金融数据跨境流动规制的核心问题和中国因应

马　兰*

摘　要：金融数据跨境流动规制，本质上是国家公权力对金融市场和经济社会生活进行管理而实施的法律限制。这一规制有其国家和社会经济根源，并且应维持在合理限度。金融数据范围、金融数据控制者、金融数据跨境传输的目的和条件是金融数据跨境流动规制的核心切入点。纵观全球立法实践，金融数据呈现出分级分类特征，金融数据控制者的范围有所扩张，而金融数据跨境传输的不同目的对应了不同的跨境传输条件。中国在金融数据保护立法方面作出了持续性努力，但仍存在一些尚待完善的问题。为应对当前问题并放眼未来发展，中国应调整规制思路，并在金融数据范围、金融数据控制者以及金融数据跨境传输目的和条件方面予以完善。

关键词：金融数据　数据跨境流动　金融数据控制者　金融数据跨境传输目的

伴随区块链、数字货币、移动支付、智能投顾等科技手段对传统金融行业带来颠覆与重塑，[①] 金融数据跨境流动正在呈现指数式增长。它在促进金融全球化纵深发展的同时，也给金融业带来网络风险等重大威胁。对此，各国或地区对金融数据实行不同程度的本地化要求或施加多样的跨境传输条件，[②] 加剧了金融数据跨境流动的现实需求和监管要求之间的矛盾。中国对金融数据跨境流动的规制是及时的，但是否是必要的、合理的，还需从金融监管的视角深入问题的不同侧面，一探究竟。

本文首先分析有关金融数据跨境流动规制的理论性问题，以在本文的问题域内明确规制的必要性、规制目标和合理限度。其次，对金融数据跨境流动规制的三个核心问题，即金融数据的范围、金融数据控制者和跨境传输金融数据的目的和条件进行分别论述，探析国际规制的具体内容和可资借鉴之处。最后，结合中国实践和现有问题，提出具体的应对建议。

一　金融数据跨境流动的规制理论

相较普通意义上的“数据跨境流动”（cross-border data flow），研究金融数据跨境流动需以金

*　马兰，法学博士，对外经济贸易大学法学院，中国银行保险监督管理委员会博士后科研工作站。本文为作者个人学术观点，不代表所在单位意见。

① 参见〔英〕苏珊娜·奇斯蒂、亚诺什·巴伯斯：《Fintech：全球金融科技权威指南》，邹敏、李艳敏译，中国人民大学出版社 2017 年版，第 16 页。

② See Joshua Paul Meltzer, “The Internet, Cross-Border Data Flows and International Trade”, (2014) 2 (1) *Asia & the Pacific Policy Studies* 90, p. 100.

融规制为本，兼具国际贸易视角。本节将对金融数据跨境流动规制涉及的理论性问题进行探讨，包括含义界定，规制的必要性、规制的目标和限度，以及规制的核心内容。

（一）金融数据跨境流动规制的界定

根据 1980 年 OECD《关于隐私保护与个人数据跨境流动的指南》（以下简称《OECD 隐私指南》），“数据跨境流动”是指点到点的跨越国家、政治疆界的数字化数据传递。[①] 这一定义更多体现出了数据流动的“跨境”特征，跨境既包括从一国或地区境内向境外提供数据，也包括从境外直接访问存储于境内的数据。而对于“金融数据跨境流动”的含义，除跨境这一共性要素外，更需侧重于对金融数据本身的界定。

目前国内外对金融数据（financial data）[②] 尚未有较为明确的定义，仅有个别代表性的法律法规对“个人金融信息”（personal financial information）作出界定。例如，中国采用总括加列举的方式，规定“个人金融信息”是指金融（业）机构通过开展业务或者其他渠道获取、加工和保存的个人信息，包括个人身份信息、财产信息、账户信息、信用（贷）信息、金融交易信息、鉴别信息、衍生信息及其他反映特定个人某些情况的信息。[③] 在 1999 年美国《格雷姆－里奇－比利雷法案》（The Gramm Leach Bliley Act，GLBA）中，主要采用“非公开信息”（Non-public information，NPI）的概念，指消费者提供给金融机构的、源于消费者任何交易或所获得的服务的个人可识别的金融信息，这些信息不包括可公开获取的信息。[④] 中、美的界定具有以下共同点：一是个人属性，即个人金融信息可以识别到特定的个人；二是金融属性，即获取、处理数据的是金融机构，而且是在金融机构提供金融产品或服务时所获取的。从美国对 NPI 的定义来看，个人金融信息通常是私密的，不可通过公开渠道所获取。

金融数据的含义显然比个人金融信息宽泛。主要体现在两方面：第一，“数据”是未经过滤的符号或来自各种活动和输入的信号；通过过滤、聚合或排序等可以转换为“信息”。[⑤] 从这个意义上来说，金融数据是大的集合概念，可同时包含金融机构收集的原始数据和经处理加工后的信息。第二，金融机构的客户包括个人客户和企业客户，其收集、处理的数据既包括个人金融信息，也包括企业客户信息，而日常存储处理还涉及金融机构自身的数据，但目前各国或地区主要是将个人金融信息纳入规制范畴。这是因为数据跨境流动规制问题的源起就是保护个人隐私权利，并且有关金融数据跨境流动的规制内容通常是内嵌于整体的数据保护立法框架中。迄今，国内外立法中对数据主体应享有的权利已有所拓展，但对于数据主体是否包含法人这一问题还处在探讨之中。[⑥]

综上，本文结合上述个人金融信息的定义要素和其他现有立法实践，对金融数据作出如下

---

① 参见韩静雅：《跨境数据流动国际规制的焦点问题分析》，载《河北法学》2016 年第 10 期，第 170 页。

② Financial data 在一些情形下也被用来指财务数据，本文未在英文含义和翻译层面上作出区分。

③ 参见《中国人民银行金融消费者权益保护实施办法》（2016 年）第 27 条、《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（2011 年）第 1 条、《个人金融信息保护技术规范》（2020 年）第 3.2 条。

④ See 15 USC § 6809 (4), https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=15-USC-697127498-707328615&term_occur=999&term_src=title:15:chapter:94:subchapter:I:section:6802 (last visited March 26, 2020).

⑤ See UNCTAD, “Digital Economy Report 2019 – Value Creation and Capture: Implications for Developing Countries”, https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466 (last visited March 14, 2020).

⑥ 有学者认为，企业所享有的数据权利属于一种新型财产权。参见王媛：《浅析大数据背景下的企业数据权利》，载《河北企业》2019 年第 6 期，第 158 页。

界定：金融数据是指金融（业）机构通过提供金融产品或服务[①]或者其他渠道获取、加工和保存的个人客户信息和企业客户信息。但鉴于企业客户信息尚未被纳入金融数据跨境流动的规制范畴，本文所探讨的金融数据范围主要是个人客户信息。而金融数据跨境流动规制，则是指所有通过强制金融机构将金融数据保留在某个边界内或对金融数据传输到境外施加额外要求的措施。[②]

（二）金融数据跨境流动规制的必要性、规制目标和限度

金融数据跨境流动规制，本质上是国家公权力对金融市场和经济社会生活进行管理而实施的法律限制。[③] 这种法律限制有其必要性，而规制的必要性则决定着规制的目标。进而，既然是国家公权力对市场的介入，对金融数据跨境流动的规制必然有其范围和程度。

1. 金融数据跨境流动规制的必要性和规制目标

金融数据跨境流动规制的必要性包括两个层面。其一，在国家安全层面，限制金融数据的跨境流动根源于维护网络空间主权和国家安全。网络空间主权是国家意志对其所辖领域内的网络设施、主体及行为具有的“普遍权力”。[④] 由于网络空间无法构成国际政治法律中的“全球公域”，[⑤] 跨境传输将使得金融数据瞬间从一国的网络空间进入另一国的网络空间，在事实上导致数据传输方所在国丧失对其金融数据的控制权和管辖权，将一国公民的金融信息暴露于别国视野之内，由此而引发的数据不当处理、数据泄露乃至网络攻击等诸多风险，将对国家安全形成重大威胁。因此，国家必须强制介入金融数据的跨境传输过程来确保数据安全，以维护网络空间主权和国家安全。

其二，在经济社会层面，限制金融数据的跨境流动根源于金融风险的传导性、信息不对称性和金融业的战略重要性。首先，金融风险的传导性不仅意味着单家机构的风险将快速扩散至整个金融业，还意味着金融业风险向整个经济社会的蔓延。对于产品体系、服务渠道、运营方式等快速数字化的金融业来说，重大数据泄露、重要数据资产丢失等所引发的风险和次生风险可能是致命的。尤其对于大型跨国金融机构，若其收集的金融数据分散存储于全球分支机构的服务器中，该机构一旦倒闭，金融监管部门将不得不向各数据中心所在国申请管辖协助，[⑥] 在付出高昂代价的同时延误了计算损失和评估影响的时机，可引发更广范围的风险。因此，一国保留金融数据本地化存储的政策空间对防范和应对金融风险是至关重要的。其次，金融业的信息不对称性造成了金融机构和消费者对金融数据所享有权益之间的失衡。消费者对金融服务的需求使其不得不向金融机构提供相关的金融信息，而消费者却鲜少有渠道获得有关金融机构的全部信息，更难以对境外数据泄露等主张权利救济。这种信息不对称易引发金融机构对客户金融信息的滥用而造成个人

① 相较《中国人民银行金融消费者权益保护实施办法》（2016 年）和《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（2011 年），《个人金融信息保护技术规范》（2020 年）第 3.2 条将“通过开展业务”改为了“通过提供金融产品或服务”，笔者认为更能准确反映出金融数据的使用场景。

② See Martina F. Ferracane, “Restrictions to Cross-Border Data Flows: a Taxonomy”, https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf (last visited March 26, 2020).

③ 参见韩龙：《金融法与国际金融法前沿问题》，清华大学出版社 2019 年版，第 15 页。

④ 参见张新宝、许可：《网络空间主权的治理模式及其制度构建》，载《中国社会科学》2016 年第 8 期，第 140 页。

⑤ 参见杨帆：《国家的“浮现”与“正名”——网络空间主权的层级理论模型释义》，载《国际法研究》2018 年第 4 期，第 42 页。

⑥ 参见杨幸幸：《〈美墨加协定〉金融服务规则的新发展——以 GATS 与 CPTPP 为比较视角》，载《经贸法律评论》2019 年第 4 期，第 53 页。

隐私权、财产权等合法权益受到侵害，因此一国法律有必要强化对金融消费者所享有合法数据权益的保护。再次，金融业具有战略重要性，金融稳定和安全关系着经济增长和社会稳定，因此全球对金融数据的跨境流动通常实施“特别行业”的严格规制政策，例如将金融数据划归为关键信息基础设施或关键数据等。

以上国家安全层面和经济社会层面规制的必要性也决定了金融数据跨境流动规制的三个目标，即维护国家安全、维持金融稳定和安全、保护金融消费者合法权益。此外，考虑到数字经济时代数据作为关键生产要素的重要价值和数据跨境处理能力对金融机构竞争力的重要作用，对金融数据跨境流动进行规制的效果应当是防止数据滥用，而不是减少数据的使用。鉴此，应当将“挖掘金融数据价值、提升金融服务质效”作为金融数据跨境流动规制的第四个目标，以在安全和发展之间作出相应平衡。而一旦思维转变过来，金融数据就能被巧妙地用来激发新产品和新型服务。①

2. 金融数据跨境流动规制的限度

有研究指出，金融规制只有在其避免发生的损失或取得的利益大于规制监管的成本和代价时，才是正当和合理的。② 从利益来看，金融数据跨境流动有利于全球消费者获取优质的金融服务，促进金融数据的价值挖掘，激发金融创新；而从规制成本来看，金融数据本地化政策将提升金融机构的业务和合规成本，限制金融机构向客户提供核心产品和服务，并降低金融业产能。③ 对这一利益和成本的平衡是全球金融监管者共同面临的课题，不同的国家和地区主要给出了以下两种规制路径和三种具体方案：

第一，美欧在原则上允许金融数据自由跨境传输，但这种自由不是普遍的绝对自由，而是一种附加了诸多条件的“有限自由”规制路径。首先，美国对内和对外所实施的规制要求呈现明显的“双标”特征。对外方面，美国基于数字贸易的先发优势和出口利益，一贯通过商签自由贸易协定（Free Trade Agreements，FTAs）或通过美国商会等对特定国家提出政策建议来推进金融数据的自由跨境流动，以提升其金融机构的全球竞争力。而对内，美国金融监管部门要求迅速、直接、完整且持续地获取金融机构的信息，若外国金融机构无法实现这一监管要求，则必须在美国境内设立数据中心，同时还需履行严格的金融数据合规义务。其次，欧盟不区分对特定行业的数据规制，实行基于风险的规制路径（risk-based approach），要求对金融数据跨境流动的规制与可能产生的风险相适应，例如不能超过保护个人数据的必要限度。④

第二，中国、印度尼西亚、俄罗斯、越南、韩国等国家对金融数据跨境流动采取“普遍限

① 参见〔英〕维克托·迈尔－舍恩伯格、肯尼思·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社2013年版，第16页。

② 参见韩龙：《金融法与国际金融法前沿问题》，第37页。

③ See Brendan O' Connor, “Quantifying the Cost of Forced Localization”, http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization (last visited March 27, 2020); Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, “Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization”, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf (last visited March 27, 2020); Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, and Bert Verschelde, “The Costs of Data Localization: Friendly Fire on Economic Recovery”, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (last visited March 27, 2020).

④ See OECD, “The OECD Privacy Framework 2013”, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited March 30, 2020).

制”的规制路径，要求金融机构核心系统本地化和金融数据在本地存储。[①] 需要指出的是，尽管美欧一直对中国采取的上述政策多加指责，但笔者认为，金融核心系统本地化和金融数据本地存储是两个性质不同的问题，必须分别探讨规制限度的合理性。首先，金融核心系统本地化的规制措施与这些国家的金融市场发展状况、对外资金融机构的监管手段和监管科技发展程度息息相关，属于一国金融规制的自主权利。金融机构的核心系统在物理上体现为存储或处理金融数据的计算机基础设施，也即通常所说的数据中心。要求核心系统本地化是对外资金融机构的业务连续性和风险防范进行监管的首要方式，同时也是金融机构安全稳健运营的前提基础，不规制的代价相比规制的成本而言要高昂得多。其次，对于要求金融机构在境内存储金融数据的规制措施，则是国际上通常从服务贸易角度探讨的数据跨境流动问题，因为如若禁止基于业务需求跨境传输金融数据，确实会对金融机构为客户提供金融服务产生影响甚至降低其竞争力。此外，由于数据并不是稀缺资源，要求核心系统本地化并不妨碍在一定条件下允许金融机构跨境传输开展业务所必需的金融数据。对此，下文还将从不同方面详细论述。

（三）金融数据跨境流动的核心规制内容

金融数据的跨境流动包含三个关键要素，即“跨境传输什么”、“谁来跨境传输”、“如何跨境传输”。这三个要素也是一国法律对金融数据跨境流动进行规制的核心切入点。鉴此，本文将探讨以下三个核心问题：第一，是否需要在数据源头上对金融数据跨境流动施加监管？此即金融数据跨境流动规制所涵盖的数据范围问题。第二，对跨境传输金融数据的机构应施加何种规制措施？此即金融数据跨境流动规制所涵盖的数据控制者问题。第三，在跨境传输金融数据时，应满足哪些监管要求？是否有其目的限定和条件限制？此即金融数据跨境流动的目的限定和条件限制问题。下文第二、三、四节将分别展开论述。

二　金融数据跨境流动规制所涵盖的数据范围

金融机构客户的金融信息既包括姓名、性别、身份证等基础身份信息，也包括信用卡信息、交易流水、支付信息等敏感和保密信息。在跨境传输时，身份信息的泄露可能会使得消费者遭遇骚扰电话甚至财产损失，但信用卡、交易、支付等信息的泄露几乎百分百地引起信用卡被盗刷等风险，从而大幅增加消费者遭受财产损失的可能性。这一明显的区分意味着法律规制的触角必须伸向金融数据本身，从源头上对金融数据的跨境流动实施分级和分类规制。

（一）金融数据的分级分类法律标准

首先，金融数据的分级是将其划分为不同级别，国内外立法中主要规定了两种方式。一种是按照数据的敏感程度和安全防护级别来划分，将金融数据分为一般数据、敏感数据、关键或重要数据，并对其施加不同程度的跨境流动规制。例如，印度《2018 个人数据保护法（草案）》

① See Albright Stonebridge Group, “Data Localization: A Challenge to Global Commerce and the Free Flow of Information”, https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf (last visited April 14, 2020).

（Personal Data Protection Bill 2018）规定，对一般个人数据，可经数据主体同意后在特定条件下进行跨境传输；对敏感个人数据只有满足为特定人员或机构提供健康服务或紧急事件服务所必须、并且数据接收方可提供充分保护的条件下进行跨境流动；而关键个人数据只能在印度境内处理。①

敏感数据指一旦遭到泄露或修改，会对数据主体造成不良影响的信息，可包括密码、财务数据、健康数据、官方标识符、性生活、性取向、生物数据、基因数据、宗教或政治信仰、受到行政或刑事处罚的情况等。② 各国或地区通常禁止处理或跨境提供敏感数据，除非符合更加严格的条件，并采取去标识化、匿名化等适当的安全措施。例如，瑞士规定，处理敏感数据必须经数据主体明示同意，而且只能基于法令的明确规定。③ 欧盟规定，如果非欧盟国家出于反洗钱要求需要跨境传输大量的敏感信息，“公共利益”也不能作为该跨境传输的正当性理由。④ 值得指出的是，中国2017 年发布的《信息安全技术 数据出境安全评估指南（征求意见稿）》⑤ 和 2020 年发布的《信息安全技术 个人信息安全规范》等技术标准中已体现出对敏感数据进行分级规制的成型思路，但是对敏感数据本身的出境条件未作出明确规定。

对关键数据，印度尚未公布具体范围。中国《网络安全法》提出的“重要数据”、“关键信息基础设施”的概念与之类似。重要数据是指“与国家安全、经济发展以及公共利益密切相关的数据”，而关键信息基础设施的范围也非常广泛，金融业同能源、交通等重要领域整体均包含在内。这样的划定实际上并未对金融数据进行分级分类规制，在实践中难以执行。

另一种分级方式是根据未经授权查看对数据主体的信息安全和财产安全造成的危害程度，将金融数据分为用户鉴别信息（C3）、可识别信息主体身份与金融状况的个人金融信息（C2）、机构内部的信息资产（C1）等三个级别，危害程度逐级降低。⑥ 用户鉴别信息是金融机构开展业务时为认证该用户真实身份的信息，包括但不限于银行卡密码、账户密码、用于用户鉴别的个人生物识别信息等，这些信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害。可识别信息主体身份与金融状况的个人金融信息包括支付账号及其等效信息、账户登录的用户名、交易信息等等，一旦未经授权查看或变更，会对信息主体造成一定危害。而机构内部的信息资产主要是金融机构内部使用的账户开立时间、开户机构等信息，未经授权查看或变更会对数据主体造成一定影响。这种分级方式紧密结合了金融数据的使用场景，具有创新性和很强的实用性。

其次，金融数据的分类通常是按照金融数据的信息内容来划分，可以分为身份数据、交易数据、信用数据、衍生数据等。“身份数据”包括姓名、性别、身份证等基本信息；“交易数据”包括金融机

---

① 参见胡文华、孔华锋：《印度数据本地化与跨境流动立法实践研究》，载《计算机应用与软件》2019 年第 8 期，第 307 页。

② 参见中国 2020 年《信息安全技术 个人信息安全规范》第 3.2 条；韩国 2011 年《个人信息保护法》（Personal Information Protection Act）第 23 条；欧盟 2018 年《通用数据保护条例》（General Data Protection Regulation，GDPR）第 51 条、53 条、54 条；瑞士 2019 年修订的《联邦数据保护法》（Federal Act on Data Protection，FADP）第 3 条 c 款。

③ 参见瑞士 2019 年修订的《联邦数据保护法》（Federal Act on Data Protection，FADP），https：//www. admin. ch/opc/en/classified - compilation/19920153/index. html，最后访问时间：2020 年 4 月 14 日。

④ European Data Protection Supervisor，“Guidelines on Data Protection in EU Financial Services Regulation”，https：//edps. europa. eu/sites/edp/files/publication/14 - 11 - 25_ financial_ guidelines_ en. pdf（last visited April 14，2020）.

⑤ 尽管法律法规的征求意见稿本身无法律效力，本文将征求意见稿与已生效的法律法规一并讨论。原因包括两方面：一是目前国内正在积极制定数据保护有关立法，一些典型的法律法规草案还处于征求意见阶段；二是公开征求意见是法定的立法环节，从征求意见稿的内容中可体现出立法思路和规制要点，并且分析规制思路的发展脉络。

⑥ 参见《个人金融信息保护技术规范》（2020 年）第 4.2 条。

构在开展业务过程中获取、保存、留存的个人信息。客户基本信息和交易信息通常是金融机构在展业过程中必须使用或处理的信息。据笔者不完全统计，目前至少有美国、英国、新加坡、中国香港等 43 个国家和地区允许金融企业在特定条件下向集团总部、第三方等跨境传输客户基本数据和交易数据。[①] 相较而言，中国 2019 年《银行业金融机构反洗钱和反恐怖融资管理办法》严格禁止跨境转移客户身份数据和交易数据，在国际上属于较为特例的情形。

“信用数据”包括信用卡还款情况、贷款偿还情况等能反映个人信用情况的信息，一些国家限制使用或禁止跨境提供信用信息。例如，美国 2003 年《公平和准确信贷交易法》规定，限制使用与个人信誉、信用状况、一般信誉、个人特征或决定信用、雇佣或保险资格的生活模式相关的信息。[②] 中国 2013 年《征信业管理条例》规定，中国公民的所有征信信息都须在境内处理和存储。

“衍生数据”包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映个人特征的信息，即“用户画像”。这类数据的质量对精准定位金融消费者、分配金融产品资源具有重要价值。例如，智能投顾即是通过算法来精准匹配消费者和金融产品。目前国内外立法对衍生数据的跨境流动尚无专门规制，但从数据的性质和应用场景来看，衍生数据具有更高的敏感度和更强的个人可识别性，应当加强保护并限制跨境传输。

（二）特定类型金融数据的本地化存储或限制跨境传输要求

除上述对金融数据的分级分类外，一些国家和地区还要求特殊类型的数据必须在境内储存或限制数据传输，主要包括健康数据、支付清算数据和会计数据等。

首先，“健康数据”属于敏感数据，保险公司承保人身险时需了解所有与健康状况相关的要素，例如发病率和残疾、医疗保健需求、分配给医疗保健的资源、死亡原因等。[③] 在当前大数据背景下，保险公司在提供服务过程中收集的单个客户健康数据经汇集加工，可反映出国民的年龄分布、疾病分布、医疗状况、死亡原因等国民健康基本面数据，由保护个人隐私上升至维护国家安全层面。因此，欧盟、澳大利亚等多个国家对金融企业收集的健康信息予以严格规范。例如，欧盟 2018 年《通用数据保护条例》（General Data Protection Regulation，GDPR）规定，“只有在为公共利益所必须时才能不经数据主体同意处理健康数据，并且不能被银行或保险公司基于其他原因所处理”。[④]

---

① 包括欧盟 27 个成员国、英国、美国、加拿大、墨西哥、新加坡、日本、澳大利亚、韩国、越南、马来西亚、新西兰、印度、印度尼西亚、俄罗斯、中国香港、中国澳门。具体法律法规参见：欧盟 2018 年《通用数据保护条例》（GDPR）；美国 1999 年《格雷姆－里奇－比利雷法案》（The Gramm Leach Bliley Act，GLBA）；加拿大 2019 年修订的《个人信息保护和电子文件法》（Personal Information Protection and Electronic Documents Act，PIPEDA）；墨西哥 2010 年《私人信息联邦保护法》（The Federal Law on the Protection of Personal Data Held by Private Parties）；新加坡 2008 年修订的《银行法》（Banking Act）；日本 2003 年《个人信息保护法》（The Personal Information Protection Act）；澳大利亚 1988 年《隐私权法》（Privacy Act）；韩国 2011 年《个人信息保护法》（Personal Information Protection Act）；越南 2010 年及 2017 年《信贷机构法》（Law on Credit Institutions）；马来西亚 2017 年《客户信息管理及披露的规定》（Management of Customer Information and Permitted Disclosures，MCIPD）；新西兰 1993 年《隐私法》（Privacy Act）；印度央行 2016 年《了解你的客户指引》（Know Your Customer Direction）；印度尼西亚 1998 年修订的《银行法》（Law of the Republic Indonesia No. 7 of 1992 concerning Banking as Amended by Law No. 10 of 1998）；俄罗斯 2006 年《联邦个人信息法》（The Russian Federal Law on Personal Data）；中国香港 2013 年《个人资料（私隐）条例》；中国澳门 2005 年《个人资料保护法》。

② United States，Fair and Accurate Credit Transactions Act，https：//www. investopedia. com/terms/f/facta. asp（last visited April 14，2020）.

③ EU，GDPR，Recital 54 Processing of Sensitive Data in Public Health Sector，https：//gdpr－info. eu（last visited April 14，2020）.

④ EU，GDPR，Recital 54 Processing of Sensitive Data in Public Health Sector，https：//gdpr－info. eu（last visited April 14，2020）.

2012 年，澳大利亚颁布《个人控制电子健康记录法案》（Personally Controlled Electronic Health Records Act），要求个人健康记录只能在澳大利亚境内存储。2014 年，原国家卫生和计划生育委员会发布的《人口健康信息管理办法（试行）》规定，不得将人口健康信息在境外的服务器中存储。但是，该办法的适用对象是医疗卫生计生服务机构，内容简单且适用范围较窄。

其次，在支付清算服务的提供过程中，付款人和收款人之间需要通过各自的服务提供商交换姓名、银行帐号和交易合同等内容，以保证支付转账的顺利进行。支付清算数据的安全直接影响客户的资金安全，为维护支付系统和金融体系的稳定性，一些国家对该类数据出境施加更严格的要求。例如，印度禁止支付数据出境。美国要求，信用卡公司处理、存储或转移付款卡数据要符合“支付卡行业数据安全标准”（Payment Card Industry Data Security Standard，PCI-DSS）。中国 2016 年《银行卡清算机构管理办法》规定，银行卡清算机构为处理跨境交易向境外发卡机构或收单机构传输境内收集的个人金融信息的，需先经当事人授权，并通过业务协议等有效措施要求境外机构保密。

再次，“会计数据”是在会计事项处理中，以“单、证、帐、表”等形式表现的各种未经加工的数字、字母与特殊符号的集合。丹麦、芬兰、英国等要求企业的会计信息必须在境内存储。例如，丹麦 2015 年《簿记法》（Bookkeeping Act）要求公司在丹麦将会计数据存储五年。在特殊情况下，丹麦商业和公司代理机构可以授予公司在国外保存会计记录的权限。但是，实践中例外情形的适用非常严格，很少授予许可。芬兰 1997 年《账户法》（Account Act）要求公司的会计记录副本必须存储在芬兰。倘若可以保证与数据的实时连接，则可以将记录存储在另一个欧盟成员国中。[①] 根据英国 2006 年《公司法》（Companies Act），如果会计记录保存在英国以外的地方，则必须将账务信息等发送到英国并保存在英国境内，并且必须始终接受检查。[②]

三　金融数据控制者和其跨境传输数据时的法定义务

“数据控制者”概念主要由欧盟 GDPR 提出，指“能单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、行政机关或其他非法人组织”。由于金融数据流动的实际情形较为复杂，通常难以真正区分数据控制者和处理者，[③] 本文以“金融数据控制者”指代包括金融数据处理者在内的更广泛的主体。在实践中，提供金融服务并收集、处理金融数据的企业类型是非常多元的，明确金融数据跨境流动规制的适用对象并落实相应的义务和责任无疑是必要且重要的。

（一）金融科技背景下金融数据控制者范围的扩张

金融科技背景下，金融数据治理体现出科技化和自动化特征。[④] 互联网金融公司、金融科技公司、互联网金融平台等凭借多场景、多维度的大数据优势，通过互联网渠道的迅捷和便利切入传

① See Nigel Cory, “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?”, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost (last visited April 14, 2020).

② United Kingdom, Companies Act 2006, Chapter 46, http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf (last visited April 14, 2020).

③ See Kathryn Wynn, “GDPR: the ‘Controller v Processor’ Debate in Financial Services”, https://www.pinsentmasons.com/out-law/analysis/gdpr-the-controller-v-processor-debate-in-financial-services (last visited April 14, 2020).

④ 参见刘元兴、王好好：《金融数据治理的特征与趋势》，载《银行家》2018 年第 24 期，第 2 页。

统的消费金融、支付、财富管理等业务市场，使得海量的金融数据向这些公司和平台汇聚集中。伴随新技术在金融业的应用促使传统金融业态发生革新，金融数据控制者的范围发生了明显扩张，包含了以下三类机构：第一类是由国家金融监管部门监督管理的持牌金融机构，即传统上提供金融服务的银行、保险公司、证券公司等；第二类是持牌的非金融机构，例如第三方支付机构、外包服务机构等；第三类则是为持牌金融机构提供基础支持服务而需要处理金融数据的企业，例如提供身份验证服务的电信服务商、信息技术提供商、风控服务解决方案提供商、市场营销服务提供商等。

这一扩张趋势已体现在了有关金融数据跨境流动的最新国际条约实践中。在早期签订的《北美自由贸易协定》（NAFTA）、《美国—韩国自由贸易协定》（KORUS）和 2018 年签署的《全面与进步跨太平洋伙伴关系协定》（CPTPP）等典型自由贸易协定中，金融数据跨境转移条款都仅约束缔约方境内设立的金融机构。2019 年 2 月 1 日生效的《欧盟—日本经济伙伴关系协定》中，金融数据转移条款采用了“金融服务提供者”措辞，适用范围予以扩展。2019 年 9 月签署的《美国—日本数字贸易协定》明确规定了协议涵盖的金融服务提供者既包括金融机构（financial institutions），也包括受到缔约方金融监管部门监管、颁发许可、授权或注册的金融服务提供者（financial service suppliers）。具体而言，“金融机构”指“缔约方境内被授权开展业务并作为金融机构监管的金融企业”；而“金融服务提供者”虽然不是金融机构，但强调是纳入金融监管范畴且提供金融服务的企业。[①] 这一规定意味着，缔约方应当允许这两类主体基于正常商业经营跨境传输金融数据，同时也有权对这两类主体在跨境传输金融数据的过程中施加个人数据保护等义务。

在国际法层面，中国目前签订的 17 个 FTAs 中尚未有金融数据跨境转移条款，亦未有机会对金融数据控制者有所着墨。但值得指出的是，人民银行和全国金融标准化技术委员会于 2020 年 2 月 13 日发布的《个人金融信息保护技术规范》首次明确规定，“金融业机构”包括两类机构，一类是由国家金融监管部门监督管理的持牌金融机构，另一类是涉及个人金融信息处理的相关机构。由于该《规范》适用于提供金融产品和服务的金融业机构，而前文述及的第三类机构是为持牌金融机构提供身份验证、信息技术、风险控制、市场营销等基础支持服务，本质上不属于金融服务。此外，结合该《规范》中关于信息外包等内容的规定可以进一步判断，这里的第二类机构应该是前文中所指的第三方支付机构、外包服务机构等持牌的非金融机构。

此外，《网络安全法》从网络空间的角度对“网络运营者”进行界定，包含了“网络所有者、管理者和网络服务提供者”在内的所有金融企业，需履行义务的机构范围最广；2020 年发布的《信息安全技术 个人信息安全规范》从个人数据的角度对“个人信息控制者”进行界定，指有权决定个人信息处理目的、方式等的组织或个人，需履行义务的机构范围也很广；而银行业、保险业等法律法规的适用对象则主要是银行和保险公司等金融机构，不约束非金融机构的数据跨境传输行为。因此，国内关于金融数据控制者的概念和范围还需在不同法律法规之间进行衔接和协调，以进一步明确规制的机构类型。

（二）金融数据控制者跨境传输数据时的法定义务

金融数据控制者能够决定数据的处理目的和方式，各国或地区通常对其施加最大的数据保护义

① See Article 1（d）and Article 11（Cross-Border Transfer of Information by Electronic Means）of the Agreement between the United States of America and Japan concerning Digital Trade.

务。金融数据控制者在跨境传输金融数据时的法定义务主要包括数据安全保护义务和数据质量保障义务。

首先，数据安全保护义务是金融数据控制者的首要义务，该义务根植于个人隐私保护，但又是不同于个人隐私保护的独立义务。[①] 在某些情形下，数据保护的范围比个人隐私保护更广，因为对个人隐私的侵害还取决于数据收集和使用的具体情形，但数据保护规则适用于数据处理的全过程。

从“数据价值链”来看，[②] 金融数据跨境传输位于数据流动的中端，其前端是金融数据的收集或处理，后端是金融数据接收方对数据的使用，跨境传输数据安全的实现必须依赖于前、中、后端数据保护的密切配合和无缝衔接。在前端，金融机构在设立之初通常都被要求构建完整有效的数据治理架构，包括建立涉及客户信息、账务信息和产品信息等的核心系统并独立运营、建立数据安全策略与标准、划分数据安全等级、完善数据安全技术等。在后端，数据控制者应确保数据接收方有充分的数据保护水平或者保证对数据不做他用。在跨境传输时，数据安全保护包括金融数据控制者自身数据的安全保护和客户信息安全保护两方面。[③] 根据美国纽约州 2018 年《金融服务公司网络安全要求》（Cyber Security Requirements for Financial Services Companies）和欧盟 GDPR，数据控制者在跨境传输金融数据时承担“以风险防范为导向”的数据安全保护义务。[④] 数据控制者必须定期评估所面临的可能危害自身网络和信息安全以及客户信息安全的风险，并且要提交年度合规证书。同时，数据控制者须履行对客户的告知义务。GDPR 还规定，针对可能对数据主体的权利产生具体风险的跨境传输，数据控制者应在数据传输前通告监管部门进行“事前检查”。

其次，数据质量保障义务是防范金融数据传输风险的重要前提。金融数据的质量对金融机构自身和金融非现场监管来说都至关重要，低质量的数据不能反映金融业务的实际运行状况，无法为数据跨境传输时的风险评估和金融监管提供真实有效的依据。[⑤] 早在 1980 年，《OECD 隐私指南》即确立了“数据质量原则”，规定“个人数据应与使用目的有关，并且在达到这些目的所必需的范围内，个人数据应准确、完整并保持最新”。[⑥] 实际上，该原则的提出就是源自欧洲委员会部长委员会在 1973 年和 1974 年对关于电子数据银行的两起案件的审理，数据质量对金融业的重要性可见一斑。

从 OECD“数据质量原则”中引申出了判定数据质量的四个关键性要素，即相关性、准确性、完整性和即时性，这四个要素已被吸纳进了欧盟、韩国、加拿大等多个国家和地区的立法实践中。[⑦] 具体而言，相关性是指数据控制者所收集的个人数据应当与使用目的相关；准确性和完整性则是指数据应当精确无误并且完整，以便能反映数据主体的利益；而即时性是指数据控制者

---

① See European Data Protection Supervisor, “Guidelines on Data Protection in EU Financial Services Regulation”, https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf (last visited April 14, 2020).

② 伴随数据体量的增长，支持挖掘数据价值的公司发展了一条全新的“数据价值链”，包括数据采集、数据存储、数据建模和数据可视化等。See UNCTAD, “Digital Economy Report 2019 – Value Creation and Capture: Implications for Developing Countries”, https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466 (last visited April 14, 2020).

③ 参见辜明安、王彦：《大数据时代金融机构的安全保障义务与金融数据的资源配置》，载《社会科学研究》2016 年第 3 期，第 76 页。

④ 参见洪延青：《透析金融数据保护的美欧中立法要点和趋势》，载《中国银行业》2018 年第 11 期，第 40 页。

⑤ 参见刘元兴、王好好：《金融数据治理的问题与对策》，载《银行家》2019 年第 1 期，第 2 页。

⑥ See OECD, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited November 10, 2019).

⑦ 参见欧盟 2018 年 GDPR 第 5 条、韩国 2011 年《个人信息保护法》（Personal Information Protection Act）第 3 条、加拿大 2019 年修订的《个人信息保护和电子文件法》（Personal Information Protection and Electronic Documents Act, PIPEDA）第 4.6 条。

应及时更新数据，删除陈旧过时的信息。金融企业对数据质量四要素的保障能够使其在开展业务时对客户作出准确的判断，以降低不当使用客户信息的可能性。在金融数据的跨境传输环节，良好的数据质量有助于金融企业作出合理的风险评估结论，也有助于提升金融监管部门对数据跨境传输目的和风险评估进行审查的效率。

四　金融数据跨境流动的目的限定与条件限制

收集个人数据只能出于特定、明确和合法的目的，并且不得以与这些目的不一致的方式对数据进行进一步处理，此即数据跨境流动的“目的限制”原则。跨境传输的目的不仅是各国或地区是否允许金融数据跨境流动的先决条件，同时也是金融数据出境安全评估的首要环节。实践中，金融机构跨境传输数据通常是基于三种目的需求和三类数据接收方：一是因日常商业经营需要向集团总部跨境提供客户信息；二是因外部审计等原因跨境向第三方提供客户信息；三是因日常监管要求等原因跨境向金融监管部门提供客户信息。这三类目的及其适用条件之间既有联系亦有区别。鉴于法律来源于社会现实并需与时俱进地回应社会现实，只有从金融数据跨境流动的实际出发进行立法，才可有效发挥法律的规范作用和社会作用。

（一）基于日常商业经营目的向集团总部跨境传输数据

银行业全球化经营的特征最为明显，向集团总部传输数据的情形在银行业尤为突出。在银行境外分支机构与总行联动开展贸易融资、双边理财等跨境金融业务时，都需要向总行跨境传输金融数据。FTAs 中一般允许“基于日常商业经营”目的跨境转移金融数据。相关表述分为两类：一类是概括规定允许“为商业经营目的”[①] 或“金融机构日常经营所要求”[②] 来跨境转移数据。另一类将“商业经营目的”进一步限定在金融企业的“牌照、授权或注册的范围之内”，[③] 在限定跨境转移数据范围的同时强化了金融监管权力。但两种规定都很笼统，且未规定对应的条件限制。

从各国国内法来看，据笔者不完全统计，目前有 43 个国家和地区允许其境内的外资银行在特定条件下跨境向集团总部提供客户信息。[④] 各国或地区规定的数据跨境传输条件不尽相同，但基本上都落入了欧盟 GDPR 规定的以下四个条件限制之中：[⑤]

1. 向集团总部跨境传输金融数据须具备法律基础。欧盟 GDPR 要求跨境传输数据是履行与数据主体间的合同所必要的，或者是在订立合同之前根据数据主体的要求所进行。“为履行合同所必要”既包括数据跨境传输目的上的必要性，还包括数据范围上的必要性。例如在德国，客户汇款至中国，完成汇款所必需的姓名、账号、金额等信息可以提供给中国，其他信息则不能提供。

---

① 参见《美国—韩国自由贸易协定》附件 13－B（具体承诺）B 节（信息转移）；《欧盟—日本经济伙伴关系协定》第 8. 63 条（信息转移和信息处理）。

② 参见《全面与进步跨太平洋伙伴关系协定》第 11 章（金融服务），附件 B（具体承诺）B 节—信息转移；《美国—日本数字贸易协定》第 11. 1 条。

③ 参见《美墨加协定》第 17. 17 条（信息转移）。

④ 包括欧盟 27 个成员国、英国、美国、加拿大、墨西哥、新加坡、日本、澳大利亚、韩国、越南、马来西亚、新西兰、印度、印度尼西亚、俄罗斯、中国香港和中国澳门。

⑤ GDPR 第 2 章“原则”，第 5 至第 7 条；第 5 章“将个人数据转移到第三国或国际组织”，第 45 至第 48 条。

2. 须经客户同意，数据控制者需提供相关证明。几乎所有国家和地区都有该要求，但具体同意的标准存在差异。例如，瑞士、俄罗斯、韩国都要求获得客户的书面许可，韩国还要求在客户同意函中明确信息提供的范围、目的和提供对象。①

3. 向集团总部跨境传输金融数据是为数据控制者履行法律义务所必须。对于“履行法律义务所必须”的界定，欧盟 GDPR 主要从合法性、合理性和必要性进行审查。而瑞士、新加坡、马来西亚、印度尼西亚等将该情形仅限定在了并表管理、内部审计和风险管理等方面。这些场景下需要的金融数据是汇聚和批量形式的数据，不具有个人识别性。例如，瑞士只允许基于并表管理的需要向集团总部传输数据，集团总部要证明获取数据的必要性，证明数据不会用作其他用途，并且第三方无法通过集团总部获得这些信息。

4. 金融机构分支机构和集团总部之间须签署包含标准数据保护条款的协议。该标准协议通常必须符合数据保护法律的规定，并且经监管部门批准。墨西哥还规定，协议内容须包含数据传输方和接收方履行的相同义务。②

值得指出的是，2019 年发布的《中国人民银行金融消费者权益保护实施办法（征求意见稿）》第 34 条在金融数据应本地存储的原则之外，提出了因业务需要确需向境外提供消费者金融信息时需符合 5 项条件：（1）为处理跨境业务所必需；（2）经金融消费者书面授权；（3）信息接收方为完成该业务所必需的关联机构（含总公司、母公司或者分公司、子公司等）；（4）通过签订协议、现场核查等有效措施，要求境外机构为所获得的消费者金融信息保密；（5）符合法律法规和其他相关监管部门的规定。由此可以看出，该《实施办法》规定了允许在金融机构集团内部跨境传输数据的例外情形，需满足的条件与上文中的条件相类似，但规定得十分笼统，并且“业务所需”未能体现出是须具备法律基础、履行法律义务的内涵。

（二）基于外部审计等需求跨境向第三方转移数据

跨国经营的金融机构在年度审计或专项审计时，都需向审计师跨境传输金融数据。例如，对于在境外上市的中资银行，由于境外审计师需对整个集团的合并财务报表进行审计，需获取包括该银行全球分支机构在内的集团经营数据。据笔者不完全统计，目前有 22 个国家和地区允许金融机构在特定条件下基于外部审计等需求跨境向第三方转移数据。③ 相较向集团总部跨境传输金融数据，向第三方转移数据的条件限制呈现出三分法特征：

首先，英国、德国、瑞士、捷克等国家对向集团总部和向第三方跨境传输数据规定的适用条件相同，基本包含在前述四项条件之中。尽管如此，在金融监管实践中，金融机构向审计师跨境传输数据受制于更严苛的操作方式。例如在英国，外国银行的分支机构不能直接向境外审计师（例如毕马威中国）跨境传输数据，而是通过英国境内的审计师（如毕马威英国）传输至该境外

① 参见瑞士 2019 年修订的《联邦数据保护法》（Federal Act on Data Protection，FADP）第 4 条和第 6 条，瑞士 2019 年修订的《银行法》（Swiss Federal Act on Banks and Savings Banks）第 4 条；俄罗斯 2006 年《联邦个人信息法》（The Russian Federal Law on Personal Data）第 12 条；韩国 2011 年《个人信息保护法》（Personal Information Protection Act）第 17 条和第 32 条。

② 墨西哥 2011 年《私人信息联邦保护法细则》（The Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties）第 74 条，https://iapp.org/media/pdf/resource_center/2%20Regulations%20to%20the%20FLPPDHPP.pdf，最后访问时间：2020 年 5 月 7 日。

③ 包括美国、英国、德国、瑞士、捷克、俄罗斯、土耳其、加拿大、秘鲁、墨西哥、新加坡、日本、越南、马来西亚、菲律宾、印度、印度尼西亚、泰国、澳大利亚、新西兰、中国香港和中国澳门。

审计师，并且数据传输的双方之间必须有允许信息传输和数据保护的协议安排。

其次，一些国家对向第三方跨境转移数据规定了更加严格的条件限制。例如，根据美国 1978 年《金融隐私权利法》（Right to Financial Privacy Act），金融机构不得直接或通过任何关联公司向非关联第三方披露非公开个人信息，除非符合四项条件：一是银行已向消费者提供初始通知；二是银行已向消费者提供不允许披露的权利和操作方法；三是在向非关联第三方披露信息之前，银行已给予消费者合理的机会选择不允许披露；四是消费者没有选择不允许披露。

第三，韩国、奥地利允许金融机构在特定条件下向集团总部跨境传输数据，但不允许向审计师等第三方跨境传输数据。奥地利 1993 年《银行法》（Austrian Banking Act）第 30 条第 9 款规定，在奥地利注册成立的金融机构子公司可按照集团合并报表的要求跨境向集团总部提供客户资料，但不能直接跨境向第三方机构提供相关信息。而韩国监管部门提供的“金融交易信息同意书”中规定，信息提供仅限于对金融机构集团总部或分支机构以及监管部门，不包括审计师等第三方机构。①

总结而言，立法实践中向审计师等第三方机构跨境传输数据比向集团总部传输数据要求更严。这两种数据传输目的都可具备合法性和必要性，但在数据安全和风险防范来看存在差异。一是从数据安全本身来看，在集团内部数据治理架构和数据处理标准较为统一，更便于通过现场检查或非现场监管等方式预警和监测数据跨境传输的风险，而第三方机构对数据的使用和处理目的则较难监控。二是从数据安全所搭载的资金安全来看，因金融服务合同的存在，在集团内部发生数据泄露风险后对客户的资金安全保障更强，而第三方因不和客户直接签署合同，数据泄露后对客户资金保障的责任难以有效落实。

（三）基于境外监管要求跨境向金融监管部门转移数据

金融监管部门要求跨境传输数据的原因包括出于日常监管要求金融机构提供境外经营信息、加强金融监管和提高交易透明度，以及进行反洗钱、反恐怖融资检查。与前两种跨境传输数据有所不同，向境外金融监管部门传输数据是向公权力传输数据，直接涉及金融数据跨境传输双方金融监管权之间的冲突问题。一国或地区是否允许其境内的金融机构直接向母国监管当局跨境传输数据，在很大程度上取决于是否承认母国监管当局的金融监管权力、以及双方金融监管部门之间是否存在监管合作和信息共享等协议安排。

据笔者不完全统计，目前有 14 个国家和地区允许在特定条件下向境外监管部门提供金融数据。② 在具体条件限制上，立法实践存在两点共同之处。首先，最大的共性是向境外监管部门提供数据必须经本国或地区金融监管部门批准。例如，土耳其须获得银行监管委员会的批准，新西兰须获得储备银行的批准。③ 其次，跨境传输双方政府之间需有双边金融监管合作等协议或加入有关多边数据保护公约。例如，墨西哥要求，非所在国监管机构隶属于欧洲理事会发布的《个人数据自动化处理中的个人保护公约》签署国，在经墨西哥国家银行、墨西哥国家私人信息数

① Korea, Consent to Provision of Financial Transaction Information, https://apps.rbcits.com/RFP/gmi/marketnewsflash/South%20Korea%20-%20Consent%20letter%20-%20Corporate%20-%20December%202017.pdf (last visited April 14, 2020).

② 包括德国、捷克、俄罗斯、土耳其、加拿大、墨西哥、新加坡、韩国、马来西亚、印度、印度尼西亚、新西兰、中国香港和中国澳门。

③ 参见土耳其 2013 年《银行法》（Banking Law）第 73 条，土耳其 2016 年《个人数据保护法》（Law on the Protection of Personal Data）第 9 条；新西兰 2016 年《银行注册和监管原则陈述》（Statement of Principles-Bank Registration and Supervision, BS1）。

据保护局等同意后，墨西哥银行机构可跨境向非所在国监管机构提供客户信息。[①]

在允许数据出境的具体情形上，各国和地区的关注点则存在多元性。例如，加拿大规定，只有境外监管机构在对金融机构处理的交易进行反洗钱等监管检查时，才可通过该金融机构集团总部要求提供加拿大境内的客户信息。[②] 新加坡规定，向境外监管机构提供客户信息，还需根据对方法律规定，对方监管机构不会进一步披露相关信息。

综上，各国或地区对跨境传输金融数据三种目的的法律规制呈现出明显的分级化特征。有条件地允许基于日常商业经营目的向集团总部跨境传输数据的国家最多；基于外部审计等需求跨境向第三方转移数据次之，并且总体上条件限制更为严格；而跨境向金融监管部门转移数据则更多取决于金融监管部门之间的监管合作协议安排。

五　中国对金融数据跨境流动的规制发展和主要问题

近年来，中国在数据保护立法方面作出了持续性努力。国家安全部门、网络信息部门、金融监管部门等分别颁布相关的法律法规，对金融数据跨境流动的规制产生了积极作用和深远影响。与此同时，在规制思路、金融数据的范围、金融数据控制者、金融数据跨境传输的目的和条件等方面还存在一些尚待完善的问题，下文将展开分析。

（一）中国对金融数据跨境流动的规制思路和立法发展

以 2017 年《网络安全法》的实施为分界点，中国对金融数据跨境流动采取的规制思路和立法情况呈现出以下发展脉络。

《网络安全法》实施之前，源于金融业的分业监管模式，中国有关金融数据跨境流动的法律规定散见于与银行业、保险业、证券业相关的法律法规中，规定较为零散、笼统、覆盖面较窄。规制措施包括两大方面，一是要求银行、保险公司等的核心系统在境内独立运营，并将其纳入对申请设立外资金融机构的准入要求，规定在《外资银行管理条例》《外资保险公司管理条例》等法律法规中。二是要求金融机构在中国境内收集的个人金融信息在境内存储，例如《关于银行业金融机构做好个人金融信息保护工作的通知》第 6 条、《中国人民银行金融消费者权益保护实施办法》（2016）第 33 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。这一境内存储要求与这一时期金融监管面临的信息泄露挑战紧密相关。这一时期，金融机构内部人员违规操作、违法出售客户信息等造成客户财产严重损失的案件屡见不鲜，对金融机构的运营和市场信心造成了不良影响。因而金融规制的重点是要求金融机构对客户的金融信息予以严格保密、依法保护，不得对外提供。[③]

2017 年，《网络安全法》的实施使有关数据安全的规制提升到维护国家网络空间主权和国家

---

① 墨西哥 2014 年修订的《信贷机构法》（Credit Institutions Law）第 117 条和第 142 条；墨西哥 2010 年《私人信息联邦保护法》（The Federal Law on the Protection of Personal Data Held by Private Parties）第 39 条。

② 参见加拿大 2019 年修订的《个人信息保护和电子文件法》（Personal Information Protection and Electronic Documents Act，PIPEDA）Schedule I 4. 3，https：//laws – lois. justice. gc. ca/eng/acts/P – 8. 6/，最后访问时间：2020 年 4 月 3 日。

③ 例如，2012 年 3 月 15 日，中央电视台曝光了有关商业银行员工向不法分子出售客户个人金融信息，并导致大量客户总计 3000 余万元存款被盗的事件。人民银行随即下发《中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知》（银发〔2012〕80 号），要求各银行业机构严格遵守有关客户金融信息保密、不得对外提供的规定。

安全的高度，并确立了原则上禁止金融数据跨境流动的上位法依据。《网络安全法》第 31 条规定金融业属于“关键信息基础设施”，第 37 条则要求关键信息基础设施的运营者在境内收集和产生的个人信息和重要数据在境内存储，因业务需要确需向境外提供的，应当进行安全评估。《网络安全法》创设了 3 个重要概念，即数据范围上的“个人信息”、“重要数据”和数据控制者意义上的“关键信息基础设施运营者”，以及 1 项制度——数据出境的安全评估制度，积极推动了金融数据跨境流动的法律规制发展，同时也引发了国内外金融企业的广泛关注和诉求建议。例如，中国美国商会和中国欧盟商会连续两年在《美国企业在中国白皮书》和《欧盟企业在中国建议书》中指出中国金融数据本地化政策存在的一系列问题，[①] 概括而言主要包括以下三方面：

首先，在金融数据范围方面，《网络安全法》的配套法规《信息安全技术 数据出境安全评估指南（2017 年征求意见稿）》规定，金融业的“重要数据”包括但不限于自然人、法人和其他组织金融信息等，使得《网络安全法》中个人信息和重要数据的分类失去了原有意义。其次，在数据控制者方面，将金融业全部划归为关键信息基础设施，引起了金融业界的普遍担忧。原因是，不同于交易场所、清算支付系统等确属金融基础设施，单家金融机构的数据中心、业务系统等数据泄露会损害消费者合法权益，但可能不会达到危害国家安全、国计民生的程度，尤其是对一些中小金融机构来说更是如此。若全部划归为关键信息基础设施将大幅提升外资金融机构的合规负担，影响其深度参与中国金融市场。再次，对于数据出境的安全评估机制，配套法规《个人信息和重要数据出境安全评估办法（2017 年征求意见稿）》规定，金融机构应先进行自评估，再报请行业主管或监管部门进行安全评估审查。较为繁琐的安全评估审查可能导致金融数据实际上很难跨境传输，同时带来额外的行政负担。

《网络安全法》实施之后的近三年，多部法律法规的密集出台使得中国对金融数据跨境流动的规制正在逐步走向更加专业化和完善化。首先，相较上述 2017 年发布的两份征求意见稿，2019 年发布的《个人信息出境安全评估办法（征求意见稿）》和《信息安全技术 个人信息安全规范》（2020 年）体现出以下两方面新发展：一是在数据分类上似乎摒弃了《网络安全法》中对个人信息和重要数据的分类，单独就个人信息相关的安全评估和技术规范进行规定。而原来关于重要数据的内容，可能内嵌于未来关于关键信息基础设施的规定中。二是关于数据出境安全评估，2019 年《个人信息出境安全评估办法（征求意见稿）》进一步规定，个人信息出境安全评估须向所在地省级网信部门申报。

其次，金融业有关数据保护的规制思路从维护安全的单一视角逐渐转向了兼顾金融机构的业务需求。如 2019 年《中国人民银行金融消费者权益保护实施办法（征求意见稿）》，首次明确规定了允许在金融机构集团内部跨境传输金融数据的情形和需符合的条件。另外，2020 年 2 月发布的《个人金融信息保护技术规范》，首次对金融数据的分级分类、金融业机构作出了明确规定，并且要求向包含集团关联机构在内的主体跨境传输金融数据，都应开展数据出境安全评估，规制更为严格。该《规范》属于推荐性行业标准，但在实践中具有较强的指导意义。此外，人民银行于 2019 年 10 月向各银行下发《个人金融信息（数据）保护试行办法（初稿）》以征求意见，也释放出有关金融数据规制法律正在努力制定中的积极信号。

① 中国美国商会：《美国企业在中国白皮书》，https：//www. amchamchina. org/policy - advocacy/white - paper/，最后访问时间：2020 年 4 月 1 日；中国欧盟商会：《欧盟企业在中国建议书》，https：//www. europeanchamber. com. cn/en/home，最后访问时间：2020 年 4 月 1 日。

（二）中国当前规制中存在的主要问题

第一，对金融数据跨境流动的规制思路有待转变和协调。全面禁止金融数据的跨境流动在实践中导致了规制利益和成本之间的失衡。原因是，禁止金融数据跨境流动本是为保护金融消费者权益、防范金融风险、维护国家安全，但规制之手仅从安全角度切入的不良影响即是忽视了金融市场的需求、降低了金融市场活力。一方面将导致跨国金融机构无法正常开展业务，可能消减外资金融机构深度参与中国金融市场的信心和意愿；另一方面，可能迫使金融机构付出高昂合规成本的同时暗地里进行数据转移，而这些数据的暗地转移将会在监管范围之外产生更大的隐形风险，从而与规制目标背道而驰。正因如此，将“挖掘金融数据价值、提升金融服务质效”纳入对金融数据跨境流动规制目标，对抓住数字经济发展机遇来说是必要且重要的。因此，需要转变全面禁止金融数据跨境流动的规制思路。此外，相关的法律法规之间还存在规制思路上的冲突，规制的尺度宽严不一，有待进一步协调。

第二，未将金融数据的分级分类与跨境传输规制相关联。尽管《信息安全技术 个人信息安全规范》（2020 年）等技术标准中已体现出对敏感数据进行分级规制的成型思路，《个人金融信息保护技术规范》更是首次对金融数据规定了用户鉴别信息、可识别个人金融信息、以及机构内部信息资产的分级，但这种分级分类没有与跨境传输相关联，从而导致了跨境传输环节金融数据范围上的混乱不清。例如，《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》要求在境内收集的身份信息、财产信息等六类个人金融信息都不得向境外提供；《中国人民银行金融消费者权益保护实施办法（2019 年征求意见稿）》和《个人金融信息保护技术规范》都规定“因业务需要”可向境外提供金融数据，但未规定可以提供的金融数据范围；而《银行业金融机构反洗钱和反恐怖融资管理办法》严格禁止跨境转移客户身份数据和交易数据，《征信业管理条例》禁止跨境传输征信信息。这些规定之间存在重合和冲突之处，使得金融机构在跨境传输金融数据时没有明确的操作指导。

第三，金融数据控制者的范围和跨境传输数据的法定义务有待细化和统一。首先，目前《网络安全法》《信息安全技术 个人信息安全规范》《个人金融信息保护技术规范》，以及银行业、保险业、证券业各自的法律法规中对金融数据控制者可能包括的机构范围有着不同的理解。这种交叉规制可能产生的效果是，对于同一家金融企业而言，就同一事项需满足不同维度不同监管项下的合规义务，大幅提升其合规负担；相反，也可能导致本应纳入规制范围内的机构类型，仍游离在规制视野之外。因此，有必要对金融数据控制者的范围进行细化和统一规定。其次，尽管各项法律法规中均对金融机构收集、处理、删除等全部数据周期的法定义务进行了规定，但对其跨境传输数据时应承担的法定义务还着墨不多，这在实际上也进一步加剧了跨境传输金融数据可能引发的风险。

第四，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。首先，自从《网络安全法》实施以来，相关的法律法规一直没有规定什么是“因业务需要”确需数据出境的情形。必须进一步明确到底包括哪些情形，才能为业界提供切实有效的合规指导，有的放矢地防范跨境传输数据时可能引发的风险。其次，《个人金融信息保护技术规范》规定，向包含集团关联机构在内的主体跨境传输金融数据，都应开展数据出境安全评估。而根据《个人信息出境安全评估办法（2019 年征求意见稿）》，所有金融数据出境前都应向所在地省级网信部门申报，至少 15 个工作日才可完成安全评估。这一规定在理论层面是逻辑严谨的，但在一定程度上偏离了金融机构和金融消费者对金融数据的实际需求。因为，就在键盘敲下一个字的瞬间，或许某外国银行分行基

于并表监管要求已将一批数据传回境内母行，无法等待至少 15 天的审批期限。“因业务需要确需提供数据”的含义不明，加之安全评估流程的繁琐和复杂，将导致金融数据“事实上”难以出境。

六　中国应对金融数据跨境流动规制问题的相关建议

面对当前全球疫情蔓延、新技术迭代、金融业态革新、网络风险高发的复杂形势，必须把握发展与安全、创新与风险防范的动态平衡，通过完善中国立法来为金融数据跨境流动夯实法治根基。在前文分析的基础上，本文提出以下四方面完善中国金融数据跨境流动规制的建议。

（一）调整规制思路：坚持核心系统本地化并适当放宽金融数据跨境流动限制

在现阶段的监管水平和监管能力条件下，中国金融监管部门对金融数据的监控主要是通过对金融机构电子系统的现场检查和非现场监管中对金融机构报送的数据进行审查来实现。因此，应坚持对于金融核心系统本地化的要求，守住不发生系统性金融风险的底线。

在此基础上，对于金融数据本身的跨境流动，建议紧密贴合金融数据的实际应用场景，对金融数据出境的跨境流动限制适当予以放宽。数据是数字经济时代驱动经济增长的核心生产要素，金融数据的跨境流动对金融全球化和数字贸易发展都至关重要，因此全面禁止金融数据出境的规制路径不具备操作可行性，更不利于当前中国发展数字金融的战略部署。更为务实的规制路径是深入挖掘金融数据、金融数据控制者、跨境传输的目的和条件等不同方面的规制要点，在掌握数据“红线”的基础上赋予金融机构充足的运营空间，以进一步激发金融市场活力和金融创新能力。

在规制思路的调整上，首先应坚持四位一体的规制目标，即维护国家安全；维持金融稳定和安全；保护金融消费者合法权益；挖掘金融数据价值、提升金融服务质效，并将其纳入关于金融数据保护的专门立法当中。其次，现阶段应当坚持在中国境内收集的金融数据应当在中国境内存储、处理的基本原则。原因包括以下两方面：一是《网络安全法》确立了原则上禁止金融数据跨境流动的上位法依据，金融业需在上位法授权范围内制定法律法规，不宜突破上位法规定。二是金融业相继颁布的法律法规中均采纳这一基本原则，由于金融数据已成为金融机构的一项重要资产，对金融数据跨境流动的规制调整也是牵一发而动全身的，因此对基本原则的调整需建立在审慎研究、时机成熟的基础之上。实际上，从前文对国际规制和中国现状的分析来看，真正引发问题的并不是要求金融数据在本地存储的基本原则，而是在于规定了对这一原则的例外情形，即“因业务需要确需数据出境”，但却没有对这一例外情形进行清晰和详细的规定，在实践中导致了例外情形的失效，进而引发了金融业界的广泛关注。

正因如此，应当秉持务实精神和问题导向，对“因业务需要确需数据出境”的情形和对应的条件进行详细而清晰地规定，这也是规制思路调整的重点所在。在此基础之上，需对各项不同法律法规之中有关金融数据跨境流动规制的条款进行统一和协调。诚然，不同法律法规实施的背景和侧重的规制目标不尽相同，但关于可允许金融数据跨境流动的情形和对应的条件应当是统一的，否则将在实践中引发执行上的疑惑和混乱。

（二）明确金融数据范围：将分级分类与跨境传输规制相衔接

首先，建议统一现有法律法规中对金融数据的分级和分类方式，包括分散地规定在专门法规

之中特殊类别的金融数据。对于分类而言，目前国内立法较为统一，而统一分级的方式理论上有两种：一种是按照一般数据、敏感数据、重要数据来分级。但从前文提及的最新立法思路来看，重要数据的概念未来是否沿用尚不确定，使得这一分级方式能够有效实现跨境传输分级规制的可行性降低。另一种是按照《个人金融信息保护技术规范》中对金融数据进行的 C3（用户鉴别信息）、C2（可识别信息主体身份与金融状况的个人金融信息）、C1（机构内部的信息资产）的分级方式，这一分级方式更加贴近金融数据应用实际，更为科学合理。

其次，在统一金融数据分级分类的基础上，按照金融数据的级别和类别施加不同层级的跨境传输要求，制定针对性的跨境传输条件。对金融数据分级和分类的目的就是为了最终实现分级的跨境传输规制。从理论上来说，C1 级金融数据包括账户开立时间、开户机构等在金融机构内部使用的数据，原则上可在经数据主体同意的情形下跨境提供；C2 级均是可以识别到特定个人的金融信息，跨境传输需符合特定条件并采取匿名化处理等方式；而 C3 级金融数据安全和保密级别最高，应禁止跨境传输。这是一种简单且理想化的结论，而现实情形是非常复杂的。由前文所述，很多国家对客户身份信息和交易信息是允许向集团总部等主体跨境提供的，这是因为这两类数据通常是金融机构开展跨境业务所必需的。而对于信贷信息、健康数据、支付清算数据、会计数据等敏感数据原则上禁止跨境流动，仅有在基于重大公共利益等原因时才可进行跨境传输。例如，对于健康数据，如果是为救助投保人的生命、健康等原因，可以在其授权同意、数据接收方有充分保护水平，签订数据跨境传输协议等条件下向境外医疗机构跨境传输。

再次，对金融数据的分级和分类需紧密结合数据出境的具体场景来判断跨境传输金融数据的必要性、合理性和正当性。例如，对于一笔汇款业务，需要跨境传输金融数据可能仅包括客户的姓名、账号、金额等，倘若还跨境传输了客户的指纹、信用情况等，则是不必要、不合理和不正当的。此外，金融数据的某一类里还可再分类，某一级里也可再分级，因此无法一刀切划定跨境传输的分级规则，还需在实证调研的基础上进行详细研究，囿于篇幅所限本文暂不一一展开。

（三）统一金融数据控制者：细化金融机构范围并明确法定义务

首先，有必要进一步细化和统一纳入规制范畴的金融数据控制者包含的机构类型，以明确相关法律法规适用的对象。从规制的维度来看，《网络安全法》和《信息安全技术 个人信息安全规范》与金融规制的维度不同，理论上金融业所有涉及网络运营或收集、处理个人信息的都应遵守其规定，因此不存在可统一之处。但金融监管部门可依据上位法律的授权，对金融行业纳入规制范畴的机构类型进行规定。

从金融规制的主体来看，笔者认为可按照《个人金融信息保护技术规范》中对金融业机构的界定来统一，即将传统的金融机构和持牌的非金融机构纳入金融数据跨境流动的规制范畴。原因有两个方面：一方面，从规制的全面性和未来趋势考虑，理论上应当将为持牌的金融机构提供身份验证、风险控制、技术支持等基础服务的公司纳入规制范畴。因为在大数据深度运用于金融业的背景下，持牌金融机构与这些基础服务商将继续加强合作以促进其金融产品的精准投放、市场营销等，以提高市场竞争力。另一方面，从金融监管的职能和权限来看，应强调数据控制者的金融属性，即金融数据控制者是提供金融产品或服务的机构，这些机构包括持牌的金融机构和非金融机构，是在金融监管范围之内的。而对于基础服务提供商，应遵循《网络安全法》和有关个人信息保护的关于数据出境的规定，当处理、加工金融数据时，可参照执行金融数据跨境流动

的规定。

其次，建议进一步明确跨境传输环节金融数据控制者的数据安全保护义务和数据质量保障义务。数据安全保护义务须贯穿于数据跨境流动的前端、中端和后端，并且以防范风险为导向，针对数据出境的具体风险进行适当放宽或加严。同时，数据控制者收集数据须与使用目的相关，保障金融数据的准确和完整，并及时予以更新。

（四）区分金融数据跨境传输目的：灵活开展数据出境安全评估

首先，明确区分金融数据出境的不同目的和情形，分别规定需满足的跨境传输条件。第一，进一步明确各相关法律法规中“因业务需要”确需数据出境的情形，至少包括基于日常商业经营目的向金融集团的关联机构（含总公司、母公司或者分公司、子公司等）传输数据。此种情形下跨境传输金融数据需满足的条件包括：（1）跨境传输金融数据具备法律基础，是为履行与消费者之间的合同所必要的。例如，外国银行分行向其总部跨境传输客户申请贷款所提交的身份信息、信贷信息等，前提是客户欲和该外国银行分行签订贷款合同；（2）必须经客户明示同意；（3）跨境传输金融数据是为履行法律义务所必须，可从合法性、合理性和必要性进行审查。例如基于并表管理、内部审计和风险管理等目的跨境传输的是汇总和批量式数据，因此不应当跨境传输具有个人可识别性的金融信息；（4）金融机构分支机构和集团总部之间须签署包含标准数据保护条款的协议。该标准协议通常必须符合数据保护法律的规定，并且经监管部门批准。第二，补充规定确需数据出境的两种情形：一是对基于外部审计目的向第三方跨境传输数据，可要求数据接收方承担数据保密和数据保护义务，并规范数据跨境传输的操作路径；二是对基于境外监管要求向金融监管部门跨境传输数据，应经金融监管部门事前审批，并根据双边监管合作和信息交换协议情况，视情决定是否允许金融数据出境。

其次，建议对目前金融数据出境的安全评估机制进行灵活度上的调整。数据具有天然的流通属性，而金融业更是依靠数据驱动的行业，将金融数据出境的全部审查均集中于安全评估环节，一方面与金融实践相脱节，另一方面将在安全评估环节集中大量的行政负担，可能导致的不良影响就是审查员为审慎起见从严把握审查标准，以避免金融数据出境可能引发的风险。但是，风险本身无法单纯依靠事前审查得以规避，还需结合事中事后监管。因此，建议考虑是否可将金融数据跨境传输环节的审查内容、责任和风险分散到日常金融监管、有关金融数据跨境传输的制度性条件上来。为此，本文提出三项初步建议：一是建议对于金融机构在开展业务过程中所必需的向集团关联机构跨境传输金融数据等情形，可以结合金融业非现场监管在每年报送机构数据时进行报告，无需进行事前的个案审查。对于需大批量传输金融数据或者传输的金融数据范围超出使用目的而使风险等级升高时，金融机构应提前通报监管部门以进行事前的数据出境安全评估审查。二是强化关于数据保护的机制性条件，例如建立数据保护的认证机制，对于向满足充分保护要求的数据接收方传输数据，金融机构可定期向监管部门进行报告；对于向不满足充分保护要求的数据接收方传输数据，可审查金融机构是否采用了有约束力的规则、跨境传输双方是否有标准数据保护条款的协议等要素。三是加强网信部门与金融监管部门的数据共享和协作。按照《个人信息出境安全评估办法（2019 征求意见稿）》，地方网信部门将作为金融数据出境安全评估的监管部门，而金融监管部门在日常监管中也持续掌握被监管金融机构的营业数据等信息。尽管未来具体的分工尚不清晰，但可以预见的是，负责金融数据出境安全评估审查的部门应与金融监管部门

之间加强数据共享和协作，一方面有利于提升数据出境审查的质效，另一方面也有利于金融监管中的风险防范。

结　语

2020 年，全球疫情的蔓延将数字金融提上了发展的快车道。金融线上服务的方便和迅捷在公民疾病保险、中小企业借贷等方面发挥了重要作用，金融数据的流动促进了金融服务实体经济，也激发了金融业发展的广阔空间。在全球数据安全立法的浪潮下，制定专门的金融数据保护法律是大势所趋。危和机并存之时，坚实的法治基础将为中国抓住数字金融发展机遇打好根基。金融数据跨境流动规制应坚持四位一体的规制目标，既要维护国家安全、维持金融稳定和安全、保护金融消费者合法权益，也要挖掘金融数据价值、提升金融服务的质效。为此，建议坚持核心系统本地化并适当放宽金融数据跨境流动限制，将分级分类与跨境传输规制相衔接，细化金融机构范围并明确法定义务，同时区分金融数据跨境传输目的，灵活开展数据出境安全评估。放眼全球数字经济蓬勃发展和中国金融科技迅速迭代的未来，以良好的法治保障金融数据的治理和保护，中国金融业将在数据流动的开放中进一步提振外资金融机构深度参与中国金融市场的信心，也将在数据审慎监管中守住不发生系统性风险的底线，行稳致远。

Core Issues in the Regulation of Cross-border Flow of Financial Data and China's Response

Ma Lan

Abstract: The regulation of cross-border flow of financial data is essentially a legal restriction imposed by the State public power to manage financial markets and economic and social life. This regulation has its national and socio-economic roots and should be maintained at reasonable limits. The scope of financial data, the controller of financial data, and the purposes and conditions of cross-border flow of financial data are the core entry points for the regulation of cross-border flow of financial data. Throughout the global legislative practice, financial data exhibits hierarchical classification characteristics, the scope of financial data controllers has expanded, and different purposes of cross-border flow of financial data correspond to different cross-border transmission conditions. China has made continuous efforts in financial data protection legislation, but there are still some problems that need to be improved. To cope with current problems and focus on future development, China should adjust its regulatory thinking and improve its regulations concerning the scope of financial data, financial data controllers, and the purposes and conditions of the cross-border transfer of financial data.

Keywords: Financial Data, Cross-border Data Flow, Financial Data Controller, Purposes of Cross-border Transfer of Financial Data

（责任编辑：李西霞）