数字化时代的数据安全与隐私保护困境如何破局

本文从网络安全角度，深入分析数据安全与隐私保护的痛点问题，并探讨如何通过数据安全防护体系建设和隐私保护体系管理手段，筑牢安全隐私防线。

文丨**薛涵予** 赛迪顾问网络与数据安全研究中心

在数字化转型纵深推进的背景下，个人信息安全事件呈现高发态势，持续引发社会对隐私保护的深度关切。中央广播电视总台“3·15”晚会专项调查揭露的“大数据营销”黑产链，暴露出不法分子通过自动化爬虫、AI 画像等非法手段构建公民信息数据库的产业化犯罪特征。与之形成共振的“开盒”事件，更凸显出网络暴力与精准诈骗交织的新型安全威胁，使公众深刻认识到隐私泄露已从潜在风险演化为具象化社会危害。

数据安全与隐私防护的重要性

数据安全与隐私保护构成数字化时代信息治理的两大支柱，两者在目标导向与技术路径上既存在本质差异又形成深度协同。数据安全着眼于数据全生命周期的系统性防护，通过加密算法、访问控制、冗余备份等技术手段，确保数据在产生、传输、存储、使用及销毁过程中的保密性、完整性与可用性，其核心在于构建抵御内外部威胁的防御体系；隐私保护则聚焦于个人信息主体的权利实现，强调个体对数据收集、使用、共享等环节的知情权与控制权，本质是在数据价值挖掘与个人权益保障间建立动态平衡。

数据安全与隐私防护是数字社会稳健运行的基石，其重要性贯穿于个人权益保障、企业竞争力维系、国家安全维

护三大维度。在个人层面，数据资源中蕴藏着身份特征、行为轨迹等敏感信息，其全生命周期管理直接关联公民人格尊严与财产权益，数据安全防护体系的构建已成为守护公民数字人权的必然选择。对企业而言，数据资产既是驱动智能决策的核心要素，更是构筑商业护城河的关键载体，从客户画像到生产工艺参数，任何环节的数据泄露都可能导致市场优势瓦解与经营风险失控。上升到国家战略高度，涉及国家命脉的关键基础设施运行数据、重大科研项目核心数据的安全防护，更是直接关系到社会治理效能与数字主权的完整性。

我国数据安全与隐私保护面临的痛点与难点

当前，我国数据安全治理面临数据安全外部威胁升级与隐私保护内生风险交织的双重挑战。外部智能化攻击手段不断升级，传统防护体系难以应对 AI 驱动的勒索攻击、数据窃取等新型威胁；内部治理存在数据滥用、权限混乱、流程失控等管理漏洞，加剧了隐私泄露风险。

从外部技术安全挑战看，现有防护体系存在技术迭代、管理适配、能力建设方面的系统性短板，难以有效应对复杂多变的攻防态势，我国数据安全防护面临多重压力。一是网络攻击手段持续智能化升级，勒索病毒、钓鱼攻击等新型威胁利用人工智能技术实现精准突破，直接威胁企业核心系统和敏感数据安全。二是技术防护与管理体系存在结构性脱节。企业现有安全管理制度多停留在原则性规范层面，缺乏与数据分类分级相适配的技术实施指南，导致加密策略、访问控制等安全措施在实际业务场景中执行偏差。三是核心技术能力尚未形成突破性优势。数据安全产品同质化严重，在关键技术领域缺乏自主可控的解决方案，难以满足新型数字场景防护需求。安全服务能力仍以基础运维为主，在风险评估、应急响应等高端服务环节存在专业人才缺口，制约整体防护效能提升。

从内部管理保护层面审视，隐私治理面临系统性难题。一是数据采集使用边界模糊，导致过度收集、违规共享等问题频发，用户知情同意机制往往流于形式化操作。二是数据共享链条缺乏全流程监控，二次使用场景超出授权范围的现象普遍存在。三是企业内部权限管理粗放、员工操作行为失范、数据生命周期管控缺位等内生性风险叠加，进一步削弱了防护效能。破解这些困境需构建法律规范、技术手段与管理机制的三维治理框架，通过细化数据权属规则、优化隐私保护技术、强化全流程审计追溯，实现数据价值释放与安全的动态平衡。

针对数据安全与隐私保护建设的几点建议

在应对数据安全与隐私保护的复杂挑战时，需构建多维协同的治理体系。从监管层面来看，建议国家加强数据安全治理机制建设，构建多方协同治理体系。一是进一步完善法律法规，对人工智能、物联网等新技术衍生的风险场景进行法律适配性修订，确保法律体系与

来源：赛迪顾问

图 1 数据全生命周期防护流转图

技术创新同步演进。二是构建动态化标准更新机制。分行业制定数据安全实施标准，针对金融、医疗、政务等关键信息基础设施领域，明确数据采集、存储、传输、销毁全流程的技术规范与操作标准。三是健全全链条应急响应机制。构建“国家－行业－企业”三级联动的应急体系，建立常态化攻防演练机制，制定标准化应急处置流程。

从技术防控层面来看，建议企业强化数据全生命周期加密防护，加快数据安全技术的研发。一是以数据全生命周期为核心的思路来实现数据安全的全方位治理。目前数据的共享交换已经变成跨部门、跨层级间流动的常态化过程，所以构建以数据流转为视角的数据全生命周期防护的治理体系，保障数据价值的最大实现。二是推进前沿安全技术融合创新。重点突破抗量子密码算法、隐私计算等基础技术瓶颈，加速安全大模型等新型防御工具的研发迭代。推动量子通信技术与传统加密体系有机融合，构建面向未来十年的安全技术储备。同步探索人工智能在威胁情报分析、风险预测等场景的深度应用，形成技术演进与安全需求的双向驱动机制。

在构建数据隐私保护体系过程中，需形成国家主导、企业管控与个人参与的治理路径。一是建议国家层面加强数据隐私监管力度，建立健全数据隐私保护的监管体系，明确监管主体和职责，加强对数据处理活动的监督检查。强化执法检查与阶梯式惩戒措施，提升违法成本，并建立社会协同治理机制，畅通公众监督与维权渠道，系统性完善数据隐私治理体系。二是企业层面需建立权责明晰的主体责任体系。通过划定数据控制者与处理者的权责边界，实施数据处理权限动态分级管控机制。三是个人层面应强化数据主权意识，建立主动防护习惯。用户应系统掌握数据权益边界，通过定期审查应用权限设置、关闭非必要数据采集功能、识别诱导性隐私条款等行为，构筑防护第一道防线。对位置信息、通讯录等敏感权限实施分级动态管控，避免过度暴露个人信息维度。

责任编辑：杜玢翰　投稿邮箱 zhouhl@staff.ccidnet.com