数据跨境流动背景下金融科技信息安全监管协同机制研究

郭力维

中信财务有限公司，北京 100004

摘要：随着全球化进程加速与数字经济蓬勃发展，数据跨境流动已成为金融科技行业常态。在此背景下，金融科技信息安全面临跨境数据泄露、监管规则冲突等复杂风险，传统单一的监管模式难以应对。本文深入剖析数据跨境流动对金融科技信息安全监管带来的挑战，探讨构建高效的监管协同机制，涵盖国内跨部门协同、国际间监管合作等方面。

关键词：数据跨境流动；金融科技；信息安全；监管协同机制

DOI：10.63887/fet.2025.1.3.19

1 引言

1.1 研究背景

在数字技术深度融合金融领域的时代，金融科技业务突破地域限制，数据跨境流动规模与日俱增。以跨境支付为例，根据相关机构统计，2023 年全球跨境支付市场规模已超过 200 万亿美元，且每年以两位数的增长率持续攀升[1]。跨国数字信贷、全球智能投顾等业务也快速发展，海量客户身份信息、交易数据在不同国家和地区间频繁传输。然而，各国数据安全法律法规、监管政策存在差异，数据跨境流动过程中面临数据被窃取、滥用、监管套利等风险[2]。例如，2022 年某国际知名支付平台在将用户数据传输至境外服务器进行处理时，因未满足数据接收国关于敏感数据本地化存储的隐私保护要求，导致超过 500 万用户的银行卡信息、交易记录等敏感数据泄露，引发美国、欧盟等多国监管机构的联合调查与高额处罚，该事件不仅使平台市值大幅缩水，也给全球金融科技行业的数据跨境流动安全敲响了警钟[3]。

1.2 研究意义

理论上，本研究有助于丰富金融科技监管与数据跨境流动领域的学术研究，完善信息安全监管协同机制的理论体系。通过深入分析数据跨境流动与金融科技信息安全监管之间的内在联系，探索协同机制的运行逻辑和作用机理，为该领域的理论发展提供新的视角和思路[4]。

实践中，为监管部门提供构建协同监管机制的策略与方法，解决监管碎片化、规则不统一等问题，降低金融科技信息安全风险。例如，通过建立国内跨部门协同机制，明确各监管部门职责，避免出现监管空白与重叠，提高监管效率；通过国际监管合作机制，参与国际规则制定，推动监管互认，降低金融科技企业跨境业务的合规成本。同时，促进金融科技企业合规开展跨境业务，保障金融市场健康有序发展，维护国家金融安全与数据主权[5]。

2 数据跨境流动背景下金融科技信息安全监管现状与挑战

2.1 数据跨境流动的发展态势

当前，数据跨境流动呈现出规模庞大、形式多样的特点。金融科技企业通过云服务、跨境数据中心、国际合作项目等方式，实现数据在全球范围内的存储、处理与传输。以跨境电商金融服务为例，消费者在境外购物平台的支付数据、消费偏好数据等，需跨境传输至金融机构与电商平台的后台系统进行分析处理。在实际运营中，一家中等规模的跨境电商企业，每日产生的跨境交易数据量可达 TB 级别，这些数据涉及多个国家和地区的金融监管要求。

同时，随着 5G、物联网等技术的普及，金融科技领域的数据跨境流动将更加频繁与复杂，对信息安全监管提出更高要求。例如，在智能穿戴设备与金融服务结合的场景下，用户的健康数据、消费数据等会实时跨境传输，用于个性化金融服务推荐，数据的实时性和多样性增加了监管的难度和复杂性 。

2.2 金融科技信息安全监管现状

目前，各国在金融科技信息安全监管方面已开展诸多工作。部分国家制定了严格的数据出境审查制度，要求金融机构在数据跨境传输前进行安全评估。例如，俄罗斯出台相关法规，规定涉及本国公民个人信息的数据，未经特殊审批不得传输至境外服务器；印度也加强了对金融数据跨境流动的监管，要求金融机构确保数据接收方所在国家或地区具有同等的数据保护水平。

一些国际组织也在推动跨境数据流动规则的协调，如欧盟的《通用数据保护条例》（GDPR）对全球数据监管产生了广泛影响。GDPR 不仅对欧盟境内的数据处理活动进行严格规范，还通过“长臂管辖” 原则，对涉及欧盟公民数据的境外企业产生约束，许多全球金融科技企业为满足 GDPR 要求，不得不投入大量资源进行数据合规改造。

国内方面，我国陆续出台《数据安全法》《个人信息保护法》等法律法规，加强对数据跨境流动的规范。但在金融科技领域，仍存在监管主体职责不明确、监管标准不一致等问题。例如，在金融科技企业的数据跨境传输审批过程中，不同地区、不同部门的审查标准和流程存在差异，导致企业合规成本增加，监管效率低下 。

2.3 面临的主要挑战

2.3.1 监管规则冲突：

不同国家和地区对数据跨境流动的监管要求差异显著。例如，欧盟强调数据的 “充分性保护”，要求数据仅可传输至数据保护水平与欧盟相当的国家或地区；而美国则采用 “自愿性” 原则，通过行业自律和安全港协议等方式管理数据跨境流动。这种规则冲突导致金融科技企业在跨境业务中面临合规困境，增加运营成本与法律风险。以某跨国金融科技公司为例，其在欧盟和美国同时开展业务，为满足双方不同的数据监管要求，不得不建立两套独立的数据管理系统，每年额外增加数百万美元的运营成本。

2.3.2 信息共享壁垒：

各国监管机构之间缺乏有效的信息共享机制，难以实时掌握跨境数据流动中的风险动态。当发生跨境数据泄露事件时，由于信息沟通不畅，无法及时协同处置，延误风险控制时机。例如，2021 年某国际金融集团发生数据泄露事件，涉及多个国家和地区的客户数据。由于各国监管机构之间信息共享滞后，未能及时采取联合应对措施，导致该事件的影响范围不断扩大，最终造成数十亿美元的经济损失。

2.3.3 技术监管难度大：

金融科技应用的区块链、加密通信等技术不断迭代，数据在跨境流动过程中可能经过多次加密与匿名化处理，给监管机构识别、监测和追踪数据安全风险带来极大挑战。传统的监管技术手段难以适应复杂多变的金融科技业务场景。例如，在基于区块链的跨境支付业务中，交易数据以分布式账本的形式存储在多个节点，且采用加密技术进行保护，监管机构难以对交易的真实性和安全性进行有效监管。

2.3.4 主权与安全矛盾：

各国在保障数据主权与促进数据跨境流动之间寻求平衡时存在矛盾。为维护国家数据主权与信息安全，部分国家采取严格的监管措施，这在一定程度上限制了金融科技的跨境创新与发展。例如，一些发展中国家为保护本国数据主权，要求金融科技企业将数据完全本地化存储，禁止关键金融数据出境，这使得国际金融科技企业在进入这些市场时面临巨大障碍，也阻碍了全球金融科技行业的协同发展 。

3 金融科技信息安全监管协同机制构建

3.1 国内跨部门协同机制

3.1.1 明确监管职责分工：

建立由金融监管部门（如央行、银保监会、证监会）牵头，联合网信部门、公安部门、工信部门等组成的协同监管小组。明确各部门在金融科技信息安全监管中的职责，如金融监管部门负责业务合规性监管，

重点审查金融科技企业跨境业务的资质、交易合规性等；网信部门侧重数据安全与网络安全监管，对数据跨境传输的安全性、网络安全防护措施等进行监督；公安部门打击跨境数据犯罪，对数据泄露、非法获取数据等违法犯罪行为进行调查和惩处，避免出现监管空白与重叠。在实际工作中，可制定详细的职责清单和工作流程，确保各部门协同有序开展监管工作。

3.1.2 加强信息共享与协作：

搭建统一的金融科技信息安全监管信息共享平台，整合各部门掌握的数据跨境流动监测数据、风险预警信息、企业合规情况等。平台采用先进的数据处理和共享技术，实现数据的实时更新和交互。通过定期召开联席会议、建立联合执法机制等方式，实现部门间的信息互通与协同行动，提高监管效率。例如，当网信部门监测到某金融科技企业存在网络安全漏洞，可能导致数据跨境泄露风险时，可通过信息共享平台及时将相关信息推送给金融监管部门和公安部门，三方迅速联合开展调查和处置工作。

3.1.3 制定统一监管标准：

组织多部门联合制定金融科技信息安全监管标准，涵盖数据跨境传输的安全评估流程、加密技术要求、数据留存期限等方面。在制定标准过程中，充分参考国际先进经验和行业最佳实践，结合我国实际情况，确保国内监管标准的一致性和可操作性，为金融科技企业提供明确的合规指引。例如，对于数据跨境传输的加密技术要求，可统一规定采用符合国家标准的加密算法，并明确加密强度标准，避免企业因标准不统一而产生合规困惑 。

3.2 国际监管合作机制

3.2.1 参与国际规则制定：

积极参与国际金融科技信息安全监管规则的制定与协调，加强与国际组织（如金融稳定理事会、巴塞尔委员会）、主要经济体的沟通与合作。组建专业的国际规则研究团队，深入研究全球金融科技信息安全监管趋势和规则动态，结合我国金融科技发展特点和需求，提出具有建设性的规则建议。推动建立公平、合理、包容的跨境数据流动国际规则，提升我国在国际金融科技监管领域的话语权。例如，在国际组织关于跨境数据流动规则的研讨会议中，积极分享我国在金融科技信息安全监管方面的经验和成果，争取更多国际规则制定的主动权。

3.2.2 建立双边与多边合作协议：

与其他国家和地区签署金融科技信息安全监管合作协议，明确双方在数据跨境流动监管中的权利与义务。合作协议内容应包括信息共享机制、联合监管行动、跨境数据安全事件联合处置机制等。在发生风险事件时，双方能够及时共享信息、协同开展调查与处置工作。例如，我国可与 “一带一路” 沿线国家签署金融科技信息安全监管合作协议，建立定期的信息交流机制，共同应对跨境数据安全风险，促进区域金融科技合作与发展。

3.2.3 开展监管互认与等效评估：

推动与其他国家在金融科技信息安全监管标准方面的互认，通过等效评估机制，认可对方监管措施的有效性。建立专业的评估机构和评估流程，对其他国家的金融科技信息安全监管体系进行客观、公正的评估。降低金融科技企业跨境业务的合规成本，促进跨境金融服务的便利化发展。例如，我国与欧盟可开展金融科技信息安全监管标准的互认工作，对于符合双方监管标准的金融科技企业，在数据跨境流动审批等方面给予简化流程和便利措施 。

3.3 技术协同创新机制

3.3.1 研发智能监管工具：

联合高校、科研机构与金融科技企业，共同研发适用于数据跨境流动监管的智能技术工具。利用大数据分析、人工智能等技术，对跨境数据流量、流向、异常行为进行实时监测与分析，实现风险的自动识别与预警。例如，开发基于人工智能的跨境数据风险监测平台，通过机器学习算法对海量的跨境数据进行分析，自动识别数据泄露、异常传输等风险行为，并及时发出预警信号。同时，平台还可提供风险评估报告和应对建议，为监管机构决策提供支持。

3.3.2 加强技术标准统一：

推动建立国际通用的金融科技信息安全技术标准，如数据加密标准、安全认证标准等。积极参与国际技术标准的制定和修订工作，与国际标准化组织、行业

协会等合作，促进各国在金融科技信息安全技术标准方面的协调与统一。确保不同国家和地区的监管技术手段具有兼容性，便于开展协同监管。例如，在数据加密标准方面，推动全球统一采用高强度的加密算法和密钥管理规范，提高跨境数据传输的安全性。

3.3.3 构建技术共享平台：

搭建全球金融科技信息安全技术共享平台，促进各国监管机构、企业与技术机构之间的技术交流与合作。平台设置技术成果展示、经验分享、合作交流等板块，方便各方分享先进的监管技术经验与创新成果。例如，定期举办全球金融科技信息安全技术研讨会，邀请各国专家学者、企业代表和监管人员参加，共同探讨技术难题和解决方案。

4 结论

在数据跨境流动背景下，构建金融科技信息安全监管协同机制是应对复杂风险、保障金融安全的必然选择。通过建立国内跨部门协同、加强国际监管合作以及推动技术协同创新，能够有效解决监管规则冲突、信息共享壁垒等问题，提升监管效能。未来，随着金融科技的持续发展与数据跨境流动的进一步深化，监管协同机制需要不断优化与完善，以适应新的风险挑战，推动金融科技行业在安全、合规的轨道上实现高质量发展。

参考文献

[1]孙坚强,张楠.跨境资本流动监管研究——基于粤港澳大湾区的研究视角[J].国际经贸探索,2025,41(06):93-106.

[2]徐浩宇.金融数据跨境流动合规治理:生成逻辑、实践困境及其应对路径[J/OL].国际经贸探索,1-15[2025-06-21].

[3]陈星雨.海南自贸港离岸贸易中的物流金融创新路径研究[J].中国航务周刊,2025,(24):61-64.

[4]罗君名,谭向洋.海南数据贸易理论与实践探讨[J].合作经济与科技,2025,(13):62-65.

[5]吴晓求,郭彪,芦东,等.中国建设金融强国的双支柱架构：人民币国际化与资本市场开放[J/OL].财贸经济,1-20[2025-06-21].