]. 信息安全研究, 2024, 10(9): 877–884.
- LIU C Y, YAN L, WU D L, et al. Circulation Policy and Practice of Global Data Elements[J]. Journal of Information Security Research, 2024, 10(9): 877–884.
- [21] 江欣欣, 由鲜举. 俄罗斯数据安全政策法规概述[J]. 保密科学技术, 2021(4): 62–66.
- GANG X X, YOU X J. Overview of Russian data security policies and regulations[J]. Secrecy Science and Technology, 2021(4): 62–66.
- [22] 杨辉, 王锋, 杜潇霖, 等. 国内外数据要素标准研究综述[J]. 质量与认证, 2024(7): 30–33.
- YANG H, WANG F, DU X L, et al. Summary of research on data element standards at home and abroad[J]. China Quality Certification, 2024(7): 30–33.
- [23] 陈晶晶, 张晓. 数字商务标准体系框架设计实证研究[J]. 中国标准化, 2024(13): 66–70.
- CHEN J J, ZHANG X. Empirical research on framework design of standards system for digital commerce[J]. China Standardization, 2024(13): 66–70.
- [24] 耿一丹, 潘榕, 董桂官, 等. 扩展现实(XR)标准体系研究[J]. 信息技术与标准化, 2024(9): 29–34.
- GENG Y D, PAN R, DONG G G, et al. Research on the integrated standard system of extended reality(XR) [J]. Information Technology & Standardization, 2024(9): 29–34.
- [25] 王华, 曹扬, 韩国权, 等. 全国一体化大数据中心标准体系研究[J]. 中国标准化, 2023(S1): 108–115.
- WANG H, CAO Y, HAN G Q, et al. Research on national integrated big data center standard system[J]. China Standardization, 2023(S1): 108–115.
- [26] 国家质量监督检验检疫总局, 中国国家标准化管理委员会. 标准体系构建原则和要求: GB/T 13016—2018[S]. 北京: 中国标准出版社, 2018.
- General Administration of Quality Supervision, Inspection and Quarantine of the People’s Republic of China, Standardization Administration of the People’s Republic of China. Principles and requirements for constructing standard system: GB/T 13016—2018[S]. Beijing: Standards Press of China, 2018.

[27] 代红, 张群, 尹卓. 大数据治理标准体系研究[J]. 大数据, 2019, 5(3): 47-54.

DAI H, ZHANG Q, YIN Z. Study on big data governance standard system[J]. Big Data Research, 2019, 5(3): 47-54.

[28] 杨锐, 公伟, 王曙光, 等. 数据安全和隐私保护标准体系研究初探[J]. 大众标准化, 2021(16): 1-3.

YANG R, GONG W, WANG S G, et al. Research on the standard system of data security and privacy protection[J]. Popular Standardization, 2021(16): 1-3.

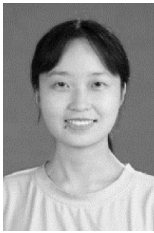
[29] 张峰, 江为强, 王光涛. 电信领域数据安全标准体系现状与思考[J]. 中国信息安全, 2022(4): 36-39.

ZHANG F, JIANG W Q, WANG G T. Present situation and thinking of data security standard system in telecommunications field[J]. China Information Security, 2022(4): 36-39.

作者简介



王威（1977- ），女，北京软件产品质量检测检验中心有限公司副主任，主要研究方向为系统与软件产品质量检测和标准化。



袁煜琳（1998- ），女，中国科学院信息工程研究所博士生，主要研究方向为数据隐私保护。



于晶（1986- ），女，博士，中国科学院信息工程研究所高级工程师，主要研究方向为数据隐私保护。



楼莉（1977- ），女，北京软件产品质量检测检验中心有限公司部门部长，主要研究方向为系统与软件产品质量检测和标准化及实验室质量体系建设。

收稿日期: 2024-08-10