电子政务

E-Government

ISSN 1672-7223,CN 11-5181/TP

《电子政务》网络首发论文

题目：　数字经济下金融数据风险及治理研究

作者：　夏诗园，尹振涛

收稿日期：　2021-10-26

网络首发日期：　2022-04-12

引用格式：　夏诗园，尹振涛．数字经济下金融数据风险及治理研究[J/OL]．电子政务．https://kns.cnki.net/kcms/detail/11.5181.TP.20220410.2108.016.html

数字经济下金融数据风险及治理研究*

夏诗园**①　尹振涛②
①中华人民共和国审计署审计科研所　北京　100086
②中国社会科学院金融研究所　北京　100710

摘　要：数据是数字经济的关键生产要素，作为数据密集型行业，金融市场拥有的海量数据在产生巨大价值的同时也极易成为网络攻击的重点对象，提高金融市场数据治理能力已成为防范金融系统性风险、实现金融业可持续发展的关键。在分析金融数据风险及形成原因的基础上，针对我国金融数据治理中存在的缺乏金融数据共享激励机制、金融机构数据共享动力不足，金融信息孤岛问题难以短期解决，金融数据跨境流动规则冲突等治理挑战，借鉴国外发达国家数据治理经验，基于我国金融市场发展现实提出数字经济下加快金融数据风险防范和治理的相关建议。

关键词：数字经济；金融数据；金融信息；金融安全；数据治理

近年来，数字技术的快速发展，为高质量数据的互联互通和深度使用提供了保障，但同时对数据治理也提出了更高要求。我国高度重视数据要素及其治理工作，特别是《关于新时代加快完善社会主义市场经济体制的意见》《关于构建更加完善的要素市场化配置体制机制的意见》等文件的先后出台，标志着数据要素被正式纳入生产要素范围，数据要素市场化配置发展也有了政策遵循。作为数据要素最密集的行业之一，金融市场在数字化转型中产生的不当行为极易导致信息泄露等数据治理乱象，给金融用户信息安全造成巨大风险隐患。探索金融数据风险及其形成原因，分析我国金融数据治理挑战，以及探讨发达国家先进数据治理经验，对于加速培育我国金融数据要素市场，全面提升金融数据治理能力，挖掘金融数据价值，防范金融系统性风险，稳增长、调结构、促转型和惠民生等具有重要现实意义。

一、金融数据风险及形成原因

新技术、新模式和新业态给传统金融市场带来新的生机和活力，金融数据成为重要的生产资料。对金融市场、金融机构和金融基础设施等相关数据进行监测和分析，可为分析宏观经济数据和微观行为间的相互联系、深入探索金融运行规律提供有效途径[1]。与此同时，高质量数据能提升金融业务价值[2]，是企业实现组织目标的重要资产，也是分析和认知诸如系统性风险、市场风险、流动性风险、信贷风险和运营风险等金融风险的基础[3]，更是影响各项决策活动的重要依据[4]。数据日趋复杂和数据量的爆炸式增长，也使企业在使用数据方面变得越来越成熟，推动新需求的产生[5]。

与此同时，金融数据非竞争性的天然属性以及海量堆积，极易使其超越传统法律框架的有效规制，埋下风险隐患。电子数据的收集和共享增加了包括隐私、安全、责任和市场竞争等在内的一系列治理问题[6]，尤其是物联网等金融科技的快速发展引发了许多迄今尚未解决的法律和监管问题，如隐私、数据所有权问题等[7]。另外，信息是商业银行的重要资产之一，随着信息技术的快速发展，信息系统在银行业务流程的嵌套程度日益加深，恶意攻击、数据泄露等危害数据安全事件也不断增多[8]，银行相关信息的丢失会对银行的财务和声誉造

*基金项目：国家社会科学基金青年项目“去杠杆进程中地方政府债务管控研究”（项目号：19CJY054）。
**通讯作者
收稿日期：2021－10－26　　修回日期：2021－11－30

成严重损害[9]。无论是从国家安全的角度衡量，还是以组织声誉来衡量，数据泄漏都可能产生破坏性后果[10]。收集和使用大量个人信息的机构应采取相应措施，以保护数据主体免受风险侵害[11]。

金融信息的扩张速度极快，对数据治理也提出了新的要求[12]。特别是随着云计算等数字技术的快速发展，采用相关技术的企业、公共组织和政府不断增多，也使这些组织面临着新的、更复杂的挑战[13]。数据治理功能是通过提供对企业数据的数据质量的可见性来进行的[14]，通过对数据资产的管理行使权力、控制和共享决策，为相关机构、组织等确保数据和信息得到有效管理管理的能力，为适当的人员在适当的时间提供适当的信息，数据治理正受到专家们越来越多的关注[15]。许多组织都意识到，客户数据是一项宝贵的资产，需要仔细保护，其价值需要积极“治理”[16]。数据治理不仅是一门新兴学科，体现了数据质量、数据管理、数据策略、业务流程管理和风险管理的融合；同时，数据治理也是一项过程，通过对企业重要数据资产进行管理[17]，可为企业提供更高质量的数据，更快更好的决策以及更高的市场地位[18]。成功实施数据治理的四个关键原则包括明确的所有权、价值认可、有效的数据政策和程序以及数据质量，有效的数据治理框架的优势包括高效的数据管理、较低的信息成本以及完善的法规法规和控制工作[19]。数据治理可对企业的业务绩效和合规性产生积极影响，但当今仍有许多企业数据管理和数据质量较差，尚未开发出提升数据治理效果的具体方法[20]。数据治理在很大程度上仍不具有正式程序和形式，在特定的企业中缺乏相应的组织结构和更广泛的支持，在许多政府部门，数据治理水平仍有待提升，应以宏观审慎视角探讨数据治理问题[21]。

（一）金融数据风险种类

1.宏观层面：金融数据主权风险和社会风险

(1)金融数据主权风险

金融数据是国家重要战略资源，这些数据中涉及个人隐私、企业商业秘密、社会治理、国防和安全等要素，蕴含一国经济金融市场发展现状及未来趋势，如可根据跨国电子商务订单数据推测消费者的购买力、相关行业的宏观经济运行等。随着全球数据跨境流动日益频繁，以美国为首的发达国家凭借其先进的数字技术，数据存储和处理优势，通过金融数据大型分析平台和先进的数据分析手段阻碍数据权益的平衡分配，挤占全球数据红利，为中小金融科技机构设置障碍；亦或是通过占用、非法搜集他国脱敏和未脱敏的重要金融数据资源维持数据霸权，给我国金融市场安全和国家数据主权安全造成极大威胁。近年来，美国政府为遏制我国快速发展，针对中国企业在美国上市提出了更为严格的网络安全审查制度、信息安全制度以及额外信息披露要求，如何保证我国企业在国外上市后关键信息基础设施、核心重要数据不被其他国家影响、控制和利用是需关注的重点。

(2)社会风险

个人或金融机构数据使用不当或被泄露，不但会直接侵害个人金融信息主体的合法权益、影响金融业机构的正常运营，还可能会带来系统性金融风险[22]，威胁金融安全，严重时可能会随着经济链条蔓延到整个社会。与此同时，微观主体信息侵权等违规违法事件的发生使公民举证存在一定困难，维权无果给公民带来了巨大经济和身心损害，在不理智行为驱动下可能会衍生群体事件，影响社会稳定，对政府信誉也产生一定损害。

2.中观层面：金融数据市场垄断风险

作为数字经济重要的生产要素，金融数据影响金融市场价值分配。近年来，我国金融科技行业发展迅速，大型金融科技公司凭借绝对技术优势、较强的议价能力和显著的网络溢出效应，不断扩大消费群体和业务范围，积累了大量个人信息和金融交易数据，形成数据寡头滥用市场地位，主要表现为：其一，通过协议等形式与强势企业达成更加隐形的金融数据共谋行为，利用技

术持续监控市场价格和对手价格调整自身定价以遏制竞争对手；其二，大型金融科技公司通过价格欺诈、拒绝或限制交易、捆绑销售、差别待遇等方式提高竞争对手进入市场的门槛，或通过恶意刷单、恶意点评、诋毁其他数字平台的品牌形象等不正当手段提升自有竞争性金融产品或服务的市场占有率，极易滋生灰色交易，严重影响金融市场自由、公平的竞争秩序。

3.微观层面：金融市场微观主体隐私和利益受侵害风险

基于微观层面，金融数据风险是指，数字经济下微观个体在进行金融交易时，金融数据平台通过搜集、分析和使用个体用户数据时产生的无意或故意的数据泄露、滥用和污染等行为造成的风险。

⑴金融消费者福利损害风险

其一，数据被滥用和被泄露风险。随着数字消费的快速发展，金融消费者在使用金融手机应用或第三方开发者软件办理金融业务时，会被强制性要求在隐私协议或各种授权中允许搜集或查询信息的权利，用户的一切网上信息包括身份、位置、购物偏好、支付密码等各类信息都被后台记录下来，大数据杀熟、过度营销等金融数据被滥用、被泄露现象屡见不鲜。

其二，消费者福利受侵害风险。在数字经济背景下，金融消费者处于明显信息劣势。通过对消费者决策环境、交易规则和定价模型的反复实验带来的自动决策和偏好匹配虽方便消费者搜寻目标商品，但数据驱动的预测和分析也可能会利用消费者的保留价格和行为弱点以更隐蔽的方式影响消费者决策，误导消费者行为，侵犯了消费者的自主选择权。此外，大型金融科技公司在对中小型金融机构进行数据垄断的同时，也导致许多金融消费者无法获得成本更低、效率更高、类型更为多样的金融科技服务。

⑵金融机构利益损害风险

其一，数据泄露风险。数据泄露包括故意泄露和非故意泄露两种：一方面，金融机构内部人员可能会受利益驱使非法倒卖或故意泄露信息；另一方面，金融领域长期以来一直是黑客攻击的主要目标，虽然金融科技、物联网等技术由于数据不可窜改等特征具有较高的安全性，但数字技术的快速发展也使网络攻击手段不断升级，攻击方式也更加多样，金融机构可能会由于管理不善或遭受恶意非法入侵等事件意外泄露重要信息。

其二，数据污染风险。数据无标签的属性极易在数字交易过程中被复制和篡改，一旦样本受到恶意破坏，模型结果就会大相径庭，会给金融机构造成高昂的数据清理费用，从而影响金融企业机构决策，不利于金融机构的长期发展。

其三，数据共享风险。我国个人金融数据的收集与传递整体上呈现割裂局面，缺乏数据共享的市场结构[1]，在数据共享、委托处理和传输过程中，第三方数据处理机构缺乏数据安全合规能力所导致的风险将直接影响到金融机构利益。

（二）金融数据风险产生原因

1.金融数据安全宏观制度和顶层设计漏洞滋生金融数据风险隐患

第一，金融数据治理相关法律法规有待完善，金融数据管理制度不健全。海量金融数据的开放和共享迫切需要相应的标准规范和相关法律法规的支持，我国虽已发布了《个人信息数据法》《数据安全法》等法律法规，以及《个人金融信息保护技术规范》《金融数据安全分级指南》《征信业务管理办法（征求意见稿）》《中国银保监会监管数据安全管理办法（试行）》等规范性文件，但总体来说在金融信息收集、使用和披露过程中仍缺乏具体执行条例，现有宪法和法律规范文件中关于个人金融信息数据保护的相关条款较为零散且过于抽象，可操作性仍需提升。

第二，缺乏金融数据治理生命周期全流程管理机制监督，金融数据流通受限。具体表现为：在数据交易之

前的准备阶段，对金融数据产品和经销商的评估有待加强，无法保证数据质量；在数据交易进行阶段，交易匹配定价体系不够完善容易滋生数据黑市；在数据交易后，缺乏全国统一的可信数据流通体系的支撑。

第三，金融数据权属划分不明确，数据共享机制不畅。当前我国金融数据存在权属界定标准、数据定价标准和运行机制不统一，缺乏数据效益、成本估算机制、数据共享原则等操作规范，导致数据所有权和使用权分立，数据开放共享难度激增。金融数据确权的争议使金融数据财产所有者一旦遭遇纠纷案件，无法充分、合理、有效地保护自身权益。

2.金融数据安全监管乏力不利于金融市场良好秩序的形成

第一，金融数据保护制度不健全导致风险监管乏力。当前，我国个人金融信息保护制度尚不健全，缺乏个人信息的跨部门监管机制，虽已形成了以银行业金融机构为主的金融数据治理框架，一行两会也内设金融消费者权益保护部门，但传统分业监管模式明显不适应金融数据市场的高效流动性及混业特征。加之金融数据监管执法体系权责不明、协调不畅，金融监管理念及监管规则差异等，导致部分金融机构仍游离于监管规则之外，金融数据监管存在空白和漏洞。与此同时，我国金融数据跨境安全评估方式和监管制度尚处于探索阶段，无法满足进一步对外开放下金融数据加速跨境流动的需要。

第二，金融数据监管手段单一，效率低下。传统金融数据治理人工现场监管模式对金融数据风险的识别和预测风险效果不佳，通常都是在发生金融数据侵权事件之后监管部门才介入进行调查，监管行为存在滞后性。

第三，金融数据监管处罚缺乏触发标准，处罚强度不够。与发达国家相比，我国针对滥用金融数据等行为缺乏统一的触发机制和处罚标准，在处罚方式上也主要以行政约谈方式为主，对金融数据泄露事件的处罚力度较低，对犯罪行为的震慑力不高，犯罪成本太低导致无法从根本上抑制犯罪行为。

第四，金融数据监管执法队伍有待加强。现有金融监管执法人员在金融知识、业务水平等方面素质存在差异，金融数据监管执法能力有待提升，缺乏监管执法人员培养的长效机制，不利于金融市场的可持续发展。

3.金融数据安全意识落后，金融机构数据治理能力不强损害微观主体利益

第一，金融数据安全意识滞后，企业数据治理文化尚未形成。许多金融机构特别是中小金融机构仍存在重发展业务、轻安全风险的短视思想，金融科技研发经费投入有限、岗位职责不够明确和细化，缺乏专业、系统的数据分析人才队伍，对员工金融数据安全意识的培养不重视，数据安全文化氛围尚未形成。有的机构简单地将数据安全保护归因于安全产品的堆积，无法形成金融数据治理产品、技术和人才的强大合力，对金融数据安全和金融机构运营造成风险隐患。

第二，金融数据处理方式不规范，数据利用率不高，资产价值有待挖掘。从金融机构内部来说，当前金融机构分析业务数据时主要以结构化数据为主，对于其他大量非结构化数据的整合和利用度不够。由于金融数据来源众多，数据结构复杂多样，不同数据之间存在不一致甚至矛盾，金融机构收集数据时在确保数据定义一致性方面面临诸多挑战。从金融机构外部角度来说，对于来自外部渠道数据的获取和处理方式尚不够规范和合规，数据异常和数据失真现象时有发生。由于金融机构的关键数据管理权限和职能常分散在不同部门，导致跨部门、跨领域、跨系统数据治理成本高、协调困难，金融数据价值未得到充分挖掘。

第三，金融数据治理架构缺乏，治理工具和技术薄弱。许多金融机构虽设有与数据治理相关的内部组织部门，但缺乏可行的数据安全防护体系建设方案、制度规划设计、责任管理体系等，治理流程和环节缺乏刚性控

制，数据治理工作重技术部门轻业务部门，事前监督机制不完善，事后问责机制不明确、不到位。同时，金融数据网络安全基础设施整体实力薄弱，信息系统架构关键技术存在漏洞，后台技术管理和网络维护方面管理缺失等，导致网络安全事件频发。

二、我国金融数据治理挑战及国际经验

为应对数字经济时代安全威胁的挑战，很多国家都采取了相应举措，吸纳国际经验有助于我国金融数据治理少走弯路。

（一）我国金融数据治理挑战

1.缺乏金融数据共享激励机制，金融机构数据共享动力不足

一方面，金融机构普遍将数据作为涉及本机构商业秘密和竞争力的战略性资源，基于经济利益角度考虑，与其他企业、机构进行数据共享的主动性较低；另一方面，金融机构现有数据涉及个人、商业和国家秘密，当前数据泄露和窃取案件屡见不鲜，数据共享可能产生的法律风险使金融机构数据共享心存疑虑。

2.新金融场景和新业态形式不断涌现，增加金融数据安全治理难度

数字经济下新金融场景不断涌现，金融业态界限越来越模糊，数据在不同金融业态和不同金融部门之间共享和流动是数字经济的必然要求[23]。与此同时，由于新金融业务表现形式复杂多样，且兼具传统金融风险和金融科技风险、资产证券化风险等金融风险属性，在后期处置过程中，由于部分新金融企业产品形式多样鱼龙混杂、线上快速交易与线下非法集资相结合、跨区域集资网络借贷、业务范围极广等因素影响，金融风险更具隐蔽性和跨区域分散性，给风险处置和追查带来巨大困难。导致监管部门无法实时跟踪、分析新金融机构的详细情况，也无法提前预警发现风险，加大了金融数据治理难度。

3.金融信息孤岛问题难以短期解决

当前，大规模数据散布在众多金融机构和信息系统中。从金融机构内部层面来看，一般来说，金融机构会基于服务需求使用多个供应商和非开源技术，导致金融机构内部出现多个独立的金融数据库，各部门掌握的金融数据相互分离；从金融机构外部角度来看，金融机构数据接口不统一，数据融合的应用标准尚未建立，导致许多场景下金融数据共享仍停留在表面。

4.数据安全行业缺乏内生发展机制

一方面，传统数据安全系统以静态为主，数字经济下金融场景变化快、数据量级大，金融机构对原有金融数据安全系统升级时所产生的成本和协调难度较大；另一方面，作为网络安全行业的一小部分，我国数据安全行业还处于初级发展阶段，行业发展生态系统尚未形成，行业规模较小，缺乏内生发展机制。

5.金融数据跨境流动规则冲突

当前，我国金融数据在跨境流动中，缺乏监管跨境数据流的统一框架和跨境数据流监管的国际合作机制，金融数据跨境传输数据的法定义务有待细化和统一，未明确区分金融数据跨境传输的不同目的和需要安全评估的情形[24]。各国基于自身国家安全和经济发展的角度制定了不同的跨境数据监管政策和数据流量规则，极易在实践中发生冲突。

（二）金融数据治理的国际经验

1.优化金融数据安全顶层设计，完善数据安全标准体系，为防范化解风险提供宏观制度遵循

第一，不断强化数据保护相关立法。为保护消费者数据权利、防范数据侵权行为，欧盟发布了《通用数据保护规则》《数据保护法》《为保持欧盟个人数据保护级别而采用的数据跨境转移工具补充措施》《通用数据保护条例》等政策文件，新西兰出台《2020年隐私法》，日本和新加坡修订了本国《个人信息（数据）保护法》，加拿大出台了《数字宪章实施法案2020》等，

持续优化政策环境，提升数据信息安全，为私营部门个人信息保护框架提供政策指导。

第二，加强消费者生物识别方面的立法。为防止消费者生物特征数据不被非法使用，许多发达国家从顶层设计和专项法律法规层面对人脸、声音、指纹等生物特征数据进行专项保护，严格防范新技术、新应用带来的数据安全风险。美国在州层面提出了《国家生物特征信息隐私法》专项立法，各州还根据地区实际情况出台了人脸识别相关法律。欧盟发布了人工智能战略等文件，监管企业和政府在公共场所使用摄像头收集个人生物特征数据的行为。

第三，制定战略计划规划。美国将发展网络安全产业提升到国家战略高度，增加网络安全预算，发布《联邦数据战略与2020年行动计划》。英国通过了“网络安全加速器计划”培养有潜力的网络安全企业，解决数据孤岛造成的不充分竞争问题。此外，还实施了“开放银行改革计划”，成立专门的开放银行倡议执行实体来确保数据安全获取及共享。

第四，设立金融数据监管机构。发达国家积极建立相关的金融数据安全机构、国家数据库或可疑交易监测分析中心，搜集和分析金融情报、监测资金总体流向和趋势以应对洗钱和恐怖组织融资等犯罪行为。如美国商务部成立了专门的咨询委员会加强对联邦数据隐私的保护，德国成立了国家网络安全局负责启动网络安全创新项目，研究如何应对网络威胁，加强德国“数据主权”。巴西成立了国家个人数据保护局，通过制定相关规则促进企业开展数据安全风险评估，监督惩处违法违规行为，促进数据保护方面的国际合作和数据共享等。欧盟设立了数据保护专员公署，负责监督个人数据及隐私保护，为个人信息相关事宜提供政策建议，开展欧盟内部信息共享与合作等。

第五，出台数据安全标准指南，完善数据安全标准体系，扩大数据主体权利。如欧盟颁布《数据保护指令》确立数据保护范围和数据主体权利，符合金融科技发展和数据保护的发展趋势。美国在“棱镜门”事件后，为进一步提升自身网络空间数据安全性，发布了《提升美国关键基础设施网络安全的框架规范》等数据安全网络和业务系统政策文件。同时，启动大数据相关研究，成立了大数据公开工作组，编写形成并发布了《NIST大数据互操作框架》系列标准。积极出台用户身份识别指南，加强数据安全评估和相关认证体系，如TRUSTe隐私认证得到世界范围内消费者的认可；另外，积极提升数据保护技术水平，加强网络安全产品创新。Facebook通过开源差分隐私库，苹果公司通过模糊定位技术，亚马逊推出Macie服务，新西兰企业运用区块链技术加强对数据的保护。以色列建设了一批高科技网络安全产业园，通过多种渠道展示和宣传网络安全企业的技术能力，鼓励国内企业与其他国家企业进行交流与合作，不断加大APT攻击、DDoS防御、网络取证、隐私保护等创新产品的出口。

2.将金融数据纳入反垄断监管，强化数据跨境流动监管力度，为金融数据要素市场提供良好发展环境

第一，将金融数据纳入反垄断监管内容。2019年2月，德国联邦卡特尔办公室裁定Facebook在收集和使用用户数据时存在剥削性滥用，要求其暂停相关行为并整改，该判例提供了将隐私数据纳入反垄断监管的案例。美国司法部正着手调查Visa和大型金融科技机构的合作关系，美国消费者金融保护局要求大型科技公司提交如何收集使用消费者支付数据信息的材料，从而判断这些大型科技公司是否存在金融数据的垄断行为。

第二，强化数据跨境流动监管，保障关键领域数据安全。2001年，欧洲委员会通过了《有关监管机构和跨境数据流通的附加协定》，确保个人数据在处理过程中得到保护，消除数据跨境自由流动障碍。美国主张个人数据跨境自由流动，但限制重点行业和领域的技术数据出口，利用“长臂管辖”规则强化对境外数据的执法能力。新加坡以建设亚太数据中心为导向，积极加入亚太

经合组织主导的跨境隐私规则体系，秉承数据跨境流动开放的态度，制定和完善数据跨境流动管理规则，吸引跨国公司投资数字基础设施建设，推动数字贸易发展。

第三，加强金融数据共享。美国金融统计数据库统计类型全面，范围广泛，金融数据虽分布在不同的监管部门，但数据收集、核实具有高度的标准化智能化流程和完善的跨部门协调组织共享数据程序。金融危机爆发后，美国进一步完善了金融数据的协调和共享机制。联邦金融机构检查委员会是最重要的跨部门协调组织，不仅实现了金融机构各类数据的科学统计，还建立了专门的信息共享责任小组和报告小组。同时，美国还成立了金融稳定监管委员会，进一步将非银行金融机构的数据统计纳入统一框架，并决定成立数据委员会和金融研究办公室，收集、分析和处理数据，形成一系列研究报告；英格兰银行借助如Gabriel等在线数据搜集系统搜集金融机构数据，同时，除了涉密部分之外，将其搜集的数据最大限度地免费开放给公众供其查询。英格兰银行提供表格和图片等多样化的查询结果，并对相关数据进行解释，还提供了相应专栏进行交流和答疑。德国金融数据库数据涵盖的范围较广，有时序数据库、宏观经济时序数据库以及欧洲中央银行体系数据库三个部分，分属于德国央行、德国金融监管局和德国联邦统计局三个部门，对三个部门的主要职责进行了分工并通过立法的形式进行了明确。

3.提升微观主体金融数据安全意识，加强违法问题处罚力度，规范交易主体行为

第一，提升金融数据安全知识宣传。自2004年起，美国于每年10月设立国家网络安全意识月，按照主题设置形式开展相应的网络安全活动，并向公众提供相应的建议。同时，为加强网络安全宣传，美国在联邦政府与国土安全部、国家网络安全联盟、国家信息安全局、各级地方政府和其他联邦部门间建立了灵活的跨部门、多层次的合作机制。通过线上线下结合，利用如社交媒体等公众喜闻乐见的方式，引导网民积极参与，具有成本低、投资少、易被网民接受等优点。此外，还推出了多种语言的网页，进一步推动美国与其他国家在网络安全意识教育月的合作。欧盟自2011年以来开始举办“欧洲网络安全月”，该宣传活动的最大特点是鼓励广泛的利益相关方参与，并且制定了非常简洁的参与程序，私营部门和民间机构是欧洲网络安全月的主要支撑力量。同时，欧盟成员国平时也会通过各国网站、社交媒体等方式加强宣传，以提高公众网络安全意识。

第二，加强违法问题处罚力度，规范金融微观主体行为。随着大型互联网平台企业的不断壮大，数据垄断问题越来越严重，由此产生的对数字权利的滥用可能威胁到国家安全。各国通过高惩罚等手段进一步限制，以防止他们滥用其数据优势侵犯消费者隐私或非法数据贩运。欧洲地区加大了对大型互联网企业数据安全违规的单项处罚力度。例如，2017年6月，谷歌滥用搜索引擎市场获取的数据优势推广自身旗下的比价购物服务，损害竞争对手利益，被欧盟开出24.2亿欧元的巨额罚单，爱尔兰对Facebook非法跨境传输数据处以高达28亿美元的罚款。

三、加强金融数据治理相关建议

加强金融业数据和信息的保护，既是金融业自身发展的客观要求，也是行业监管、国际竞争与合作的需要。根据数据安全相关法律法规要求，金融业应不断深化对数据安全的认识，积极应对和解决各种数据安全挑战。

（一）加快金融数据治理立法进程，优化金融数据治理顶层架构，确保金融数据主权不受侵害

第一，加快推动数据安全保护的配套法律法规建设，进一步明确个人金融交易信息在网络平台上使用的标准、流程和规范。数据确权是数据共享和流转的基础，但由于数据所有权、使用权和收益权难以界定，数据非法贩卖和无序竞争等乱象频频发生[25]。应立足于金融数据确权，对数据收集、存储、分享等各流程以及金融数据流通范围、流通规则、保护对象、权责关系和利

益分配以法律的形式进行明确，确保有章可循。

第二，构建国家数据安全的分级分类管理体系。在现有金融行业数据分类分级标准的基础上，推动重要数据的识别，强化相关部门与监管部门、国际标准化组织部门间的学习和合作，加快数据安全评估，形成行业重要数据目录。

第三，加强金融数据披露范围，突破部门和行业隐性壁垒。发布切实可行、具有指导意义的金融数据披露标准，对披露范围、数据更新和质量标准提出明确要求，推动数据公开和披露程序的标准化。引导和支持各类金融机构依法开放金融数据源，探索构建金融业与其他行业的数据互动机制，鼓励金融机构提高数据流通和共享频率，将解决信息孤岛问题作为构建数字共享新生态系统的重中之重，加快建设统一的政府信息共享平台，打破数据壁垒，防止算法共谋。

第四，搭建数据跨境国际合作平台，提高国际话语权。从国际秩序大局出发，积极参与和推动跨境数据流动国际规则体系的制定和完善，提高我国国际话语权。夯实域外管辖和跨境适用的法律基础，积极搭建金融数据跨境国际合作平台，监管境外金融机构在境内金融业务中的跨境数据流动、数据传输和应用，有效评估数据活动的风险，加强跨境执法国际合作。

（二）引入监管沙箱机制，加强对金融数据垄断及其他违法行为的监督执法，维护金融市场良好秩序

第一，完善监督组织结构，明确监督机构职责，将金融数据纳入反垄断体系。建立严格的数据交易监管体系，引入科学的业务集中度审查和报告标准，推动建立数据反垄断体系，加快制定金融科技营业执照或备案相关制度，规范金融科技企业获取、利用、传输和共享数据必须遵循的基本原则，并纳入监管体系。根据监管要求、行业特点和实际业务需求，明确金融数据监管机构的职责与权限。加强对行业重点信息和个人敏感信息的保护，加强对非法使用数据的披露和处罚，建立问责机制。监管部门应增加金融数据垄断或其他违法行为的罚款金额，配合司法部门打击各类违法违规行为，促进金融科技公司特别是特定金融科技应用的开发者能够以合法的方式、合理的成本获取数据源，规范大数据杀熟行为，促进金融市场的竞争、维护金融安全。

第二，提升金融数据监管技术水平，加强金融数据风险预警。逐步推动完善重要领域和重要机构的数据风险监管规则，充分发挥金融科技在金融风险监测预警领域的作用，加快网络安全态势感知、风险识别、行为识别、场景驱动智能控制、有效跟踪等技术的快速实施，准确高效地完成非结构化、非标准化数据的转化和聚类分析，实现风险信息的有效筛选和主动识别，实时监测风险态势并进行异常预警和溯源处置。在监管沙箱框架下探索和尝试金融数据开放共享机制，探索使用Regtech加强算法合规自动监管，综合运用加密存储、数据脱敏等技术采集、处理、利用和流通金融数据，防范数据开放技术带来的新风险。

（三）加强金融数据安全组织管理和技术水平，提高数据质量，防止数据被滥用、污染和泄露，维护金融微观主体合法权益

1.金融消费者层面

首先，要增强金融数据安全意识，重点关注金融服务中常见问题和金融热点，增强对金融产品和服务的认识以及风险责任意识，定期更换密码等重要信息，加强自身隐私金融数据相关信息的保护；其次，要增强金融风险识别能力，避免盲目投资和冲动交易，增强金融风险识别能力，远离和抵制非法金融活动；再次，要增强维权意识，培养良好、科学的金融线上线下交易习惯，了解金融消费者投诉处理渠道，一旦权益受损应迅速拿起法律武器及时维护自身合法权益，提升维权意识。

2.在金融机构层面

第一，加强数据安全内部金融数据管理体系和制度建设，明确各部门职能分工。构建以金融机构领导为主

体的数据安全治理团队，制定本机构内部数据管理的方针、制度和相关管理规程。构建以数据为中心的内部管理体系和内审监督机构，满足数据分类、身份认证、权限管理、异常检测和处理的总体安全要求，对数据安全流程的规范化和合规性负责。全面提高数据安全防护能力，做好数据备份和恢复工作，加强内部数据风险监管。

第二，夯实金融数据安全风险的技术防范手段，防范数据泄露风险。运用数据安全治理思想，从被动防御转向主动防御，借助大数据分析和人工智能，加快大数据环境下金融数据安全技术研究，探索金融数据治理各业务领域的应用前景和技术流程手段，推动网络安全态势感知、风险识别、行为识别等技术的实施，提高对未知威胁的防护能力和效率。引导和推动科研机构和企业加强研究和技术创新，打造产品核心竞争力，稳步降低对国外产品和技术的依赖。加强培养专业的复合型人才，加强对相关人才的培训管理，加强对数据治理和数字技术开发应用急需专业技术人员的吸纳。

第三，提升金融数据的规范化管理，防止数据污染，有效释放数据价值。确定金融数据质量控制归口管理部门，成立由相关部门、监事会、董事会和高级管理人员组成的金融数据质量管理委员会，牵头进行金融数据质量控制和管理，探索数据质量管理评价体系建设，加强金融数据资产管理和金融数据分级管理，根据数据层次制定差异化的控制措施，实现金融数据的精细化管理。

第四，防范金融数据共享中潜在风险。建立政府部门间有效信息共享平台机制，扩大数据共享范围，增加数据共享渠道，弥补各平台数据不足，提高监管效率，为市场主体提供准确、快速、安全的信息验证渠道，防范欺诈风险。金融机构应探索监管统计体系建设，不断加强金融数据采集的规范化和源头管理，加强金融数据应用情况的效果评价，加强对金融数据价值挖掘，提高金融数据的应用水平。

第五，大力进行金融消费者权益保护教育宣传。继续把推广金融知识作为常态工作，充分发挥线上宣传平台和线下网点优势，因地制宜开展多种形式教育宣传活动，积极传播金融知识，扩大金融宣传范围。提高宣传活动的普遍性和针对性，加强金融政策、金融业务知识、支付安全知识、个人金融信息保护等重点宣传，积极组织业务骨干重点加强对特定群体的关注等。

参考文献：

[1]杨帆. 金融监管中的数据共享机制研究[J]. 金融监管研究，2019(10): 53–68.

[2]Korhonen J J, Melleri I, Hiekkanen K, et al. Designing data governance structure: An organizational perspective[J]. The GSTF Journal on Computing, 2013(02): 11–17.

[3]Emieux V, Fisher B, Dang T. The visual analysis of financial data[J]. Handbook of Financial Data & Risk Information II, 2014(02): 279–326.

[4]Putro B L, Surendro K, Faust H. Leadership and culture of data governance for the achievement of higher education goals (Case study: Indonesia University of Education)[C]. Proceedings of International Seminar on Mathematics, Science, & Computer Science Education, 2016. DOI:10.1063/1.4941160.

[5]Al–Ruithe M, Benkhelifa E, Hameed K. A conceptual framework for designing data governance for cloud computing[J]. Procedia Computer Science, 2016, 94: 160–167.

[6]Allen C, Des Jardins T R, Heider A, et al. Data governance and data sharing agreements for community–wide health information exchange: Lessons from the beacon communities[J]. Generating Evidence & Methods to Improve Patient Outcomes, 2014, 2(01): 01–09.

[7]Kerber W, Frank S. Data governance regimes in the digital economy: The example of connected cars[J]. Social Science Electronic Publishing, 2017(10): 1–6.

[8]Goldstein G C J. Information technology–related

operational risk: An empirical study[D]. New York：The Graduate School of Syracuse University，2009: 1–164.

[9]Biolcheva P. Risk prevention of data leakage by commercial banks[J]. Nauchni Trudove, 2016(02): 76–121.

[10]Mettler T, Winter R. Are business users social? A design experiment exploring information sharing in enterprise social systems[J]. Journal of Information Technology, 2016, 31(02): 101–114.

[11]Blocki J, Christin N, Datta A, et al. Audit mechanisms for provable risk management and accountable data governance[M]. Heidelberg: Springer, 2012: 38–59.

[12]Felici M, Pearson S. Accountability for data governance in the cloud[C]. Summer School on Accountability and Security in the Cloud Springer, Cham, 2014: 3–42.

[13]Al–Ruithe M, Benkhelifa E, Hameed K. Key dimensions for cloud data governance[C]. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2016：379–386.

[14]Tahiliani M, Laik P, Bahl G, et al. Data governance manager for master data management hubs: US, US8458148 B2[P]. 2016.

[15]Brous P, Janssen M, Vilminkoheikkinen R. Coordinating decision–making in data management activities: A systematic review of data governance principles[C]. International Conference on Electronic Government & the Information Systems Perspective Springer, Cham, 2016: 115–125.

[16]Gregory A, Hunter K. Data governance—protecting and unleashing the value of your customer data assets[J]. Journal of Direct Data & Digital Marketing Practice, 2011, 13(01): 40–56.

[17]Otto B. Data Governance[J]. Business & Information Systems Engineering, 2011, 3(04): 241–244.

[18]Waddington D. Data governance, MDM and data quality[J]. Information Management, 2010, 20(05): 14–16.

[19]Wei–Skillern J, Silver N. Four network principles for collaboration success[J]. Foundation Review, 2013, 5(01): 121–129.

[20]Martijn N, Hulstijn J, Bruijne M, et al. Determining the effects of data governance on the performance and compliance of enterprises in the logistics and retail Sector[C]. Conference on e–Business, e–Services and e–Society. Springer International Publishing, 2015: 454–466.

[21]Flood M D, Mendelowitz A I, Nichols B. Monitoring financial stability in a complex world[M]. Heidelberg: Springer, 2012: 15–45.

[22]郑岩. 数字金融背景下个人金融数据风险监管问题[J]. 沈阳师范大学学报：社会科学版，2021，45(02)：38–45.

[23]李笑，华桂宏. 中国高科技企业OFDI速度对创新绩效的影响——基于总体创新、颠覆式创新和渐进式创新视角[J]. 南方经济，2020(11)：28–46.

[24]马兰. 金融数据跨境流动规制的核心问题和中国因应[J]. 国际法研究，2020(03)：82–101.

[25]吕佳蕾，李正印. 数字金融的发展风险及监管应对[J]. 全国流通经济，2021(13)：154–156.

作者简介：

夏诗园，女，河南周口人，经济学博士，金融学博士后，中华人民共和国审计署审计科研所副研究员，主要研究方向：宏观经济运行、金融计量与金融工程、金融风险与金融监管。

尹振涛，男，山东青岛人，经济学博士，中国社会科学院金融研究所副研究员，中国社会科学院金融研究所金融科技研究室主任，主要研究方向：金融科技与金融监管。