Dispute Settlement 争议解决, 2022, 8(1), 142-150
Published Online March 2022 in Hans. http://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2022.81021

Hans汉斯

金融数据跨境流动法律规制问题研究

张泊远

华东政法大学，上海

收稿日期：2022年2月25日；录用日期：2022年3月12日；发布日期：2022年3月22日

摘　要

在当今社会经济全球化趋势下，金融机构正常业务的开展离不开金融数据的跨境传输流动，其所作出的每一项管理决策，如资金流向、产品定价、市场营销等都依托于科学可靠的统计数据而作出，可以说信息数据已然成为金融行业的一项基本生产工具。然而金融数据的规模庞大，类别包罗万象，其中不乏一些兼具复杂性与敏感性的数据，在跨境流动的过程中极易对个人隐私甚至国家安全造成威胁。我国在金融数据跨境流动的监管规则上将一般规定与特别规定相结合，蕴含着利益平衡的辩证理念，但与此同时也存在着一些缺陷，例如对某些重要的金融数据概念界定不明确，不同监管规则之间衔接不流畅等问题，在金融数据越发重要的今天，我国应当构建体系协调，咬合紧密的金融数据跨境监管规则，在利益平衡理念的基础上建立金融数据的分级分类动态监管规则，并积极投身于国际化数据流动规则的制定，以便更好地维护国家信信息与公民隐私安全。

关键词

金融数据，跨境流动，特殊规制

Study on the Legal Regulation of Cross-Border Flow of Financial Data

Boyuan Zhang

East China University of Political Science and Law, Shanghai

Received: Feb. 25th, 2022; accepted: Mar. 12th, 2022; published: Mar. 22nd, 2022

Abstract

Under the trend of globalization, financial institutions cannot carry out their normal business without the cross-border transmission and flow of financial data, and every management decision they make, such as capital flow, product pricing, marketing, etc., relies on scientific and reliable statis-

文章引用: 张泊远. 金融数据跨境流动法律规制问题研究[J]. 争议解决, 2022, 8(1): 142-150.
DOI: 10.12677/ds.2022.81021

tical data, so it can be said that information data has become a basic production tool for the financial industry. However, the scale of financial data is huge and the categories are all-encompassing, including some data with complexity and sensitivity, which can easily pose threats to personal privacy and even national security in the process of cross-border flow. China's regulatory rules on cross-border flow of financial data combine general and special provisions, which embody the dialectical concept of balance of interests, but at the same time there are also some shortcomings, such as the unclear definition of certain important financial data concepts, the lack of fluency between different regulatory rules, etc. In today's increasingly important financial data, China should build a coordinated system and tightly bite financial data cross-border regulatory rules, in the concept of balance of interests. In today's financial data is more and more important, China should build a coordinated system and tightly bite financial data cross-border regulatory rules, establish a hierarchical classification of financial data based on the concept of balance of interests and dynamic regulatory rules, and actively participate in the development of international data flow rules, so as to better maintain the security of national information and citizens' privacy.

Keywords

Financial Data, Cross-Border Flows, Special Regulations

1. 引言

数据的概念十分宏观，细分之下包含诸多领域的诸多分支，且不同行业与领域的数据规制具有较高专业性，因此不论是国内还是国外都对数据跨境流动采取了分业监管的模式。由于金融数据的识别、分类、处理、评估具有较强的专业性，根据我国 2020 年《数据安全法(草案)》的规定，应当由金融业主管部门履行对本行业数据安全的监管职责并采取特殊规制措施来管理金融数据的跨境流动。相比于大部分行业，金融行业对于数据跨境流动的数量需求更大、速度要求更高。金融业是全球化特点极为突出的行业，金融机构的全球布局和集团化经营都决定了金融数据在几乎所有经营场景下都可能涉及跨境流动问题。对金融机构而言，跨境支付清算、境外尽职调查、监管信息报送、机构风险管理、集团数字化经营等场景都涉及海量数据的跨境问题，各国金融主管部门和监管机构同样在执法调查、反洗钱协作等领域存在数据传输的需求。另外，金融数据的跨境流动需要平衡的利益较多。一是金融数据往往包含较多敏感性和隐私性较强的客户信息，二是网络攻击、数据泄露等事件可能导致国家的金融安全遭受严重破坏。三是金融数据的跨境流动可以为一国带来巨大的经济效益并促进一国数字经济的发展。四是金融机构的经营单元呈现出全球配置的趋势，资金流、信息流具有全球流动的需要，合理规制金融数据跨境流动，对于国外金融机构参与中国金融市场建设，扩大金融开放，具有重要意义。

2. 金融数据跨境流动规制的必要性

2.1. 国家安全层面

对金融数据跨境流动行为作出规制的出发点在于维护一国的网络空间主权与国家安全。所谓网络空间主权是指一国所享有的对其所辖领土范围内的网络设施、网络使用主体及其行为进行规制的“普遍权力”[1]。由于网络数据传播存在着隐蔽性迅捷性等特点，且网络空间不属于国际政治法律语境下“全球

公域”的概念，因此当金融数据瞬间从一国网络空间进入另一国网络空间时，数据传出国便丧失了对这部分数据的控制权和管辖权，当一国公民的私人金融信息暴露于境外领域时，因信息处理不当、数据泄露、黑客攻击等引发的一系列风险将会直接将国家安全置于一个相当脆弱的地位，极易引发全国性的政治与经济风险，因此国家有必要对金融数据的跨境流动作出一定规制，在不损影响经济发展和信息互通的同时，切实维护好网络空间主权和国家安全。

2.2. 经济社会层面

对金融数据跨境流动作出规制的原因在于金融风险的传导性和金融市场国际化的要求。第一，金融风险的传导性是指单家金融机构数据泄露的风险会迅速传播至全金融行业乃至某一国家或地区的经济社会，在当今数字化时代下，各个金融机构的客户信息、产品体系、运营方式等资料均以数字方式存储于云端，因此重要数据资产的泄露和丢失往往会对机构产生致命的打击。对于一些在全球各个国家开展业务的大型金融机构来说，其经营过程中所产生的金融数据同样被分散地存储在各个国家的服务器中，其一旦面临倒闭风险，政府金融监管部门将不得不向各个数据服务器所在国家申请司法协助，这无疑是巨大的执法成本，同时意味着损失计算与影响评估时机的延误，并有可能衍生出更广范围的金融风险，因此一国立法对金融机构数据国内存储作出要求还是十分有必要的。第二，金融行业在我国具备着越发重要的战略地位，为达成与国际社会金融市场的接轨，我国金融市场的开放程度越发深入，随着 2018 年国内原油期货的上市，铁矿石、PTA 国际化战略的实施，来自其他国家的交易者得以直接在我国境内的期货市场监控中心开户并参与期货交易。在人民币支付结算领域，人民币跨境支付系统(二期)已上线运行，截止 2020 年底，其业务范围已覆盖到全球 148 个国家和地区。在国家政策层面，国务院金融稳定发展委员会于 2019 年 7 月发布了金融开放新“十一条”，颁布了诸如允许外资机构对所有种类债券评级、允许境外金融机构投资设立、放宽外资保险公司准入条件等十一条新规。与此同时，对外资金融机构的限制放宽也有可能导致对我国本土金融市场产生新危险，例如境外金融公司通过网络爬虫等非法手段收集金融数据，实现其非法风控和债务催收的目的。由此可见，对我国金融市场国际化提供政策支持不能以牺牲网络安全和公民隐私为代价，更需要在宏观政策的基础上细化金融数据跨境流动的实施细则，提供明确的指引。

3. 金融数据跨境流动规制中的数据范围界定

金融机构的客户信息可划分为基础身份信息与敏感保密信息两类，前者主要包括客户姓名、性别、身份证号码等，后者主要包括信用卡信息、交易详情、支付信息等。在金融数据跨境流动的过程中，前者的泄露往往使消费者遭受骚扰电话的困扰，财产损失尚属少数，但后者的泄露几乎必然会引起信用卡盗刷、恶意挂失等风险，从而使机构客户财产受损的可能性大大增加。因此，法律有必要对这两类不同的金融数据实行分类和分级监管，建立起更为具体和具有实操性的规制细则。

3.1. 金融数据的两类分级标准

如上所述，国内外立法中金融数据的分类主要采取了两种方式，第一种方式将金融数据划分为一般数据、敏感数据、关键或重要数据，这种方式的分类依据是数据的敏感程度与安全防护级别，并在此基础上对数据适用不同条件的跨境流动规制[2]。采取这种分类方式的国家包括印度与瑞士等，在印度 2018 年颁布的《个人数据保护法(草案)》中，一般个人数据在符合一定条件后，仅需数据主体同意即可进行跨境流动；而敏感数据的跨境流动需要严格满足两个条件，第一是为特定人员或机构提供健康服务或紧急事件服务所必须，第二是接收数据的国家必须对数据提供充分的保护；而对于关键或重要数据，则只被允许在印度领域内进行传输。

根据各国通行的立法规定可知，敏感数据是指在遭受泄露和修改后会对机构客户产生严重不良影响的信息，一般来说包括以下几项：交易密码、财务状况、健康指标、官方标识符、性爱情况、性取向、指纹等生物信息、基因信息、宗教信仰与政治倾向、受行政和刑事处罚情况等。目前世界上大部分国家和地区均对敏感数据的跨境流动作出了严格的限制，即使允许传输也应当采取去标识化、匿名化等安全措施。根据瑞士的法律规定，敏感数据的跨境流动需要满足两个要件，首先是数据主体的明示同意，第二是基于法令的明确规定。同时这种对金融数据流动实行分级监管的思路也被我国所采纳吸收，例如在2017年所发布的《信息安全技术数据出境安全评估指南(征求意见稿)》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，已经出现了对金融数据分级监管的内容，但是仍然缺少对敏感数据跨境流动时其本身所需满足要件的规定。

而对于关键数据的含义，印度法律并未作出具体规定，而我国《网络安全法》中所提到的“重要数据”、“关键信息基础设施”可以视为与之含义相近似的概念，根据《网络安全法》的规定，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”，关键信息基础设施所指范围甚广，包括金融、交通、能源等多个行业在内。但如此规定仍属粗犷模糊，实际上并未做到对金融数据进行分类分级规制，因此可操作性较弱[3]。

另一种分类方式则是以未经许可的查看对数据主体信息安全和财产安全可能造成的损害程度为标准，例如我国的《个人金融信息保护技术规范》中，将金融数据分为C3、C2、C1三个级别，C3是指用户鉴别信息，主要包括银行卡磁道数据(或芯片等效信息)、卡片验证码、卡片有效期、银行卡密码、网络支付密码等；账户(支付账号、证券账号、保险账户)登录密码、交易密码、查询密码等个人生物识别信息，这些信息在未经授权的情况下遭到查看或删改会对数据主体的财产安全和信息安全造成严重的危害；C2主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息以及用于金融产品与服务的关键信息，主要包括支付账号、证件类别识别码与证件信息、手机号码、账户登录用户名、用户鉴别辅助信息(动态口令、短信验证码、密码提示问题答案等)、个人财产信息、交易信息、借贷信息、个人金融信息主体照片、音视频等影像信息，家庭住址等能够识别特定主体的信息，此种信息遭到未经授权的查看或删改时会对数据主体造成一定程度的危害，其危害程度低于C3；C1则是指为机构内部使用的个人金融信息资产，主要包括账户开立时间、开户机构、基于账户信息产生的支付标记信息以及C2和C3中未包含的其他个人金融信息，此种信息遭到未经授权的查看或删改时会对数据主体造成一定影响。可以看出从C3到C1其危害程度逐级减弱，且此种分类方式与金融数据的使用场景息息相关，具有较强的实践操作性和创新性。

3.2. 特定类型金融数据的特殊要求

除了上述两种分类方式以外，还有一些特殊类型的金融数据在一些国家受到更为严格的管控，即只允许在境内存储及传输，这类数据主要包括健康数据、支付清算数据、会计数据等。

“健康数据”实际上属于敏感数据的一种，一国境内的保险公司在承保人身险时往往需要尽可能多地了解与被保险人身体健康有关的各项数据，包括但不限于发病率、残疾或医疗保健需求、分配给医疗保健的资源、死亡原因等信息。每一个单独的被保险人数据的保护价值虽然是有限的，但通过移动大数据方法，对保险公司业务经营过程中所采集的所有单个客户数据进行收集汇总后，所获得的数据甚至能反映出一国国民的年龄与疾病分布情况、医疗水平发展状况、人口死亡率与死亡原因情况等各项国民健康基本面，这些数据的价值也就不局限于保护个人隐私，更是上升到了关涉国家安全的高度，因此欧盟、澳大利亚等多个国家对金融企业收集的健康数据采取了严格的规范措施。

“支付清算数据”则是指在银行等金融机构在提供清算服务的过程中，为保障支付活动的顺利进行，

付款人和收款人之间通过各自的服务提供商所交换的姓名、银行账号、交易合同等数据。由于这些支付清算数据直接影响着数据主体的银行资金安全，因此许多国家出于维护支付系统和金融体系稳定性的需要，对此类金融数据的跨境流动采取了严格的限制，代表国家如印度，禁止此类支付清算数据出境，美国更是为此类数据专门制定了《支付卡行业数据安全标准》，要求信用卡公司处理、存储、转移相关数据的活动在此标准的规制下进行。而中国于 2016 年颁布了《银行卡清算机构管理办法》，其中第 7 条第 2 款规定：“银行卡清算机构和境外机构为处理银行卡跨境交易且经当事人授权，向境外发卡机构或收单机构传输境内收集的相关个人金融信息的，应当通过业务规则及协议等有效措施，要求境外发卡机构或收单机构为所获得的个人金融信息保密。”

“会计数据”则是指在会计事项处理过程中所产生的以“单、表、帐、证”等形式呈现出的各种未经加工的数字、字母与特殊符号的集合，诸如英国、丹麦、芬兰的一些国家对此类数据出境作出了严格限制，要求其必须在境内服务器存储。

4. 金融数据跨境流动的规制模式

4.1. 美国模式：内外二元化规制

长期以来，美国政府和金融业界秉持着过于严苛的法律规制将会“不可避免地阻碍商业活动”这一观念，并且基于自身信息和金融大国的地位，在金融数据跨境流动的规制问题上，采取着较为宽松的做法，即加强国际间合作促进金融数据跨国自由流动，将自身数据优势转化为经济收益[4]。

与对外促进数据流动的做法不同，美国政府对国内的诸多领域的数据流动和存储作出了较为严格的限制，在金融业内，美国于 1978 年所颁布的《金融消费者隐私权法》中对金融机构获取用户金融记录的途径、方法与程序作出了具体规定，并且禁止金融机构在未获得客户授权且未尽到通知义务的情况下擅自将用户的金融信息提供至联邦政府。而在 1999 年颁布的《金融服务现代化法》的第五章公民隐私权保护的内容中则具体体现了金融信息保护的五项基本原则，即通知(Notice)、选择(Choice)、市场公开(Marketing Disclosure)、安全(Security)、执行(Enforcement)，为配合该法案的施行，美联邦贸易委员会又制定了两部配套实施细则，分别是以保护隐私为目的的隐私规则和保障信息安全为目的的安全保障规则。在州层面上，纽约州于 2017 年 3 月颁布了国内首部针对金融机构制定的网络安全法规《23 NYCRR 500》，这部法规要求银行、保险公司等受政府监管的金融机构为其客户的数据安全制定网络安全计划并严格施行，定期评估自身可能遭受信息危害的可能性大小并根据评估结果制定相应的安全策略。由此可见，美国在国内数据流动层面十分注重保护用户隐私，对数据流动多施加严格限制。

但美国在国际条约层面却呈现出与国内立法上相反的二元化机制，主张数据自由跨境流动，其出发点多是基于数据流动所带来的巨大经济效益，在双边和多边条约中加入数据自由流动的内容成了美国为达成这一目的所使用的主要手段。根据 2012 年的《美韩自由贸易协定》的第十五章第 15.8 条规定，缔约各方应当尽量采取行动避免对金融数据跨境流动产生不必要的障碍，在第十三章的附件 13-B 中还特别规定了“每一缔约方应允许另一方的金融机构以电子或其他形式将信息传入和传出其领土，以便该机构在日常业务过程中需要此类数据时可以进行数据处理”，这一突破性的规定使得金融数据在美韩两方之间的流动几乎不会面临任何阻碍。在 2018 年达成的《美墨加协定》中延续了这一处理思路，并在《北美自由贸易协定》的基础上对金融服务规则作出了大量修改细化，其第 17.7 条规定：“当金融机构或跨境金融服务提供者在授权许可的范围内为商业目的而活动时，任何缔约方不得阻止其以电子或其他方式进行包括个人数据在内的跨境数据传输。本条款并不限制缔约方拥有采取或维持保护私人数据、个人隐私以及个人记录和账户机密措施的权利，只要该措施不削弱该条款下的义务和承诺。”第 17.18 条规定：“任何缔约方均不得要求金融机构或跨境金融服务提供者在该缔约方境内使用计算机设施或将其置于缔

约国境内，作为在该领土内开展业务的条件。”本条规定的目的在于将原本数据本地化存储的要求转为非必要条件，使得美加墨三国间数据流动更为顺畅。

综合美国国内立法和国际条约的情况可以看出，美国一方面基于传统观念上保护银行客户隐私的考量，制定一系列措施限制金融数据的自由流动，以此降低金融机构客户人身与财产受到侵犯的可能性；另一方面又基于自己信息和金融大国的国际优势地位，在保障安全的前提下促进金融数据最大限度的跨境传输，以充分发挥数据的经济价值。在这两种看似截然相反的价值取向上，美国似乎更倾向于后者，但因此也导致了近些年来银行金融机构数据泄露事件频发等一系列问题，如何在发挥数据经济价值和保障金融安全之间达到平衡已经成为美国亟待思考的问题。

4.2. 欧盟模式：强隐私保护与接收地信息安全评估

为促进欧洲各国经济市场的开放互通，欧洲理事会于 1981 年通过了《与个人数据自动化处理有关的个人保护公约》，这是第一份作用于欧洲整体的对数据跨境流动进行规制的法律文件。欧盟成立后，对于数据流动的法律法规又出现了新的发展，1995 年发布的《关于个人数据处理保护与自由流动指令(95/46/EC)》中更是体现了将公民的人权保护价值置于金融数据流动价值之上的理念，其中第 25 条确立了“充分保护原则”，即数据接受国对数据的保护必须达到欧盟所认可的标准，而这一标准则需要根据数据类型、传输原因、持续时间等多种因素综合评估后才能作出。

21 世纪之后，随着互联网技术的普遍应用，个人数据产生的速度也越来越快，规模越来越庞大，这对欧盟加快制定更为精细化、体系化的数据流动细则提出了新的挑战，2016 年通过的《一般数据保护条例》对数据跨境流动作出了更为严格的限制，其中第五章第 45 条的规定与 95 指令中充分保护原则一脉相承，同时也进一步指出，欧盟数据立法不应仅仅聚焦于基础的数据保护环节，而应当成为数据立法的更核心要求。《一般数据保护条例》将个人信息保护上升至基本权利的高度，认为个人数据处理的目的在于服务人类，这意味着在欧盟对数据跨境流动进行规制的全过程中，基本人权的价值被置于首位[5]。

这一理念也被细化落实于欧盟国家的各行业，具体到银行金融领域来看，2010 年通过的《关于设立欧洲银行业管理局的条例(第 1093/2010 号)》第 71 条规定：“条例不影响成员国在第 95/46/EC 号指令下与个人数据处理有关的义务或欧洲银行业管理局在履行职责过程中应遵循的第 45/2001 号(欧共体)条例下与个人数据处理有关的义务。”由此可见，与银行金融数据有关的法律规制仍需要在欧盟整体的数据规定框架下展开，即金融数据的跨境流动同样适用于《一般数据保护条例》的规定。

但是在经济全球化的背景下，各国金融数据相互流动交融乃是不可逆转的趋势，具有强烈的现实必要性，若一味地对数据流动加以制约也不利于欧盟金融市场的发展，因此欧盟也在逐步探索风险可控范围内促进数据流动的规制路径，2015 年通过的《关于内部市场的支付服务指令(第 2015/2366 号)》是在金融数据开放利用方面所做的一次突破性尝试，其中规定了银行有权在获得客户明确同意的前提下，向第三方支付服务提供商开放用户的账户信息，允许其访问用户的账户数据。由此可见，欧盟这一举措旨在为金融数据在欧盟范围内自由流动提供便利，与此同时，欧盟也出台了对于银行金融数据流动的新型监管技术标准，以防范可能的数据泄露风险，维护金融稳定。

5. 我国金融数据跨境流动规制思路与主要问题

5.1. 我国金融数据跨境流动规制思路

当前阶段，我国对金融数据跨境流动的规制已经形成了“特殊规定 + 一般规定”的法律体系，这就意味着金融机构等数据处理者一方面要遵守金融管理部门所制定的数据跨境规则，另一方面还要遵守网络信息部门有关数据管理的一般法律法规。

从“特殊规定”来看，我国各级金融管理部门对个人金融数据的传输提出了严格的本地化存储的要求，例如2011年中国人民银行所发布的《关于银行业金融机构做好个人金融信息保护工作的通知》，其中第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。”银保监会2019年发布的《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。”2013年发布的《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。”由此可以看出，我国法律在一般情况下均要求境内的金融机构对收集到的客户信息进行本地化存储，只有满足特定条件才能向境外提供。

于2020年2月颁布的《个人金融信息价保护技术规范》是一部对金融数据跨境流动作出较为全面规定的细则，虽然其在法律地位上属于行业技术规范，但其内容进一步明确了金融信息本地化存储的一般原则，其主要内容包括：数据的传输要符合“因业务需要，确需向境外机构传输”；数据接收方应当是总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构；符合国家法律法规及行业主管部门有关规定；获得个人金融信息主体明示同意；应依据国家、行业有关部门制定的办法与标准进行安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。

从“一般规定”来看，金融数据的跨境流动还应当遵守网络信息部门所出台的一般性规定，《网络安全法》中有关数据传输的规定体现在第37条：“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；法律、行政法规另有规定的，依照其规定。”从本条规定可以看出，《网络安全法》中有关信息本地存储的要求仅针对“关键信息基础设施的额运营者”，但是依据《个人信息和重要数据出境安全评估办法(征求意见稿)》第2条的规定：“网络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，应当按照本办法进行安全评估。”由此可见，该意见稿并未沿用《网络安全法》的规定，而是将数据本地化存储的主体扩展至全部网络运营者，这意味对数据本地化存储提出了更为严格的要求[6]。

5.2. 我国当前规制中存在的主要问题

我国在针对金融数据跨境流动的立法活动中坚定了正确的方向，实施了有力的举措，符合当前社会经济的发展趋势和金融市场的客观需要，但同时也面临着以下几个亟待思考和解决的问题。

第一，上位法所配套法律法规体系尚不健全，相关部门曾在2017年就《网络安全法》的配套细则征求意见，但目前仍未发布配套法规，这种政策上的不确定性难以满足金融机构开展业务所需的稳定预期，例如“关键信息基础设施运营者”、“个人信息以及重要信息”的定义仍未界定清晰，且在执法过程中出现了外延不断扩大的现象，不仅对政府造成了较高的实操难度，更是加剧了金融机构运营成本和合规审查负担。如前所述，《个人信息和重要数据出境安全评估办法(征求意见稿)》第2条中将义务主体扩展至所有的“网络运营者”，这就导致各家金融机构在无论何种类型或级别的金融数据跨境流动前都必须履行申报和安全评估义务。

第二，多个规制主体的规制思路有待进一步协调。网信部门的规制思路正是《网络安全法》及配套法律法规所呈现的整体思路，意在维护数据主权的同时注重发挥数据跨境流动的经济价值，属于一般规

制。但由于银行金融数据具有隐私属性强、数据泄露的后果严重等特性，我国金融监管部门采用了不同于上述一般规制的方式来规制银行金融数据，由此制定的各类规范更侧重保护金融信息、维护国家金融安全和防控金融风险，属于特殊规制。两者有待进一步协调，明确金融监管部门制定的规制体系与网信部门制定的规制体系之间是何关系。实际上，银保监会已意识到这一问题。其在2018年5月出台的《银行业金融机构数据治理指引》第24条规定：“银行业金融机构采集、应用数据涉及到个人信息的，应遵循国家个人信息保护法律法规要求，符合与个人信息安全相关的国家标准”，这就充分体现了其对银行金融数据的规制做到体系自洽、实现监管逻辑上统一的要求。

6. 对我国金融数据跨境流动法律规制的完善建议

6.1. 协调金融数据跨境流动规则

1) 注重不同部门规则之间的协调。由于分业监管的历史原因，针对金融行业数据流动的专门规定较为分散，且互相之间并未实现合理衔接。我国金融数据跨境流动规则的构建，应当在数据流动整体框架之下赋予人民银行、银保监会、外管局等机构制定统一金融数据流动规则的权限，构建起清晰完整、层级分明的数据规则体系，[7]并且做好与《网络安全法》及其配套规则的衔接。如在《个人信息保护法(草案)》中就提到法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定，这实际上为金融业这类数据流动时效性要求较高的行业提供了可能的便利条件。

2) 关注当前数据处理者范围扩张的趋势。由于我国金融数据跨境流动既要接受金融业的特殊监管，又要遵守网络安全的一般规定，因此哪些机构适用金融业特殊监管就至关重要。除了持牌金融机构以外，我国大量的金融科技公司和支付机构也同样从事着个人金融数据的收集、处理活动[8]。因此，笔者认为应当牢固把握数据处理的金融属性，正如采用《个人金融信息保护技术规范》中的思路，将所有从事金融信息处理的相关机构全部纳入监管，从而合理识别数据处理者，实现从行业监管到行为监管。

6.2. 将跨境规制与现有金融数据分级分类体系相关联

如前所述，现有规则已按照敏感程度将金融数据分为C3到C1三个类别。《金融数据安全数据安全分级指南》细化了分级的标准和流程，除此之外，也可根据数据主体不同，或按照其他标准与监管要求将金融数据分级分类。

笔者建议选择一种已有的金融数据分级分类标准，与跨境流动制度相连结，根据级别与类别的不同设定具体的评估要求。例如，对于C3这种敏感程度最高的用户鉴别信息，除法律法规及监管机构另有规定外，原则上应当禁止出境；对于C2这类可识别特定个人主体身份和金融状况的信息，可要求先对数据进行“加工、清洗与处理”，例如使用匿名化与假名化等方式处理后方可出境；对于C1金融机构内部使用的个人金融信息，可以基于数据主体的知情同意进行跨境传输，也可以考虑赋予数据主体可携带权，自行决定是否将非敏感信息与其他金融机构共享。当然，上文只是按照金融数据出境的敏感程度、风险或流动价值进行区别保护的举例，在制定规则时应当考虑具体场景，进行利益的博弈与选择，细化规则使其具有可操作性。

参考文献

[1] 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(3): 82-101.

[2] 王远志. 我国银行金融数据跨境流动的法律规制[J]. 金融监管研究, 2020(1): 51-65.

[3] 马其家, 李晓楠. 论我国数据跨境流动监管规则的构建[J]. 法治研究, 2021, 133(1): 92-101.

[4] 程红星, 王超. 金融市场基础设施数据跨境流动法律问题研究[J]. 证券法律评论, 2019(1): 180-190.

[5] 高富平. 个人信息保护: 从个人控制到社会控制[J]. 法学研究, 2018(3): 84-101.
[6] 谢远扬. 个人信息的私法保护[M]. 北京: 中国法制出版社, 2016: 6.
[7] 何渊. 数据法学[M]. 北京: 北京大学出版社, 2020: 41.
[8] 许多奇. 个人数据跨境流动规制的国际格局及中国应对[J]. 法学论坛, 2018(3): 130-137.