Advances in Social Sciences 社会科学前沿, 2025, 14(8), 243-252
Published Online August 2025 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2025.148711

Hans汉斯

金融数据法律规制的现状反思与完善路径

彭明入

广西大学法学院，广西 南宁

收稿日期：2025年6月16日；录用日期：2025年8月4日；发布日期：2025年8月13日

摘　要

金融数据由于其经济属性与社会属性的双重特性，导致权属界定与治理难度增大，在安全和利用价值之间需要寻求动态平衡。现阶段，我国金融数据法律规制体系存在数据质量管理不足、金融用户与机构之间的风险承担失衡、中小型金融机构数据治理能力薄弱、监管体系分散与协调不足等问题限制了金融数据作为生产要素的潜能释放。通过强化数据质量管理与数据标准化建设，提升金融数据的准确性、一致性和可用性，为数据要素市场化流通提供基础支持；完善法律规制体系，明确金融数据权属与流通规则，建立科学合理的分级保护与责任分配机制，推动金融数据治理的法治化进程；构建多层次、多维度的数据监管体系，加强科技与传统监管的融合，探索人工智能、大数据和区块链等新兴技术在监管中的应用，实现对金融数据的动态化管理和实时风险监控；通过政策引导与资源倾斜，帮助中小型金融机构弥补数据治理能力短板，降低合规成本，提升数据治理水平。

关键词

金融数据治理，法律规制，数据安全

Reflections on the Current Situation and Improvement Paths of Legal Regulation of Financial Data

Mingru Peng

Law School of Guangxi University, Nanning Guangxi

Received: Jun. 16th, 2025; accepted: Aug. 4th, 2025; published: Aug. 13th, 2025

Abstract

Due to the dual characteristics of economic and social attributes of financial data, defining ownership and governance becomes more challenging, necessitating the pursuit of a dynamic balance between

文章引用: 彭明入. 金融数据法律规制的现状反思与完善路径[J]. 社会科学前沿, 2025, 14(8): 243-252.
DOI: 10.12677/ass.2025.148711

security and utilization value. At present, China's legal regulatory framework for financial data faces issues such as inadequate data quality management, an imbalance in risk-sharing between financial users and institutions, weak data governance capabilities in small and medium-sized financial institutions, and a fragmented and poorly coordinated regulatory system, all of which constrain the full potential of financial data as a factor of production. By strengthening data quality management and standardization efforts, we can enhance the accuracy, consistency, and usability of financial data, providing foundational support for the market-oriented circulation of data elements. Improving the legal regulatory framework, clarifying ownership and circulation rules for financial data, and establishing a scientifically sound and reasonable graded protection and responsibility allocation mechanism will advance the legal governance of financial data. Constructing a multi-tiered and multidimensional data regulatory system, enhancing the integration of technology with traditional supervision, and exploring the application of emerging technologies such as artificial intelligence, big data, and blockchain in regulatory practices will enable dynamic management and real-time risk monitoring of financial data. Through policy guidance and resource allocation, we can assist small and medium-sized financial institutions in addressing their shortcomings in data governance capabilities, reducing compliance costs, and elevating their data governance standards.

Keywords

Financial Data Governance, Legal Regulation, Data Security

1. 引言

随着科技与金融的不断融合，金融行业的数字化进程加速。数据的地位从过去被视为金融业务运行的附属产品上升为推动金融业务发展的要素。数据的经济价值和重要性愈发显现，受到国家和社会的高度重视。在大数据技术迅速发展的背景下，人工智能、区块链、云计算等新兴数字技术对传统金融行业带来了巨大冲击。不仅加速了金融服务理念的变革和经营模式的重塑，还推动了金融业态和产品的频繁迭代。数据规模也呈现出指数级增长，数据已成为业务运营、战略决策和风险管理中的重要资源。如何高效利用和管理海量数据成为一大难题：一方面，对金融数据质量的要求越来越高；另一方面，金融数据安全与隐私保护的问题日益凸显。因此，金融数据治理需要实现“挖掘数据价值”和“保障数据安全与隐私”两大目标的平衡。

2. 金融数据的概念

在理论研究上看，金融数据由于同时具有经济属性与社会属性增加了对其权属定性的难度。但是，金融数据权属的研究却进展显著，衍生出财产权理论、人格权理论及新型权利理论等理论学说。在法律法规上看，国内法律法规尚未对金融数据作出明确的定义。现行法律对“金融数据”或“金融信息”的具体内涵与外延没有统一规定，而相关部门规章也未对此作明确界定。要实现对金融数据的规范治理需要通过立法明确“数据”与“信息”的定义。在语义层次上看，数据与信息既密切相关，又有明显区别。数据通常是信息的记录形式，主要体现在其技术属性上，而信息是数据经过解读后的表达[1]。在数字技术语境下，数据被认为是以电子或其他形式存在的信息载体。《数据安全法》基于此将“数据”界定为“任何以电子或者其他方式对信息的记录”，那么信息则是数据经解读后呈现的内容。在范围上看，金融数

据的涵盖范围明显广于个人金融信息。金融数据不仅包括金融机构收集的原始数据，还包括经过处理生成的信息。而金融机构的服务对象包括个人客户和企业客户，因此，金融数据涉及的内容既包含个人金融信息，也包括企业客户信息。

3. 平衡金融数据权属、数据安全与价值挖掘

3.1. 平衡金融数据权利与数据价值

在数字经济浪潮与金融创新加速融合的宏观背景下，金融数据法律规制体系正遭遇制度构建与实践需求错位的双重困境：数据权利制度的核心在于构建静态私权保护框架，通过法律条文精准界定数据主体、数据控制者以及数据处理者的权利义务边界；而数据价值实现路径则聚焦于动态要素配置效率，强调数据在多元市场主体与差异化应用场景中的流通转化。根据产权经济学理论，明晰的产权界定是数据要素实现市场化高效配置的必要前提。但是，金融数据来源的多元性、类型的复杂性，叠加现行法律体系存在的结构性缺陷，致使金融数据权利的法律属性、权利范围及归属认定长期处于模糊状态，严重掣肘金融数据流通共享生态的培育与发展。以个人信息保护法律框架和民事财产权制度为基石的金融数据权利保护体系，与以金融监管规则为导向的数据流通规范体系之间，存在显著的制度鸿沟与衔接断裂，形成制约金融数据治理效能提升的主要矛盾。

金融数据权利体系的模糊与复杂，已成为数据流通利用的根本性制度壁垒。基于经济学理性人假设，金融数据控制者参与数据流通的主要驱动在于其合法权益能获得坚实的法律保障，有效规避潜在的权利争议风险。但在理论研究与法律实践层面，数据权利的法律性质、构成要素及归属界定等基础性问题仍存广泛争议。以“数据二十条”提出的“三权分置”政策设想为例，该方案更多体现为宏观政策层面的方向性指引，尚未完成向具体法律制度的实质性转化，且在数据人格权益保护维度存在明显制度空白。金融数据生成过程涉及客户、金融机构、监管部门等主体，涵盖个人敏感信息、企业运营数据及公共管理数据等类型，使得金融数据权益的识别与划分工作面临巨大挑战。在数据流通实践场景中，相关主体普遍陷入“流通犹豫”困境：一方面，由于权利界定模糊，主体担忧数据流转过程中侵犯其他方在先权益；另一方面，因缺乏健全的权益保障机制，主体对自身数据权益能否得到有效维护心存疑虑。当前我国金融数据流通模式呈现显著的单向性特征，主要表现为金融机构向监管部门的数据报送，机构间的数据共享机制发育滞后。现行金融监管规则在制度设计中对数据权利保护的关注度不足，且因其法律效力层级较低，难以满足金融数据全场景流通与深度开发的制度需求。

金融数据处理中的合法利益豁免机制存在适用范围有限与制度短板。客户数据尤其是个人金融数据因其承载的敏感信息与财产权益属性，成为金融数据治理的一大难点。依据《个人信息保护法》的规定，个人金融数据处理活动必须严格遵循法律规范。该法第 13 条确立的知情同意规则例外情形，为金融机构基于合同履行、法定职责等特定目的处理个人金融数据开辟了“合法利益豁免”通道，使其能开展数据传输、共享等流通活动。但是，这在金融机构间数据共享场景中面临严峻的适用性挑战。虽然该机制在一定程度上降低了金融机构处理个人金融数据时面临的权利主张风险，但机构间的数据共享多以商业利益获取为目标，明显超出金融业务开展与监管合规的合理利益边界。根据行业调研数据显示，在涉及商业合作的数据共享场景中，因无法适用豁免条款而需获取客户同意的数据请求，其实际通过率不足 30%，充分表明金融机构间数据共享面临着难以突破的现实障碍。

3.2. 平衡数据流通与数据安全

在数字技术深度重塑金融业态的背景下，数据治理领域“安全保障与价值释放协同推进”的理念，在金融数据治理实践中遭遇结构性矛盾。从治理目标的本质来看，金融数据流通旨在构建覆盖全行业的

要素配置网络，通过数据在不同主体和场景间的流转，实现数据资源的经济价值与社会价值最大化；而数据安全保障则聚焦于构建全生命周期防护体系，致力于维护数据资产在采集、存储、处理、传输等各环节的保密性、完整性与可用性。但是，这两大治理目标在实际操作上出现互斥性：金融数据的流通天然伴随着处理主体数量的增多和操作频次的提升，数据交互过程不可避免地扩大了风险暴露范围；反之，严格的数据安全规制措施所带来的合规成本攀升，又对数据流通的效率和规模形成刚性约束，使得安全与发展的平衡成为金融数据治理的一大难题。

金融数据流转过程中潜藏着个人信息泄露与数据滥用的风险。作为数据要素市场化配置的环节，金融数据的流通涉及复杂的数据权属转移与多维度处理活动，尤其在金融机构间的数据共享场景下，数据使用边界模糊与责任界定不清的问题更为突出。金融数据涵盖用户身份识别信息、资产负债详情、交易行为特征等高度敏感内容，尽管匿名化、去标识化等技术手段被广泛应用，但在当前技术条件下，仍难以完全消除数据被重新识别的可能性。欧盟数据保护委员会(EDPB) 2023 年发布的研究报告显示，在金融数据流通场景中，约 45%的隐私泄露事件源于数据处理环节的权限管理缺陷。当数据副本脱离原始控制主体后，无论是向监管机构报送，还是在同业机构间共享，若缺乏完善的数据治理机制，极易滋生数据滥用行为。典型表现包括未经授权的数据访问、超范围的数据使用，以及违反数据使用协议的数据商业化开发等，不仅直接侵犯用户的合法权益，还可能引发系统性金融风险，威胁金融市场稳定。

金融体系内部数据安全防护能力的差异加剧了数据流通中的安全隐患。尽管金融行业依托《个人金融信息保护技术规范》《金融数据安全数据生命周期安全规范》等技术标准，构建了相对完备的数据安全防护框架，但不同规模和类型的金融机构在技术投入、人才储备和合规管理水平方面存在较大差距。大型金融集团凭借雄厚的资金实力和技术优势，建立采用高级加密算法、部署实时安全监测系统、建立应急响应机制等数据全生命周期的防护体系；而中小金融机构受制于资源限制，在数据加密技术更新、漏洞扫描频率、安全人员配置等方面存在明显不足。防护能力的不均衡使得数据流通链条中的薄弱环节成为安全风险的突破口。根据金融稳定理事会(FSB)的统计数据，近年来约 68%的数据泄露事件与第三方合作机构或中小金融机构的安全防护不足相关，凸显出数据流通中风险传导的连锁效应。

安全与流通的双重目标要求会给金融机构带来巨大的技术成本和合规成本。金融数据治理的理想状态是在确保数据安全可控的前提下，实现数据的高效流通与价值增值。金融机构需在技术和合规层面进行大量投入：在技术层面，不仅要建设跨机构的数据共享基础设施，统一数据接口标准，还需引入联邦学习、多方安全计算、隐私计算等前沿技术，以保障数据在流通中的安全性和隐私性。以构建一套符合行业标准的数据共享平台为例，从系统架构设计、安全防护部署到技术方案研发，整体成本可能超过数千万元。在合规层面，随着数据流通场景的不断拓展，金融机构的合规管理范围从传统的数据采集和使用环节，延伸到数据传输、共享等新增环节。行业调研显示，数据流通场景下金融机构的合规成本较单一使用场景平均增加 60%~80%。如此高昂的技术和合规成本，对中小金融机构形成明显的挤出效应。世界银行 2024 年的研究报告指出，约 80%的中小金融机构因成本压力推迟或取消数据共享项目，严重制约了金融数据生态的健康发展。

4. 金融数据法律规则的国际考察

4.1. 欧盟《通用数据保护条例》(GDPR)的制度创新与全球效应

2018 年 5 月生效的 GDPR 不仅延续了欧盟对个人数据隐私保护的立法传统，还体现了应对数字经济时代技术变革的战略考量，其确立的规则体系对全球数据治理格局产生了深远影响。相较于 1995 年《数据保护指令》，GDPR 在多个维度实现了突破性创新。

在法律适用范围方面，GDPR 突破传统属地管辖原则，创新性地引入“属人”管辖概念。对于设立在欧盟境内的机构，无论数据处理活动发生于何处，均需严格遵守 GDPR 规定；而对于欧盟境外主体，只要其数据处理行为涉及欧盟境内数据主体的个人信息，或对欧盟个人活动实施监控，同样受该法规约束。双重管辖机制显著扩大了法律覆盖面，强化了对欧盟公民数据权益的跨境保护力度。

数据主体权利的拓展是 GDPR 的一大创新亮点。法规新增的删除权(被遗忘权)赋予数据主体在特定条件下要求删除个人信息的权利，有效解决信息过度留存问题；数据可携带权则保障用户能够获取并转移自身数据，促进数据在不同服务提供商间的有序流动。对知情权与访问权的进一步细化，使数据主体能够更全面地了解数据处理的目的、方式及存储状态，显著提升了个人对自身数据的实际控制权。不仅重塑了数据主体与处理者之间的权利义务关系，也促使企业对数据管理流程进行系统性重构以满足合规要求。

GDPR 对数据控制者与处理者的责任规制更为全面和严格。首次将数据处理者纳入直接监管范畴，明确界定双方在数据处理全流程中的具体义务，包括详细记录数据处理活动、对高风险处理行为开展事前影响评估、建立 72 小时数据泄露报告机制等。法规还对数据安全保障措施提出更高标准，要求控制者与处理者采取技术与组织措施确保数据安全，并对双方签订的数据处理合同内容作出细致规定，将监管范围延伸至数据处理的各个环节，形成完整的责任追溯体系。

在监管与救济机制构建上，GDPR 形成了严密的制度设计。通过建立监管一致性机制，协调欧盟成员国间监管机构的合作，降低重复监管带来的成本负担；严苛的处罚条款以企业全球营收为基准设定罚款标准，最高可达 4%，形成强大的法律威慑力；完善的司法救济途径保障数据主体的合法权益，允许其在权益受损时提出损害赔偿请求，并赋予消费者机构代为行使救济权利的资格，实现了对数据主体权益的全方位、多层次保护。

4.2. 美国金融数据治理立法的分散式架构与演进轨迹

作为全球信息技术创新的核心地带，美国在享受数字技术带来的产业红利时，也持续面临着严峻的数据安全威胁。据网络安全研究机构统计，过去十年间，美国境内发生的数据泄露事件已突破万起大关，其中 2018 年脸书(Facebook)高达 5000 万用户数据泄露事件，不仅引发资本市场剧烈震动，还在全美范围内掀起了关于数据隐私保护的深度讨论。尽管数据安全问题频发，但受联邦制政治体制下州权与联邦权的博弈、不同利益集团诉求难以调和等因素制约，美国联邦层面至今未能出台一部统一的数据隐私保护法案。值得注意的是，作为现代隐私权理论的发源地，美国构建起了一套极具特色的分散化立法体系。该体系通过至少 12 部联邦法律，针对不同行业特性制定差异化保护规则，并借助州级立法创新，逐步填补联邦监管空白。

联邦层面：多维度金融数据治理法律体系的构建与发展

美国联邦金融数据保护立法的演进，始终围绕着政府权力与公民隐私权益的平衡展开。1978 年，《金融隐私权法》(Right to Financial Privacy Act)的颁布，为美国金融数据治理奠定了重要的法律基础。该法案明确规定，联邦机构若想获取金融机构所保存的消费者金融记录，必须严格遵循法定程序。只有在获得消费者的书面授权，或者持有有效的行政传票、司法传票、搜查令等法律文书的情况下，金融机构才能够向联邦机构提供相关记录。有效遏制了政府对个人金融信息的过度干预，为个人金融数据保护设立了第一道坚实防线，其确立的“必要且合法”数据调取原则，至今仍是美国金融数据监管的重要准则。

1999 年，《金融服务现代化法》的出台，标志着美国金融数据治理进入了体系化发展阶段。法案的第五部分着重强化了金融机构在消费者隐私权保护方面的主体责任，要求银行、证券、保险等各类金融机构，必须建立起涵盖数据全生命周期的安全管理机制。2008 年全球金融危机爆发后，美国于 2010 年推

出了《多德–弗兰克华尔街改革和消费者保护法案》，在金融数据治理领域开启了新一轮制度革新。法案设立了消费者金融保护局(Consumer Financial Protection Bureau, CFPB)，并赋予其对信用卡、住房贷款、消费信贷等全业务场景的数据处理活动进行独立监管的权力。CFPB 通过制定详细的监管标准、开展常态化的合规检查、建立高效的投诉处理机制等方式，确保金融机构在数据的收集、分析、使用等各个环节，都能充分保障消费者的合法权益。此外，联邦层面还出台了多部涉及消费者金融隐私保护的法律。例如，《公平信用报告法》对信用数据的采集、使用和披露流程进行了全面规范；《公平和准确信贷交易法》进一步强化了信用报告的安全管理；《电子资金转账法》则致力于保障电子支付过程中数据的传输安全。

州级层面：数据治理立法的创新实践与突破

美国州级立法在数据治理领域发挥着重要的创新引领作用。作为众多互联网科技企业的集聚地，加利福尼亚州在 2002 年率先颁布了《数据泄露通知法案》，这一举措开创了全美数据泄露管理制度的先河。该法案明确规定，企业一旦发生数据泄露事件，必须在规定的时间期限内，向受到影响的消费者发出通知。这一规定旨在通过信息公开机制，促使企业加大在数据安全方面的投入，同时也让个人能够及时知晓自身数据安全状况，以便采取相应的补救措施。受加州立法的影响，此后美国各州纷纷效仿，截至目前，美国已有 48 个州陆续制定了类似的数据泄露通知法规，初步形成了覆盖全国的监管体系。

随着网络攻击手段的日益多样化和数据泄露事件的频繁发生，原有的数据泄露通知法规逐渐暴露出监管上的不足。2018 年，万豪酒店 5 亿客户数据泄露、Equifax 信用机构 1.43 亿用户信息泄露等一系列重大数据安全事件的发生，给美国社会带来了巨大冲击，也促使各州加快了立法修订的步伐。修订后的法规普遍新增了免费信用监测服务条款，明确要求涉事企业在数据泄露事件发生后，必须为受影响的个人提供至少一年的免费信用监测服务，以此降低因数据泄露可能引发的身份盗用、金融诈骗等次生风险，充分体现了数据治理立法的动态适应性。在州级立法成果中，《2018 年加州消费者隐私法案》(California Consumer Privacy Act of 2018, CCPA)及其后续修订法案具有里程碑式的意义。CCPA 赋予了消费者数据访问权、删除权、拒绝出售权等多项重要权利，同时要求企业必须清晰公开数据的收集类别、使用目的以及共享对象，并对违规企业设定了高额的罚款标准，最高可达 2500 美元/消费者或企业全球营收的 4%。2020 年通过的《加利福尼亚州隐私权法案》(California Privacy Rights Act, CPRA)则进一步拓展了消费者的权利边界，将精准定位数据、种族信息、宗教信仰、基因数据、私人通讯记录、性取向以及具体健康信息等 11 类敏感个人信息纳入了严格的保护范畴。此外，CPRA 还专门设立了加州隐私保护局(California Privacy Protection Agency, CPPA)，赋予其规则制定、执法检查、行政处罚等核心职能，标志着美国州级数据治理从以往较为分散的立法模式，逐步向专业化、体系化的监管模式转型。

5. 金融数据法律规制面临的困境

5.1. 金融数据质量不高

在金融科技快速发展的背景下，高质量的金融数据已经成为支持创新型金融服务和精准决策的重要资源。当前我国金融行业在数据质量方面仍然存在诸多问题，对金融数据的挖掘和高效应用构成了严重阻碍，导致行业发展受到一定程度的限制。

首先，金融数据的准确性仍需提高。作为数据分析和应用的基础，准确性直接影响金融数据的价值实现[2]。由于金融数据来源复杂、缺乏统一的治理标准，我国金融机构在数据采集和处理过程中存在较多问题。一些机构由于未能运用科学化和标准化的管理方法导致大量错误数据或异常数据(即“脏数据”)的出现，极大地削弱了金融数据的准确性和完整性。例如，部分银行仍采用传统的统计调查方式获取下属机构报送的数据，不可避免地存在人为干预甚至数据修饰的情况，使数据真实性难以保证。此外，传

统的数据处理模式严重依赖人工操作，极易产生输入错误或其他偏差，降低了数据的可信度和实用性。不仅为金融风险的预警和治理增加了难度，还直接影响了金融机构的决策效率和质量。而金融数据的动态变化特性也加剧了数据准确性问题。由于金融活动中数据的变化频率较高，未能及时更新或处理的数据往往会迅速失去其时效性，成为“过期数据”。滞后的数据不仅对金融机构的战略规划和业务决策产生误导，也可能在应用中带来潜在的风险隐患。

其次，数据一致性难以有效保障。金融机构业务的复杂性和广泛性导致其内部各部门在数据采集和统计标准上存在差异。例如，不同部门可能在同一数据的描述、统计口径或处理方式上采用不同的规范，往往使得同一数据在不同场景下被解读为完全不同的含义，数据一致性因此无法得到充分保障，给金融机构的整体数据治理带来了巨大的清洗成本。

由于数据在统计标准和处理规范上的差异，金融机构在建模过程中可能无法保证数据的可靠性和准确性，从而影响分析结果的科学性。限制了金融数据挖掘的深度，削弱了数据对金融产品设计、风险控制和业务优化的支持作用。

5.2. 金融机构与金融用户的风险承担失衡

当前的金融数据治理主要是平衡数据价值的挖掘与数据安全的保障。但是，金融数据一方面为金融机构带来了商业价值和创新动能，另一方面也引发了数据行业和金融行业普遍存在的过度收集、违规使用和超期存储等问题。强势主体由于具备技术能力和资源上的天然优势，在数据处理和风险分配上占据了主导地位，而相对弱势的用户群体则因为技术劣势或对便利目的的追求承担了更多的金融数据安全风险。

一是强势主体对风险的转移。在金融数据治理中，强势主体是指那些在数据处理技术、资源整合能力以及风险分配权力方面占据明显优势的机构或组织，主要是金融机构及其合作的数据公司。这些强势主体通过掌控数据的采集、分析和利用实现了商业利益的最大化。在利益驱动下，金融机构与数据公司通过直接或间接方式获取用户数据以进一步挖掘这些数据的潜在商业价值，通过对数据的商业化运作实现资本融资。这种行为逐渐成为行业惯例，并形成了数据商业化和资本化的链条。但是，这也导致了数据权益分配的严重失衡。在数据交易中，强势主体利用其技术和资源优势将数据相关的安全风险转移给用户群体。用户的数据在采集、存储和利用过程中存在着显著的信息不对称，数据主体对自身数据的流向和用途知之甚少。这种风险转移机制使得数据主体的合法权益处于被侵害的高风险状态，而强势主体则在风险分配中处于相对受益的一方。

二是弱势主体的风险承受困境。相比之下，金融数据治理体系中的弱势主体通常是普通用户或数据提供者。他们在数据治理中的弱势地位主要表现为缺乏对数据风险的认知能力、风险防控手段以及参与数据使用决策的权力。在数据的采集、存储和应用等环节中，弱势主体往往被动接受所有可能存在的风险，而无力干预或规避。金融用户在接受金融服务或产品时，其群体构成的多样性导致了数据保护需求和认知水平的显著差异：部分用户由于缺乏对数据安全的足够关注，往往将便利性或收益性放在首位，而忽视了数据可能被滥用的潜在风险；而在不同金融平台提供的金融数据安全保障服务中，即使用户可以选择风险较低的平台，数据安全问题仍然很少成为其选择服务的主要标准，使得用户在数据利用链条中处于更加被动的地位。此外，金融用户在数据处理的环节中缺乏知情权和选择权，无力干预数据的进一步利用过程，他们在风险分配中的话语权几乎为零，既无法获得相关风险的补偿，也缺乏隔离或抵御风险的能力。这种被动局面使得他们成为金融数据利用过程中风险的主要承担者。当用户对金融数据安全问题采取漠视或妥协态度时进一步助长了强势主体的数据滥用行为，使数据安全问题不断积累并向更大范围扩散。不仅威胁到个体用户的合法权益，也可能引发金融行业数据治理的失衡，最终对金融市场的稳定性产生负面冲击。

5.3. 中小型金融机构数据治理能力不足

中小型金融机构在数据治理方面的能力相对较弱，数据治理意识也普遍不足。当前，中小型金融机构在数据治理上的劣势可以归因于多个方面。首先，中小型金融机构受制于基础设施的限制。与大型金融机构相比，中小型金融机构在与金融科技公司或大数据公司的合作中缺乏足够的议价能力[3]。为了降低成本，它们通常选择与价格较低的数据公司或科技公司合作。但是，这些公司通常技术水平有限，甚至可能涉及非法数据收集等违规行为，从而为金融数据安全埋下隐患。其次，中小型金融机构在数据治理上的意识相对薄弱。大多数中小型金融机构规模较小，其日常经营本身已经面临较大压力，因此对数据治理的重视程度较低。在一些经营状况不佳的中小型金融机构中管理层优先考虑的是公司的生存问题，而数据治理工作往往被忽视。这种状况容易导致恶性循环：中小型金融机构在有限的存续时间内难以建立起系统化、规范化的数据治理框架。即便是在经营相对稳定的中小型金融机构中，开展数据治理工作仍需要付出较高的“合规成本”。在成本与收益的权衡之下，管理层往往选择将资源集中于其他更为紧迫的业务问题，而数据治理工作因此被简化甚至忽略。缺乏数据治理意识的现象使得中小型金融机构难以认识到数据在市场竞争中的战略价值，也未能充分探索数据应用的实际场景。导致了金融机构之间的数据流通意识不足，在整体理念上也未能形成以数据驱动的行业共识。第三，中小型金融机构数据治理的成本过高。为了推动金融数据在机构之间的有效流通，金融机构需要引入隐私计算、区块链等新技术建立一个实现数据互联互通的平台，并制定统一的技术标准以解决数据兼容性问题，而新技术的研发和部署往往需要耗费大量资源和资金。对于大型金融机构而言，由于其资源和技术优势，高昂的技术成本和合规成本对其影响有限。但对于中小型金融机构来说，这些成本则构成了巨大的压力。中小型金融机构由于资源有限，在应对复杂的数据治理和流通需求时显得力不从心。高额的技术投入和合规成本往往会削弱其在金融数据流通中的竞争力，抑制其参与数据流通的积极性，从而加剧其与大型金融机构之间的数据治理能力差距。

6. 金融数据法律规制的完善路径

6.1. 强化数据质量管控，释放数据要素价值

为了挖掘金融数据作为生产要素的潜力，提升数据质量是关键。金融数据的质量直接影响其在金融机构决策、业务创新和风险管理中的应用效果，因此需要从内部组织管理、数据资产维护、分级管理与外部监管等维度进行全面优化：

一是优化内部组织架构以支撑数据质量管理。金融数据质量管理涉及多部门协作的复杂工程，需要有明确的组织架构和管理流程予以支持。一方面，商业银行等金融机构应基于各自业务特点成立专门的数据质量管理委员会，由不同部门负责人、高级管理层及监事会成员共同组成。其主要职责在于统筹协调金融数据质量管理工作，构建数据质量管理考核评价体系，将评价结果纳入绩效管理框架，以增强各部门和员工对数据质量的关注程度和责任意识。另一方面，由于金融数据管理往往存在部门分工不清、权责交叉等问题，导致管理工作碎片化。因此，应明确数据质量管理的归口部门，由该部门制定和优化数据管理制度，根据业务需求和外部监管要求，动态调整相关规章制度，确保数据质量管理的持续性与有效性。

二是加强金融数据资产管理。金融机构应围绕数据标准化建设，构建全局数据模型，通过科学的技术架构对数据资产目录进行全面管理和动态维护。实现对数据资源的集中管理与全面掌控，从根本上解决数据利用率低下和质量参差不齐的问题。通过标准化的数据管理体系，金融机构不仅能提升数据的准确性和可用性，还能降低因数据重复采集、错误处理等问题引发的资源浪费，提高数据在业务分析和决策中的应用价值。

三是建立科学的金融数据分级管理体系。鉴于金融数据的多样性和复杂性，以及不同数据在敏感性、隐私性和安全性方面的差异，金融机构需要基于科学的分级策略对数据进行分类管理。金融机构应综合考虑国家安全、企业利益以及用户隐私保护等因素制定全局性的数据分级管理方案。对敏感性较高的数据，应采取严格的访问权限控制和操作审计措施，确保数据的使用安全；而对于敏感性较低的普通数据，则可以采取相对灵活的管理方式，以提高数据利用效率。实现对不同类型数据资源的差异化管理，推动数据管理的精细化发展。

四是强化金融数据质量的监管与控制。外部监管部门应完善金融数据质量监管体系，将数据质量管理情况作为评价金融机构风险控制能力的重要指标之一。对于涉及数据失真或违规行为的机构应采取严格的惩处措施，以形成有效的威慑力，促使金融机构主动规范其数据管理行为。此外，金融机构还应建立常态化的内部数据质量审查机制，通过运用技术手段对数据管理中可能存在的漏洞进行及时发现与修复，确保数据的真实性、完整性与准确性。例如，采用自动化技术可以在提高数据处理效率的同时，减少人工操作中的失误，从而优化数据质量管理流程，提升整体治理水平。

6.2. 提升数据治理能力，实现金融数据价值

中小型金融机构在数据治理方面普遍存在能力不足的现象，需要从多维度对数据治理进行系统性优化，挖掘和释放金融数据的潜在价值。通过构建科学的治理体系，强化数据管理与应用能力，有效提升数据资源的利用效率，为金融机构的业务创新与可持续发展提供有力支持。

一是建立系统化的金融数据管理制度，完善机构内部的数据治理架构。中小型金融机构应结合实际发展需求，在监管机构的指导下探索适合自身特点的管理模式，构建包括数据监督、检查机制以及技术支持等内容的内部管理框架。在此基础上动态调整相关评价指标与制度，以确保其始终符合行业规范和机构内部的实际运营需求。

二是加强数据采集与管理的规范化。中小型金融机构需要从数据的源头入手，对采集、录入、存储等环节实行严格的标准化管理，确保信息的完整性与准确性。为此，可通过构建专门的监管统计系统，对数据采集与处理过程进行全程监控，以实现信息处理的精准化与自动化。可以引入先进的自动化技术优化流程控制，将数据处理的效率大幅提升，减少人工干预可能引发的错误或偏差，使数据治理更加高效且稳定。

三是提高金融数据的应用水平。随着大数据技术的广泛应用，数据驱动已成为金融机构提升竞争力的重要方向。中小型金融机构应摒弃传统以满足监管要求为目标的被动治理方式，转而聚焦于数据的实际价值开发。通过对多元化数据资源的挖掘，在业务创新、风险管控、内部运营和客户服务等领域实现广泛应用。提升金融机构的业务灵活性与服务精准度，助力其实现运营模式的优化与效率的全面提升。

四是完善数据治理评估与问责体系。中小型金融机构应建立覆盖全流程的评估机制，对数据治理工作的各环节进行持续地监测与反馈。通过评估及时发现治理过程中存在的问题与不足，采取针对性的改进措施。通过构建内部问责机制，明确各环节的责任主体，对治理中出现的问题及时追责，有助于增强数据治理工作的执行力与规范性，从而推动治理能力的持续提升。

6.3. 完善金融数据监管体系，防范新风险

一是明确监管职责，建立多层次监管框架。当前，我国金融数据监管尚未建立明确的监管职责分工和统一的监管框架，导致不同金融机构在实践中标准和规范不一。为此，需要从制度设计入手，构建多层次的监管体系。首先，国务院金融稳定发展委员会和中国人民银行应承担宏观审慎监管职责，通过协调各部门的金融数据管理职能，理顺各自的权责关系，形成统一的监管合力。银保监会和证监会可分别

对银行和资本市场中的开放银行业务进行监管，加强对机构合规操作的监督。此外，还需发挥金融行业自律性组织的作用，通过发布行业规范和行为守则，推动各参与方在数据管理和技术应用上的自我约束。整体监管框架应以消费者权益保护为核心，以包容审慎为原则，确保监管体系既能适应金融数据发展的需求，又能有效应对其所带来的潜在风险。

二是推动数据标准化与接口规范统一。当前，不同金融机构之间在数据格式、接口设计和共享协议等方面存在较大差异，导致数据交换效率低下并增加了潜在风险。为此，监管机构需尽快制定覆盖数据存储、描述、格式以及发布规则的统一标准，从技术层面促进数据流通的规范化和高效化。第一，在接口规范方面，可以借鉴英国开放银行的成功经验，通过统一 API (应用程序接口)标准，明确接口的开发、设计和维护要求，从而实现不同机构间的金融数据无缝对接。对于数据共享的边界问题，监管机构需根据数据敏感性进行分类管理，将数据划分为公开数据、客户交易数据、聚合数据等类别，为每类数据设置相应的开放权限和保护机制。在确保数据安全的同时释放数据的共享价值。第二，强化数据安全管理。金融机构通过数据共享模式将用户数据暴露在多主体间，使得用户隐私保护和信息安全面临更大挑战。为此，金融监管机构需完善现有的数据安全标准，例如在用户授权、身份认证、数据加密和欺诈监控等方面引入更高的技术要求。加强对非法数据获取和滥用行为的打击力度，以增强机构的责任感和安全意识。此外，第三方服务提供商由于资质良莠不齐可能引发数据泄露、操作失误等风险。为此，监管机构需建立严格的市场准入机制，对第三方机构的技术能力、数据管理能力以及合规性进行全面评估。明确各参与方在数据泄露或滥用情况下的法律责任分配，确保消费者的合法权益不受损害。

三是加快推进科技与传统监管的融合应用。随着金融数据的发展，其技术复杂性和风险多样性超出了传统监管手段的能力范围。为此，监管机构需推动科技监管手段的应用，例如利用大数据、人工智能、区块链等技术，建立动态化、智能化的监管体系，实现对数据流动的实时监控，并通过算法模型预测潜在风险。尽管科技监管能提升监管效率，但其也存在，如技术漏洞或算法偏差带来的失误等问题。因此，传统的人力监管仍是不可或缺的补充。通过将科技监管与人工监管相结合弥补单一监管模式的不足，确保监管决策的准确性和全面性，提高监管机构应对复杂风险的灵活性。

7. 结论

完善金融数据法律规制的核心在于实现发展与安全的平衡。一方面，应加快金融数据相关立法进程，通过明确数据权属、规范数据流通规则，为金融数据的使用与保护提供制度保障；另一方面，监管部门需要加强协调，利用科技手段完善监管模式，推动金融机构在数据治理中的主动性。中小型金融机构作为推动普惠金融的重要力量，需要政策和技术层面的支持，以提升其数据治理能力，减少因资源不足导致的行业发展不均衡问题。此外，技术标准的统一和安全机制的建立是推动金融数据高效流通的重要环节。通过制定统一的接口标准、分级管理机制以及安全规范，可在保障数据隐私和安全的基础上，实现金融数据的高效共享与利用。

金融数据法律规制需要在政策制定、监管执行和技术支持上形成系统性和协调性，以应对数字化时代金融数据治理的复杂性与动态性。将来，伴随金融科技的深化发展，金融数据治理不仅需要维护行业秩序和消费者权益，还要释放数据价值，为国家数字经济的发展提供强有力支撑。

参考文献

[1] 黄茂钦, 周坤琳. 金融数据治理的激励与规制路径探析[J]. 中国应用法学, 2020(6): 111-124.

[2] 董小君, 宋玉茹. 加快推进我国金融数据治理现代化建设研究[J]. 行政与法, 2022(8): 11-21.

[3] 陈振云. 我国金融数据治理法律构建的三个维度[J]. 贵州大学学报(社会科学版), 2022, 40(5): 80-92.