聚知刊出版社
JZK publishing

金融大数据的隐私安全与合规治理探析

饶秀翠

贵阳银行股份有限公司，贵州贵阳，550000；

摘要：随着大数据技术在金融领域的广泛应用，金融大数据的隐私安全与合规治理成为关键议题。本文深入剖析金融大数据隐私安全面临的挑战，包括数据泄露风险、滥用问题以及技术漏洞威胁等。同时，对当前金融大数据合规治理的现状进行梳理，涵盖国内外相关法规政策以及行业标准规范。在此基础上，提出加强金融大数据隐私安全保护的技术手段与管理策略，以及完善合规治理体系的建议，旨在为金融行业在大数据时代实现安全、合规发展提供有益参考。

关键词：金融大数据；隐私安全；合规治理

DOI：10.69979/3029-2700.26.01.027

引言

数字化时代，大数据技术已深度渗透金融行业各环节，从客户画像、精准营销到风险评估、欺诈检测，为金融机构带来效率提升与创新机遇。但金融大数据在释放价值的同时，也引发严峻隐私安全与合规问题。金融数据含客户个人身份、财务状况、交易记录等敏感信息，一旦泄露或不当使用会给客户造成不可估量和难以弥补的损失，金融机构还将面临声誉风险与法律风险。近年，全球对数据安全与隐私保护愈发重视，法规趋严，金融机构数据合规使用及处理越发重要。因此，研究金融大数据隐私安全与合规治理具重要现实意义。

1金融大数据隐私安全面临的挑战

1.1 数据泄露风险

1.1.1 外部攻击威胁

金融行业因数据高价值，逐渐成为黑客攻击的核心目标。SQL 注入（注入恶意 SQL 命令）、DDoS 攻击（分布式拒绝服务攻击）等传统网络攻击仍十分猖獗，以窃取数据为目的的攻击规模与频次持续攀升。北京金融信息化研究所《金融业数据安全发展与实践报告（2024）》所述，当前，数据安全风险形势日益严峻，数字化转型使数据风险暴露面扩大，传统网络攻击威胁持续，数据泄露和勒索事件频发。大量金融机构曾遭遇外部恶意攻击，攻击者入侵信息系统获取客户敏感数据，在黑市出售牟利，典型手段包括网络钓鱼诱骗用户泄露账号密码、利用系统漏洞植入恶意软件窃取数据等。值得关注的是，人工智能技术被应用于攻击手段后，黑客攻击更精准、更难防范，直接导致金融机构的防御成本大幅增加[1]。

1.1.2 内部管理漏洞

金融机构内部管理缺陷易引发数据泄露。部分机构存在过度授权问题，员工拥有超出工作需求的数据访问权限，一旦账号被盗用或员工出现私自下载拷贝、泄露数据等违规操作，极易造成严重的数据安全事件。第三方合作管理不足亦是重要风险点，金融业务外包是常见的一种业务合作模式，外包服务商通常会接触到大量金融数据，若机构监管不力，服务商可能因自身防护缺失或违规操作导致数据泄露。此外，部分金融机构员工缺乏数据安全培训，安全意识薄弱，易受外部诱惑或操作失误等导致数据泄露，为不法分子提供可乘之机。

1.2 数据滥用问题

1.2.1 未经授权的数据使用

部分金融机构在收集客户数据时，未充分获得客户的明确授权，或者在超出授权范围的情况下使用数据。例如，在客户同意将数据用于贷款审批的情况下，金融机构却将数据用于其他营销活动或与第三方共享，侵犯了客户的数据隐私权。部分金融机构还可能通过技术手段对数据进行深度挖掘和分析，以实现商业利益最大化，往往忽视了客户的隐私权益保护。

1.2.2 数据二次售卖与非法交易

客户数据在黑市上具有较高的价值，一些不法分子与内部人员勾结，将的客户数据进行二次售卖，形成非法的数据交易链条。这种行为不仅严重损害了客户的利益，也破坏了市场的正常秩序。某些机构或数据中介机构为了获取经济利益，可能会非法收集、整合各类数据，并在未经授权的情况下将其出售给其他机构，用于精准营销、欺诈活动等非法用途。

1.3 技术漏洞威胁

1.3.1 传统技术架构安全隐患

当前许多金融机构的核心系统仍基于传统架构，安全防护机制相对薄弱。在各类系统快速迭代过程中，新旧系统的兼容性问题可能导致大量的安全漏洞。传统的数据库管理系统可能存在权限管理不完善、数据加密强度不足等问题，使得攻击者能够轻易获取或篡改数据。一些老旧的网络架构缺乏有效的入侵检测与防御系统，难以应对新型网络攻击[2]。

1.3.2 新兴技术带来的新风险

大数据、人工智能、区块链等新兴技术在金融领域应用时，会引发新的隐私安全风险。大数据的集中存储与大规模处理，增加了数据泄露风险点；人工智能算法可能存在数据集中的系统性偏差、模型决策过程难以被人类理解等问题，易导致客户数据不当处理。区块链虽有去中心化、不可篡改优势，但代码缺陷或设计问题、节点安全问题可能引发数据安全事件。此外，量子计算技术发展对现有加密算法构成潜在威胁，其大规模应用或使当前金融数据加密保护失效。

2 金融大数据合规治理现状

2.1 国内外相关法规政策

2.1.1 国外法规

欧盟《通用数据保护条例》（GDPR）对金融数据隐私保护与合规治理要求严苛，明确数据主体知情权、访问权等权利，强制金融机构在数据收集、存储等全环节获取明确同意并落实安全措施，违规最高罚全球营业额 4%。美国《金融服务现代化法案》《公平信用报告法》聚焦消费者隐私与数据安全，规范数据处理。美联储等机构依行业特性定规则，在金融科技领域兼顾创新与灵活监管，但因监管分散，存在部分规范协调不足的问题。

2.1.2 国内法规

我国近年持续推进金融数据合规治理立法。《中华人民共和国数据安全法》明确数据安全管理体制、保护义务及安全事故应急处置，为金融数据安全搭建基本法律框架。《中华人民共和国个人信息保护法》聚焦个人信息权益保护与处理规范，要求金融机构处理个人信息时，遵循合法、正当、必要、诚信原则，并采取安全技术措施。《银行保险机构数据安全管理办法》针对银行保险机构，细化数据分级分类、访问控制、加密、备份恢复等要求。法律法规的不断规范，构建起我国金融数据合规治理法律体系，强化了金融机构数据安全责任。

2.2 行业标准规范

中国互联网金融协会已发布《金融数据安全治理实施指南》《金融数据安全技术防护规范》等多项标准，从数据治理、资产管理、技术防护、应急管理维度，为金融行业数据安全治理提供指引，核心是推动机构健全安全管理体系、提升防护能力，保障数据全生命周期安全。其中，《金融数据安全技术防护规范》明确数据存储、传输等环节技术要求，含加密算法选择、访问控制策略；《金融数据安全应急响应和处置指引》规定事件应急流程与处置措施，旨在降低数据安全事故引发的损失。

3 加强金融大数据隐私安全保护的措施

3.1 技术手段

3.1.1 数据加密技术

数据加密技术是保护金融大数据隐私安全的关键手段。数据存储时，需对敏感数据全量加密，即便数据被非法获取，攻击者也无法直接读取，例如用 AES 算法加密客户身份证号、银行卡号、交易记录等信息。数据传输环节，通过 SSL/TLS 协议加密传输，避免数据在网络中被窃取或篡改。针对关键数据，可采用同态加密技术，实现加密状态下的数据计算与分析，进一步强化数据安全性与隐私性[3]。

3.1.2 访问控制技术

建立完善访问控制机制是限制金融数据访问权限的关键。常用基于角色的访问控制（RBAC）模型，依据员工工作职责与业务需求分配角色，每个角色对应特定数据访问权限，仅授权用户在权限范围内访问数据。同时采用多因素身份认证技术，结合密码、指纹识别、短信验证码等方式，提升身份验证安全性，防范非法用户窃取账号密码访问数据。此外，需对数据访问行为实时监控与审计，及时发现、预警并处理异常访问行为。

3.1.3 隐私计算技术

隐私计算技术为金融数据安全共享与分析提供新方案。多方安全计算（MPC）支持金融机构不共享原始数据即可联合计算分析，如联合信用评估中，借助 MPC 技术，在不泄露客户原始数据的前提下共同计算信用评分，既挖掘数据价值又保护数据安全。联邦学习（FL）通过多参与方联合模型训练且不传输原始数据，使不同金融机构能利用各自数据联合建模，提升模型准确性与泛化能力，同时保障数据隐私。同态加密技术实现加密数据特定计算，适用于金融领域加密数据的统计分析、风险评估等场景，确保数据全流程隐私安全。

3.2 管理策略

3.2.1 完善数据安全管理制度

金融机构需健全数据安全管理制度，明确管理目标、原则、流程与责任。制定数据分级分类标准，按敏感程度与重要性分类管理金融数据，对不同级别数据采取差异化安全保护措施。建立数据全生命周期管理制度，覆盖采集、存储、传输、使用、共享、销毁各环节，明确各环节管理要求与操作规范。同时加强第三方合作管理，在协议中明确其数据安全责任，严格授权与监控第三方数据访问使用，并定期开展安全评估。

3.2.2 加强员工数据安全培训

提高员工的数据安全意识和技能是防范数据安全风险的重要环节。金融机构应定期组织员工参加数据安全培训，培训内容包括数据安全法律法规、行业标准规范、数据安全基础知识、安全操作流程以及常见的数据安全风险防范方法等。通过案例分析、模拟演练等方式，增强员工对数据安全问题的认识和应对能力。建立员工数据安全考核机制，将数据安全工作表现纳入员工绩效考核体系，激励员工积极遵守数据安全管理制度，对违反数据安全规定的员工进行严肃处罚。

3.2.3 建立数据安全应急响应机制

金融机构需制定完善的数据安全应急响应预案，明确事件处置流程与责任分工。搭建数据安全监测与预警系统，实时监控数据系统运行状态，及时识别潜在风险并发出预警。若发生数据安全事件，需迅速启动应急机制，通过数据备份恢复、系统修复、事件调查追踪等措施处置，最大程度降低损失。此外，需定期演练与评估应急预案，结合演练结果和实际情况优化预案，保障应急响应机制的有效性与可靠性。

4 完善金融大数据合规治理体系的建议

4.1 加强法规政策执行与监管力度

监管部门需加大金融机构法规执行的监督检查力度，确保其严格遵守数据安全与隐私保护法规。建立常态化监管机制，定期评估审查金融机构数据治理情况，对违规行为依法严惩，提高违规成本。同时加强金融数据跨境流动监管，结合国家安全战略与数据保护要求，制定严格跨境流动规则，保障数据跨境传输安全合规。此外，需加强国际合作交流，参与国际数据安全规则制定，借鉴先进经验，提升我国金融数据合规治理的国际影响力[4]。

4.2 推动行业自律与标准化建设

金融行业协会需充分发挥作用，推动建立并完善行业自律机制。组织金融机构联合制定行业自律准则，引导机构自觉遵守数据安全与隐私保护规范，强化行业内部监督约束。同时，进一步推进金融大数据相关标准的制定与推广，提升标准权威性和适用性，助力金融机构间数据共享与协同发展。鼓励机构参与标准制定，结合行业实际需求与技术创新，及时更新完善标准体系，为金融大数据合规治理提供坚实技术支撑。

4.3 促进合规技术创新与应用

需加大金融大数据合规技术研发支持，鼓励科研机构、高校与企业合作，攻克数据安全与合规治理关键技术难题。推动人工智能、区块链、云计算等新兴技术的应用创新，如用人工智能实现数据合规自动化检测分析，借区块链实现数据可信存储与流转记录，靠云计算构建安全的数据存储处理平台。同时建立合规技术创新成果推广机制，加速新技术在金融行业普及，提升金融机构整体合规治理水平[5]。

5 结论

金融大数据的隐私安全与合规治理是金融行业数字化时代的核心课题。当前金融数据价值凸显，隐私安全风险与合规挑战也随之加剧。通过应用数据加密、访问控制、隐私计算等技术，及完善数据安全管理制度、加强员工培训、建立应急响应机制等管理策略，可有效提升隐私安全保护水平。同时，强化法规执行与监管、推动行业自律及标准化建设、促进合规技术创新，能完善合规治理体系。唯有隐私安全与合规治理协同发力，方能保障金融大数据合法安全应用，推动金融业数字化转型可持续发展。

参考文献

[1]刘旭杰.金融科技赋能征信数据安全流通的路径探讨[J].征信,2025,43(05):58-67.

[2]刘俊.大数据环境下金融信息安全防范与保障体系研究[J].高科技与产业化,2025,31(04):108-110.

[3]叶晓东,肖惠玲.中国式现代化背景下金融数据安全研究[J].经济研究导刊,2025,(08):134-137.

[4]王慧娟,高娅楠,卢薇青.数据安全体系助力金融数据要素流通与共享[J].上海信息化,2025,(04):38-41.

[5]张伟,庞小欢.新形势下金融数据安全治理探析[J].农业发展与金融,2025,(02):84-87.

作者简介：饶秀翠（1990.09.21-），女，汉族，籍贯：贵州修文，职务/职称：工作人员/中级经济师，学历：本科，研究方向：互联网金融。