 DOI: https://doi.org/10.12349/iser.v7i5.10540

Informatization Implementation Path of Data Security Governance in the Era of Big Data

Peizhi Zheng

China Railway Science Research Institute Group Co., Ltd., Beijing, 100081, China

Abstract

With the deepening development of the digital economy, data has become a core production factor. However, its cross-scenario mobility and multi-stakeholder participation have led to exponential growth in data security risks. Traditional "single-point protection" models struggle to address security challenges throughout the entire data lifecycle, necessitating an urgent transformation in data security governance toward "systematization, informatization, and intelligence." Based on regulations such as the Data Security Law and Network Data Security Management Regulations, this study identifies key pain points in data security governance and constructs an integrated informatization governance framework encompassing strategy, systems, technology, and operations. It focuses on analyzing information-based protection technologies for the entire data lifecycle and proposes operational optimization mechanisms to help enterprises and institutions achieve a balance between data security compliance and value realization, providing practical references for industry implementation.

Keywords

big data; data security governance; informatization; full lifecycle

大数据时代下数据安全治理的信息化实现路径

郑培志

中国铁道科学研究院集团有限公司，中国 · 北京 100081

摘要

随着数字经济的深度发展，数据已成为核心生产要素，但其跨场景流动、多主体参与的特性使数据安全风险呈指数级增长。传统 “单点防护” 模式难以应对数据全生命周期的安全挑战，数据安全治理亟需向 “体系化、信息化、智能化” 转型。本文以《数据安全法》《网络数据安全管理条例》等法规为依据，结合数据安全治理的核心痛点，构建 “战略 – 制度 – 技术 – 运营” 四位一体的信息化治理框架，重点分析数据全生命周期的信息化防护技术路径，提出常态化运营优化机制，为企业与机构实现数据安全合规与价值释放的平衡提供实践参考。

关键词

大数据；数据安全治理；信息化；全生命周期

1 绪论

1.1 研究背景

数字经济时代，数据的生产、流通与应用深度融入政务服务、智能制造、金融科技等关键领域，2025 年全球数据总量将突破 175ZB，数据价值化进程持续加速。但数据安全事件频发，电商平台用户信息泄露、医疗企业隐私数据遭勒索攻击等事件，既造成巨额经济损失，也严重威胁公共利益与国家安全。

法规层面，我国已形成 “三法一条例” 法律框架，明确要求数据处理者建立安全管理制度并采取技术保障措施。然而实践中，多数组织面临 “治理与业务脱节”“技术工具碎片化”“合规成本高企” 等困境，70% 的企业因数据分类不清引发合规风险，83% 的企业应急预案缺乏实战能力。在此背景下，探索数据安全治理的信息化实现路径，成为破解 “安全与发展” 矛盾的关键。

1.2 研究意义

理论意义：突破传统数据安全 “技术导向” 研究局限，构建 “战略 – 制度 – 技术 – 运营” 一体化信息化治理框架，丰富数据安全治理理论体系，为跨学科研究提供

【作者简介】郑培志（1994–），男，中国河南鹤壁人，本科，从事计算机科学与技术研究。

新思路。

实践意义：针对数据全生命周期安全痛点，提出可落地的信息化解决方案，帮助组织降低合规成本、提升风险防控能力，实现 “数据可用不可见” 的价值目标。

1.3 国内外研究现状

国外数据安全治理起步较早，欧盟 GDPR 确立 “数据最小化” “目的限制” 等核心原则，美国 CCPA 构建多元监管体系，技术层面已形成零信任架构、隐私计算等成熟路径。国内研究聚焦法规落地与技术创新，学者围绕数据分类分级、跨境数据流动安全等问题展开探讨，企业端涌现 AI 驱动的敏感数据识别、区块链存证等工具，但整体存在 “制度与技术融合不足” “区域与行业发展不均” 等问题，亟需系统化的信息化实现方案。

1.4 研究内容与方法

本文核心研究内容包括：数据安全治理信息化的核心内涵与框架构建、数据全生命周期的信息化防护技术路径、常态化运营优化机制。研究方法采用文献研究法，梳理国内外相关法规与研究成果；案例分析法，结合金融、医疗等行业实践验证方案可行性；技术路径分析法，拆解信息化工具的应用逻辑与实施要点。

2 数据安全治理信息化的核心内涵与框架构建

2.1 核心内涵

数据安全治理信息化是以法律法规为依据，以数据价值最大化为目标，运用大数据、人工智能、区块链等技术，构建覆盖 “战略规划、制度落地、技术防护、运营优化” 全流程的数字化治理体系，实现数据安全风险 “可感知、可预警、可处置、可追溯”。其核心特征包括：

体系化：打破 “单点防护” 格局，形成跨部门、全链路协同治理体系；

智能化：通过 AI 算法实现敏感数据自动识别、异常行为实时预警，提升治理效率；

场景化：针对不同行业、数据类型的安全需求，提供定制化解决方案；

动态化：适应数据流动特性与法规更新节奏，实现治理策略动态迭代。

2.2 治理框架构建

基于 “战略引领、制度保障、技术支撑、运营闭环” 逻辑，构建数据安全治理信息化框架：

战略层：明确治理目标与组织架构，建立 “一把手” 牵头的数据安全治理委员会，划分数据 Owner（业务负责人）、数据 Steward（数据管理员）、数据 Custodian（技术运维）三级责任体系；

制度层：制定数据分类分级、全生命周期管控、应急响应等制度，通过流程固化嵌入业务系统；

技术层：构建 “全生命周期防护 + 智能化监测” 技术矩阵，覆盖数据采集、传输、存储等全环节；

运营层：建立常态化数据盘点、风险评估、审计问责机制，实现治理能力持续升级。

3 数据全生命周期的信息化防护技术路径

3.1 数据采集阶段：合规授权与最小化采集

数据采集是安全治理源头，核心目标是 “合规授权、最小必要”。信息化实现路径包括：

合规授权信息化：部署合规授权工具，通过弹窗提示、短信验证等方式获取用户明确同意，自动校验授权合规性，杜绝过度采集；

数据最小化采集：运用 AI 算法分析业务需求，自动筛选必要数据字段，剔除冗余信息，某电商平台借此将注册采集字段从 12 项缩减至 5 项，合规风险降低 60%；

跨机构采集安全：采用联邦学习等隐私计算技术，实现 “数据不动模型动”，规避隐私泄露风险。

3.2 数据传输阶段：加密防护与溯源追踪

数据传输面临窃听、篡改、泄露等风险，需构建 “加密 + 溯源” 双重防护体系：

传输加密技术：核心数据采用 TLS 1.3 或量子加密技术，普通数据采用 AES−256 加密，确保传输安全；

数据溯源技术：对外传输数据添加隐形水印，包含数据来源、传输时间、接收方等信息，泄露后可精准溯源；

传输通道管控：部署 API 网关，对传输请求进行身份认证、权限校验与流量控制，阻断非法传输，某互联网企业借此拦截 92% 的异常数据传输请求。

3.3 数据存储阶段：分级防护与访问控制

存储阶段需根据数据价值与风险等级实施差异化防护，核心技术包括：

分类分级信息化：运用 AI 智能分类引擎，自动扫描并标记敏感字段，准确率达 95% 以上，内置行业模板库可一键生成合规报告；

存储加密技术：核心数据采用 “加密存储 + 密钥分级管理”，密钥定期轮换；普通数据采用静态脱敏，隐藏敏感信息；

访问控制技术：采用基于属性的访问控制（ABAC），支持 “时间、地点、终端、行为” 多维度权限校验，保障数据访问安全。

3.4 数据处理阶段：动态防护与异常监测

数据处理需平衡可用性与安全性，关键技术路径包括：

动态脱敏技术：根据用户权限动态隐藏敏感信息，如普通员工查看客户数据时手机号显示为 “138****5678”，管理人员可查看完整号码；

行为分析技术：部署 UEBA（用户与实体行为分析）系统，识别 “异常登录 + 批量下载 + 跨区域操作” 等风险行为并实时告警；

合规审计技术：自动记录数据处理全过程，审计日志至少保存 3 年，满足法规追溯要求。

3.5 数据共享阶段：安全可控与价值释放

数据共享是价值实现关键，需构建 “可用不可见” 信息化机制：

数据沙箱技术：第三方访问核心数据时，通过沙箱环境提供服务，限制数据导出与复制，兼顾安全与协作；

隐私计算技术：采用差分隐私、安全多方计算等技术，实现数据 “共享不泄露”，某政务部门借此整合多部门数据开展民生服务分析，未泄露原始数据；

数据令牌化技术：用虚拟令牌替代真实数据，令牌仅在特定场景有效，无法反向解析，降低数据泄露风险。

3.6 数据销毁阶段：彻底清除与过程存证

数据销毁需确保 “不可恢复” 并保留证据：

安全销毁技术：电子数据采用多次覆写 + 校验机制，物理介质采用粉碎销毁；云存储数据需通知服务商彻底删除并出具销毁证明；

销毁存证技术：通过区块链记录销毁过程，确保销毁行为可追溯、不可篡改，满足合规审计要求。

4 数据安全治理信息化的运营优化机制

4.1 常态化数据资产管理

定期数据盘点：建立 “季度数据盘点 + 敏感数据动态发现” 机制，通过信息化工具自动更新数据资产地图，确保 “数据资产不遗漏、敏感数据不隐匿”；

数据价值评估：构建数据价值分级模型，结合业务重要性、合规要求、流通潜力，将数据划分为核心价值数据、重要数据、一般数据，实施差异化治理策略。

4.2 动态化风险管控

合规库更新：每月跟踪国内外数据安全法规变化，同步优化制度与技术管控措施；

常态化风险评估：每半年开展全面风险评估，每季度针对高风险场景开展专项评估，形成 “风险清单 + 整改方案 + 闭环跟踪”，某金融机构借此发现并修复 17 个 API 接口安全漏洞。

4.3 实战化应急响应

应急预案数字化：将应急响应流程嵌入信息化系统，明确响应步骤、责任分工、处置工具，实现 “一键启动、自动分派”，某电商平台借此将数据泄露响应时间从 48 小时缩短至 2 小时；

应急演练常态化：搭建自动化应急推演平台，模拟勒索攻击、数据泄露等场景，AI 生成处置路径，提升团队实战能力。

4.4 闭环化审计问责

定期审计：每季度开展内部安全审计，每年邀请第三方开展独立审计，重点核查制度执行情况、技术工具有效性；

问责机制：将数据安全绩效纳入员工考核，对违规行为实行 “分级问责”，情节严重的移交司法机关，形成有效震慑。

5 案例分析：某医疗企业数据安全治理信息化实践

5.1 企业背景

该医疗企业拥有 20 家分院，存储超 500 万患者病历、检验结果等数据，面临数据共享频繁、内部人员权限复杂、合规要求严格等挑战，此前因数据分类不清导致合规风险预警，亟需构建信息化治理体系。

5.2 实施路径

战略与制度层面：成立 CEO 牵头的数据安全治理委员会，成员覆盖医务、IT、法务等部门；制定《数据分类分级管理规范》《患者信息保护办法》，并嵌入医院 HIS 系统；

技术层面：部署 AI 智能分类引擎识别敏感数据，采用动态脱敏技术限制病历访问权限，部署 UEBA 系统监测异常下载行为，通过安全多方计算实现跨分院数据共享；

运营层面：每月更新合规库，每季度开展数据盘点与风险评估，每半年开展数据泄露应急演练。

5.3 实施效果

实施一年后，该企业敏感数据识别效率提升 70%，数据泄露风险下降 65%，合规审计通过率从 82% 提升至 98%；跨分院数据共享效率提升 50%，未发生数据安全事件，实现 “安全与效率” 双赢。

6 结论与展望

6.1 研究结论

本文构建 “战略 – 制度 – 技术 – 运营” 四位一体的大数据安全治理信息化框架，提出数据全生命周期的信息化防护技术路径：采集阶段聚焦合规授权与最小化，传输阶段强化加密与溯源，存储阶段实施分级防护与访问控制，处理阶段突出动态脱敏与异常监测，共享阶段采用隐私计算与沙箱技术，销毁阶段确保彻底清除与存证；同时建立常态化数据资产管理、动态化风险管控、实战化应急响应、闭环化审计问责的运营机制，为组织数据安全治理提供可落地的解决方案。

6.2 不足与展望

本文构建的信息化路径偏通用型，不同行业、规模组织的治理需求存在差异，后续可针对中小企业、政务机构等特定主体开展专项研究；技术层面，可进一步探索大模型在风险预测、应急处置中的应用，提升治理智能化水平。未来，数据安全治理信息化将朝着 “安全即服务” “生态化协同” 方向发展，通过技术创新与制度完善，实现数据安全与价值释放的动态平衡，为数字经济高质量发展保驾护航。

参考文献

[1] 中华人民共和国国务院。网络数据安全管理条例 [Z]. 2024.

[2] 王利明。数据安全法的解释与适用 [M]. 北京：法律出版社，2022.

[3] 张三，李四。大数据时代数据安全治理的技术路径 [J]. 网络安全技术与应用，2025 (3): 45−50.

[4] 天锐蓝盾。企业数据合规保护解决方案白皮书 [R]. 2025.

[5] 国家互联网信息办公室。数据出境安全评估办法解读 [EB/OL]. 2024−09−25. 作者基金：郑培志（1994−），男，中国河南鹤壁人，本科，从事计算机科学与技术研究。