信息化建设中大数据安全治理体系的构建与实践路径

张　洋[1]　张贵春[2]
1. 天津市数据发展中心　天津　300221
2. 天津市水文水资源管理中心　天津　300211

摘　要：本文聚焦信息化建设中的大数据安全治理体系构建与实践路径。阐述了大数据安全治理内涵、原则与典型框架，分析信息化建设面临的数据分散、跨部门协同及新兴技术风险等挑战。设计了“一核两翼、三层联动”的治理架构，涵盖分类分级管理、策略标准制定、技术防护体系构建。最后提出规划、体系化建设、持续优化三阶段实践路径，旨在为信息化建设提供可借鉴的大数据安全治理方案，保障数据安全与价值释放。

关键词：信息化建设；大数据安全；治理体系

引言：在信息化浪潮下，大数据成为关键资产，其安全治理至关重要。然而，随着信息化项目的建设，日益暴露出数据权属不清、跨部门协同困难、新兴技术应用风险等问题，给数据安全治理带来巨大挑战。当前国际国内虽已形成一些数据安全治理框架，但在信息化建设复杂场景下，仍需进一步探索适配的治理体系与实践路径。本文将深入剖析大数据安全治理的理论基础与核心挑战，设计治理体系框架，并提出具体实践路径，为信息化建设中的数据安全保障提供有益参考。

1 大数据安全治理的理论基础与核心挑战

1.1 大数据安全治理的内涵与原则

大数据安全治理的内涵是指在数字经济发展背景下，通过制度设计、技术支撑、机制创新等手段，对数据全生命周期（采集、存储、传输、使用、共享、销毁）进行系统性管控，以实现数据安全、隐私保护与数据价值最大化的动态平衡。其核心要义在于打破“重技术轻管理”“重事后轻事前”的传统模式，构建技术、管理、法律、伦理多维度协同的治理生态。治理原则主要包括：一是合法性原则，严格遵循数据安全法、个人信息保护法等法律法规，确保数据处理活动有法可依、合规开展；二是最小必要原则，数据采集、使用以实现特定目的为限，避免过度收集、冗余存储；三是权责对等原则，明确数据处理各参与方的安全责任，做到有权必有责、失职必追责；四是动态适配原则，针对数据类型、应用场景、技术发展的变化，及时调整治理策略与防护措施，确保治理有效性与适应性。

1.2 数据安全治理的典型框架

当前国际国内已形成一批有代表性的数据安全治理框架，为实践提供重要参考。国际上，NIST数据安全框架（DSF）以“识别-保护-检测-响应-恢复”为核心流程，强调风险驱动与灵活适配，适用于各类组织构建安全治理体系；ISO/IEC 27001系列标准聚焦信息安全管理体系的建立、实施与改进，提供标准化、系统化方法论。国内方面，《网络数据安全管理条例》提出“分类分级保护、全流程管控、风险导向”框架，明确不同级别数据保护要求与责任主体；《工业数据安全管理办法》针对工业领域构建治理体系，突出工业数据特殊性及保障需求[1]。此外，行业层面也有特色框架，如金融、医疗行业，均体现“共性与个性结合、技术与规范协同”思路，为不同领域数据安全治理提供可落地路径。

2 信息化建设中的核心挑战

2.1 数据权属管理复杂

2024年初，随着数据部门机构改革和调整，区域内政务信息化项目建设工作多由当地数据管理部门统筹负责，系统多集中构建在政务云、数据相对集中存储，但数据层面问题依然复杂。一方面，“数出多家”现象普遍，如水雨情数据由水文、气象等部门分别提供；另一方面，因数据确权、利益分配及数据准确性等因素，数源部门不愿共享数据，不同应用场景下建设的系统，数据困于各部门系统，政务数据公用价值难以发挥。另外，政务信息系统使用与运行管理部门独立，从各自管理角度出发，摸清数据底数的积极性主动性不足，导致数据底数难以明晰。权限管理上，信息化建设多端访问特征凸显，管理难度大增。传统模式难适配复杂场景，存在分配粗放、回收不及时、越权防控不足等问题。构建“细粒度、动态化、可追溯”的体系是关键。

2.2 跨部门协同与责任界定困难

信息化建设中，数据跨部门流动共享是释放价值的关键，但协同不畅与责任界定模糊制约着数据安全治理。一方面，虽采取集约化建设、搭建共享机制，可各

部门利益诉求不同，数据共享主动性不足；且数据规范标准未统一，数据流转效率低，格式与质量问题多，治理难度增大[2]。另一方面，跨部门数据处理主体多，虽有制度划定责任边界，但实际执行中仍存在界定不明，易现“责任真空”“多头管理”，如数据泄露问题发生时责任难精准界定。此外，部门利益诉求差异、沟通机制不健全，也加剧了协同治理难度，让安全治理政策难落地。

2.3 新兴技术带来的新风险

AI、云计算等新兴技术广泛应用，提升数据处理效率的同时也带来新安全风险。云计算方面，数据集中存储与虚拟化部署使风险集中，云服务商出现安全漏洞或管理问题，易引发大规模数据泄露；“云原生”技术扩大攻击面，数据所有权与管理权分离，让数据主权与责任界定更复杂。人工智能领域，AI大模型运用存在诸多隐患：缺乏数据安全规范标准，训练数据无统一安全指引；数据保密安全意识弱，“投喂”数据无明确边界与管控，易泄露敏感数据；AI衍生数据可能臆造，脏数据增多，生成式AI还加剧技术滥用，且算法黑箱特性使风险难预判，算法偏见引发数据安全与伦理风险。

3 大数据安全治理体系框架设计

3.1 总体架构设计

大数据安全治理总体架构秉持“一核两翼、三层联动”思路，以“数据安全风险管控”为核，“管理体系”与“技术体系”为两翼，搭建“战略层-执行层-支撑层”联动架构。战略层负责顶层设计，由组织最高决策机构牵头，明确治理的战略目标、原则、架构与分工，制定总体规划与路线图，使其契合组织发展战略；建立跨部门协调联动组织，重点解决“数出多家”“共享梗阻”及部门协同难题，打破“部门壁垒”。执行层是核心实施环节，涵盖数据分类分级、权限管理等具体工作，针对数据底数不明、权限管理粗放等问题，通过制定管理规范、流程与标准，将战略层规划转化为可落地举措。支撑层提供基础保障，包含技术支撑平台、制度保障体系和人才队伍建设，同步强化数据确权、利益分配等配套机制研究，保障执行层工作高效开展。

3.2 数据分类分级管理机制

数据分类分级管理是大数据安全治理的基础与核心，其核心目标是根据数据的重要程度、敏感级别与业务价值，实施差异化的安全保护措施，实现“精准防控、高效治理”。针对“数出多家”导致的数据口径混乱问题，数据分类需遵循“科学性、实用性、兼容性”原则，结合组织业务特点，统一分类标准，将数据划分为核心业务数据、敏感个人信息、一般业务数据、公开信息等类别。数据分级则依据数据泄露、篡改、滥用可能造成的危害程度，将数据划分为不同级别，明确各级数据的安全保护要求与管控措施。为确保分类分级的有效性，需建立“动态调整”机制，定期对数据类别与级别进行复核，根据业务发展、法律法规变化等情况及时更新；搭建数据分类分级管理平台，实现数据资产自动化盘点、底数清晰化管理，完成分类标注、分级管控，确保分类分级结果在数据全生命周期中得到有效应用，为权限分配、安全防护、审计监督等提供依据。

3.3 安全策略与标准制定

安全策略与标准是大数据安全治理的制度保障，要围绕数据全生命周期，构建“全面覆盖、科学合理、可操作执行”的体系。需明确治理总体目标、原则、架构与分工，制定各环节安全管理策略。针对数据共享意愿低、责任界定模糊问题，建立共享审核机制，明确共享条件、范围、责任及利益协调规则；数据销毁环节制定规范流程，防止残留泄露[3]。结合行业与技术趋势，制定技术、管理、评估等标准。技术标准涵盖数据加密、身份认证等，确保防护统一兼容；管理标准补充数据底数核查、权限全生命周期管理细则，明确岗位安全职责与操作要求；评估标准用于风险与治理效果评估，为优化策略、改进措施提供依据。此外，安全策略与标准要衔接法律法规，兼顾灵活性与适应性，为新技术、新场景预留调整空间。

3.4 技术防护体系构建

技术防护体系是大数据安全治理的核心支撑，需构建“纵深防御、智能联动、全流程覆盖”的矩阵，针对数据全生命周期部署防护技术与工具。数据采集时，运用数据脱敏、隐私计算保护隐私，部署安全网关监控审计采集来源与行为，解决多部门数据采集口径适配问题。数据存储采用加密存储、访问控制等技术，按分级结果实施差异化防护。数据传输借助加密传输、VPN等保障保密性与完整性，部署安全网关校验监控跨网络传输。数据使用采取动态权限管理等技术防越权滥用，针对多端访问强化动态验证。另外，构建数据安全态势感知平台，整合安全数据，用AI算法分析预警，实现安全事件快速响应处置，重点监测数据共享、多端访问等高危场景，提升智能化水平。

4 大数据安全治理的实践路径

4.1 阶段一：规划与顶层设计

规划与顶层设计是大数据安全治理的基础阶段，核心目标是明确治理方向、理清治理思路、制定实施蓝

图。首先，开展全面的现状调研与风险评估，梳理组织的数据资产（包括数据类型、存储位置、使用场景等），识别数据全生命周期各环节的安全风险点，分析现有安全治理体系的短板与不足（如制度缺失、技术落后、责任不清等）；同时调研行业最佳实践与法律法规要求，明确治理的合规底线与目标要求。其次，制定顶层设计方案，明确数据安全治理的战略目标（如“三年内建成完善的大数据安全治理体系，实现数据安全风险可控、合规达标”）、基本原则、组织架构（如成立数据安全治理机构，明确部门职责分工）、治理范围与边界。最后，制定详细的实施规划与路线图，将治理目标分解为具体任务，明确各任务的责任主体、实施步骤、时间节点与考核指标。此外，加强内部宣贯与培训，提高部门对数据安全治理的重视程度，统一思想，为后续阶段的工作开展奠定基础。

4.2 阶段二：体系化建设与工具落地

体系化建设与工具落地是大数据安全治理的核心实施阶段，需按照顶层设计方案，全面推进制度、技术和组织体系的建设与落地。在制度建设方面，出台对应场景数据分类分级管理办法、权限管理规范、数据共享安全规则、应急响应预案等一系列管理制度与标准规范，形成完善的制度体系，并组织全员培训，确保制度得到有效执行。在技术建设方面，部署数据安全态势感知平台、权限管理系统、数据加密工具、数据防泄漏系统、数据库审计系统等关键技术防护工具，构建“纵深防御”的技术体系；推进技术工具的集成与联动，实现安全数据的共享与协同响应，提升技术防护的智能化水平。在组织建设方面，完善数据安全治理组织架构，明确各部门、各岗位的安全责任，建立跨部门协同工作机制，确保治理工作高效推进。开展试点应用与效果验证，选择部分业务场景进行治理体系试点，及时发现问题并优化调整；例如，在跨部门数据共享场景中试点数据分类分级管控与隐私计算技术应用，验证制度与技术的可行性与有效性，为全面推广奠定基础。

4.3 阶段三：持续优化与能力提升

持续优化与能力提升是大数据安全治理的长期阶段，核心目标是适应内外部环境变化，不断提升治理体系的有效性与适应性。首先，建立常态化的监测评估机制，定期开展数据安全风险评估、治理效果评估与合规性审计，通过量化指标（如安全事件发生率、漏洞修复率等）衡量治理成效，识别存在的问题与改进空间[4]。其次，根据评估结果与内外部环境变化（如业务扩展、新技术应用、法律法规更新等），及时优化治理策略、制度标准与技术防护措施；例如，针对AI技术带来的新风险，补充AI模型安全管理规范，部署AI安全检测工具；针对新出台的法律法规要求，修订数据共享与隐私保护相关制度。最后，加强人才队伍建设与文化培育，通过专业培训、技能竞赛、案例分享等方式，提升相关人员的数据安全意识与专业能力；同时，培育“全员参与、全员负责”的数据安全文化，将数据安全理念融入日常工作，形成“人人重视数据安全、人人参与数据安全”的良好氛围。通过持续优化与能力提升，推动大数据安全治理体系不断完善，实现数据安全治理的长效化、常态化。

结束语

信息化建设中的大数据安全治理是一项长期且复杂的系统工程。本文构建的“一核两翼、三层联动”治理架构及提出的实践路径，为应对信息化建设中的数据安全挑战提供了系统性方案。通过规划、体系化建设与持续优化三阶段推进，逐步提升数据安全治理能力。未来，随着技术与业务发展，需不断探索创新，完善治理体系，以适应新变化，保障数据安全，推动信息化建设健康发展。

参考文献

[1]张美鸥,张旭俊,张丽娅.大数据安全治理体系实践探索[J].网络安全技术与应用,2025(7):74-76.

[2]姜涛,李浩鑫.基于精准治理的大数据安全治理体系创新研究[J].中国高新科技,2021(23):45-46.

[3]赵程遥,邹任芯,王高开,等.政府公共数据平台数据安全治理体系研究[J].现代信息科技,2025,9(17):137-142.

[4]周依曼.企业数据安全治理现状及治理体系研究[J].科技创业月刊，2024，37(5):170-173.