引用格式：许林波，柳经纬.标准化视野下数据安全规范体系发展的困境与突破[J].标准科学，2025(11):6-15.
XU Linbo,LIU Jingwei. The Dilemma and Breakthrough in Developing a Data Security Regulatory System from the Perspective of Standardization [J].Standard Science,2025(11):6-15.

标准化视野下数据安全规范体系发展的困境与突破

许林波[1]　柳经纬[2]

（1.江西财经大学 法学院；2.中国政法大学 比较法学院）

摘　要：【目的】数据安全规范体系包含法律规范和技术标准两部分内容，以技术标准为核心，二者共同规制整个数据生命周期全链条活动。随着标准化工作的推进与数据安全保障的强化，有必要进一步推动该体系规范功能的发挥。【方法】通过梳理现有数据安全规范体系的主要构成，剖析存在的发展困境。【结果】一方面，在我国数据安全法律规范发展迅速的背景下，标准体系的建设相对滞后，存在标准体系的整合与协调难度较大、应对新兴技术挑战的更新速度有限、标准的落地实施和监督机制有待加强等问题；另一方面，数据安全法律引用标准的情况仍然较为保守，尚未形成直接引用与普遍性引用相结合的完整格局。【结论】在标准化视野下完善数据安全规范体系，既要加快建立健全数据安全标准体系，又要推动数据安全法律对现有标准的直接引用，构建更为紧密的联系与互动。

关键词：数据安全；技术标准；标准引用；标准化

DOI编码：10.3969/j.issn.1674-5698.2025.11.001

The Dilemma and Breakthrough in Developing a Data Security Regulatory System from the Perspective of Standardization

XU Linbo[1]　LIU Jingwei[2]

(1.School of Law, Jiangxi University of Finance and Economics; 2. College of Comparative Law, China University of Political Science and Law)

Abstract: [Objective] The data security regulatory system comprises both legal norms and technical standards, with the latter serving as the core component. Together, they govern activities across the entire data lifecycle. As standardization efforts advance and data security safeguards intensify, there is a growing need to enhance the regulatory effectiveness of this system. [Methods] By examining the structure of the existing data security regulatory framework, it analyzes the challenges it faces. [Results] It is found that: On one hand, despite the rapid development of data security laws in China, the corresponding standards system lags behind, facing issues such as difficulties in integration and coordination, limited capacity to keep pace with emerging technologies, and insufficient implementation and supervision mechanisms. On the other hand, the referencing of standards within data security legislation remains relatively conservative, lacking a comprehensive framework that combines both direct and widespread adoption of standards. [Conclusion] To improve the data security regulatory system from

基金项目：本文受2021年度国家社会科学基金重大项目“基于法治、国家治理和全球治理的技术法规研究”（项目编号：21&ZD192）资助。

作者简介：许林波，法学博士，讲师，硕士生导师，研究方向为标准化法、诉讼法。
柳经纬，教授，博士生导师，研究方向为标准化法、民商法。

a standardization perspective, it is essential not only to accelerate the establishment of a robust data security standards system but also to promote the direct incorporation of existing standards into data security laws, thereby fostering stronger linkages and interaction between legal and technical norms.

Keywords: data security; technical standards; standard referencing; standardization

0 引言

数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。目前，大数据被广泛运用于多个领域，但在数据处理过程中存在着诸多安全风险，易发生侵害公民和组织的合法权益的现象，进而影响国家安全与经济社会发展，因此需要法律对数据处理活动给予监管以解决信息安全问题。数据安全相关标准作为落实数据安全相关法律法规要求的重要延伸[1]，在针对数据是否符合数据安全要求、是否存在侵害公民和组织的合法权益的危险等技术问题进行判定时，可作为判定依据。通过《中华人民共和国数据安全法》（以下简称《数据安全法》）“引用”数据安全相关标准的方式，形成数据安全技术法规的规范体系，共同发挥着规范数据处理活动，保障数据安全，促进数据依法合理开发利用，保护公民、组织的合法权益的作用。

1 数据安全法律规范体系

《数据安全法》是为了规范数据处理过程中关于数据的收集、存储、使用、加工、传输、提供、公开等活动的法律规范。在我国，它包括《中华人民共和国立法法》规定的具有法源地位的关于数据安全的法律、行政法规、部门规章及地方性法规和规章。

在法律层面，我国已构建了以《数据安全法》为核心的数据安全法律体系，其内容涵盖了数据保护、网络安全、个人信息保护等多个方面，为数据安全提供了坚实的法律基础。这些法律相互补充，共同维护了国家数据安全和公民个人信息安全。2021年9月1日起实施的《数据安全法》是我国数据安全的基本法。它规定了数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放以及法律责任。除《数据安全法》外，涉及数据安全的法律还包括《中华人民共和国保守国家秘密法》《中华人民共和国居民身份证法》《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》等。在行政法规层面，我国通过制定一系列条例和管理办法，对数据安全进行了全面而细致的规范，不仅加强了对个人信息和重要数据的保护，还规范了网络数据跨境安全管理，为数据安全的监管提供了有力的法规支撑。其中，最主要的是国务院于2024年9月颁布的《网络数据安全管理条例》。该条例主要规定了个人信息保护、重要数据安全、网络数据跨境安全管理、网络平台服务提供者的义务、监督管理及法律责任。此外，与数据安全有关的行政法规还包括《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《商用密码管理条例》《中华人民共和国电信条例》《互联网信息服务管理办法》《企业信息公示暂行条例》《关键信息基础设施安全保护条例》《未成年人网络保护条例》等。在部门规章层面，我国针对数据安全的不同领域和环节，制定了详细的规章制度。其内容不仅涵盖了数据出境、个人信息保护等关键领域，还涉及了区块链、算法推荐等新兴技术的安全管理。制定部门以国家互联网信息办公室为主，根据调整的领域不同，还涉及国家发展和改革委员会、工业和信息化部、公安部、国家市场监督管理

总局等部门。这些规章的制定和实施，进一步细化了数据安全的管理要求，提高了数据安全的监管水平。与数据安全相关的部门规章包括国家互联网信息办公室发布的《区块链信息服务管理规定》《儿童个人信息网络保护规定》《网络信息内容生态治理规定》《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》，以及由国家保密局、国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部、国家安全部、财政部、商务部、教育部、科学技术部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家密码管理局等部门单独或联合发布的《通信网络安全防护管理办法》《规范互联网信息服务市场秩序若干规定》《电信和互联网用户个人信息保护规定》《涉密信息系统集成资质管理办法》《汽车数据安全管理若干规定（试行）》《网络安全审查办法》《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》等。在地方性法规层面，我国各地根据本地实际情况和需要，制定了大量的数据安全相关地方性法规和规章。这些地方性法规不仅细化了国家层面的数据安全法律要求，还针对本地特色和需求进行了有针对性的规定，为数据安全提供了更加具体和可操作的法规依据。根据国家法律法规数据库和中国政府网国家规章库以及各级人大、人民政府官网提供的信息，江苏省、浙江省、广东省、福建省、安徽省、湖北省、湖南省、江西省、贵州省、四川省、陕西省、河北省、山东省、辽宁省、吉林省、北京市、上海市、天津市、重庆市等省、直辖市，以及济南市、贵阳市、深圳市、宁波市、烟台市等地市相继制定了与数据安全相关的地方性法规和规章，总计110余部。其中比较有代表性的，如《浙江省数据条例》首创“数据知识产权登记”制度，推动数据资产化进程，规范数据交易场所运营规则；《深圳经济特区数据条例》是全国首个综合性数据地方立法，确立“数据权益”法律属性，首创“数据公平竞争”条款，规范大数据“杀熟”行为。

随着数字经济高质量发展的稳步推进，数据安全领域面临新的挑战，数据安全建设刻不容缓。为此，世界各国都在积极构建数据安全政策法规体系，我国通过相关规范为数据处理活动提供安全保障，针对数据安全领域的立法[①]已逐步进入规范化、体系化发展阶段。如上所述，我国在数据安全法律规范体系的构建上取得了显著成就，形成了法律、行政法规、部门规章和地方性法规相结合的全方位、多层次法律体系。这一体系不仅涵盖了数据安全的各个方面和环节，还针对不同领域和场景进行了详细规范。尤其是地方数据立法，更是呈现多样化、精细化趋势。各具特色的地方立法通过衔接《数据安全法》《个人信息保护法》等上位法，既保障国家安全又促进区域数字经济发展，形成“共性底线+特色创新”的立法范式。然而，随着技术的不断发展和数据安全形势的不断变化，仍需不断完善和优化这一法律体系，以适应新的挑战和需求。同时，加强法律法规的宣传和普及工作，增强全社会的数据安全意识也是当前和未来的重要任务。

2　数据安全标准体系

2.1 数据安全标准体系基本框架与内部联系

2.1.1 整体架构与组成部分

我国数据安全标准体系涵盖多个方面，旨在全面保障数据在各个环节的安全。2015年《大数据标准化白皮书 v2.0》所提出的大数据标准体系框架，包含基础标准、技术标准、产品和平台标准、安全标准、应用和服务标准五大类别。基础标

① 此处“立法”指广义立法，即国家机关依据法定的职权和程序创制、修改、废止规范性法律文件的活动。

准为整个体系奠定总则、术语等基石；技术标准对大数据相关技术予以规范，涵盖数据治理、数据质量等核心方面；产品和平台标准针对大数据技术产品及应用平台，明确其规范要求；安全标准贯穿数据全生命周期，从数据的产生、存储、处理到销毁，防止数据被非法获取、篡改或滥用；应用和服务标准致力于规范大数据的应用场景与服务模式[2]。

随着大数据、人工智能、物联网等新技术的快速发展，数据安全面临新的威胁和挑战，要求对各个领域的安全标准体系进行新的细化构建。以数据流通安全标准体系框架为例，其包括基础标准、通用要求、技术标准、管理标准、产品与服务标准及保障能力标准6个部分。基础标准为整个体系提供统一的术语、模型和框架；通用要求从分类分级、基线要求和方法指南等方面为数据流通提供方向性指导和规范性约束；技术标准针对数据流通全生命周期安全，确立了基础设施安全、数据匿名化、风险监测等关键技术环节的标准；管理标准规范了数据流通过程中的应急处置、安全事件管理等流程；产品与服务标准聚焦于保障数据安全产品和服务的质量；保障能力标准着重评估和提升组织在数据安全流通方面的能力。

我国数据安全标准文件根据功能性质可分为数个类别，包括术语/导则、合规测评、基础设施、密码技术、行业安全、应用场景、IPDRR框架等多个类别，每个类别下又包含众多具体标准，共同构成了一个全面且层次分明的标准体系架构。例如，在术语/导则方面，GB/T 25069—2022《信息安全技术 术语》等标准对网络信息数据安全领域的相关概念进行了统一界定，为整个标准体系奠定了基础；合规测评类标准如，GB/T 22240—2020《信息安全技术 网络安全等级保护定级指南》等，为衡量组织的数据安全状况提供了依据，确保其符合相关法规和标准要求。

2.1.2 数据安全各领域相关标准体系之间的关系

数据安全标准体系可细化为多个领域的安全标准体系，各个领域之间又存在着区别和联系。如上文提及的数据流通安全标准体系更侧重于数据流动过程中的安全性，关注跨主体、跨系统、跨境流通时的法律合规性，以及数据在多个平台或系统间流动时的监控、识别和追溯。而工业和信息化部印发的《电信和互联网行业数据安全标准体系建设指南》从基础共性、关键技术、安全管理和重点领域等方面形成了电信和互联网行业的数据安全标准体系整体框架，与数据流通安全标准体系相互补充，共同构建起全面的数据安全保障体系。同时，网络信息数据安全标准体系与其他相关领域标准体系（如信息技术标准体系、通信行业标准体系等）也存在一定的关联与交叉，在实际应用中需要相互协调与配合，以确保整个数字化生态系统的安全稳定运行[3]。

在数据安全标准体系框架构建方面，我国已形成较为完善的架构，涵盖了从基础标准到应用标准的多个层次，为数据安全保障提供了全面的指导。我国数据安全相关标准由全国专业标准化技术组织和部委、协会或者集团公司组织参与制定。具体来说，全国信息安全标准化技术委员会和全国数据标准化技术委员会是负责数据安全标准制定的主要标准化技术委员会。数据安全相关标准可基本分为国家标准、行业标准、地方标准、团体标准和企业标准，其中国家标准数量较多，行业标准、地方标准、团体标准数量相对较少。对于现行数据安全相关标准的研究，本文认为基础标准已有坚实的研究基础，应当将研究重点放在应用层面的关键技术标准和管理评估标准上，才能够与数据安全标准的现实应用紧密结合。

2.2 数据安全标准体系的主要内容

数据安全标准体系的建构必须围绕数据处理的全生命周期展开，服务数据收集、存储、使用、加工、传输、提供、公开的每个环节。因此，按照标准的作用范围，我国现有的数据安全标准体系主要包括以下内容。

2.2.1 应用型关键技术标准体系

（1）数据加密与访问控制技术标准

数据加密是保障数据机密性的关键技术，相

关标准对加密算法的选择、密钥管理、加密技术应用及合规性检查等进行了规范。我国在密码领域积极推进安全标准体系建设，其国家标准已包括基础类标准、基础设施类标准、产品类标准、应用支撑类标准等。例如，GB/T 36322—2018《信息安全技术 密码设备应用接口规范》详细规定了密码设备在数据加密过程中的应用接口要求，确保加密操作的规范性和安全性。访问控制技术标准则致力于提出合理的访问控制要求和方法，确保只有授权用户才能够访问敏感数据，以此防止数据泄露和非法访问。例如，GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》明确了不同安全等级下的访问控制策略，对网络信息系统中的访问权限进行严格管理。

（2）数据匿名化与隐私保护技术标准

为保护用户隐私，数据匿名化技术标准日益受到重视。这些标准明确了隐私技术的多种方法和实施步骤，如差分隐私、数据脱敏等技术的应用标准，在数据利用与隐私保护之间寻求平衡。隐私保护技术标准包括差分隐私标准、匿名化标准、去标识化标准等，为数据处理过程中的隐私保护提供了技术指导，如GB/T 37964—2019《信息安全技术 个人信息去标识化指南》，该标准详细阐述了个人信息去标识化的原则、方法和实施流程，为数据处理者在保护用户隐私的前提下进行数据开发利用提供了操作规范。

（3）数据溯源与风险监测技术标准

数据溯源技术标准规定了对数据来源和流转过程进行记录和追踪的方法，以便在发生安全事件时能够快速定位问题源头。风险监测技术标准则着重于对数据流通环节中的风险进行实时监控和预警，及时发现潜在的安全威胁。例如，GB/T 36635—2018《信息安全技术 网络安全监测基本要求与实施指南》对网络安全监测的范围、方法、流程及监测数据的处理和分析等方面进行了规定，为网络信息数据的风险监测提供了技术依据；GB/T 31722—2015《信息技术 安全技术 信息安全风险管理》则从风险管理的角度为数据溯源和风险监测提供了整体的框架和方法，指导组织识别、评估和应对数据安全风险[4]。

2.2.2 管理与评估标准体系

（1）数据安全管理体系标准

数据安全管理体系标准规范了组织在数据安全管理方面的各项工作，包括安全策略制定、人员管理、安全培训、应急响应等。例如，GB/T 32916—2023《信息安全技术 信息安全控制评估指南》为组织评估其信息安全控制措施的有效性提供了方法和指导，有助于组织及时发现管理体系中的薄弱环节并加以改进[5]。

（2）安全评估与认证标准

安全评估标准用于衡量组织的数据安全状况，确定其是否符合相关法规和标准要求。认证标准则为组织提供了一种证明其数据安全能力的方式，增强市场信任度。信息安全评估相关国家标准包括系统类标准、产品类标准、服务类标准等，用于规范安全评估、测试与评价、检测与认证等工作。在认证标准方面，GB 42250—2022《信息安全技术 网络安全专用产品安全技术要求》对网络安全专用产品的安全性提出了明确要求。

（3）数据流通安全管理标准

在数据流通环节，管理标准确保了数据提供方、使用方、平台管理方等各参与方的行为安全可控、可追溯。行业标准和地方标准结成一张大网，共同构建安全管理标准体系。以YD/T 4241—2023《电信网和互联网数据安全评估技术实施指南》为代表的行业标准为电信和互联网领域的数据流通安全评估提供了具体的技术指导和操作方法，有助于规范数据流通行为，防范数据安全风险；地方标准DB3201/T 1040—2021《政务数据安全管理指南》则针对政务数据的流通特点，制定了相应的安全管理规范，保障政务数据在流通中的安全合规。

2.2.3 现行数据安全标准体系的审视与发展

尽管目前我国数据安全领域的标准体系研究取得了一定进展，但仍面临诸多挑战。未来数据安全标准体系将朝着更加精细化、智能化、国际化的

方向发展。随着数据安全形势的日益严峻，标准将更加注重对新兴技术和应用场景的适应性，如量子加密技术、边缘计算等。人工智能技术将被广泛应用于标准的制定、评估和监测过程中，提高标准的科学性和有效性。同时，标准体系将更加注重与法律法规的衔接，确保数据安全管理的合规性。随着数据安全相关法律法规的不断完善，标准将进一步细化和落实法律要求，为数据安全监管提供有力支持。

为应对上述挑战，我国现行数据安全标准体系的建立健全主要围绕以下重点方向：（1）加强标准制定机构之间的沟通与协作，建立统一的标准协调机制，定期对现有标准进行梳理和整合；（2）加大对新兴技术标准研究的投入，鼓励产学研用各方共同参与标准制定，提高标准的前瞻性和适应性；（3）重视对标准实施监督机制的查缺补漏，加强对标准执行情况的检查和评估，对不符合标准的行为进行及时纠正和处罚，通过建立专门的监督机构或利用第三方评估机构，对组织的数据安全标准执行情况进行监督和评估；（4）加强国际交流与合作，积极参与国际标准制定，提升我国在网络信息数据安全领域的国际话语权。通过参与国际标准制定，将我国的先进经验和技术融入国际标准中，以此掌握主动权，推动我国标准体系的不断完善[6]。

3 数据安全规范体系建设的多维困境

随着数字经济的快速发展，数据安全已成为国家安全的重要组成部分。我国虽已初步建立数据安全技术标准体系，但在体系协调性、技术适配性及执行有效性方面仍面临严峻挑战。数据安全法律规范普遍性引用①相关标准的共存模式，也限制了数据安全规范体系中规范功能的全面发挥。

3.1 标准体系碎片化带来的系统性风险

我国数据安全技术标准体系的整合协调困境集中表现为“三重复三缺失”的结构性矛盾。中国信息通信研究院发布的《数据安全标准体系研究报告（2023）》显示，现行有效的数据安全相关标准达156项，其中国家标准58项，行业标准98项，涉及33个标准化技术委员会。这种多头管理的标准化模式，导致不同部门制定的标准存在内容重复、技术指标冲突等问题。例如，GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》与JR/T 0197—2020《金融数据安全 数据安全分级指南》在加密算法应用要求上存在参数差异[7]。更深层次的矛盾在于标准体系框架的顶层设计缺失。虽然《数据安全法》确立了“国家数据安全工作协调机制”，但标准制定过程中部门利益博弈、行业特性差异等因素，导致跨领域数据安全要求的系统性整合难以实现。以医疗数据为例，其既要符合GB/T 39725—2020《信息安全技术 健康医疗数据安全指南》的匿名化处理要求，又要满足《人口健康信息管理办法（试行）》的可追溯性规定，这种技术标准的冲突直接制约了医疗大数据的开发利用。

3.2 技术迭代加速引发的标准滞后性矛盾

当前数据安全标准体系面临技术迭代加速带来的“标准有效期悖论”。国际IT咨询机构Gartner发布的《2023年数据安全技术成熟度曲线》显示，生成式AI、量子计算等前沿技术的演进周期已缩短至12~18个月，而我国标准制修订周期平均需要24个月。这种时滞性导致标准尚未发布即面临技术过时的风险。以联邦学习技术为例，虽然国内已开展相关标准预研，但2023年3月17日发布的GB/T 42452—2023《系统与软件工程 功能规模测量 COSMIC方法》在模型逆向攻击防护等方面尚未覆

① 从引用标准的方式来看，有直接引用和普遍性引用之分。参见国家标准GB/T 20000.1—2014《标准化工作指南 第1部分：标准化和相关活动的通用术语》第 13.2.3 条（普遍性引用[法律对标准的]）。

盖最新的差分隐私增强技术。其具体表现在3个方面：（1）标准预研机制缺乏前瞻性，对技术发展趋势的预判能力不足；（2）快速通道机制应用受限，现行《国家标准管理办法》规定的应急标准程序启动条件严苛；（3）企业参与度不足，头部科技企业的技术创新成果难以及时转化为标准内容。这种状况导致我国在区块链数据存证、AI模型安全检测等新兴领域持续处于标准跟随状态。

3.3 执行监督缺位导致的标准虚化困境

数据安全标准落地难的本质是治理效能的结构性缺失，这种差异折射出监管资源配置的失衡问题，现有监督体系过度依赖行政检查，未能构建多元共治格局。具体症结包括：标准符合性评估体系不健全，缺乏权威的第三方认证机构；违规成本偏低，《数据安全法》第四十五条第一款规定的最高200万元罚款与数据泄露可能造成的数亿元损失严重失衡；技术支持手段不足，监管部门难以对海量企业的标准执行情况进行动态监测。以数据出境安全评估为例，虽然GB/T 35273—2020《信息安全技术 个人信息安全规范》已对评估流程作出规定，但基层监管部门普遍缺乏专业人才和技术工具进行有效审查。

3.4 普遍性引用为主的援引模式造成的标准适用乏力

对于法律而言，标准发挥着重要的支撑作用。目前在环境保护、医药卫生、产品质量、安全生产、食品安全、工程建设、能源等领域，法律援引标准已成为十分醒目的法律现象[8]。这是因为标准与法律均具有“假定条件”和“行为模式”的构造，标准的具体性和更新及时性有助于将抽象的法律规范转换为充满细节的技术要求和技术方案，使之成为及时回应且可操作的行为指引。对于技术而言，标准发挥着重要的增效作用。尽管标准不属于我国正式法源，不具有形式上的约束力，但由于鲜明的行为导向功能和信号功能，不仅能经由法院和行政机关援引产生规范效果[9]，还能够构成行政机关判断事实认定构成要件的基准，从而拘束行政机关的决定[10]。因此，标准一方面通过“专业性术语体系部分”统一纷繁多样的技术表达和方案，另一方面通过“含有技术要求的法律文本部分”强制或指导相关领域的产品或行为，成为参照系数，以符合社会普遍期望。

基于上述紧密联系与功能互补，在数据领域，标准治理已获得我国法律明确认可，法律引用标准的情况普遍存在。引用标准的方式可分为直接引用与普遍性引用。其中，普遍性引用是指在法规中不直接、具体地引用某标准（即无标准代号、顺序号及名称等标准内容），而是指定特定机构的或具体领域内的所有标准作为引用标准的一种引用方式[11]，亦可称为间接引用[12]、指引性引用[13]。《中华人民共和国网络安全法》第十五条、《数据安全法》第十六条、《中华人民共和国个人信息保护法》第五十八条，从不同维度确立了国家建立网络安全、数据安全、个人信息保护标准体系的立法目标。总体而言，我国现行数据安全领域的法律引用标准的情况绝大部分属于普遍性引用；行政法规部分则呈现对半现象，最多一半行政法规普遍性引用标准；大部分部门规章普遍性引用标准，其中尤以国家互联网信息办公室出台的规章为主；地方性立法中绝大部分地区均普遍性引用标准，部分欠发达地区甚至并未引用。可见，普遍性引用是我国数据安全法律规范与技术标准关联构造的主要模式。以《数据安全法》第二十七条为例，其规定数据处理活动“应当依照法律、法规的规定”，但对具体技术标准仅作“符合相关标准”的笼统规定。《个人信息保护法》第五十一条要求采取“加密、去标识化等安全技术措施”，同样未指明具体技术参数。这种“宣示性”条款形成“法律定框架、标准定细则”的衔接机制。

法律与标准的衔接机制直接决定着规范体系的运行效能[14]。现有法律文本普遍采用“应符合相关技术标准要求”等普遍性引用模式，这种制度设计在实践中的结构性矛盾日益凸显。数据安全规范体系中的普遍性引用模式带来的直接后果是数据安全技术标准的适用乏力，具体表现为法律实施效能弱化、标准效力位阶错位及技术创新与

标准迭代脱节3个方面。

4 完善数据安全规范体系的应对策略

面对数据安全技术标准体系建设的现实困境，应当从系统性视角剖析现有问题，有针对性地通过增强法律条款可操作性、构建完整责任链条、促进标准体系动态发展，全面提升数据安全标准治理效能，提出具有可操作性的治理路径。在援引模式方面，则需在深入剖析现行引用模式的制度缺陷的基础上，尝试建立“直接引用为主、普遍性引用为辅”的新型模式，并构建一套系统性转型方案。

4.1 建构立体化标准治理体系

破解标准体系碎片化困局，需要构建“三维协同”的标准化治理新范式。首先在制度维度，建议建立国家数据安全标准化委员会，整合现有33个标准化技术委员会的职能，严格遵循《国家数据标准体系建设指南》的整体布局，明确标准制定权限划分与协调机制。通过建立标准冲突识别算法模型，运用自然语言处理技术对既有标准进行数字化比对，系统识别并解决技术指标矛盾。其次在技术维度，推行“核心标准+行业扩展”的模块化标准架构。参照欧盟《数据治理法案》经验，建立具有强制效力的基础性标准框架（如数据分类分级、加密算法基准），各行业在此框架下制定扩展性实施指南。以工业数据安全为例，可在《工业控制系统信息安全防护指南》要求的基础上，针对电力、制造等细分领域制定补充技术要求。最后在国际化维度，建立标准互认的动态调整机制。深度参与ISO/IEC 27000信息安全管理体系标准的制修订工作，推动我国自主可控的加密算法纳入国际标准。依托“数字丝绸之路”建设，与东盟、金砖国家等建立区域性标准互认联盟，构建具有中国特色的标准国际化路径。通过这三重维度的协同推进，可有效解决标准体系的整合协调难题。

4.2 创设敏捷化标准演进机制

构建面向未来的数据安全标准体系，需要建立“三螺旋”创新驱动机制。（1）技术预见机制创新，建议组建国家数据安全技术预见中心，运用专利地图分析、技术路线图等方法，建立新兴技术风险评估模型。例如，针对量子计算可能破解现有加密体系的风险，提前布局抗量子加密算法标准研制。（2）标准研制模式变革，推行“开源标准”新范式。借鉴Linux基金会“开放链”项目经验，建立数据安全标准开源社区，允许企业、科研机构在标准草案框架下进行技术验证与迭代优化。在自动驾驶数据安全领域，可先行试点开源标准模式，通过多方协同快速形成技术共识。（3）建立“沙盒监管”标准试验机制。在自由贸易试验区、国家数字经济创新发展试验区设立标准应用沙盒，对新制定的数据跨境流动安全标准、AI伦理治理标准等进行压力测试。例如，在上海自由贸易试验区临港新片区开展智能网联汽车数据安全标准试点，通过真实场景验证标准有效性，缩短技术成熟到标准落地的传导周期。这3个维度的创新将有效提升标准体系的技术响应能力[15]。

4.3 打造全生命周期监管生态

破解标准实施难题需要构建“四维一体”的治理新体系：第一维度是完善法治保障，建议在将来《数据安全法》修订时，在“总则”部分增加强调数据安全法律规范引用数据安全标准的条款，并专设“数据安全标准引用规则”一章，明确标准实施的刚性约束。借鉴欧盟《数字服务法案》经验，建立标准执行分级管理制度，对关键信息基础设施运营者设定强制性认证要求，对中小企业提供合规指导服务。第二维度是技术创新应用，建设国家数据安全标准智能监管平台。该平台应集成区块链存证、AI合规检查等技术，实现对标准执行情况的全流程追溯。例如，利用知识图谱技术构建标准条款数据库，自动比对企业的数据安全措施是否符合相关技术要求。在数据分类分级管理领域，可开发智能识别系统辅助企业完成数据资产盘点。第三维度是市场机制培育，发展标准认证服务产业。制定《数据安全标准认证机构管理办法》，培育具有国际公信力的第三方认证机构。在

金融、医疗等重点领域推行标准认证结果互认机制，将认证结果纳入企业信用评价体系。对通过认证的企业给予政府采购加分、税收优惠等政策激励。第四维度是能力建设提升，实施“数据安全标准官”制度。参照欧盟数据保护官（DPO）模式，在重点行业/企业设立专职标准合规岗位，建立从业人员资格认证体系。同时加强基层监管队伍的专业化建设，在省级市场监管部门设立数据安全标准执法大队，配备专业技术检测设备。通过这4个维度的协同发力，可显著提升标准实施监督效能。

4.4 建立“直接引用为主、普遍性引用为辅”的梯度引用体系

《中华人民共和国标准化法》第二条明确赋予标准“技术法规”属性[16]。直接引用模式通过立法授权实现标准效力转化，符合法律保留原则。德国《联邦数据保护法》第九条直接援引ISO/IEC 27001标准的实践表明，该模式具有法理可行性。数据安全领域的标准援引体系建设应当从现有的普遍性引用出发，以实现直接引用为目标，并兼顾考虑数据安全规范工作的专业特点，从以下3个角度推行梯度化、差异化、推进式改革：（1）基础性标准直接引用。对数据分类分级、加密算法等基础规范，直接在法律条款中列明标准代号，如规定“个人信息加密应当符合GB/T 39786—2021二级以上要求”。（2）专业性标准授权引用。在附则中授权监管部门制定标准清单，建立动态调整机制。（3）新兴领域标准预留接口。对量子加密等前沿领域，设置“符合国家规定的最新标准”等弹性条款。

此外，在配套措施方面亦应有所创新，如在《数据安全法》实施细则中设立技术标准审查专章，明确标准制定、修订的法定程序；参照美国NIST SP 800–53模式，建立标准分级引用目录，区分强制性标准与推荐性标准[17]；借鉴欧盟标准化委员会（CEN）经验，设定年度标准复审周期，确保法律引用的标准版本时效性等。再如，对现行数据安全相关标准进行合规性审查，开展标准法律适用性评估，确定可直接引用的标准清单；在《网络数据安全管理条例》修订中，增设标准直接引用示范条款；设立跨部门技术标准协调委员会，解决标准交叉引用产生的规范冲突。

值得注意的是，为防控标准滞后性风险，还应配套建立“标准版本动态标注”制度，在法律引用条款中注明“现行有效版本”，授权标准化行政主管部门定期更新版本信息。同时设置标准紧急修订程序，对重大技术变革建立绿色通道。同时，须建立标准体系顶层设计机制，按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的要求规范标准制定程序，实施标准间协调性审查，避免标准交叉重复。

5　结 语

数据安全规范体系的建设与完善是一项包含技术标准体系与法律规范体系在内，围绕标准与法律的完善及二者的融合展开的系统性工作。数据安全技术标准体系的完善是一个动态演进的过程，需要制度创新与技术赋能的深度融合。通过构建系统化的整合机制、敏捷化的创新机制、立体化的实施机制，不仅能有效解决现有标准体系的三大核心问题，更为数字中国建设提供坚实的技术规则保障。未来研究可进一步关注标准体系与法律规范的互动模式创新，探索建立技术标准法律地位动态调整机制，推动形成具有中国特色的数据治理现代化方案，构建新型法律标准引用模式则是完善数据安全治理体系的关键制度创新。通过建立以直接引用为主的新型范式，不仅能够提升法律规范的系统性、操作性和时效性，更有利于形成法律与标准协同共治的现代化治理格局。这需要立法机关、标准化组织、产业主体等多方协同，在法治框架下推进技术标准与法律制度的深度融合，为数字中国建设提供坚实的制度保障。

参考文献

[1] 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.

[2] 中国电子技术标准化研究院. 《大数据标准化白皮书v2.0》发布大数据标准体系框架 [J]. 中国标准导报, 2016 (1):9–10.

[3] 工信部印发《电信和互联网行业数据安全标准体系建设指南》[J].自动化博览, 2021(1): 7.

[4] 王威等.数据流通安全标准化研究[J].大数据,2024(6): 92–106.

[5] 上官晓丽, 王秉政. 网络安全国家标准体系建设研究[J].信息技术与标准化, 2021(5):7–10.

[6] 黄亦宁. 国际法视角下我国网络空间法律法规完善策略[J].网络安全和信息化, 2024(9):5–7.

[7] 陈海航. 金融科技企业数据治理中的技术标准及其效力[J].金融法苑, 2022(6):79–87.

[8] 柳经纬. 论标准对法律的支撑作用[J].厦门大学学报（哲学社会科学版）, 2020(6):152–162.

[9] 许可.《个人信息安全规范》的效力与功能[J]. 中国信息安全, 2019(3):44–47.

[10] 宋华琳. 论技术标准的法律性质:从行政法规范体系角度的定位[J]. 行政法学研究, 2008(3):36–42.

[11] 崔晓军, 汪开斌, 黄潇, 等. 气象法规引用标准研究[J]. 标准科学, 2024(5):47–53.

[12] 柳经纬. 法律引用标准的三重意义[J]. 电子知识产权, 2023(6):4–15.

[13] 王永. 燃气报警器安装：法律法规、政策措施与标准[J].标准科学, 2023(5):31–36.

[14] 许可. 数据交易流通的三元治理：技术、标准与法律[J]. 吉首大学学报（社会科学版）, 2022(1):96–105.

[15] 范志勇. 论金融监管者的数据安全保护义务[J]. 行政法学研究, 2022(3):135–154.

[16] 许林波, 柳经纬. 技术法规的规范性及其实现路径[J]. 甘肃社会科学, 2024(5):175–187.

[17] 程方正, 彭飞荣. 可信人工智能标准体系建设研究[J]. 标准科学, 2023(9):9–23.