

中银研究产品系列

- 《经济金融展望季报》
- 《中银调研》
- 《宏观观察》
- 《银行业观察》
- 《国际金融评论》
- 《国别/地区观察》

作者：钟红 中国银行研究院

电话：010 - 6659 4016

签发人：陈卫东

审稿：钟红 边卫红

联系人：吕昊旻

电话：010 - 6659 4016

* 对外公开

** 全辖传阅

*** 内参材料

金融数据跨境流动安全与监管研究*

近年来，跨境金融服务在移动支付、数字货币、大数据、区块链等金融科技手段的推动下蓬勃发展，快速增长的跨境金融数据成为了重要的市场资源。虽然金融数据跨境流动提升金融服务效率，推动金融全球化的纵深发展，但也在一定程度上给国家、企业和个人信息带来安全隐患。当今世界各国都面临着跨境金融数据流动性和安全性的权衡，存在不同的监管模式。本文通过梳理中外金融数据跨境流动法律基础和监管政策，着重就数字经济背景下国家金融数据安全和监管中存在的主要问题进行分析，并对我国进一步做好金融数据跨境流动监管提出建议。

金融数据跨境流动安全与监管研究

随着数字经济的全面发展，数据发挥着越来越重要的作用，习近平总书记曾指出，“要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”金融是产生、积累和存储数据最多的行业之一，金融数据涉及到用户信息、商业交易、国家安全等多方面。虽然金融数据跨境能够最大程度地释放数据红利，提升金融效率，但是金融数据跨境牵涉主体众多，近年来经济金融敏感数据非法流向境外的事件层出不穷，严重危害我国国家安全。

为更好地保护我国金融数据安全，在形成了以《网络安全法》《数据安全法》《个人信息保护法》为基础的数据跨境流动法律框架上，我国陆续出台多项涉及到金融数据跨境流动的法律法规和行业准则。2022 年 7 月 7 日，国家互联网信息办公室颁布《数据出境安全评估办法》，对数据出境安全评估工作进行了更为具体的规定，也让跨境流动的监管有了更为实操性的法律依据，该办法已于 2022 年 9 月 1 日正式生效。在此基础上，分析现阶段美国、欧盟、日本等多个国家和地区在跨境金融数据监管方面的措施，能够更好地为我国金融数据跨境在流动性和安全性上的权衡建言献策，对解决我国金融数据跨境的现存问题具有重要意义。

一、金融数据跨境流动面临的主要背景

（一）金融数据数量大、种类多，跨境流动本身伴随着一系列复杂的风险

在经济金融全球化背景下，跨境贸易等经济活动的扩张随之带来了对跨境金融的强烈需求。据国际数据公司（International Data Corporation，简称 IDC）预测，全球数据总量将从 2018 年的 33ZB 增至 2025 年的 175ZB¹。其中，金融服务是全球数据增长的重要推动力。金融数据跨境流动能够有效提升商业效率，并为金融机构从产品定价、风险管理、渠道管理和客户服务等方面提供重要支撑。但是，由于跨境金融数据规模大、敏感性高、出境频繁，一旦出现重大数据泄露和重要数据资产丢失等情况，原有

¹ ZB，计算机术语，中文名是泽字节，外文名是 Zettabyte，1ZB=2⁷⁰B。

金融机构建立的数字化产品体系、服务渠道和运营模式将受到冲击，容易引发不可控制的多种风险，严重时甚至直接威胁国家金融安全。

（二）跨境金融数据流动背后蕴含着个人隐私、企业权益和国家安全等风险

受经济金融全球化的影响，金融数据的范围从单一的个人隐私数据扩展到企业商业机密、社会权益、国家安全等多个种类。由于网络空间无法构成国际政治法律中的“全球公域”，所以金融数据跨境流动面临着本国控制权和管辖权丧失的问题，导致本国金融数据在域外网络空间无法受到保护，我国公民的个人隐私、企业商业机密、国家安全数据等都将暴露在别国视野之内。一旦发生数据处理不当、数据泄露、数据丢失、恶意利用等情况，将对国家安全造成巨大威胁。尤其是 2013 年美国“棱镜门”事件曝光后，各国政府纷纷加强对本国跨境数据的监管，避免类似事件对国家安全造成侵害。

（三）跨境金融数据在流动性和安全性之间存在此消彼长的关系

跨境金融数据流动是一把双刃剑，流动性和安全性是重要考量。一方面，金融数据流动能够帮助企业提升效率，利用可以掌握的海量金融数据进行研究分析，强化与海外市场的融合程度，提升跨境企业的经济效率和利润；另一方面，金融数据的过度流动面临数据本地化存储、安全传输、隐私保护等问题，部分外国政府试图通过互联网途径挖掘我国重要的商业机密信息、经济运行状况、金融产品创新等敏感数据，一旦这些关键数据被外国获取并恶意利用，将对我国经济造成巨大破坏。

（四）跨境金融数据流动存在国家间数字金融红利分配不均的问题

在司法执法层面，部分发达国家实施“长臂管辖”，以促进自由流动和境外执法权等理由推行数据领域的霸权主义，要求发展中国家向其输出重要金融数据，利用数据引流效应享受金融数据红利，导致发展中国家金融安全受到威胁。在业务发展层面，部分跨国金融企业通过掌握使用者的金融信息，凭借网络外溢效应形成规模经济，通过积累大量个人信息和金融交易数据拓展业务宽度与深度，在一定程度上形成数据垄断，获取额外利益。

二、金融数据跨境流动监管的国际治理

目前，全球的金融数据流动主要存在三种策略：一是以美国、日本为代表的发达国家更加强调金融数据流动性，希望通过金融数据自由流动来形成引流效应，获得更大的数据价值。二是以中国、俄罗斯、印度为代表的一些国家强调金融数据的安全性，主要以“本土化”策略为主，以限制重要数据出境、数据本地化储存等方式优先保护国家安全。三是介于金融数据流动性和安全性之间的其他国家和地区，如欧盟、新加坡等，对内实行较为宽松的数据流动机制，对外以多边协议的方式维护数据立法话语权。

（一）美国：提倡金融数据跨境自由流动，以“长臂管辖”扩张跨境数据执法权

一是立法上强调在流动性基础上保护国家安全。在实践中，发达国家能够更好地利用数据引流效应在跨境活动中占据主导地位。因此，美国在金融数据立法上、在保护国家安全基础上更加注重数据开放和自由流动。2010 年，美国首先针对“重要数据”形成管控非秘数据列表（Controlled Unclassified Information），并指出美国政府禁止向外国传播涉及到本国国家安全的相关数据。2018 年 3 月，美国国会通过《澄清合法使用境外数据法案》（Clarifying Lawful Overseas Use of Data Act，简称 CLOUD Act），进一步扩张美国获取存储于境外数据的能力，为美国云数据建立额外保护措施，同时，针对中国等发展快速的国家设置数据壁垒，防范重要领域的数据外流。2019 年，美国制定《2019 国家安全和个人数据保护法案》（National Security and Personal Data Protection Act of 2019），明确指出禁止向有关国家传输个人数据，尤其提到禁止个人数据流向中国等“威胁美国国家安全”的国家。

二是在监管中实施“长臂管辖”，通过域外立法实施“霸权主义”。在“长臂管辖”的影响下，美国在金融数据主权方面表现强势，凭借其在经济和军事上的实力，以反腐败、反洗钱、反恐怖主义、维护国家安全为由实施跨境执法。例如，2001 年出台的《爱国者法案》（USA PATRIOT Act），以防止恐怖主义为目的扩张了美国执法机关的权限，明确美国可以以国家安全为由获取全球范围内的数据，尤其是针对与外

国人士或政体有关的金融活动。《澄清合法使用境外数据法案》（CLOUD Act）中也确立“数据控制者标准”，进一步扩大美国对境外数据的调取权限和域外管辖权。

三是在国际合作中推动区域性、多边性金融数据跨境自由流动。美国在金融数据流通上以多边合作构建“小圈子”。一方面，积极参与并主导区域性的国际组织（如 APEC）大力推动区域性的数据跨境自由流动；另一方面，与欧盟、日本等国家和地区达成双边协议，积极建立国际间金融数据跨境自由流动体系。例如，2005 年，美国签署《亚洲太平洋经济合作组织隐私框架》（APEC Privacy Framework），形成区域间的跨境隐私规则体系，倡导在保障安全的情况下促进跨境数据自由流动。2018 年，美国与墨西哥、加拿大签署《美墨加三国协议》（U.S.-Mexico-Canada Agreement），规定三国开展境内业务的基础是金融数据的流动性，禁止三方中的金融机构或跨境金融服务提供者采用数据本土化策略。

（二）日本：尝试构建“多边信任”基础上的自由数据流通体系

一是建立在信任与安全基础上的数据跨境流动体系。日本积极参与国际金融数据跨境流动的规则制定，提倡数据跨境自由流动，探索数据驱动型经济发展。2019 年，在达沃斯召开的世界经济论坛会议上，日本政府提出“基于信任的数据自由流动”（Data Free Flow With Trust, DFFT）机制。一方面，强调各个国家和地区要保护好涉及个人隐私、知识产权、国家安全情报等方面的数据；另一方面，倡导医疗、工业、交通等领域的非个人匿名数据自由流动，在开放和信任的基础上打造新型全球数据治理体系。

二是积极参与国际规则构建，在信任基础上开拓海外金融数据合作。日本政府通过与海外国家建立区域性数据流动协议的方式提升与其他国家的接轨水平，主动参与国际数据流动的规则构建。2018 年，以日本为代表的 11 个国家签署《全面与进步跨太平洋伙伴关系协定》（Comprehensive and Progressive Agreement for Trans-Pacific Partnership, 简称 CPTPP），鼓励跨境数据自由流动，提出取消跨境数据交换限制，最大限度地实现贸易自由化。2019 年 2 月，日本与欧盟签署的《经济伙伴关系协定》（Japan-EU Economic Partnership Agreement, 简称 EPA）正式生效，欧盟通过对日本

“充分性认定”的决定，在强力保护保障基础上，允许个人信息在这两个经济区内自由流动。2019 年 6 月，日本在 G20 峰会上签署了《大阪数字经济宣言》（Osaka Declaration on Digital Economy），提出建立允许数据跨境自由流动的“数据流通圈”，在数据流动和电子商务国际规则的制定基础上，进一步推动全球数字经济发展。2019 年 9 月，日本与美国签署《美日数字贸易协定》（U.S.-Japan Digital Trade Agreement），明确两国间基于信任实现无障碍跨境数据传输，并承诺禁止数据本地化要求。

（三）俄罗斯：避免数据外流，推进完全本土化数据政策

一是以国家安全为核心原则，以本地化存储为主要方式。在数据跨境立法上，俄罗斯将国家安全作为首要需求。因此，俄罗斯跨境数据流动呈现出明显的本土化特征，数据出境范围逐步缩小。2006 年，俄罗斯出台《俄罗斯联邦信息、信息技术和信息保护法》、《俄罗斯联邦个人数据法》，要求在本国数据跨境传输之前需要确保境外主体对数据进行充分保护，并预置安全阀条款，强调任何危害国家安全的跨境数据转移都应该被禁止。2014-2016 年，俄罗斯在此基础上对立法进行修改，进一步收窄数据跨境范围，更加注重对国家安全的保护。2015 年，俄罗斯修订《个人数据法》，明确国内外数据存储硬件必须使用俄罗斯服务器，减少数据外流的可能性。

二是金融机构数据引流能力差，以严格限制为监管手段。俄罗斯经济对外依存度较低，实施完全本土化金融数据政策的一个原因是本国缺乏强有力的数据引流能力，放开金融数据跨境管制会给本国经济安全带来威胁。因此，俄罗斯通过牺牲跨境数据流动性的方式换取数据安全性。在保护数据安全的措施方面，俄罗斯成立专门数据保护监管部门，通过处罚和检查的方式对跨境数据流动进行监管，对违法行为从严处罚，Linkin、Twitter、Facebook 等公司都曾因违反数据本土化政策受到处罚。

（四）印度：本土化政策受到国际冲击，一度被称为“新德里地方保护主义”

印度注重保护国家安全，在倡导数据本土化的同时受到内外因素的共同影响。1993 年，印度出台《公共记录法》，规定禁止向境外传输公共数据，除非是政府性质的“公共目的”。2017 年，印度央行规定本国在支付金额运营等领域的金融数据均做

本土化处理，禁止对外传输。2018 年，印度《个人数据保护法案（草案）》对数据跨境流动做出限制，要求关键数据不能出境，一般数据出境需设置数据脱敏期，并在境内留存副本。但是，这一规定被众多境外金融机构和企业反对，称其为“新德里地方保护主义”。在国际压力下，印度逐渐放松数据本土化政策，在 2019 年修订《个人数据保护法案（草案）》中适度缩小本国数据本土化范围。

（五）欧盟：对内以提倡“自由流动”实现流动性，对外以“充分性认定”原则协调安全性

一是在欧盟内部倡导金融数据的自由流动。欧盟倡导成员国之间金融数据的自由流动，主张消除成员国内部之间的数据流动壁垒，通过协作效应实现更大的地区数据红利。在立法上，欧盟倡导跨境数据流动的相对开放，并在此基础上对特定涉及到国家安全的数据进行保护。1981 年，欧盟颁布的“第 108 号公约”——《有关个人数据自动化处理中的个人保护公约》（Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data）指出，个人数据在缔约国之间应该自由流通，同时也明确相关数据会受到适当水平的保护。2019 年 5 月，在《通用数据保护条例》的基础上，欧盟通过《欧盟内非个人数据自由流动框架条例》（Framework for the Free Flow of non-Personal Data in the European Union），禁止成员国制定限制数据在成员国境内自由流动的法律，以此保障欧盟内部数据的自由流动性。2020 年 2 月，欧盟发布《欧洲数据战略》（A European Strategy for Data），旨在构建一个自由流动的数据流动体系，用数据促发展。2022 年 4 月，欧盟议会就《数据治理法案》（Data Governance Act）进行最终投票表决，旨在促进整个欧洲各国内部的数据共享，增强欧盟各国之间对数据的控制和信任。

二是欧盟对数据外传进行严格监管。“内松外严”是欧盟的主要监管方式，通过对欧盟外的国家增设数据流通壁垒，以此来保护本地区金融数据的安全。2018 年，欧盟出台了《通用数据保护条例》（General Data Protection Regulation，简称 GDPR），制定欧盟对共同体外国家和地区和金融数据各类政策，规定只有通过欧盟“充分性认定”的国家和地区才能够实现与欧盟间的数据自由流动，享受不经过数据主体授权使

用欧盟数据的权利，但是欧盟“充分性认定”评估相对严格，仅有 10 余个国家和地区被纳入其中。欧盟以“充分性认定”的监管机制为基础，在保护本地区数据流动的同时，也吸引更多国家和地区接受和加入欧盟内部金融数据跨境自由流动，尽可能实现金融数据跨境流动安全性和流动性的协调。

三是金融数据监管“长臂管辖”原则初现。2018 年，欧盟出台的《通用数据保护条例》对数据监管范围、处罚力度、数据主体等做出更多规定。一方面，欧盟进一步扩大了对数据监管的权限，在适用范围上，法案适用于境内外所有处理欧盟个人数据的企业，这意味着《通用数据保护条例》可以管辖到几乎全部与欧盟有关的别国企业，“长臂管辖”原则初现；另一方面，欧盟对跨境数据流动的处罚力度不断增加，以重罚为手段，倒逼国内外企业提高跨境数据保护意识，完善区域内跨境数据保护制度。

三、我国金融数据跨境流动的法律依据

目前，我国已经形成以《网络安全法》、《数据安全法》、《个人信息保护法》为框架，以《个人信息和重要数据出境安全评估办法（征求意见稿）》、《数据安全管理办法（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》等行政法规和部门规章为补充的数据跨境流动法律制度体系。在金融数据跨境的实践中，《金融数据安全 数据安全分级指南》、《个人金融信息保护技术规范》、《中国人民银行金融消费者权益保护实施办法》等文件进一步对金融数据跨境流动做出更为详尽的规定。

（一）“三大支柱”：《网络安全法》、《数据安全法》、《个人信息保护法》构筑我国数据跨境制度法律框架

2017 年，我国出台第一部全面规范网络环境安全管理方面的基础性法律——《网络安全法》，明确网络安全与信息化发展并重原则。一方面，第 18 条指出，“国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展”，承认公共数据资源的开放性；另一方面，《网络安全法》第 21、37、66 条多次强调，在网络安全等级保护制度基础上，对关键信息基础设施实行重点保护，

尤其是对关键信息基础设施运营者提出应保护用户个人信息、禁止关键数据出境、重要数据强制本地存储的要求。

2021 年，我国制定《数据安全法》，旨在规范信息技术发展下数据的开发和利用，在落实总体国家安全观要求的背景下，《数据安全法》延续数据本土化策略，第 36 条规定“非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据”。同时《个人信息保护法》对个人信息跨境提供做出明确规定，尤其是对个人信息处理者、关键信息基础设施运营者等主体做出严格要求，即转移到境外的个人信息的保护不应低于我国的保护标准。

总之，《网络安全法》、《数据安全法》、《个人信息保护法》是数据跨境流动法律研究的“三大支柱”，为进一步扩大法律的可操作性，多项行政法规、部门规范文件和行业指南陆续出台，共同构建起跨境金融数据流动的法律框架。

（二）“多层补充”：行政法规、部门规范文件和行业指南文件是数据跨境制度的补充

我国现行法律仍坚持以本土化为主要的数据跨境流动策略，为数据出境设置“评估”环节，对不同重要程度的数据执行相应管理措施，确保流动性和安全性的协调。

《网络安全法》第 37 条规定，“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估”。此后，

《个人信息和重要数据出境安全评估办法（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》、《个人信息出境标准合同规定（征求意见稿）》、《信息安全技术数据出境安全评估指南（征求意见稿）》、《网络安全标准个人信息跨境处理活动认证技术规范（征求意见稿）》陆续出台，标志着我国对数据出境安全评估方式的不断探索，这些文件就不同类型的数据是否可以跨境传输、如何进行评估等问题制定了规范。2021 年 11 月，《网络数据安全条例（征求意见稿）》第五章“数据跨境安全管理”明确了数据出境评估主体。2022 年 7 月，国家互联网信息办公

室出台的《数据出境安全评估办法》，标志着我国对数据跨境流动的监管有了更为实操性的法律依据。

（三）金融数据：在国家数据跨境流动框架下的法律和监管框架回顾

现阶段，我国金融数据受到网络信息一般法律规则和金融行业数据跨境专门规则的“双重管理”。

在网络信息部门一般法律规则上，金融数据需要遵守网络信息部门出台的各类一般性规定。例如，《网络安全法》提及金融等重要行业及领域，因其与国家安全、国计民生、公共利益密切相关，需要在网络安全等级保护制度的基础上，实行重点保护。

《个人信息保护法》将金融账户作为个人信息的重要组成部分。《数据安全法》还对数据监管主体做出界定，第 6 条规定“工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责”，明确金融数据的监管主体。

在金融行业制定的数据跨境规则上，一方面，我国对金融数据出境的限制和要求逐步“收紧”。早在 2011 年，中国人民银行就金融数据跨境安全问题做出规定，《关于银行业金融机构做好个人金融信息保护工作的通知》（银发〔2011〕17 号）第 6 条规定，“在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息”。首次提出了金融机构对个人金融信息存储、处理和分析原则上禁止出境，只在“例外情形”允许出境。随后，中国人民银行上海分行紧急发布《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》（上海银发〔2011〕110 号），明确定义“例外情形”是指“为客户办理业务所必需，且经客户书面授权或同意，境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。银行业金融机构应当保证其境外总行、母行或分行、子行为所获得的个人金融信息保密”。2020 年 2 月，中国人民银行发布新修订的金融行业标准《个人金融信息保护技术规范》延续了我国对金融数据出境的措施，第 7.1.3（d）明确规定，“在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境

内存储、处理和分析”，金融数据仅可以在“满足法律法规、获得个人同意、开展安全评估、实现有效监督”的基础上实现个人金融信息出境，对我国金融数据提出更为严格的保护要求。2020 年 9 月，《金融数据安全 数据安全分级指南》正式发布，为金融数据安全分级制定了行业标准，规定重要数据的安全级别不应低于此标准的 5 级。

另一方面，不同金融主体逐步出台行业法规和规范，深化落实金融数据“本土化”要求。2013 年 1 月，国务院发布《征信业管理条例》，第 24 条规定“征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定”。2019 年 1 月，中国银保监会发布《银行业金融机构反洗钱和反恐怖融资管理办法》，第 28 条规定，“对依法履行反洗钱和反恐怖融资义务获得的客户身份资料和交易信息，非依法律、行政法规规定，银行业金融机构不得向境外提供”。2020 年 3 月施行的《证券法》在第 177 条规定，“未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料”。2020 年 9 月，中国人民银行发布《中国人民银行金融消费者权益保护实施办法》，第 34 条规定“银行、支付机构应当按照国家档案管理和电子数据管理等规定，采取技术措施和其他必要措施，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者被篡改。银行、支付机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供”。此法案继续在金融数据保护的基础上，对金融机构的责任作出更为严格的界定，尤其是针对金融数据“泄露、毁损、丢失”的问题，制定了相应的补救措施。

四、我国金融数据跨境流动监管的主要问题

当前，我国在金融数据跨境流动监管领域仍存在以下四个方面的短板。

（一）金融数据权属界定不清，存在监管依据缺位的情况

金融数据因其产生过程涉及主体数量多，常出现权属界定不清晰的情况，给金融监管带来挑战。一方面，金融数据增值权属性界定不清，当金融机构、跨国企业及国

外政府对原始数据进行加工、整合、分析后，原始数据在原有基础上具有新的商业价值，这部分增值数据的所有权、使用权、运营权和收益权法律边界模糊；另一方面，针对跨境金融数据的监管范围没有明确界定，存在部分不被金融监管法规覆盖的机构和企业。例如，在金融科技背景下诞生的第三方数据处理机构，这类企业以挖掘数据价值、为数据提供增值为主要服务内容，但是其获取的原始数据是否获得使用授权、数据增值收益如何分配、是否受到金融监管等问题尚未解决，缺乏相关法律界定。

（二）监管主体监管权限不清晰，部分法律法规操作性尚需完善

目前，我国已经出台多个有关数据跨境传输的规范性文件，现行的《网络安全法》、《数据安全法》、《个人信息保护法》共同构成我国跨境数据流动的三大支柱，但部分法律存在偏重原则性规定、可操作性不强等问题。一方面，在国际化背景下，金融数据跨境流动在实践中涉及到各类复杂的法律问题，涉及主体更为复杂，边界更为模糊，单纯依靠原则性法律进行金融数据跨境流动监管，会导致监管权限不足或监管部门间权限重叠问题；另一方面，金融数据监管涉及的主体众多，国务院、人民银行、银保监会等均制定了金融数据跨境的相关规则，缺乏统一的领导机构，尤其是金融数据受到网络信息部门法律要求和金融行业数据跨境专门规则的“双重管理”，两者之间的法律关系需要进一步梳理，避免监管执行尺度宽严不一等问题。

（三）监管实践存在差异，面临金融数据流动性和安全性的权衡

一方面，在数字经济迅速发展的背景下，虽然我国在各项法律法规中已明确“原则上允许跨境数据有序流动”，但为保护数据安全，在相关法律法规的限制下，我国金融数据跨境传输步骤多、流程长、难度大，针对金融数据跨境的限制性规定远多于鼓励性规定，在一定程度上抑制我国数字产业发展；另一方面，我国网络金融数据面临着来自各方的威胁，必须要守好我国金融数据“红线”。我国利用多重手段对金融数据跨境流动进行限制，本质上是通过增加金融数据出境成本从而减少各类金融数据向外流动，虽然保证了金融数据的安全性，但是数据本土化政策在一定程度上也阻断国内外挖掘金融数据价值的可能性，导致数据这一生产要素无法“物尽其用”。因此，

金融数据流动性与安全性的博弈就像是天平的两端，往往无法实现两者兼顾，这一矛盾将长期存在于立法和监管实践中。

（四）国际合作机制欠缺，我国在国际金融数据流动监管中的话语权不足

现阶段，多样的全球金融数据流动策略导致全球数据治理体系和全球化进程难以同步，无法形成相对统一的国际准则和标准，金融数据跨境流动监管的国际合作机制欠缺，我国融入国际数据流动市场难度较大。一方面，我国现阶段对金融数据出境要求严格，要求对转移到境外的金融信息的保护不应低于我国的保护标准，这无形之中给金融数据跨境流动增加壁垒；另一方面，金融数据跨境流动尚没有统一的国际规则，虽然已有超过 135 个国家和地区出台数据保护法，其中大多数国家和地区都有跨境数据流动法律或政策相关内容，但是各国和地区法律差异明显，立法原则存在冲突，国际规则不兼容，且在以美国为主导的金融数据跨境流动体系中，我国在国际立法中的参与度相对较低，话语权不足。

五、我国金融数据跨境流动监管的政策建议

面对当前日益复杂严峻的国际经济金融环境，我国应充分重视金融数据跨境流动监管的重要性，采取更加有效的措施，做好相关工作。

（一）坚持国家金融数据安全红线，审慎监管金融数据跨境流动活动

安全是发展的前提，发展是安全的保障。考虑到国际形势和本国国情，我国跨境数据流动治理需以保障国家安全、维护本国利益为主。为此，应坚持金融核心系统本地化要求，在守好金融数据安全红线基础上，适度放开金融数据跨境流动性，探索金融数据跨境流动“负面清单”新模式，对于低敏感性、较低安全级别的金融数据，减少数据出境的审核流程，实现数据开放和共享。有关部门要针对不同时期国际环境和社会发展的需要，在明确金融数据跨境流动的主要目标后，就立法和监管的松紧程度、覆盖范围等进行动态调整，协调好跨境金融数据收益和成本、流动性和安全性两组关系，构建相对开放包容、审慎监管的跨境金融数据流动规则，建立与我国国情相符、与数字经济战略目标相适应的跨境金融数据治理体系。

（二）不断完善金融数据跨境流动的相关法律法规

首先，要对现有法律法规做好规则解释，增加现有法规的可操作性，扩大金融监管法规覆盖。在法律法规设计中，进一步明确数据处理者的定义和范围，将与金融数据跨境流动业务相关的主体纳入监管范畴，保障全部金融数据跨境行为有法可依。其次，要注重各个部门法律规则之间的协调和统一，在我国各产业融合发展的大趋势下，金融与工业、电信、交通、科技等领域联系紧密，仅依靠金融行业进行数据安全监管易导致监管缺位，建议确定金融数据跨境流动的统一领导机构，协调各方利益，明确监管分工。最后，要逐步加强涉外法律法规建设，面对国外霸权主义、单边主义和保护主义，我国跨国企业应该能够通过相关法律更好地保护自身权益，做好《中华人民共和国反外国制裁法》的解释和落实，积极应对国外“长臂管辖”的各项措施，保护我国国家安全和利益。

（三）加强顶层设计，建设金融数据跨境流动监管制度体系

一方面，虽然《金融数据安全 数据安全分级指南》将金融数据划分为 1-5 级，但尚未明确哪些级别的金融数据可以自由跨境流动。建议在实务操作中加深金融数据安全分级和数据自由流动程度的融合性，监管机构针对不同主体、不同层次、不同类别、不同敏感程度的金融数据制定与之对应的监管目标；另一方面，在金融数据分类监管的基础上，监管机构要不断丰富监管手段，融合大数据、云计算、区块链、人工智能等前沿技术，提升金融数据监管的效率和精准度。同时，强调行业自律，增强企业和个人在跨境金融数据传输过程中的国家安全保护意识，形成“常规监管+非常规监管”手段的有机结合，形成监管合力。

（四）加强金融数据跨境流动多边合作，主动参与国际规则和标准的制定

一方面，我国要积极参与国际规则制定，为全球金融数据流动体系贡献中国智慧。例如，善用 WTO 安全例外条款，在维护数字经济发展和保障我国贸易自由的前提下，保护我国国家安全和主权。积极参与《区域全面经济伙伴关系协定》（RCEP）等多边协议，通过明确缔约国各方的金融监管透明度义务，探索在保护国家安全的基础上

为金融数据跨境流动开放自由空间。同时，我国有关部门也要研究好 CPTPP、GDPR 等多边地区性协议的主要内涵，更好地在国际社会维护我国国家安全、跨国企业权益和居民个人隐私；另一方面，我国应适当增加国际监管合作，主动参与国际规则制定，深化区域性国际合作，主动申请加入《数字经济伙伴关系协定》（Digital Economy Partnership Agreement，简称 DEPA）等多边合作组织，积极开展国际合作，通过双边、多边协作机制增强我国在国际金融数据治理体系中的话语权。

