大数据时代下信息安全的风险管理研究

李　雅
中国电子科技集团公司第二十二研究所　河南新乡　453000

摘　要：大数据时代下数据量爆炸式增长，数据流动性和价值挖掘需求也显著提升，但同时也带来了更复杂的信息安全挑战，引发了更严峻的信息安全问题。本文从大数据环境下的信息安全挑战出发，分析数据泄露、技术漏洞、管理缺失、权限失控、法律风险等核心问题，并提出技术 - 管理 - 法律三维一体的协同防护策略，建立动态防护体系，为构建安全可靠的大数据生态提供参考。

关键词：大数据；信息安全；信息泄露；信息保护

引言

大数据时代的到来彻底改变了信息生产、存储、处理和共享方式，为社会经济发展带来了前所未有的机遇，同时也引发了严峻的信息安全挑战。尽管《数据安全法》已实施，但部分企业仍存在 " 重数据利用，轻安全管理 " 现象。本文主要探讨关于大数据时代下信息安全面临挑战、技术策略以及管理模式。首先分析了大数据特性如何加剧传统信息安全风险，其次详细阐述了当前主流的信息安全防护技术体系，最后通过技术 - 管理 - 法律维度分析讨论大数据时代下的信息保护策略与路径，实现从被动防御转向主动风险管理。

1 大数据时代信息安全挑战

1.1 数据边界模糊化挑战

大数据分析技术能够从海量公开信息中挖掘出潜在的涉密内容，使得传统定密标准面临失效风险。例如，通过分析社交媒体上的位置信息、交通流量等公开数据，可能推断出敏感军事设施的位置和活动规律。

1.2 数据聚合分析风险挑战

通过关联多个来源的非涉密零散数据经过大数据分析，可能推导出敏感信息或国家秘密，存在数据海量化与关联性泄密风险。这种威胁在大数据时代尤为突出，多个看似无害的数据片段组合后可能暴露秘密信息，甚至通过通信记录、访问日志等原数据挖掘还原完整行为。

1.3 数据碎片化存储挑战

大数据平台通常采用分布式存储，但缺乏统一的安全策略，导致数据碎片化存储，难以实现集中管理。云存储使得不同密级数据可能混合存储，增加了越权访问的数据泄露风险。

1.4 泄密渠道多元化挑战

云计算、物联网等技术的普及使数据存储和传输的节点激增，攻击入口多样化。数据流动也突破了物理边界，泄密渠道从传统的纸质文件扩展到云端存储、移动设备、智能终端等多种形式，增加了监管难度。

1.5 技术攻击智能化挑战

攻击者利用大数据技术增强了攻击的精准性和隐蔽性，形成了 " 数据驱动型攻击 " 的新模式。发起更精准、更隐蔽的攻击，如自动化爬取、智能钓鱼等，传统的安全防护措施难以应对这些新型威胁。

1.5.1 供应链攻击

供应链安全风险在大数据生态系统中被不断放大。现代大数据应用高度依赖开源组件和第三方服务，任何环节的漏洞都可能成为系统风险的入口。

1.5.2 AI 驱动的攻击

攻击者利用深度学习技术自动化破解加密数据，使攻击更自动化、智能化，或逆向分析加密算法，威胁数据安全。

1.6 内部管理复杂化挑战

大数据环境下涉密人员接触敏感信息的范围扩大，权限管理难度增加，内部人员泄密风险显著上升。

1.7 跨境流动监管挑战

数据全球化流动趋势下，数据跨境流动失控是当前全球数据治理中的核心挑战，其根本原因在于安全与发展难以平衡。主要流失途径是通过云存储、跨国企业数据共享可能导致信息被境外组织机构获取。如何有效监管涉密数据出境

成为难题。

1.8 应急处置时效性挑战

大数据环境下，一旦发生泄密事件，信息会以指数级速度传播，传统的应急处置机制往往难以快速响应。

1.9 法律监管滞后性挑战

许多新型风险处于监管空白地带，例如，深度伪造技术生成的虚假音频视频内容，现行法律难以有效规制；而物联网设备采集的海量边缘数据，其收集和使用的边界也缺乏清晰界定。大数据技术的快速发展远超立法速度，在大数据权属、算法问责、跨境流动等新兴领域缺乏明确规则，不同司法辖区对数据保护的立法差异还可能导致合规冲突。

2. 信息安全保护的核心策略

2.1 构建智能化的保密技术防护体系

2.1.1 数据动态脱敏

数据动态脱密是一种不改变原始数据的前提下，AI 自动识别敏感信息，根据不同权限实时对敏感信息进行隐藏或替换，从而实现数据的分级保护。确保不同权限的用户能看到其被允许查看的数据内容，原始数据依然完整存储在数据库中。

2.1.2 同态加密

同态加密是指允许在不解密数据的情况下，对加密数据直接进行计算，且计算结果解密后与原始明文数据解密的结果一致。

2.1.3 联邦学习

联邦学习是指原始数据始终保留在本地，数据可用不可见。减少数据传输风险的情况下，实现跨机构数据价值挖掘。降低数据集中存储带来的大规模泄密风险，实现 " 数据不动价值动 " 的目标。

2.1.4 AI 模型安全防护

在 AI 训练阶段引入对抗样本，提高模型对欺骗攻击的鲁棒性。嵌入数字签名，防止 AI 模型被窃取或篡改。

2.2 创新保密管理模式和方法

2.2.1 进行访问者身份验证

建立零信任架构，摒弃传统基于网络边界的 " 信任但验证 " 模式，默认所有用户、设备、应用和流量均不可信。每次访问均需通过动态的访问控制策略严格进行访问者身份验证，确保安全，减少内部泄密风险。尽管实施难度较高，但随着技术的成熟零信任架构正成为企业数字转型的必选项。

2.2.2 整合多来源零散数据

建立国家级大数据安全检测平台，整合跨部门数据，并实现分类分级脱敏加密处理。建立统一标准及共享机制。结合零信任架构强化访问控制与身份验证，实时预警数据泄露风险。

2.2.3 加强保密人才队伍建设

加强涉密人员培训与权限管理，开展大数据安全演练，实时最小权限原则，避免过度授权导致内部泄密。并建立 " 三员分立 " 机制（系统管理员、安全管理员、审计员），防止权限集中导致的滥用。

2.2.4 推进保密科技自主创新

采用 " 技术检测＋专家研判＋流程管控 " 的综合方案，建立持续优化的机制。强化数据全生命周期风险管理，数据全流程管控，采集阶段采用动态脱敏，存储阶段采用区块链存证，共享阶段采用联邦学习，销毁阶段采用磁光电三重数据擦除技术。实现采集、存储、共享到销毁的闭环管控，确保操作可追溯。

2.2.5 强化内部监管与审计

明确数据共享边界并定期进行渗透测试和日志分析，识别异常访问行为（如非工作时间的数据下载、大批量数据下载等）。

2.3 完善信息保护法规制度

2.3.1 制定《数据分级分类保护法》，建立数据出境安全评估机制。

2.3.2 修订《保守国家秘密法》，将非结构化数据（如卫星影响、社交媒体）纳入监管，强化数据跨境管控。

2.3.3 规范第三方责任：云服务商、大数据企业需接受保密协议约束，并接受国家安全审查。

3. 典型大数据泄密案例

斯诺登事件：美国 NSA 利用大数据监控全球，暴露了数据聚合分析的泄密风险。

斯诺登事件又称“棱镜门”，是指 2013 年美国国家安全局承包商雇员、前中情局技术分析员爱德华·斯诺登揭露美国政府大规模监控项目的事件。斯诺登泄露的文件显示，NSA 从 2007 年开始通过“棱镜”计划大规模监控手机全球用户的电子邮件、聊天记录、视频、照片、存储数据等，直接访问微软、谷歌、苹果、雅虎、Facebook 等 9 家互联网公

司的服务器。

4. 信息泄露应急方案

4.1 时间确认

通过安全日志分析、内存取证、网络取证、数据流向等手段核实信息泄露真实性。

4.2 评估影响

进行数据敏感度评估、泄露规模评估、泄露途径与攻击者意图评估、潜在风险及法律风险评估。

4.3 紧急遏制

短期措施：隔离受影响系统（如关闭漏洞 API、暂停数据库访问）、冻结可疑账户。

长期措施：修复漏洞（如打补丁、更新访问控制策略）。

5. 结束语：

大数据时代既给保密工作带来了挑战，也提供了新的技术手段和管理思路，面对大数据时代复杂多变的信息安全威胁，构建科学的风险管理框架至关重要。传统的信息安全风险管理方法已难以应对大数据环境下的新型挑战，应建立更加动态化、智能化和系统化的管理模型，该模型需以技术防御为盾、法律规范为矛、管理落实为基，系统性地构建 " 预防 - 检测 - 响应 " 闭环的动态防御体系，实现全方位信息保护。

参考文献：

[1] 郭琦 . 基于同态密码的密文模式匹配协议【D】. 吉林：吉林大学硕士论文，2024.

[2] 陈谦 . 隐私保护的去中心联邦学习研究【D】. 西安：西安电子科技大学博士学位论文，2024.

[3] 陆星缘 . 基于全同态加密的隐私数据分类算法研究与应用 .【D】贵州：贵州大学研究生学位论文，2023.

[4] 王聪 , 基于同态加密的安全联邦学习研究【D】北京：华北电力大学 (北京) 硕士学士论文，2023.