重庆大学学报(社会科学版) 2025年第31卷第4期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 31 No. 4 2025

Doi:10. 11835/j. issn. 1008-5831. fx. 2021. 07. 005

欢迎按以下格式引用:范思博. 个人金融数据跨境流动的治理研究[J]. 重庆大学学报(社会科学版),2025(4):236-250. Doi:10. 11835/j. issn. 1008-5831. fx. 2021. 07. 005.

Citation Format:FAN Sibo. Research on the governance of personal financial data cross-border flow[J]. Journal of Chongqing University (Social Science Edition),2025(4):236-250. Doi:10. 11835/j. issn. 1008-5831. fx. 2021. 07. 005.

个人金融数据跨境流动的治理研究

范思博

(上海对外经贸大学 法学院,上海 201620)

摘要:相较于其他数据,金融数据具有天然的保密性要求。随着金融市场国际化与金融数据信息化,金融数据跨境流动成为常态,在此过程中数据的利用与隐私安全问题也逐渐突出,传统的隐私规则难以覆盖跨境需求。在法律层面,《数据安全法》初步确立数据跨境基础框架,《个人信息保护法》引入GDPR理念规范个人信息跨境;但在规章层面,中国人民银行与国家网信等部门的规则并存,存在监管思路不一,概念界定模糊,规则冲突及分级分类标准与跨境规则脱钩等问题。核心问题在于:首先,过度强调安全导致"原则上禁止"思路抑制数据价值释放与市场活力;其次,央行、网信、证监等多监管部门规则重叠冲突增加合规难度;再次,现有数据分级未有效关联跨境条件;最后,未区分跨境业务需求,境外监管要求未进行差异化规制。欧盟和美国是个人数据保护不同模式的代表,对比两大保护体系,能更清晰地认清我国规制的现状和问题:欧盟以GDPR为核心,通过充分性认定、标准合同条款(SCC)及有约束力的公司规则(BCRs)建立严格而复杂的跨境框架,虽未特设金融数据规则但整体要求极高;美国则采取分领域立法与行业自律结合模式,在金融领域有《金融服务现代化法案》等具体规则,并积极利用自由贸易协定破除壁垒,推动数据自由流动,促进数据向美国聚集。为解决个人金融数据跨境流动难的问题,可以从以下几个路径着手:第一,转变监管理念,从"原则禁止"转向"原则允许",在守住安全底线基础上承认数据要素价值及跨境流动的全球性;第二,统一协调监管,强化部门协作以消除规则冲突与真空,覆盖新型金融机构;第三,关联分级分类与跨境规则,依据数据敏感度或重要性设定差异化的出境条件与评估要求;第四,区分流动目的制定规则,对业务需求类流动细化"必要性"标准、建立高效安全评估流程,并基于对等原则谈判构建国际互认机制及发展标准合同。最终通过上述措施协调契约法、组织法、监管规则,构建既能保障安全与主权,又能促进金融市场国际化、释放数据价值并提升国际规则话语权

基金项目:国家社会科学基金重大项目"数字网络空间的知识产权治理体系研究"(19ZDA164)

作者简介:范思博,法学博士,上海对外经贸大学法学院讲师,硕士研究生导师,Email:fansibo@suibe.edu.cn。

的治理体系。

关键词：个人金融数据；跨境流动；GDPR；隐私盾协议；数据主权

中图分类号：D913　　**文献标志码**：A　　**文章编号**：1008-5831(2025)04-0236-15

一、问题的提出

因金融数据具有高敏感性和高隐私性，相较于其他行业，金融行业对客户的资料和信息具有天然的保密要求和传统，我国在大数据时代到来之前就已形成了一系列的保护规则和制度。例如《中华人民共和国商业银行法》规定银行为存款人保密的原则；《中华人民共和国证券法》（以下简称《证券法》）规定证券机构及其工作人员对投资者的信息保密，不得非法买卖、提供或者公开的规则；《中华人民共和国反洗钱法》规定行政主管部门对客户身份资料和交易信息的保密义务，仅用于行政调查和刑事诉讼的限制，以及金融机构对客户身份信息和交易记录的保存和转移；《征信业管理条例》规定个人信息采集的同意要件及例外，个人信息的用途限制，个人信息查询权以及个人信息使用的事前同意机制等。金融机构在业务活动中积累了大量的客户个人数据、交易数据和外部数据，这些数据逐渐成为金融机构的重要资产和核心竞争力。然而，金融市场日趋国际化，国际金融机构利用本国的信息基础设施在他国开展业务成为常态，在此过程中收集、处理、使用客户信息必然涉及数据的出境和入境，极大增加了金融数据泄露的风险，传统的金融行业保密规则与制度已经难以覆盖个人金融数据跨境流动的需求。同时，伴随着云计算、移动互联、物联网、工业控制、大数据等新技术的发展，数据作为生产要素参与市场化配置，传统的静态金融数据已逐步信息化与数字化，金融数据的流动与保护面临全新的要求。近年来，各国相继出台相关规则与指南，以美国和欧洲两大保护体系为代表，正在形成数据流动的国际格局。我国2021年公布的《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）以及同年颁布的《中华人民共和国数据安全法》（以下简称《数据安全法》），在数据跨境和域外效力方面借鉴了欧盟的《通用数据保护条例》（GDPR），同时具有独创性，有利于我国企业参与数据跨境谈判，与国际规则接轨。然而因各国经济发展、立法传统、文化和价值的差异以及国际局势的复杂性，全球统一的数据跨境流动规则短期内不会形成，多个司法管辖区具有不同且可能相互冲突的规则[1]。在此背景下，金融数据跨境流动治理具有研究的必要性：一方面，跨地区或跨国是网络与数据的天然属性，数据只有在流动中才能发挥其商业价值，实现数据作为生产要素的作用；另一方面，一国无法孤立地实现网络与数据安全[2]。本文拟分析美欧数据跨境的不同规制思路和规则体系，梳理我国已有的监管框架，探索国际背景下我国个人金融数据跨境流动的治理路径。

（一）个人金融数据跨境流动的界定

在数据资源中，能够识别个人的数据被称为个人数据。欧盟立法文本通常采用“个人数据（personal data）”的表述，而美国立法文本主要采用“个人信息（personal identifiable information）”的表述[3]，两个概念的出现是各地法律传统和使用习惯所致，并无本质区别，可以相互替换使用[4]。我国法律体系多用“个人信息”的表述，如《中华人民共和国民法典》《中华人民共和国消费者权益保护法》《中华人民共和国网络安全法》（以下简称《网络安全法》）等，在一些行政法规或规范性文件中使用的“个人数据（资料）”实际上也等同于“个人信息”[5]，本文中二者混同使用。金融数据的本质是

特殊的个人信息,个人信息主体本身对信息拥有完整的权利。为获取一定程度的便利(如降低交易成本等),信息主体自愿将一部分信息(如金融数据)及相应的部分权利让渡给专业机构进行处理[6]。从数据监管的角度划分,除个人金融数据外,还包括金融重要数据与其他金融数据,其中个人金融数据因涉及个人敏感信息,是金融数据的重点监管和保护对象,也是本文的研究对象。区分个人数据和非个人数据并不容易,二者转换的可能性取决于数据聚合和处理能力,这也使一些公司将非个人数据与个人数据混淆[7]。根据《中国人民银行金融消费者权益保护实施办法》(以下简称《金融消费者权益保护实施办法》)、《个人金融信息(数据)保护试行办法(初稿)》以及《个人金融信息保护技术规范》的定义,个人金融信息指"金融机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息",包括"账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息"等。

《个人金融信息保护技术规范》更新了以往各级法律法规对金融机构的不同定义:金融机构指"由国家金融监管部门监督管理的持牌金融机构,以及涉及个人金融信息处理的相关机构",可见,除了传统的银行、保险、证券类持牌金融机构,新型的互联网金融持牌机构和地方金融组织也被纳入了监管范畴。不仅如此,个人金融数据的控制者并不限于金融机构①,除上述各类持牌金融机构外,还包括互联网金融平台、金融科技公司、第三方支付机构、提供金融数据服务的外包公司等。与数据控制者相对应的是信息主体,《个人金融信息保护技术规范》定义"个人金融信息主体"是"个人金融信息所标识的自然人",而根据《金融消费者权益保护实施办法》,金融消费者指"购买、使用银行、支付机构提供的金融产品或者服务的自然人"。综上所述,个人金融信息主体的外延大于金融消费者,还包括金融机构在产品和服务以外,通过其他渠道获取、加工和保存信息的主体。

关于数据跨境流动,1980年OECD《关于隐私保护与个人数据跨境流动的指南》将其定义为"点到点的跨越国家、政治疆界的数字化数据传递"。数据跨境流动包括数据出境与入境,本文着重讨论金融数据出境的管制。

(二)个人金融数据跨境流动的目的

个人数据的收集和使用要遵循目的明确原则,即在收集时有特定和明确的目的并告知数据主体,不得收集与目的无关的数据,且应当在约定或规定的目的和用途范围内使用数据。跨境使用同样要符合目的明确原则,在实践中,个人金融数据跨境一般包括以下几种目的。

1. 跨境业务需要

这是个人金融数据跨境传输最普遍的场景,随着金融业的全球化经营、跨境理财、保险等业务成为常态,多个金融业务场景均涉及数据跨境传输,具体如下。

(1)一国分支机构为向他国集团总部传输境内数据,往往把从数据主体处收集的原始数据进行采集、筛选、整理、归类形成各种数据集(Data set),建立各种各样的数据仓库或大数据处理平台[8]。

(2)金融机构与他国第三方机构数据共享或转让,即通过Open API或SDK等方式向第三方合作机构提供接入口,共享部分或全部客户信息。分享数据是企业成本—效益分析后的必然选择,除通过Open API获取数据外,还可以通过网络爬虫或更改操作系统底层设置的方法获取数据[9]。然而在目前的自由利用模式下,数据上的权利不明确,数据的利用充满着法律的不确定性。中国人民银

① "数据控制者"由欧盟GDPR提出,是指"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"。

行2019年发布的《金融消费者权益保护实施办法（征求意见稿）》第36条规定，基于金融消费者的请求和指定，金融机构可将其金融数据转移到其他金融机构，即支持数据可携权。2020年11月1日，正式实施的《金融消费者权益保护实施办法》又将此条删去，可能是为金融机构违反法定责任后法律救济的不确定性考虑。

（3）服务外包，即委托境外关联公司或独立第三方处理业务，包括金融机构自身业务外包和审计等外部需求外包。我国《个人金融信息（数据）保护试行办法（初稿）》第21条、《个人金融信息保护技术规范》第7.1.3条、《金融消费者权益保护实施办法（征求意见稿）》第35条均对金融数据委托行为作出了规定。

2. 反洗钱等境外监管要求

应境外监管部门要求或为满足境外反洗钱、反恐等规则的适用而向境外传输金融数据，涉及数据主权。一国的监管规则对他国并无约束力，储存在他国领土范围内或属于他国分支机构的数据能否被跨境调取，调取的条件如何，均需明确的政策和规则，通常来说需要各国签订数据共享的双边或多边协定。

（三）规制个人金融数据跨境流动的必要性

1. 满足金融市场国际化和客户资料数据化背景下的业务需求

为满足跨境业务需求，实现与国际金融市场的互联互通，我国金融市场双向开放的进程不断加快。2018年，伴随着境内原油期货的上市，铁矿石、PTA国际化的实施，境外交易者得以直接在期货市场监控中心开户并直接参与境内期货交易。在支付结算方面，人民币跨境支付系统（二期）已上线运行，实际业务范围已延伸到148个国家和地区[10]。2019年7月20日，国务院金融稳定发展委员会办公室发布金融开放新“十一条”，新举措包括：允许外资机构对所有种类债券评级；鼓励境外金融机构参与设立；投资入股商业银行理财子公司；允许境外资产管理机构与中资银行或保险公司的子公司合资设立由外方控股的理财公司；允许境外金融机构投资设立；参股养老金管理公司；放宽外资保险公司准入条件；取消30年经营年限要求等[11]。金融市场快速发展的同时，金融数据安全也面临着新问题，例如境外金融机构风控外包，数据公司或所谓的金融科技公司通过爬虫等手段收集大量金融数据，非法实现贷款风控或债务催收等目的。可见，在为金融市场开放提供政策支持的同时，不仅需要相应的监管措施，还需要为金融企业数据出入境提供明确的指引和实施细则。

2. 维护数据主权，应对其他国家的“长臂管辖”

金融数据的跨境流动并不均衡与对等，一些国家制定严格法案，一方面对数据出境的接收国的保护水平提出很高的要求，另一方面采取“长臂管辖”原则，扩展域外适用和司法证据调取的范围。例如根据欧盟GDPR第3条及其域外适用指南，地域适用范围分为三个层面：（1）是否在欧盟设立实体；（2）是否为欧洲居民提供商品或服务；（3）是否监测欧洲居民行为。指南同时列举了几种即使没有在欧盟设立实体也落入GDPR调整的商业模式：精准广告、定位服务、医疗私人定制服务、视频监控等[12]。又如根据美国2018年通过的《澄清境外数据的合法使用法案》（CLOUD），即使美国公司的分支机构设立在境外，美国政府同样有权向境外机构获取数据，也就是说，只要是落入美国数据控制者手中的数据，美国政府就能直接从全球范围调取。对于敏感的个人金融数据，我国应当从维护数据主权的角度，防止金融或互联网企业巨头所在的国家依据行业的全球市场份额，扩张“网络空间领土”。

3. 维护信息主体的合法权益

伴随着金融行业的全球化,外资金融机构近年来出现多起金融数据风险事件,比如韩国金融机构1亿多条个人金融信息被泄露,中石油子公司汇丰银行账户巨额资金被马来西亚政府扣押等,造成的损失不可估量,且难以挽回[13]。金融数据的不当使用、泄露等给信息主体造成切身利益的损失,因取证难,维权成本高,主体难以通过事后的司法救济手段维护权益。因此需要责任机构明确、操作性较强的规则对跨境数据流动予以规范,以保障金融信息主体权益。

二、国际个人金融数据跨境规制模式

目前,全球范围的数据流动保护规则尚未形成,欧盟和美国是个人数据保护不同模式的代表。欧盟以数据基本权利为核心,制定综合性个人信息保护法案;美国则采取"自由市场结合强监管"模式,并未在联邦层面形成个人信息保护的统一立法,但在包括金融领域在内的重要领域,对数据流动有严格的保护要求和标准。

(一)欧盟模式

正如《欧盟基本权利宪章》第8条第1款所述,"每个人都有个人数据保护权"[14],《欧洲人权公约》还包括隐私权[15]。欧盟将数据视为信息主体的基本权利,在此基础上采用综合个人信息保护立法模式,但未针对特殊数据类型如金融数据进行单独立法。欧盟实施数字化单一市场战略,以1981年1月28日签订的《关于自动化处理的个人信息保护公约》,1995年10月24日发布的《关于个人信息处理保护及个人信息自由传输的指令》(95指令)和2018年5月25日生效的GDPR三个标志性法律文件为核心承袭,实现数据在欧盟范围内的自由流动。GDPR的适用范围得到大幅扩展,反映了隐私作为一项人权的重要性及其在欧盟中的意义[16]。GDPR第5章为个人数据的跨境传输提供了几个层次的路径。

其一,欧盟委员会将对个人数据提供充分保护的国家和地区列入白名单,允许数据转移,包括:根西岛、曼岛、加拿大(仅商业组织)、泽西岛、新西兰、日本、安道尔、乌拉圭、阿根廷、以色列、法罗群岛、瑞士和美国(限于隐私盾协议下)[17]。

其二,标准合同条款(Standard Clauses Contract,SCC),这是非白名单国家大多数企业实现数据转移的途径。欧洲数据保护委员会(EDPB)在2020年2月24日发布对此条款指南的新版本,规定接收国需完成关于整体法律环境的个案评估,包括:(1)接收国个人数据、隐私保护水平;(2)政府、情报部门访问数据的授权和程序;(3)数据主体权利的保护[18]。在欧盟法院2020年7月16日发布的Schremes Ⅱ案判决中,认定《隐私盾协议》无效,但SCC继续有效。法院指出,鉴于SCC的合同性质,仅能约束数据传输双方,对接收国政府或公共机构无约束力,但并不当然导致SCC无效。在数据转移过程中,如因接收国政府或公共机构执法等原因,使数据接收方无法遵守SCC,应当立即通知出口方公司,出口方可选择暂停或终止传输,或通知出口国的数据保护监督机关[19]。

其三,有约束力的公司规则(Binding Corporate Rules,BCRs):要求一家公司为整个公司结构中的个人数据跨境传输提供欧盟数据保护标准[17]。对于跨国企业,如果关于个人数据保护的公司规则被欧盟数据保护机构(Data Protection Agency,DPA)批准,则数据转移无需另行报备和批准。BCRs的申请程序繁琐,成本昂贵,一直以来采用率较低。但近几年,越来越多的大型跨国企业搭建起内部数据合规流程和框架,也越来越倾向于通过BCRs实现数据传输,例如欧盟网站公布的空客、

E-Bay、爱马仕、乐高、PayPal等已批准的公司[20]。

其四，特定情况克减：如以上方式皆无法达成，数据出境在严格特定条件下才可进行，例如明确告知数据主体后仍表示同意；社会公益；非重复性且关乎少量权利等，应当提供数据安全保障并进行相应评估[21]。

2015年11月，欧盟通过《支付服务指令》第2版修正案，允许银行在客户明确授权同意的情况下，向第三方支付服务机构共享客户数据或开放API接口权限，并允许跨境提供服务，旨在帮助数据获得和分析能力较弱的金融初创企业发展[22]，但对于其他银行业金融数据跨境并未有过多规定。除此之外，欧盟并没有对金融数据作出专门立法或定义。可见，在GDPR全面、严格的个人数据保护体系下，目前欧盟并未将金融数据作为特殊的个人数据类型特殊保护。基于GDPR，欧盟国内隐私法要求所有公司遵守高标准规则，即使公司仅在国内销售商品或提供服务，但这导致欧盟领域内经商成本增加，也给非欧盟国家特别是发展中国家带来挑战[23]。事实证明，BCR和SCC既昂贵又费时。对欧盟来说，需要解决的主要问题是，如何在严格隐私保护的同时，保留数字贸易的机会；对欧盟以外国家来说，以GDPR为隐私标准进行全球监管的可能性不大[24]。欧盟隐私保护的高标准源于对历史上纳粹使用个人记录进行种族灭绝，Stasi利用国家保留的个人记录建立东德集权国家的反应[25]。《欧盟基本权利宪章》将隐私作为基本人权是欧洲国家历史和文化轨迹的产物，不适用于其他国家[26]。

（二）美国模式

美国在联邦层面没有统一的数据保护基本法，其采取分领域立法，并尊重行业自律规范，鼓励通过行业自治（self-regulation）约束从业者行为，达到有效保护个人信息的目标[25]。1978年颁布的《金融消费者隐私权法》规定客户数据收集的方式和程序以及金融机构在收集过程中的义务，如不得向联邦政府披露个人信息和交易记录，除非得到客户的知情同意。1999年通过的《金融服务现代化法案》明确金融隐私保护的通知、选择、市场披露、安全和执行五项基本原则，并详细规定金融机构如何收集、保护和共享金融消费者个人信息[27]。随后，金融监管机构出台多项行业规范和补充性细则，其中包括金融信息跨境流动内容，但并未详细说明具体操作要求。随后，2000年通过的《消费者金融信息隐私法》强调《金融服务现代化法案》中对金融机构确立的三个要求：（1）以准确、清晰、显著的形式通知用户，说明可能向非关联第三方或关联公司披露非公开的个人信息的各种情形；（2）以准确、清晰、显著的形式向现有用户提供隐私政策；（3）须提供合理方式，使用户可以随时“选择退出”对非关联第三方披露[28]。在以上成文法中，并未对数据跨境流动作出过多限制。被称为“最严隐私保护法”的《加州消费者隐私法案》对此仍秉承留白态度。究其原因，除与欧洲隐私保护观念存在传统上的差异外，更重要的是，美国在信息通信和数字经济市场的领先地位得益于互联网巨头企业的聚集，而互联网商品或服务通常跨越国界，过多的规制会使企业乃至行业丧失创新与活力。此外，美国还通过双边或多边协议破除他国壁垒和限制，促进数据自由流动，或者说向美国流动。

2012年美韩签订《自由贸易协定》（FTA），约定对于电子数据跨境流动，两国应当“避免施加或保持不必要的阻碍”[29]，并在第13章“金融服务”中约定，“基于金融机构日常业务对数据处理的需要，缔约方允许对方金融机构以电子或其他方式传入或传出数据”。这一突破使金融数据的价值在美韩跨境金融产品和服务中得到充分发挥。

APEC在2012年发布《跨境隐私规则体系》(CBPR),目前已有8个国家加入。CBPR规定,只要公司层面承诺遵守APEC隐私框架的九大原则,那么处于不同成员国的不同公司则按照同一套规则保护个人信息,成员国层面不得再以保护个人信息为由限制数据跨境流动[30]。不同于欧盟在各项谈判中要求其他国家修改国内法以满足欧盟隐私保护的高要求,美国主导的CBPR约定成员国在个人信息出境时,不得要求接收国提供超过APEC的数据保护水平,也就是强制成员国按照低标准的个人信息保护制度实现跨境流动,以方便数据向美国聚拢。

2015年的《跨太平洋战略经济伙伴关系协定》(TPP)是美国第一次将限制数据本地化要求写入贸易协定,主要条款在"跨境传输电子数据"章节的第11条及13条,规定成员国应当允许个人数据跨境流动,并不得将使用境内计算机作为在境内开展商业活动的条件之一,除非出于正当公共政策目标。然而对于金融机构,协定给出两个例外条件:(1)出于个人数据、个人隐私、记录或账户的保密性;(2)出于审慎监管,指定数据接收方之前需先行获得监管许可[31]。也就是说,TPP对数据本地化的限制作用未及于金融机构,TPP项下的金融机构可以强制在本地存储数据副本,这主要是出于美联储和美国联邦证券交易委员会的监管需要。

美欧在2016年签订《隐私盾协议》,规定只要美国遵守协议的七项原则即被认为达到欧盟指令标准。2020年7月16日,欧盟法院在"Schrems Ⅱ"②一案中裁定《隐私盾协议》无效,这是欧盟法院继2015年裁定《安全港协议》无效以来,再次废止美欧之间个人数据跨境流动协议。判决指出,在该协议下,欧洲公民的个人数据因达不到保护标准,仍可能被美国情报机关获取。受此判决影响,在"隐私盾"框架下获得认证的5 384家公司需重新考虑跨境数据传输机制[32]。美国已与欧盟开启讨论,筹备出台新制度以取代目前的"隐私盾"协议。

2018年签订的《美国—墨西哥—加拿大协定》在19条约定成员国需遵循CBPR,数据跨境传输不得禁止或限制。第17.17条约定,在以经营业务为目的并得到客户授权许可的前提下,成员国不得阻止金融机构以及金融服务提供商跨境转移数据,并在17.18条约定,"使用或在境内放置计算机设施"不得作为成员国金融机构在另一成员国开展金融业务的条件,但同时要满足"该金融机构所在成员国的监管机构能够即时、直接、完整并且持续地访问和监督本国境内外金融信息"[33]。可见,协定试图突破金融数据的本地化存储限制,实现成员国之间金融数据的自由流动。

在通过以上协议寻求数据流动带来的商业利益的同时,美国也在逐步调整隐私保护框架,与国际个人信息保护要求接轨。例如2019年《联邦数据战略与2020年行动计划》确立的二十项行动方案,包括设立GDPR要求的首席数据官;2020年发布的《NIST隐私框架》,通过企业风险管理改进隐私保护。

三、我国个人金融数据跨境流动规制现状

我国的金融数据跨境流动规制立法起步较晚,逐步形成了"一般+特殊"的规制模式[34]。2017年6月1日起实施的《网络安全法》和金融领域的法律对个人金融数据的跨境流动只有原则性规定,目前的具体监管要求来自不同部门的规章和行业标准。我国2021年正式颁布《个人信息保护法》和《数据安全法》,在法律层面为数据安全和个人数据保护提供保障。《数据安全法》从域外适用效力、

② Schrems Ⅱ案的起因是爱尔兰Facebook公司向美国Facebook公司转移Max Schrems的个人数据,主要争议点是出于商业目的将个人数据从欧盟转移到第三国时,第三国的大规模监控权超出了GDPR所要求的严格必要比例。

数据安全审查制度、数据出口管制、数据对等反制措施和数据跨境调取审批制度等几个角度，初步确立了我国数据跨境流动的基本法律框架。《个人信息保护法》则是我国法律层面上第一部个人信息保护普适性和综合性的立法文件。其他规范性文件散见于金融监管部门和网信部门的规章。

（一）法律层面

1.《数据安全法》

关于数据跨境流动，《数据安全法》第2条关于域外适用效力的规定，借鉴了欧盟GDPR第58条。第24条规定“数据安全审查制度”，一方面，为危及国家安全数据活动建立“防护罩”，促进我国数据跨境流动的合规建设和第三方数据安全评估企业的发展，与网络安全审查制度共同确保数据跨境活动的安全性；另一方面，数据安全审查制度增大了重要数据跨境流动的时间跨度，降低了数据的时效性，一定程度上增加了企业数据跨境流动的成本，某种程度上可能抑制国外企业进入的积极性[35]。第25条与《中华人民共和国出口管制法》相衔接，将管制物项从“货物、技术、服务”扩大到“数据”，其目的类似美国的《2018年出口管制法》和《出口管制条例》（EAR）项下对科技数据的出境限制。第26条引入国际法中的对等原则，为我国出海企业提供竞争保障。第36条是在美国CLOUD法案出台后，我国对他国跨境调取数据“长臂管辖”的应对。

2.《个人信息保护法》

《个人信息保护法》在地域适用范围上借鉴了GDPR，但也有不同之处。

对于境内处理个人信息而言：（1）GDPR保护欧盟境内的数据主体，不限于拥有国籍、合法居留或拥有合法身份的个人[36]；《个人信息保护法》保护境内自然人个人信息，同样并未限制国籍与身份。（2）GDPR规定只要在欧盟境内设立实体，如营业场所、分支机构等，即落入GDPR管辖，不论处理个人信息的行为是否发生在境内；而《个人信息保护法》第3条规定在境内处理个人信息的活动适用本法。

对于域外效力而言，《个人信息保护法》基本与GDPR一致。GDPR规定了两种情形：（1）无论支付对价与否，向境内数据主体提供商品或服务；（2）监控境内数据主体行为。而《个人信息保护法》列举了三种情形：（1）目的是向境内自然人提供产品或服务；（2）目的是分析、评估境内自然人行为；（3）法律、行政法规规定的其他情形。

《个人信息保护法》对数据跨境进行专章规定，除已有的出境安全评估外，新增两条个人数据出境路径：（1）经专业机构进行个人信息保护认证；（2）与境外接收方订立合同。《个人信息保护法》借鉴了GDPR的SCC条款，但合同关系是否会被监管部门实质审查有待澄清。关于国际司法或行政执法协助，《个人信息保护法》规定，如需向境外提供，应当向主管部门报批，如企业服务器部署在境外，因国际司法或执法原因被直接获取中国境内个人信息的情况，可能因未被批准而违法。

《个人信息保护法》未对个人金融数据进行特别规定，仅将金融账户纳入敏感个人信息进行特别保护，未来可能以个人信息保护综合立法为核心，并陆续出台行业指南，逐渐统一不同部门对金融数据的规定，避免重复性、冲突性规范。

我国数据安全和个人数据保护的路径正逐渐清晰，但离系统化保护金融数据尚有距离。目前，我国个人金融数据跨境流动的规则主要来自金融监管部门和网信部门的规章。

（二）金融监管部门规章

2011年1月，中国人民银行发布通知（17号文）规定，境内收集的个人金融信息在境内储存和处

理并不得向境外提供[③],原则上禁止个人金融信息出境,对于例外情况,17号文并未作进一步说明,国内的跨国金融机构在诸多业务开展上无据可循,面临操作与监管层面的现实难题。2011年5月,中国人民银行上海总部针对上述问题发布新的通知(110号文),对例外情形作出规定,认定不违规需同时符合:(1)办理业务所必须;(2)客户书面授权或同意;(3)向本机构总行、母行或分行提供;(4)本机构总行、母行或分行保密[④]。110号文为境内银行业金融机构日常经营活动中的必要数据跨境流动打开了通道。五年后,中国人民银行发布的《金融消费者权益保护实施办法》将110号文的适用范围从银行业个人金融数据扩大到所有个人金融数据并细化了例外情形,指明境外机构包括总公司、母公司或者分公司、子公司及其他为完成该业务所必需的关联机构,并增加了签订协议、现场核查等要求,完善了数字化时代下对传统客户数据保密义务的合规要求。2020年修订的新版《金融消费者权益保护实施办法》要求银行和支付机构采取技术措施保管和储存消费者金融信息并规定了告知义务[⑤]。然而,2019年修订的《证券法》第177条并未将上述个人金融信息的例外情形适用于证券业,规定"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","境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动"[⑥]。

2020年2月13日,中国人民银行发布《个人金融信息保护技术规范》,4.2条将个人金融信息按照敏感程度依次分为三个类别:C3为敏感度最高的用户鉴别信息,如受到未经授权的查看或变更,会对信息主体造成严重危害的或登录、查询、交易等各类密码、个人生物识别信息等;C2为可识别特定个人主体身份和金融状况,以及用于金融产品与服务的关键信息,如支付账号、手机号码、用户登录名、安全验证码、密码提示问题等;C1是供金融机构内部使用的个人金融信息,如开户时间、机构等。规范7.1.3条d)款规定因业务需要,确需向境外机构提供个人金融信息的,须符合:(1)法律法规;(2)信息主体的明示同意;(3)依法开展出境评估,并且要确保拟传输国家数据安全保护能力达到相关要求;(4)与境外机构签订协议,监督其有效履行保密、删除、协助等义务。2020年9月23日,中国人民银行正式发布《金融数据安全 数据安全分级指南》,根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度,将数据安全级别从高到低划分为五级。影响对象指金融业机构数据安全性遭受破坏后受到影响的对象,包括国家安全、公众权益、个人隐私、企业合法权益等;影响程度指金融业机构数据安全性遭到破坏后所产生影响的大小,从高到低划分为非常严重、严重、中等和轻微。安全定级过程包括数据的资产梳理、安全定级准备、安全级别判定、安全级别审核及安全级别批准五步。对数据按照不同标准进行分级分类是金融数据监管的一大进步,有利于金融机构统筹了解、掌握数据资产状况,全面提升有效性、可用性以及数据质量。但该规定并非强制性规定,涉及个人金融信息处理的相关机构的标准仍需进一步界定[37]。

③《中国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》第6条: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。

④《中国人民银行上海总部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》第4条: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,可不视为违规。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。

⑤《中国人民银行金融消费者权益保护实施办法》第34条: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。

⑥《证券法》第177条第2款:境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。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。

（三）网信部门规章

《网络安全法》将数据出境主体范围限定在“关键信息基础设施的运营者（CIIO）”，并在37条要求本地化存储，采取原则禁止，经安全评估为例外的监管模式。随后，2017年国家互联网信息办公室和信息安全标准化技术委员会出台的《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称《办法》）与《信息安全技术 数据出境安全评估指南（草案）》（以下简称《指南》），将数据出境主体的范围扩展为“网络运营者”。同时，《办法》和《指南》规定，数据出境安全评估重点关注出境目的和安全风险，可分为安全自评估和主管部门评估。然而，将金融业全部划分为关键信息基础设施的一刀切政策并不合理。单独的金融机构尤其是中小型金融机构的数据系统和业务系统发生数据安全事故往往不会达到损害国家安全、公众利益和社会秩序的程度，关键信息基础设施的强监管要求加重了这些金融机构的合规成本和负担，也使境内外资金融机构难以深度参与中国金融市场。

2019年，《办法》在更新后发生较大变动，其将区分个人信息与重要数据进行立法，并明确了个人信息出境的申报与安全评估要求：（1）只要是在境内收集的个人信息，无论是否有境内商业实体，出境均需每2年向所在地省级网信部门申报与评估；（2）数据出境者与接收者需签订协议并申报[38]。此外，其还增加了“通过网络”等出境方式。2020年3月，国家市场监督管理总局与国家标准化管理委员会发布新版《信息安全技术 个人信息安全规范》，在第9.8节个人信息跨境传输中删除了草案中的强制性安全评估要求，仅规定遵循相关规定或标准要求。该规范作为推荐性国家标准，并不具有法律上的强制执行力，但在部门执法和企业合规过程中具有很高的参考意义。2023年国家网信办出台的《个人信息出境标准合同办法》作为《个人信息保护法》的细则，确立了个人信息出境的标准合同。

四、我国个人金融数据跨境流动面临的现实困难和解决路径

（一）平衡数据保护与金融市场需求，从原则上禁止到原则上允许流动

单个自然人的个人数据本身并无价值[39]。随着大数据时代的到来，金融机构在业务快速发展过程中，积累了海量数据，与此同时催生出多样化的金融业态，使金融数据体量和价值激增。正如奥地利科学家Viktor Mayer-Schönberger在其所著的《大数据时代》中所言，“数据被列入资产负债表，只是时间问题”，数据已成为银行业乃至整个金融行业的重要资产和核心竞争力。我国在党的十九届四中全会中首次将数据作为生产要素提出，并在随后发布的《关于构建更加完善的要素市场化配置体制机制的意见》中提出培育数据要素市场，鼓励数据资源共享，实现数据价值。数据从生产到特定分析应用的全生命周期均应当进行质量、安全和合规管理，这便是数据治理[40]。挖掘金融数据价值，使其成为数据资产来驱动金融机构发展，需要将线条化、碎片化和局部化的信息融合与整理成具有数据价值的资源。然而，根据中国人民银行科技司司长李伟在“第四届（2019）中国新金融高峰论坛”上的发言，数据孤岛问题在金融领域较为突出。金融机构对所积累的个人数据、交易数据等，存在“不愿、不敢、不能”共享的问题，无法发挥数据真正价值。所谓“不愿”，是指金融机构将客户数据看作重要资产和核心竞争力，主观上宁愿将其闲置，也不愿让其流动起来；所谓“不敢”是因为金融数据具有的高度敏感性，涉及个人敏感信息、商业秘密，特别是跨境共享可能关系国家安全，且涉及多国法律法规，有较大的合规风险，从客观上阻碍了金融数据共享；所谓“不能”，是指金融机构各自拥有不同的数据接口，特别是跨境流动传输、存储过程中对设备与技术的要求，各国

都有不同的标准,难以从技术层面实现数据的互联互通。

2019年8月,人民银行在发文中提出,要发挥金融数据集聚和增值作用,“打通金融业数据融合应用通道,破除不同金融业态的数据壁垒,化解信息孤岛”[41]。数据资产与金融资产一样,只有在流动中才能实现价值,而目前原则上禁止金融数据跨境流动规制思路仅从安全角度出发,忽视了市场需求,降低了中国金融行业在国际金融市场的活力与参与度,甚至导致一些金融机构为实现业务需求,规避合规成本,违法违规进行数据跨境转移,造成脱离监管的严重后果。可见,目前金融数据本地化一刀切的监管与规制思路无法适应金融机构的跨境经营需要,且与网络强国的战略目标不符。在制定具体监管规则前,宜将挖掘金融数据价值与数据保护共同纳入规制目标,在守住数据安全底线与红线的基础上,给金融数据市场留出足够的自主权与流动性。认识到跨境数据流动的全球不可分割性,并因此寻找政策共识和国际合作的空间与可能性,才是走向“互联互通、共享共治”的正确途径[42]。

(二)协调统一多个监管部门规制思路和规则体系

如上所述,金融监管部门与网信部门对于金融数据的监管有不同的思路和侧重点,对于金融数据控制者、金融数据主体等概念的含义和范围存在不同理解,导致同一金融机构的同一事项需满足两个部门可能重叠甚至冲突的合规要求,承担不必要的合规难度与成本。事实上,监管部门已经意识到问题的存在,如2018年银行保险监督管理委员会发布的《银行业金融机构数据治理指引》第24条规定,采集个人信息应当遵循法律法规要求,符合相关的国家标准。该条款事实上将国家标准《信息安全技术 个人信息安全规范》正式纳入了银行业金融机构的合规标准体系[43],但在实施细则部分还应当尽快落实部门监管之间的协调,避免过度监管、监管真空和监管竞争问题,并力求法律概念的统一与周延。

对于是否应当归口统一部门监管,特别是在《个人信息保护法》正式出台后,金融监管部门和网信部门在个人金融数据跨境规制中的角色划分,需综合考量部门归口或合并的复杂程度与成本,因简化局部业务而统筹不同监管部门涉及监管资源的调整和重组,在实际操作上不易实现。因此,实现金融数据跨境流动多部门监管的平衡不应当局限于简单的统一监管部门,而应当在金融市场发挥主导作用的整体思路下,一方面加强监管机构间的对话与协作,在规则制定层面统一且明确,避免重复、冲突、繁多和难以执行,一方面将陆续出现的新型金融机构,如互联网金融、地方性金融机构的金融数据出入境纳入监管体系,避免监管真空。

(三)将跨境规制与现有金融数据分级分类规范体系关联

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。然而,金融数据的跨境流动要求并未与目前或即将出台的任何一种分级分类标准相关联,导致跨境数据无法按照上述标准区别保护,也没有解决金融业部门规范间的重合与冲突。例如,上述法规均表明“因业务需要”可以向境外提供,并未限制可以提供的金融数据类型与级别,而《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”。

对此,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—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—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。

又如，金融数据出境也可按照个人金融数据、重要金融数据与其他金融数据三个类别设定相应的评估要求。根据《个人信息和重要数据出境安全评估办法（征求意见稿）》，“重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据”，《数据安全法》第31条将重要数据分为关键信息基础设施的运营者、其他数据处理者收集和产生的重要数据，《信息安全技术 数据出境安全评估指南（征求意见稿）》附录A《重要数据识别指南》给出了26个行业或领域的重要数据范围。然而，以上规则均未在数据出境层面对个人数据和重要数据加以区分。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。

（四）根据跨境业务需要或境外监管要求，制定相应的跨境规则

如前所述，金融数据跨境有不同的目的，大的方向可以分为因跨境业务需要或因境外监管要求，前者基于数据流动中的经济价值，后者承载着数据主权。如果不加以区分，一律纳入原则上不予出境或原则上予以出境，都与实际需求不相适应。2019年国际数据公司IDC发布的报告指出，2018年至2025年中国数据总量的年平均增长速度是30%，超过全球平均水平3个百分点[44]。国家依法采取措施对承载着不同利益层次和位阶诉求的数据流动予以规范和约束，妥善规定禁止和限制数据跨境流动的范围和标准，减少其对经济和技术发展的阻碍，从而在安全和经济发展之间谋求平衡[45]。

对于基于跨境业务需要的个人金融数据流动，首先应当明确与细化规则中“因业务需要”的情形，进而制定相应的安全评估要求和流程。其次，我国缺乏跨境数据流动领域的国际互信机制，实践中较少参与跨境数据流动国际谈判，缺乏话语权[46]。可根据对等原则，借鉴欧盟充分保护白名单机制，积极与我国提供跨境金融服务的主要国家进行谈判，考察拟实现自由流动国家或地区的法治程度、数据保护能力、监管力度等，为我国提供跨国服务的金融机构建立有效的数据传输路径。最后，对于不符合白名单要求的国家，可在符合我国法律法规和监管要求的前提下，在不与《个人信息出境标准合同办法》冲突的前提下，制定适应金融行业惯例和国际标准的合同范本，并辅以明确与细化的操作指南。

对于基于因反洗钱、反恐等境外监管要求而进行的金融数据流动，应当合理主张数据主权，在《个人信息保护法》向有关部门批准规则的基础上，原则上不予批准出境。储存在一国的金融数据并不当然应当被纳入该国管辖范围，一国的法律法规也不能约束他国。对于向全球提供服务的金融机构，法律适用和管辖的不确定性极大增加了运营和风险控制成本。为应对他国在数据调取等方面的“长臂管辖”，一方面应当提高执法的确定性，设置符合国家利益的数据调取和管辖规则，例如我国可结合司法实践，选择金融数据主体所在地、金融机构注册地、金融数据存储服务器所在地等进行管辖。另一方面，可以通过签订双边或多边协定确定不予出境的例外情况。随着人工智能、5G、物联网等网络和科技水平的不断创新发展，国际金融诈骗、洗钱等犯罪活动频发，相较于数据本

地化的单一化保守策略,我国应当积极部署数据的全球规制,从被动接受规制到主动参与规则制定。

针对中国出海企业、在华跨国企业在欧洲面临的个人数据转移到中国的合法性审查问题,由于中国不属于欧盟认定的个人数据充分保护国家,关于欧盟个人数据流入,大部分企业仅能依赖SCC。SCC要求对数据接收国的数据保护能力进行个案评估,然而单个企业对国家整体法律环境进行评估成本高、耗时长,且个案之间的不确定性和不一致性较大。故可以采取以下方式:第一,针对主要评估依据——第三国法律体系和公权力对个人数据的访问,可由监管机构牵头发布本国数据保护法律环境评估的白皮书,并根据立法与执法情况进行定期更新;第二,可借鉴同处于数字经济领先地位的美国,美国通过两项协议突破了GDPR的限制,实现了美欧之间的数据流动,在2020年7月《隐私盾协议》被欧盟宣布无效后,美国商务部、司法部和美国国家情报总监于9月联合发布白皮书,指导美国企业对美国整体隐私保护法律环境进行评估。

参考文献:

[1] GIEROW H J. Cyber security in China(I)[EB/OL]. (2014-10-14)[2020-11-01]. https://merics. org/de/studie/chinas-cyber-security-i.

[2] LIUDMYLA B. China's new cybersecurity law and U. S-China cybersecurity issues[J]. Santa Clara Law Review, 2018, 58: 137-163.

[3] 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.

[4] 谢远扬. 个人信息的私法保护[M]. 北京:中国法制出版社,2016:6.

[5] 何渊. 数据法学[M]. 北京:北京大学出版社,2020:41.

[6] 江翔宇. 中国金融数据保护相关问题研究[N]. CIO时代,2020-05-19(01).

[7] ZALNIERIUTE M. Transborder data flows and data privacy law[J]. Computer Law & Security Review the International Journal of Technology Law&Practice, 2014, 30(1): 104-108.

[8] 高富平. 数据经济的制度基础:数据全面开放利用模式的构想[J]. 广东社会科学,2019(5):5-16,254.

[9] 费方域,闫自信,陈永伟,等. 数字经济时代数据性质、产权和竞争[J]. 财经问题研究,2018(2):3-21.

[10] 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.

[11] 国务院金融稳定发展委员会办公室. 关于进一步扩大金融业对外开放的有关举措[R/OL]. (2019-07-20)[2021-01-01]. http://www. gov. cn/xinwen/2019-07/21/content_5412293. htm.

[12] 范思博. 数据跨境流动中的个人数据保护[J]. 电子知识产权,2020(6):85-97.

[13] 管清友. 旗帜鲜明防范外资银行泄露重要金融信息[EB/OL]. (2020-09-07)[2021-01-02]. https://baijiahao. baidu. com/s? id=1677186225137457203&wfr=spider&for=pc.

[14] SOLEMNE P, PROKLAMATION H, PROKLAMATION F, et al. Charter of fundamental rights of the European Union[J]. Official Journal of the European Communities, 2000, 12: 1-364.

[15] EUROPEAN CONVENTION ON HUMAN RIGHTS. Convention for the protection of human rights and fundamental freedoms[R/OL]. (1950-04-19)[2020-09-16]. https://www. echr. coe. int/Documents/Convention_ENG. pdf.

[16] SCHWARTS P M, PEIFER K N. Transatlantic data privacy law[J]. The Georgetown Law Journal, 2017, 106: 115-179.

[17] EU. GDPR third countries[R/OL]. (2018-05-25)[2020-05-04]. https://gdpr-info. eu/issues/third-countries.

[18] EU. Standard contractual clauses for data transfers between EU and non-EU countries[R/OL]. (2021-06-04)[2022-07-24]. https//ec. europa. eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[19] NOTE. Data protection commissioner v. Facebook Ireland Ltd. [J]. Harvard Law Review, 2021, 134(4): 1567-1574.

[20] EU. List of companies for which the EU BCR cooperation procedure is closed[R/OL]. (2018-05-24)[2020-02-16].

https://ec. europa. eu/newsroom/article29/items/613841.
[21] EU. General data protection regulation[R/OL]. (2018-05-25)[2020-03-16]. https://gdpr-info. eu.
[22] PORTO F D, GHIDINI G. "I access your data, you access mine": Requiring data reciprocity in payment services[J]. International Review of Intellectual Property and Competition Law, 2020, 51: 307-329.
[23] MATTOO A, MELTZER J P. International data flows and privacy: The conflict and its resolution[J]. Journal of International Economic Law, 2018, 21(4): 769-789.
[24] KUNER C. Reality and illusion in EU data transfer regulation post schrems[J]. German Law Journal, 2017, 18: 881-919.
[25] 龙卫球. 数据新型财产权构建及其体系研究[J]. 政法论坛, 2017(4): 63-77.
[26] WHITMAN J Q. The two western cultures of privacy: dignity versus liberty[J]. The Yale Law Journal, 2004, 113(6): 1151-1221.
[27] FEDERAL TRADE COMMISSION. Gramm-Leach-Bliley Act [R/OL]. (1999-11-12) [2020-11-14]. https://www.congress. gov/106/plaws/publ102/PLAW-106publ102. pdf.
[28] CONSUMER FINANCIAL PROTECTION BUREAU. Regulation P: Privacy of consumer financial information [R/OL]. (2011-11-11)[2020-11-18]. https://www. federalreserve. gov/boarddocs/supmanual/cch/consumer. pdf.
[29] US-The Republic of Korea. Free Trade Agreement [R/OL]. (2012-03-15) [2020-12-03]. https://ustr. gov/trade-agreements/free-trade-agreements/korus-fta.
[30] APEC. About CBPRS[EB/OL]. (2018-07-19)[2020-10-29]. http://cbprs. org/about-cbprs.
[31] Trans-Pacific Partnership[R/OL]. (2017-01-23)[2020-08-20]. https://ustr. gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text.
[32] U S DEPARTMENT OF COMMERCE. U S secretary of commerce Wilbur Ross statement on Schrems Ⅱ ruling and the importance of EU-U. S. data flows[EB/OL]. (2020-07-16)[2020-10-19]. https://useu. usmission. gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/.
[33] U S-Mexico-Canada Agreement [R/OL]. (2018-11-30) [2020-08-04]. https://usmca. com/financial-services-usmca-chapter-17.
[34] 许多奇,董家杰. 我国跨境数据流动中的金融企业合规治理[J]. 吉林大学社会科学学报, 2024(3): 41-60, 235.
[35] 魏贝,周振松.《数据安全法(草案)》规范下的数据跨境流动研究[EB/OL]. (2020-07-27)[2021-04-13]. https://baijiahao. baidu. com/s? id=1673365553821451417&wfr=spider&for=pc.
[36] EDPB. Guidelines 3/2018 on the territorial scope of the GDPR(Article 3)-version for public consultation[R/OL]. (2018-11-16) [2020-10-22]. https://edpb. europa. eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en. pdf.
[37] 吴江羽. 金融科技背景下金融数据监管法律框架构建[J]. 西南金融, 2020(11): 76-85.
[38] 国家互联网信息办公室. 个人信息出境安全评估办法(征求意见稿)[R/OL]. (2019-06-13)[2020-10-25]. https://www. moj. gov. cn/pub/sfbgw/lfyjzj/lflfyjzj/201906/t20190612_150617. html.
[39] XIAO C. Personal data rights in the era of big data[J]. Social Sciences in China, 2019, 40: 174-188.
[40] 高富平. 建立数据生产流通分析利用系统[N]. 联合时报, 2020-08-11(06).
[41] 搜狐网. 最新! 中国人民银行印发《金融科技(Fin Tech)发展规划(2019—2021年)》[R/OL]. (2019-08-24)[2021-03-13]. https://www. sohu. com/a/336137510_258957.
[42] 贾开. 跨境数据流动的全球治理:权力冲突与政策合作:以欧美数据跨境流动监管制度的演进为例[J]. 汕头大学学报(人文社会科学版), 2017(5): 57-64.
[43] 洪延青. 透析金融数据保护的美欧中立法要点和趋势[J]. 中国银行业, 2018(11): 39-42.
[44] 贾开. 跨境数据流动全球治理的"双目标"变革:监管合作与数字贸易[J]. 地方立法研究, 2020(4): 49-59.
[45] 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.
[46] 许多奇. 论跨境数据流动规制企业双向合规的法治保障[J]. 东方法学, 2020(2): 185-197.

Research on the governance of personal financial data cross-border flow

FAN Sibo

(*Law School*, *Shanghai University of International Business and Economics*, *Shanghai* 201620, *P. R. China*)

Abstract: Compared to other types of data, financial data inherently demands higher confidentiality. With the internationalization of financial markets and the digitization of financial data, cross-border flows of financial data have become commonplace. However, this process has increasingly highlighted issues concerning data utilization and privacy security, as traditional privacy regulations struggle to address cross-border requirements. At the legal level in China, the Data Security Law has preliminarily established a foundational framework for cross-border data transfers, while the Personal Information Protection Law incorporates GDPR-inspired principles to regulate the cross-border flow of personal information. However, at the regulatory level, overlapping rules from the People's Bank of China (PBC), the Cyberspace Administration of China (CAC), and other authorities coexist, leading to inconsistencies in regulatory approaches, ambiguous definitions, conflicting rules, and a disconnect between data classification standards and cross-border regulations. The core issues are as follows: First, an excessive emphasis on security has resulted in a prohibited in principle approach, stifling the release of data value and market vitality. Second, overlapping and conflicting regulations from multiple regulators—such as the PBC, CAC, and China Securities Regulatory Commission (CSRC) —increase compliance difficulties. Third, existing data classification systems fail to effectively link to cross-border conditions. Finally, there is a lack of differentiation in cross-border business needs, and foreign regulatory requirements are not addressed with tailored rules. The EU and the U. S. represent two distinct models of personal data protection. Comparing these two systems can provide clearer insights into China's regulatory challenges: The EU, centered on the GDPR, has established a stringent and complex cross-border framework through adequacy decisions, standard contractual clauses (SCCs), and binding corporate rules (BCRs). While it lacks specific financial data rules, its overall requirements are exceptionally high. The U. S. adopts a sectoral legislation and industry self-regulation model. In finance, laws like the Gramm-Leach-Bliley Act provide specific rules, while free trade agreements are leveraged to dismantle barriers, facilitate data flows, and attract data to the U. S. To address the difficulties in cross-border personal financial data flows, the following pathways can be explored: Firstly, shift regulatory philosophy from prohibited in principle to permitted in principle, recognizing the value of data as a factor of production and the global nature of cross-border flows while maintaining security baselines. Secondly, harmonize regulatory oversight, enhancing interdepartmental coordination to eliminate rule conflicts and gaps, ensuring coverage of emerging financial institutions. Thirdly, align data classification with cross-border rules, setting differentiated transfer conditions and assessment requirements based on data sensitivity or criticality. Fourthly, differentiate rules by flow purpose: refining necessity standards for business-driven flows, establishing efficient security assessment procedures, and negotiating mutual recognition mechanisms and standard contracts based on reciprocity. Ultimately, through these measures, contract law, organizational law, and regulatory frameworks can be coordinated to construct a governance system that safeguards security and sovereignty while promoting financial market internationalization, unlocking data value, and strengthening influence in global rule-making.

Key words: personal financial data; cross-border flows; GDPR; Privacy Shield Framework; data sovereignty

(责任编辑 刘 琦)