金融科技时代数据安全治理问题与建议

刘宇
（中国人民银行成都分行，四川成都 610041）

摘 要： 金融科技的迅猛发展改变了金融业的创新思路和经营理念，数据作为基础生产资料，在金融科技发展过程中起了关键的推动作用。金融领域的数据重要且敏感，在金融科技发展的同时做好数据安全保护显得尤为重要。文章从近年来发生的重大数据安全事件出发，介绍了国内外主要数据安全法律要求，分析了当前金融科技创新发展中数据利用存在的风险，最后提出了新时代金融领域加强数据安全保护的建议。

关键词： 金融科技；数据安全；数据治理
中图分类号： TP309.2 **文献标识码：** A

Data security governance issues and suggestions in the age of Fintech

Liu Yu
(*Chengdu Branch of the People's Bank of China, SichuanChengdu 610041*)

Abstract: The development of Fintech has changed the innovative thought and business philosophy of the financial industry. As the fundamental production element, data plays a key role in Fintech. Data is important and sensitive in financial field, it is crucial to protect data security while developing of Fintech .This paper started with the major data security incidents in recent years, introduced the main data laws and regulations in the domestic and overseas, analyzed the risks of data governance in Fintech innovation, and finally gives some suggestions on data security protection in the Fintech era.

Key words: fintech; data security; data governance

1 引言

近年来，以“大智移云”为代表的新技术与金融业交互融合，新兴金融产品不断涌现，金融经营模式正在发生着深刻变革，金融科技已成为引领金融机构实现创新发展和转型升级的核心力量。数据是金融机构最基础的生产资料，金融科技应用离不开大量数据的收集、聚合和分析，高质量数据整合和利用已成为金融科技创新的原动力和助推剂。与此同时，无论是金融机构，还是金融科技公司，通过不同渠道和方式收集了大量机构数据和个人信息，具有极大的分析和利用价值。若管理水平和防护措施不到位，导致数据丢失、损坏或者泄露，会给机构和个人带来难以估量的损失。因此，做好数据安全治理，对于维护金融稳定、保障人民权益具有极其重要意义。

2 数据安全形势日益严峻

数据是数字经济时代最重要的生产要素之一，大数据高速发展的同时，其安全问题也日益凸出。国内外数据破坏、泄露事件屡有发生，并且规模和严重程度越来越大，数据安全

问题已成为金融科技创新发展的制约因素之一。锁定、破坏计算机数据的勒索病毒在2017年开始大规模爆发，从WannaCry、Petya到GlobeImposter及其变种，勒索病毒更新迭代速度越来越快，攻击方式花样翻新，其攻击目标也从个人用户逐渐转向大型机构和企业用户，成为近年来网络数据安全最大的威胁。2018年，芯片代工企业台积电遭受勒索病毒攻击，短时间内生产线全部停摆，损失高达17.6亿元；华住旗下酒店发生大规模信息泄露，被公开售卖的信息包括网站注册和酒店客人的姓名、身份证、手机号码等共约5亿条信息，堪称近年来国内规模最大最严重的信息泄露事件。国外近几年也经常发生数据泄漏事件：美国信用评估巨头Equifax于2017年遭到黑客攻击，导致美国一半人口的个人信息被泄露，此次攻击的主要原因是Equifax未能及时修补Apache发布的Struts高危漏洞补丁；2018年，印度国家身份认证系统Aadhaar被爆遭到网络攻击，该系统存储了印度11.2亿人的重要身份信息，包括指纹、虹膜纪录等极度敏感个人特征信息均遭到泄露，因为个人生物信息的唯一性和不可变更性，此次信息泄露给印度公民带来了长期持续和不可预知的恶劣影响。

3 国内外数据安全保护情况

数据安全关系到金融机构资产安全、个人隐私安全和社会安全稳定,是当前网络安全的重要议题之一。近年来，面对严峻的数据安全态势，世界各国相继出台法律、法规和政策，规范数据使用，加强敏感信息和重要数据保护。

3.1 国外重要数据法律法规

近年来最著名的数据保护法律当数欧盟在2018年5月25日出台的《一般数据保护条例》（GDPR），它取代了1995年颁布的《数据保护指令》，一统欧盟内零散的个人数据保护规则，统一明确了欧盟内相关组织机构处理隐私和数据保护的要求。该法律管辖范围不但包括了欧盟境内的企业，还包括收集处理欧盟公民信息的其他全球企业，对于违反数据保护规定的企业最高处罚可达到2000万欧元或者该企业上一年度全球营业额的4%。GDPR的实施让欧盟企业真正开始将数据保护列为企业经营的必选项，主动满足合规要求，也为其他地区企业加强数据保护敲响了警钟。美国的数据和个人隐私保护法有1974年颁布的《隐私权法》，阐明了政府机构应如何收集和储存个人信息，它是世界上第一部保护隐私的法律。《加利福尼亚州消费者隐私保护法案》（CCPA）将在2020年1月1日正式实施，该法案授权消费者可以有条件控制公司收集和管理的个人信息，比如数据访问权、数据删除权、数据泄露私人诉讼权等，并规定了数据泄露的赔偿责任和金额。

3.2 国内数据法规标准

随着我国移动互联网的迅猛发展，个人信息泄露也呈现愈演愈烈的趋势，相关部门通过制定法律法规和行业规范，不断加强我国数据安全和个人隐私保护。2015年《刑法修正案（九）》明确了侵犯公民个人信息罪的判罚依据。2017年正式实施的《网络安全法》第四章明确规定了网络运营者要防止数据被泄露篡改，任何个人不得窃取重要数据和个人敏感信息，在法律上进一步完善了网络数据和个人信息保护的要求。《信息安全技术 个人信息安全规范》于2018年5月1日正式实施，该规范对企业收集、使用、共享个人信息等行为提出了详细、明确的指引和参考，为企业规范使用个人数据提供了标准。《银行业金融机构数据治理指引》要求金融机构依法合规收集和应用数据，保护客户隐私并改进数据安全技术。《移动金融基于声纹识别的安全应用技术规范》是我国金融行业第一个生物识别技术标准，明确了金融领域声纹信息采集、传输、存储、处理、删除等全生命周期数据安全要求，为生物识别技术在金融领域的安全、可靠应用奠定了良好基础。

4 金融科技数据安全存在的主要问题

通过大数据、云计算、人工智能等技术的应

用，数据在助力金融机构实现精准客户营销、优化客户服务、创新智能产品、完善风险防控等方面展现出了巨大价值，数据是核心战略资产的地位得到越来越多的认同。如何最大程度地挖掘数据价值，高质量开展数据治理是金融机构完成数字化转型、实现持续健康发展的核心动能之一。金融机构掌握了大量的金融交易数据和客户敏感信息，既是数据的生产者，也是数据的分析和存储者，规范合理利用数据，保护重要数据安全有义不容辞的义务和不可推卸的责任。目前，我国金融科技总体发展水平还处于初级阶段，相关法规标准也不健全，行业还存在野蛮生长、无序发展的乱象，数据保护不力，非法使用，违规交易等现象时有发生。

4.1 数据滥用

目前，金融行业还没有关于个人数据信息收集、使用的明确监管规则，在金融科技领域滥用个人数据的现象相对其他行业更加严重。大数据杀熟、过度营销、数据倒卖等现象在金融科技领域可谓是屡见不鲜。比如，为了实现精准营销而非法采集个人消费行为数据，为了降低信贷风险而过度收集个人交易和信用信息等，一些所谓的金融科技大数据公司就是以数据买卖和非法采集起家，甚至直接从外部购买黑灰产数据。

4.2 数据泄露

金融科技领域汇集了海量的机构市场数据、客户行为数据和交易数据，是金融机构掌握的核心数字资产，也是别有用心者觊觎窥探的宝藏。个人资产信息、征信信息、生物特征信息等都关系到每个人的切身利益和幸福生活，一旦泄露，会给个人和家庭造成不可挽回的损失。特别是个人的生物识别特征，因为具有唯一性，也很容易被复制，一旦泄露就无法挽回，会严重危害个人隐私和财产安全。从近年来重大数据泄露事件来看，泄露原因既有外部黑客攻击，也有内部管理疏漏；既有安全意识薄弱，也有安全防护措施不到位等原因。

4.3 数据污染

大数据、人工智能、深度学习等技术应用均离不开适当的算法、可靠的模型和合理的数据，一旦训练样本数据不全，或者被恶意污染导致“中毒”，训练的结果都会大相径庭，甚至是产生完全相反的结果。数据污染具有很大的隐蔽性，一项数据受到污染，将导致一连串的严重后果。做好数据治理，规范、统一内外部数据标准，加强数据安全保护是避免数据污染的切实有效途径。

4.4 数据保护力度不够

金融科技是新兴事物，总体发展仍处于初级阶段，不同机构对金融科技理解水平不一致，数据安全保护意识参差不齐，仍然存在重发展、轻安全，重利益、轻风险的经营理念。特别是一些中小机构，身份鉴别、加密存储、容灾备份等传统的数据安全保护手段都不到位，一旦发生黑客攻击、系统故障或自然灾害，信息泄露和数据丢失将不可避免，不但对个人数据安全是一大威胁，也给金融机构经营带来了巨大风险。

5 金融科技数据安全治理建议

数据治理是金融科技时代数字化转型升级的基础，而数据安全则是数据治理工作的前提。金融机构存储的数据蕴含大量私人信息和商业秘密，如果忽略数据治理中的数据安全问题，会埋下巨大安全隐患和风险。只有保障数据安全、做好数据安全治理，金融科技才能真正发挥其巨大的创新价值，助力金融机构实现转型发展的时代目标。

5.1 完善金融领域数据安全法规标准

金融机构存储的数据不但包括客户基本信息、交易行为数据，还包括金融机构自身的财务、凭证、市场等重要数据，相对于其他行业而言，金融业对业务连续性和数据安全有更加

严格的需求。应在我国现行数据安全法律、办法、规范和指南的基础上，结合我国金融行业数据管理的要求和特点，参照国外相关数据保护要求，制定适合我国金融科技发展的数据安全法规和制度。在数据安全管理和数据保护技术上更加严格要求，比如明确个人隐私和重要数据采集范围、存储方式、加密手段、使用原则、留存期限、备份方法等。应形成行业强制性标准，加大违规惩罚力度，在遵循国家数据安全保护的前提下，进一步满足金融行业业务特殊性的要求。

5.2 强化金融领域数据安全合规监管

要充分发挥新技术在促进金融监管、强化数据风险防控方面的作用。利用监管科技引导金融机构规范数据安全治理，实现监管要求的自动化、流程化和规范化管理，提升监管效率，降低监管成本。以金融机构或者互联网企业行为为导向，按照只要涉及金融业务数据均应该纳入监管范围的原则实施监管，被监管单位通过监管科技自动匹配监管要求，实现数据全生命周期和全流程监督和监测。特别是要严惩并曝光侵犯个人隐私、违规采集数据、非法数据买卖等行为，发挥警示威慑作用，建立行业数据使用自律机制，形成对金融监管的有效配合和有力支撑。

5.3 同步开展数据安全治理

数据安全是数据治理的前提，数据治理是数据安全的保障。各金融机构应按照国家和行业法律法规要求，在进行数据治理的同时，同步规划、建设和使用保护措施以确保数据的安全规范利用。应建立统一规范的内外部数据标准，根据数据的重要性对数据进行分级分类，对不同层次的数据采取不同的安全保护措施，突出重点，有的放矢。打通数据内外边界，实现数据的透明性和可追溯性，确保外部数据合理合规和安全可靠。通过完善的安全管理和有效的安全技术保证数据更加广泛的共享和应用，使安全成为竞争力，让安全成为发展的新动能。

5.4 加强数据安全技术研究和应用

保护数据安全就是要保证数据的机密性、完整性和可用性。数据安全保护与网络安全防护紧密相关，应加大数据安全技术研发力度，积极推动新技术在金融领域数据保护和操作审计中的应用，从源头切断数据泄露、滥用和污染的可能性。比如，在数据流通和数据存储阶段，通过差分隐私、同态加密等技术可以实现不泄露个人隐私条件下的数据分析处理。区块链技术可以提供可信的多方计算环境，实现高效、安全的利益分配机制。同时，区块链技术先天还具备日志记录、可追溯、不可篡改等特性，非常适合做数据安全的追溯审计。安全多方计算技术可以确保在保护数据隐私的前提下，实现多方安全协同计算，并确保各参与方得到正确的数据结果。

6 结束语

金融作为国家重要信息基础设施，是国家安全的重要组成部分。金融科技时代金融数据安全不但关系到金融机构自身的健康发展，更关系到国家社会稳定和人民切身利益。监管层应尽快建立金融领域数据保护标准和规范，利用监管科技加强数据全生命周期监管，严惩违法违规行为。金融机构应把数据安全作为企业发展的核心价值，主动满足合规要求，积极布局实践安全可信通信和加密存储技术，切实维护国家利益和保障金融安全稳定。

参考文献

[1] 杜跃进.数据安全治理的几个基本问题[J].大数据,2018,4(06):85-91.

[2] 周季礼,李德斌.国外大数据安全发展的主要经验及启示[J].信息安全与通信保密,2015(06):40-45.

[3] 胡文华.冲击与应对:GDPR与《网络安全法》比较视野下的企业合规[J].中国信息安全,2018(07):77-81.

[4] 吴沈括,孟洁,薛颖,赵小琳.《2018年加州消费者隐

私法案》中的个人信息保护[J].信息安全与通信保密,2018(12):83-100.

[5] 卞雨茗.商业银行数字化转型下的数据治理[J].银行家,2018(04):76-78.

[6] 周丹.大数据时代个人数据民法保护问题研究[D].华中师范大学,2015.

[7] 董祥千,郭兵,沈艳,段旭良,申云成,张洪.一种高效安全的去中心化数据共享模型[J].计算机学报,2018,41(05):1021-1036.

作者简介：

刘宇（1981-），男，汉族，重庆人，上海交通大学，硕士，中国人民银行成都分行，工程师；主要研究方向和关注领域：金融科技、网络安全、风险管理、数据保护。