数字时代金融数据跨境流动的风险与规制研究

彭德雷　张子琳

（华东理工大学，上海 200237）

摘　要：数字时代经济和社会发展对金融数据跨境流动提出新要求。金融数据是金融信息的重要载体，由于金融数据的敏感性，其跨境流动涉及公民个人隐私、金融机构自身利益乃至国家金融安全。在实践中，如果对金融数据跨境流动缺乏有效规制，不仅难以发掘金融数据的潜在价值，而且还将引发各类风险。当前，美欧针对金融数据跨境流动采取不同的规制模式。美国对金融数据跨境流动的限制日趋宽松；欧盟对金融数据跨境流动规制主要以《一般数据保护条例》（GDPR）为框架，更加强调保护个人权利。为应对金融数据跨境流动风险，我国有必要进一步完善金融数据跨境流动的规制措施，形成金融数据跨境流动分级监管的规制思路。与此同时，加强对个人金融信息的保护和金融机构自身数据合规体系建设，积极开展双边及多边合作，有效利用金融数据的价值。

关键词：金融数据；跨境流动；风险规制

中图分类号：F113　　**文献标识码：**A　　**文章编号：**1006-1894（2022）01-0014-12

由于互联网的快速发展，数据流动将进一步催生跨境金融服务的创新以及服务效率的提高，但同时也给金融数据跨境流动规制带来挑战。《区域全面经济伙伴关系协定》（RCEP）服务贸易章节附件一《金融服务》特别对金融数据跨境流动进行了规范，进一步凸显金融数据跨境流动议题研究的重要性。和其他数据不同，金融数据更为敏感，一旦发生数据泄露，可能直接关系到国家安全、国计民生以及公共利益。

当前，我国正在积极开展数据跨境流动的安全评估，以确保数据跨境安全有序流动。完全限制金融数据跨境流动显然有悖于全球数字经济发展，但是鉴于金融数据的重要性与特殊性，各国都十分谨慎对待金融数据跨境流动。当前各类跨国经营活动对跨境金融服务的依赖性增强，金融数据跨境流动是实现跨境金融服务的重要环节，与此同时，金融数据跨境流动存在哪些风险？如何实施有效规制？这些问题值得关注。

作者简介：彭德雷，华东理工大学法学院院长、副教授，研究方向：国际贸易及相关法律制度；张子琳，华东理工大学商学院硕士研究生，研究方向：国际贸易与国际投资。

基金项目：国家社会科学基金项目“数字贸易框架下跨境数据流动的国家规制与国际治理研究”（项目编号：19CFX083）；上海市教育法学人才项目（项目编号：2020JYFXR041）；上海市浦江人才项目（项目编号：PJ20190002076）。

一、金融数据跨境流动风险

金融数据包括个人金融数据、企业金融数据以及金融机构运营的业务数据。金融数据在进行数据传输、存储与处理过程中发生的数据泄露和非法与第三方共享数据等行为必然会威胁个人隐私、金融机构自身利益和国家金融安全。

（一）个人隐私泄露风险

相对于普通数据，金融数据涉及的信息更加敏感。2020 年发布的《个人金融信息保护技术规范》将个人金融信息按照敏感程度从高到低划分为 C3、C2 和 C1 等 3 个类别。[①] C3 是指用户鉴别信息，该信息泄露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；C2 是指可识别个人金融信息主体身份或金融状况的信息，该信息泄露会对个人金融信息主体的信息安全与财产安全造成一定危害；C1 是指金融机构内部使用的个人金融信息，该信息泄露会对个人金融信息主体的信息安全与财产安全造成一定影响。值得注意的是，两种或多种低敏感信息在大数据技术的支持下，也可能变成高敏感数据。由此可见，无论是高敏感个人金融数据还是低敏感个人金融数据，都关系到个人资信、信息安全与交易安全。个人金融隐私是公民自由决定哪些金融信息可以被其他人了解的一种权利。公民的金融信息如果在未经授权的情况下遭到查看或者变更，则该公民的金融隐私权将受到侵犯。因此，个人金融数据与个人金融隐私息息相关。

近年来，金融领域数据安全事件频发，个人金融隐私一直是美国和欧盟在规制数据跨境流动时考虑的重要问题之一。2019 年 7 月，美国第七大商业银行第一资本金融公司遭到黑客攻击，导致约 1 亿美国人和 600 万加拿大人的个人信息被窃取。2019 年 8 月，保加利亚第二大银行 DSK 因数据泄露事件被处罚，泄露的数据包括 33,000 个银行客户的姓名、国籍、地址、身份证副本、生物识别数据及关联的第三方（包括配偶、子女和担保人）等个人信息。金融服务与每个人的生活息息相关，一旦发生数据泄露事件，就会暴露大量的个人隐私。当前，金融服务的跨国性特征明显，各国在金融数据跨境流动中如何保障个人隐私安全成为亟待解决的问题。

个人金融隐私泄露的风险受到不同因素的影响。一方面，互联网技术快速发展使隐私泄露变得更加容易。互联网信息技术发展极大地便捷了金融消费者，但是，由于金融机构线上系统的固有缺陷，一旦被不法分子攻破，就会造成金融数据泄露风险。例如，第一资本金融公司在数据被窃取后发表声明，数据泄露是由于系统基础架构的配置漏洞受到攻击。另一方面，各国对金融数据的保护程度也影响个人金融数据安全。例如，目前欧盟签署的一些区域协定兼顾了个人隐私保护和数据跨境流动的平衡。

① 根据《个人金融信息保护技术规范》（2020年）第4.2条，C3类别的信息主要包括银行卡磁道数据、卡片验证码和各种交易密码等；C2类别的信息主要包括账户信息、个人财产信息和交易信息等；C1类别的信息主要包括账户开立时间和开设机构等。

如果缔约双方签订的协议中没有保护个人隐私的具体措施，便只能依赖于数据存储国已有的金融数据保护措施。如果数据存储国没有完善的数据保护体系，则进一步加大了个人金融隐私泄露风险。

（二）金融机构运营风险

金融机构的客户主要包括个人和企业，其收集的金融数据包括个人金融数据、企业金融数据以及金融机构运营的业务数据。[①]在金融机构运营过程中，保护金融数据安全是金融机构的义务，金融数据一旦在跨境流动中发生泄露、篡改、销毁，则可能引发一系列运营风险，包括引发相应的法律纠纷以及遭受行政处罚等。

当前，虽然各国越来越重视金融数据，不断完善相关立法，但因数据泄露而遭受处罚的案例并不鲜见。例如，2020 年中国人民银行对部分金融机构侵害消费者金融信息安全行为进行了立案调查，对中国农业银行吉林市江北支行等 6 家金融机构作出行政处罚决定，最高处罚金额高达 1,406 万。随着各国金融数据跨境流动规制措施的完善，金融机构的违规行为必然会受到处罚。

此外，金融机构还可能因与非关联第三方共享消费者信息而遭到罚款。例如，某跨国金融机构母公司（下称“A 公司”）所在国家的金融隐私保护相关法规不完善，而其开设的海外分支机构（下称“B 机构”）所在国金融隐私保护相关法规较为完善。出于规避风险、获取最大化利益等目的，A 公司在母国可能会过多收集消费者信息并共享给非关联第三方。由于 A 公司所在国金融隐私保护法规并不完善，A 公司可能会免受处罚；但是，当 B 机构使用同样的方式过多地收集消费者信息并分享给非关联第三方时，[②]B 机构可能会因此受到当地监管部门的处罚。因此，在金融数据跨境流动中，如果金融机构忽视数据监管的地区差异，将存在一定的违规风险。

此外，金融机构运营风险还包括技术管理风险和资产管理风险。[③]在技术管理方面，如果跨国金融机构使用境外数据中心或者云平台，很容易成为黑客的攻击目标，黑客会利用系统漏洞窃取或者篡改客户的金融数据。在资产管理方面，出于监管目的，境外监管机构要求跨境金融机构的境外分支机构披露商业数据，如果监管机构不能对披露的金融数据进行周密的保护，则会加大金融机构的运营风险。

（三）国家金融安全风险

金融安全直接关系到国家安全。维护金融安全的目标在于一国金融利益不受侵犯、金融体系正常运转以及国家主权不受到破坏和威胁，而金融数据在国家利益与国家安全中扮演着重要角色。2018 年，美国颁布《外国投资风险审查现代化法案》

① 苏海雨.金融科技背景下金融数据监管模式构建[J]. 科技与法律，2020,(1).
② 美国《格雷姆—里奇—比利雷法案》(GLBA,1999)已经对金融机构与非关联第三方共享非公开个人信息作出规定。参见：GLBA，§ 502 (a),(d)。
③ 王娟娟, 汪海. 充分重视数据跨境流动的风险[N]. 经济日报，2019–05–15.

（FIRRMA），扩大了美国外国投资委员会（CFIUS）的权限，将收集美国公民敏感数据的任何非控制性投资（noncontrolling investment）纳入国家安全审查范围。[①] CFIUS 曾以国家安全为由否决蚂蚁金服收购速汇金，美国监管部门认为中国资本介入美国金融领域可能会导致国家安全问题。尽管速汇金承诺，即便被蚂蚁金服收购之后，服务器与数据仍存放在美国境内，美国公民敏感数据不会被任何政府滥用或访问，但 CFIUS 依然反对本次收购。金融领域的企业海外投资和并购成功后，在后续国际经营实践中必然涉及金融数据跨境流动。一旦发生数据泄露，可能会直接威胁到金融安全与国家安全。金融数据也关系到国家核心信息安全，比如，通过互联网金融和消费掌握的人流、物流和资金流在为国家治理提供大数据支持的同时，也成为国家核心信息安全的重大隐患。为了保证数据安全，德国要求数据本地化存储或处理以维护国家安全。德国联邦政府通过的《联邦政府信息技术委员会第 2015/5 号决议》（Resolution 2015/5 of the Federal Governments IT Council）规定，敏感信息（包括政府机密和基础设施信息）必须存储在德国境内的服务器上。此外，云计算和软件服务的所有供应商必须保证此类信息不会在美国等外国司法管辖区受到任何披露义务的约束。

同时，金融机构对金融数据的保护也一直受到挑战，影响了金融体系稳定。金融机构掌握了海量的金融数据，这些数据蕴藏着巨大的经济价值，往往成为黑客的主要攻击目标。上文提到的第一资本金融公司发生的数据泄露就是被黑客攻击所致。2018 年 5 月，加拿大蒙特利尔银行和帝国商业银行也被网络黑客攻击。俄罗斯中央银行发布消息称，俄罗斯银行业 2018 年 1~8 月因网络攻击损失了 7,650 万卢布。[②] 海量的金融数据一旦泄露，将对金融体系造成打击，直接或间接威胁到国家安全。

二、美欧金融数据跨境流动规制模式

（一）美国金融数据跨境流动规制模式

美国主要致力于将金融数据跨境流动纳入双边和区域贸易协定中。美国 1992 年签订的《北美自由贸易协定》（NAFTA）第 14 章第 7 条规定，在金融机构的正常业务过程中进行数据处理，一方应允许另一方的金融机构以电子或其他形式将信息转入或转出该方领土。2003 年，美国与新加坡签订的《美新自由贸易协定》规定，应任何一方要求，金融服务委员会应当审议金融机构在正常业务过程中数据加工涉及的信息传输、个人数据加工和传播中的个人隐私保护。由此可以看出，美国较早开始关注金融数据跨境流动。

① Congressional Research Service, The Committee on Foreign Investment in the United States (CFIUS), February 14, 2020, p.2.
② 郝亚娟,张荣旺.汇丰银行数据泄露 金融信息安全亟须升级[EB/OL]. https://tech.sina.com.cn/it/2018-11-18/doc-ihmutuec1241486.shtml?source=cj&dv=1. (2020-04-10).

2012 年，美国与韩国签订的《美韩自由贸易协定》在附件中纳入金融数据跨境流动条款。该附件规定，出于金融机构正常的业务需要，双方应该允许以电子形式或其他形式将信息进行跨境流动，韩国应在两年内履行承诺。相比于《美新自由贸易协定》，《美韩自由贸易协定》的金融数据跨境流动条款更有开放性。值得注意的是，《美韩自由贸易协定》在电子商务章节指出了数据流动的重要性，这也表明美国此时已经重视数据自由流动带来的价值，为此后进一步推动金融数据跨境流动埋下伏笔。2015 年，美国主导的《跨太平洋伙伴关系协定》（TPP）在金融数据跨境流动方面也作出规定，即缔约方应允许金融数据跨境流动以满足金融机构日常经营需要，同时该条款不限制缔约方保护个人隐私的权利，但是出于审慎考虑，缔约方可以要求该金融机构事先获得监管机构的许可以及指定特定金融机构接收数据。[①]可见，美国金融数据跨境流动规制的影响范围通过 TPP 进一步扩大。

2018 年，《美墨加协定》（USMCA）继续对金融数据跨境流动作出要求。USMCA 第 17.17 条规定，任何一方不得阻止涵盖主体（covered person）以电子或其他方式将信息（包括个人信息）转进或转出该缔约方领土，当这项活动是在涵盖主体的许可、授权或登记范围内进行业务时；本条的任何规定都不限制缔约方为了保护个人数据、个人隐私、个人记录和账户采取保密措施的权利，但这些措施不得用于规避本条。相比于 TPP，USMCA 在以下几个方面做了改变，使其更具开放性。第一，USMCA 扩大了金融服务提供商的范围。USMCA 将 TPP 中的金融机构变更为涵盖主体。根据 USMCA 金融服务章节的定义，涵盖主体不仅包括金融机构，还包括接受该缔约方金融监管机构监管、监督、许可、授权或注册的跨境金融服务提供商。第二，USMCA 扩大了金融数据涵盖范围。USMCA 将可进行跨境流动的金融数据范围从满足日常经营的金融数据扩大为进行许可、授权或登记业务时的金融数据。第三，出于审慎考虑，TPP 规定缔约方可以要求该金融机构事先获得监管机构的许可以及指定特定金融机构接收数据，USMCA 删去这一条款，进一步提高金融数据跨境流动的自由度。此外，TPP 电子商务章节中数据跨境流动的“监管例外”和“公共安全例外”[②]对金融数据跨境流动做了相应的限制，美国则在 USMCA 中剔除了这些限制金融数据跨境自由流动的条款，进一步释放金融数据的经济价值。

从上述分析看，美国金融数据跨境流动规制模式逐渐趋向自由化，原因在于金融数据跨境顺畅流动对美国经济和金融部门至关重要。[③]美国在今后的自贸协定中仍将致力于推动金融数据跨境自由流动。

① TPP Annex11-B Section B: Transfer of Information.
② TPP Article 14.11: Cross-border Transfer of Information by Electronic Means.
③ Internet Association. Modernizing NAFTA for Today's Economy[EB/OL]. https://internetassociation.org/wp-content/uploads/2017/06/Modernizing-NAFTA-White-Paper.pdf.

（二）欧盟金融数据跨境流动规制模式

在历史传统影响下，与经济发展相比，欧盟更强调保护个人数据权利，认为不能以牺牲公民隐私权为代价促进经济发展，因此，欧盟在数据跨境流动规制方面把保护个人权利作为首要原则。1995 年，欧盟制定《关于个人数据处理保护与自由流动指令（95/46/EC）》（以下简称《95 指令》），[①]设立欧洲数据保护监督员（European Data Protection Supervisor，EDPS）；[②]2018 年，欧盟实施《一般数据保护条例》（GDPR），都体现了欧盟十分重视个人数据权利，这种基于个人权利优先的理念使得欧盟对数据跨境流动规制显得十分谨慎。

欧盟金融数据跨境流动规制模式主要表现在两个方面。第一，欧盟内部法案涉及金融数据跨境流动规制。目前，欧盟数字监管政策主要涵盖 GDPR、《欧盟非个人数据自由流动条例》《欧盟电子隐私保护条例》和《欧盟电子身份框架》等。对个人金融数据的跨境流动规制，欧盟仍以 GDPR 的个人数据保护规则为主。根据 2019 年度《GDPR 执法案例精选白皮书》，自 GDPR 生效以来，欧盟已经对超过 22 个国家和地区作出处罚，其中有 6 起就发生在金融领域。这些处罚多与个人金融数据相关，充分体现 GDPR 对个人权利保护的重视。欧盟内非个人电子数据处理则遵循《欧盟非个人数据自由流动条例》（2019 年 5 月正式生效）。[③]2015 年 11 月通过的《关于内部市场的支付服务指令（第 2015/2366 号）》放松了对数据处理的限制，在银行客户明确授权同意的前提下，第三方支付服务商可以通过银行访问其客户信息。显然，这种客户知情同意的前提只适用于访问小规模数据。第二，欧盟签署的自贸协定涉及金融数据跨境流动规制。无论是《欧盟—智利自贸协定》（2005），还是《欧盟—韩国自贸协定》（2015）、《欧盟—加拿大自贸协定》（2016）、《欧盟—新加坡自贸协定》（2019）、《欧盟—日本经济伙伴关系协定》（2019）以及《欧盟—越南自贸协定》（2020），在金融数据跨境流动条款中均包含两个内容：金融机构日常经营数据可跨境流动；缔约方需保护个人隐私。[④]欧盟希望在保障个人隐私的前提下实现金融数据跨境自由流动。对于涉及个人隐私的金融数据，欧盟希望给予充分保护；对于不涉及个人隐私的金融数据，根据《欧盟非个人数据自由流动条例》的相关规定，其限制性相对较少。[⑤]

---

① 《95指令》于2018年5月25日被GDPR取代。

② European Commission. European Data Protection Supervisor Annual Report 2018[EB/OL]. https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf. (2020–04–03).

③ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non–personal Data in the European Union。该条例第4条规定："数据本地化要求应予禁止，除非根据比例原则以公共安全为正当事由。"

④ 《欧盟—日本经济伙伴关系协定》（Agreement between EU and Japan for An Economic Partnership）第8章规定，缔约方不得采取措施阻止金融机构日常经营数据进行跨境流动；任何一个缔约方对个人隐私和个人数据的保护均不受到金融数据跨境流动的影响。Agreement between EU and Japan for An Economic Partnership: Article 8.63, Transfers of Information and Processing of Information[EB/OL]. http://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf#page=185.(2020–08–13).

⑤ 该条例序言规定："为确保有效适用非个人数据跨境自由流动原则，防止出现损害内部市场顺利运作的新障碍，成员国应当立即向欧盟委员会通报任何引入新的数据本地化要求或修改现有数据本地化要求的法令草案。"

总体来看，欧盟对待金融数据跨境流动呈现与美国不同的规制思路。第一，规制理念不同。欧盟着重强调个人隐私保护。无论是 GDPR 还是欧洲银行业监管，抑或是欧盟对外签署的自由贸易协定，均着重强调保护个人隐私。美国以促进数字跨国企业和数字贸易发展作为出发点，支持数据跨境自由流动，以降低数字贸易壁垒。第二，规制方式不同。欧盟对个人金融数据跨境流动的规制主要通过以 GDPR 为主导的欧盟内部法案进行，[①]呈现出“外严内松”的特征，对非个人金融数据的规制，则遵循《欧盟非个人数据自由流动条例》的基本规范。美国通过与他国签署贸易协定推动金融数据跨境流动监管。美国的“对外扩张”与欧盟的“含蓄内敛”形成鲜明对比，二者的规制理念和思路存在较大差异。[②]

三、我国应对金融数据跨境流动风险的规制措施

随着人民币国际化的不断深入，我国金融行业与国外金融行业交流日益密切，市场对人民币跨境信贷融资的需求必然更加旺盛；同时，中资金融机构在境外开展业务也需要进行数据跨境流动。但数字时代使得洗钱、逃避监管等灰色交易有机可乘，一些不法分子很容易利用各国之间信息不对称而逃脱监管。由此可见，如何防范金融数据跨境流动风险，同时兼顾金融机构业务效率、有效利用金融数据价值是我国需要关注的问题。

（一）确保金融数据跨境流动有法可依

首先，关于国家层面的数据安全立法 近年来我国对数据安全极为重视。2015 年《国家安全法》第 25 条要求加强保护重要领域的信息系统和数据安全。2016 年《网络安全法》第 37 条规定，关键信息基础设施的运营者收集的关键数据应当在境内存储，因业务需要确需向境外提供的，应当进行安全评估，明确了数据跨境流动的原则与条件，为以后的数据跨境流动规制奠定基调。2020 年 4 月发布的《网络安全审查办法》将安全审查进一步细化，第 9 条明确了可能威胁国家安全的因素，其中包括重要数据被窃取、泄露和毁损。2021 年 11 月，《个人信息保护法》正式实施，要求跨境流动的个人信息应当具备以下条件之一：通过安全评估、进行个人信息保护认证或者签订国家网信部门制定的标准合同。上述立法为后续规制金融数据跨境流动提供了制度依据。从国家层面的立法可以看出，我国的跨境数据规制思路整体上呈现出平衡数据安全保护与利用数据价值的特点，这种特点在金融数据跨境流动规制上也得到了体现。

① 根据GDPR第4条对“个人数据”的定义，其是指一个被识别或可识别的自然人（数据主体）的任何信息。

② 有学者认为，美国、欧盟和中国对待数字贸易的规制理念分别体现为自由主义、规制主义和重商主义，这一点也在金融数据跨境流动规制上得以体现。参见：Jonathan, E. H.The Global Battle for Digital Trade the United States, European Union, and China Back Competing Rules[EB/OL]. 2018, csis.https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/global-battle-digital-trade. (2020-04-28)。

其次，关于金融数据跨境流动规制的部门规章　中国银行业监督委员会2006年发布的《电子银行业务管理办法》第60条明确了外资金融机构向境外总行（公司）转移数据的前提，即因业务需要、保障客户的合法权益和遵守有关数据转移规定。中国人民银行也出台了一系列相关规定。2011年1月发布的《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的通知》（银发[2011]17号）第6条明确禁止金融数据跨境流动。2012年，中国人民银行印发《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071—2012），为了保护金融数据安全，将金融数据分为一般数据和敏感数据。2016年发布的《中国人民银行金融消费者权益保护实施办法》（银发[2016]314号）放宽了对金融数据跨境流动的限制，第33条规定境内金融机构在经过当事人授权、符合相关规定后可向境外传输相关个人金融信息。这一规制思路与《网络安全法》逐渐统一，表明我国逐步放松对金融数据跨境流动的限制，发掘金融数据的经济价值。2018年中国银行保险监督管理委员会（下称“银保监会”）发布《银行业金融机构数据治理指引》（银保监发[2018]22号），要求银行业金融机构划分数据安全等级、加强数据管理。中国人民银行在2020年2月和9月分别印发《个人金融信息保护技术规范》（下称《规范》）和《金融数据安全 数据安全分级指南》（下称《指南》），依照信息敏感度对金融数据进行分级。《规范》根据个人金融数据敏感程度分为C3、C2和C1等3个等级，并明确了收集、存储和使用的具体安全准则。在此基础上，《指南》根据金融业机构数据安全性遭到破坏后的影响对象和影响程度将金融数据分为5级，在《规范》划分的3个等级的基础上增加了最高等级的重要数据和可被公众得知的数据（即《指南》中的1级数据），《规范》中的C3、C2和C1分别对应4级数据、3级数据和2级数据。《指南》将分级涵盖范围从个人金融数据扩大为金融业机构数据，细化金融数据分级操作，进一步提高金融数据分级监管的可操作性。但是在具体实践中仍然可能存在一些问题，例如《规范》和《指南》对于两种或两种以上的低敏感金融数据组合能够产生高敏感金融数据这一情况并未进行详尽描述。事实上，这种较为隐蔽的措施可能加大产生风险的概率。此外，《规范》和《指南》对数据分级缺乏一定的灵活性，因为可能存在低敏感数据在另外一个场景中敏感程度会发生显著变化这一情况，关于数据特征的一般描述等在后续实践中还可进一步细化。在地方层面，某些地方政府也对金融数据跨境流动进行了有益的探索。2020年11月5号发布的《上海市全面深化服务贸易创新发展试点实施方案》试行允许符合条件的外资金融机构因集团化管理而涉及其在境内控股金融机构向境外报送有关数据，特别是涉及内部管理和风险控制类数据。

（二）实行金融数据跨境流动分级监管

事实上，全面禁止金融数据跨境流动会降低金融服务效率，也不符合现实发展需要。我国签署的RCEP服务贸易章节附件一《金融服务》规定各缔约方不得限制

以日常经营为目的的金融数据跨境流动，这一规定为我国应对金融数据跨境流动风险提供了指引。目前对金融数据跨境流动的需求可以分为两类：第一类是金融机构因日常经营所需的金融数据跨境流动，即商业目的；[①]第二类是国外监管机构要求金融机构披露金融信息，即监管目的。[②]虽然分级监管不能完全排除所有风险，但是参照国内金融数据保护模式，对金融数据进行分类分级规制措施，以应对金融数据跨境流动风险，这种做法仍然值得借鉴。[③]

首先，基于商业目的的金融数据跨境流动规制 出于商业目的的金融数据跨境流动，以数据级别作为判断是否可以出境的依据。[④]对这一规制思路可以参考 2021 年 10 月工信部发布的《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》相关要求，即将数据按照对国家安全和社会公共利益的危害程度分为一般数据、重要数据以及核心数据。其中，核心数据不得出境，重要数据需要进行数据出境安全评估。金融数据跨境流动规制可以在《指南》将金融数据分为 5 个等级的基础上区别对待。例如，4 级和 5 级数据在安全性遭到破坏后会对个人和企业权益造成十分严重的危害，对公众权益也会造成较大影响，其中 5 级数据的安全更是直接关系到国家安全，因此，对这两个等级的数据跨境流动请求应予以限制，1 级、2 级和 3 级数据应进行数据跨境安全评估。

同时，对基于商业目的的金融数据跨境流动应当设置例外情况，在安全评估之后决定是否允许跨境流动。例外情况可能包括以下几种情形：第一，是否传输量级巨大的金融数据。《规范》指出，量级巨大的低级别金融数据经过大数据技术处理可能分析出级别较高的金融信息，从而产生风险。第二，是否出于逃避监管的目的。由于各国金融信息保护政策存在较大差异，金融机构可能出于规避监管的目的进行金融数据跨境流动。第三，金融数据跨境流动的接收国家是否有保护金融数据的能力。以欧盟为例，GDPR 第 45 条明确了“第三国法律规则”是评估保护水平充分性的首要条件，如果第三国个人金融数据的相关立法不够完善，开设在欧盟境内的金融分支机构则不能将数据传输到第三国境内。

其次，基于监管目的的金融数据跨境流动规制 如果一国出于监管目的要求他国金融机构披露金融信息，可能会存在威胁他国数据主权的风险。美国微软案从侧面

① 目前有美国、英国、中国香港和中国澳门等43个国家和地区允许金融机构基于日常商业经营目的向集团总部传输数据。参见: 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)。

② 例如，美国微软案中，美国司法部要求微软披露存储在爱尔兰境内的数据以进行毒品调查。从该案件可以看出，出于监管目的的数据跨境流动确实存在，而金融数据涵盖范围较为广泛，很可能在今后被用于监管以打击跨国犯罪。Supreme Court of the United States: United States, Petitioner v. Microsoft Corporation[EB/OL]. No. 17–2, April 17, 2018. https://www.supremecourt.gov/opinions/17pdf/17–2_1824.pdf.(2020–04–29)。《美日数字贸易协定》也规定，只要一缔约方的金融监管当局出于监管监督目的，可以立刻直接获取存储在另一缔约方境内的金融数据。

③ 《个人信息出境安全评估办法（征求意见稿）》中对个人信息出境安全的评估需要考虑信息的数量和敏感程度。

④ 1 级数据可以被公众得知，如单位基本情况、法人姓名等。2 级数据包括个人行为信息（如发生业务关系时的行为数据等）、单位股东信息和联系信息等。3 级数据是指个人标签信息（如家庭关系等）、单位管理层信息（如年龄、姓名、联系方式）等。4 级数据包括个人健康医疗数据、传统鉴别信息（支付密码、U盾、交易密码等）、指纹、虹膜等个人信息与非个人信息。5 级数据是指一经破坏，对国家安全与公众权益造成十分严重损害的数据。

反映出这一风险。2013 年 12 月，因一起毒品案件的调查，美国联邦检察官获得授权书要求微软披露其客户账户相关的所有电子邮件和其他信息，但是因为信息存储在爱尔兰境内，微软认为这份授权不能在域外使用。[①]2016 年，美国联邦第二巡回上诉法院裁定司法部的搜查令无效，理由是通过美国国内法院授权的搜查令获取爱尔兰境内存储的数据违反了爱尔兰的数据保护法。[②]爱尔兰政府也认为这将会侵犯欧盟数据保护指令和爱尔兰数据隐私法，侵犯爱尔兰的数据主权。随着跨境金融的快速发展，出于打击金融犯罪的需要，我国需要与他国开展金融监管合作，在签署双边或多边区域贸易协定时，可考虑设计数据跨境流动监管合作的相关条款。

（三）不断完善个人金融数据保护体系

欧盟 GDPR 构建了颇为严格的个人信息保护机制，对我国个人金融数据保护具有重要的借鉴意义。金融机构一旦贸然将数据传输到第三国，则可能面临被惩罚的风险。加强国内对个人金融数据的保护，对接世界高水平的个人金融数据保护对规范金融机构自身行为、保护个人金融隐私也十分重要。目前，我国对个人金融数据的保护多散见于不同的法律法规中，如《商业银行法》《征信业管理条例》《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的通知》等。对个人金融数据保护的现有规范系统在法律层面上难以适应现实发展需要，也造成了部分金融机构过度收集消费者信息、与非关联第三方共享甚至售卖个人金融数据。2021 年 11 月 1 日正式施行的《个人信息保护法》成为个人信息保护领域的基本法，个人信息保护制度更趋完善。RCEP 服务贸易章节附件一《金融服务》第 9 条规定：“任何规定不限制一缔约方保护个人数据、个人隐私以及个人记录和账户机密性的权利”，这实际上也为各国进行国内立法以保护个人金融隐私提供了规制空间。此外，金融监管部门还需要不断完善消费者救济机制，公开相关救济程序，在推动相关立法基础上，完善监管部门对个人金融数据的监管，为消费者隐私受到侵犯后提供及时救济。

（四）加强金融机构自身数据合规体系建设与国际合作

目前，国内金融机构日益重视数据保护和管理。但是，随着金融服务的国际化发展和主要国家数据保护标准的推出，我国金融机构需要考虑如何对接境外金融数据保护标准，确保数据跨境流动合规。在欧盟 GDPR 实施后，我国目前并不满足欧盟“充分认定”的标准，未被列入欧盟跨境数据流动的“白名单”，从而无法将在欧盟境内采集的数据传输回国内。此外，一些合法的传输机制如“有约束力的公司规则”程序复杂，申请需要耗费较长时间。[③]这些在欧盟市场遇到的问题也将会在其他效仿欧

① Supreme Court of the United States: United States, Petitioner v. Microsoft Corporation[EB/OL]. No. 17~2, April 17, 2018. https://www.supremecourt.gov/opinions/17pdf/17–2_1824.pdf. (2020–04–29).

② Brier, Thomas F. Jr. Defining the Limits of Governmental Access to Personal Data Stored in the Cloud, An Analysis and Critique of Microsoft Ireland[J]. Journal of Information Policy, 2017, (7).

③ 京东法律研究院.一般数据保护条例(GDPR)评述及实务指引[M]. 北京: 法律出版社, 2018:119.

盟建立数据跨境流动机制的国家出现，我国金融机构需要提前做好合规路径储备。[①] 对于数据合规管理，金融机构可以参照 GDPR 提出的设置数据保护官这一做法，完善数据保护合规体系。[②]

与此同时，我国还应加强金融数据跨境流动规制合作。如果国际上没有统一的数据跨境流动规制或者双边合作，仅仅依靠各国单方面的数据规制，本国想要监管存储在他国境内的数据，必然会侵犯他国的数据保护法。我国将数据存储在国外需要依靠数据存储国对个人金融数据的保护，而且我国难以监管，不利于充分发挥金融数据的价值。我国可以积极寻求与存在共识的国家开展双边和区域合作。RCEP 在金融领域达成的关于“信息转移与信息处理”的规定，就是很好的国际合作达成规则共识的范例。随着今后金融数据跨境流动的日趋频繁，我国可继续加强双边和区域间的数据流动规制合作，充分发挥金融数据价值，确保金融数据跨境流动安全有序。

四、结语

由于金融数据的重要性与特殊性，金融数据进行跨境流动时容易产生威胁个人隐私、金融机构安全以及国家金融安全的风险。如何挖掘金融数据跨境流动的经济价值并防范上述风险已引起各国广泛关注。针对金融数据跨境流动规制，目前主要有两种导向：一种是美国通过签订双边自由贸易协定，将金融数据跨境流动纳入其中，偏向商业自由；另一种是欧盟制定的“充分认定原则”，对金融数据跨境流动给予较为严格的限制。我国对于如何有效规范金融数据跨境流动的需求较为迫切，原因在于我国互联网金融市场规模庞大，产生的金融数据量级巨大，与国外金融行业的交流日益密切，尤其是在“一带一路”建设和人民币国际化的背景下，人民币地位将不断上升，金融数据跨境流动也更加频繁。

因此，对我国而言，一方面，应不断完善金融数据国内规制和保护措施，防止国内金融数据在跨境流动时发生泄露。另一方面，我国海外金融机构应该遵守当地的数据保护政策，确保向境内传输数据时符合当地要求；国内金融机构在收集、接收相关数据时也需要做好相应的数据保护工作。总之，跨境金融服务应在确保金融数据安全前提下提高其使用价值。为此，评估金融数据跨境流动中的各类风险，考察主要国家金融数据跨境流动的规制模式，对我国应对金融数据流动风险、发掘金融数据价值以及参与国际数字规则制定等都具有重要意义。

参考文献：

[1] 荼洪旺 , 付伟 , 郑婷婷 . 数据跨境流动政策的国际比较与反思 [J]. 电子政务 , 2019,(5).

① 王融.数据跨境流动政策认知与建议[J]. 信息安全与通信保密, 2018,(3).

② 设置数据保护官可以使金融机构保护数据更加专业、对接境外标准更加准确，降低侵权风险，减轻监管机构负担，提高数据控制者的竞争力。参见: 肖冬梅, 成思雯. 欧盟数据保护官制度研究[J]. 图书情报工作, 2019,(2)。

[2] 陈咏梅 , 张姣 . 跨境数据流动国际规制新发展 : 困境与前路 [J]. 上海对外经贸大学学报 , 2017,(6).
[3] 何德旭 , 史晓琳 . 互联网时代的金融风险及其防范措施研究 [J]. 中国社会科学院研究生院学报 , 2018,(2).
[4] 胡炜 . 跨境数据流动立法的价值取向与我国选择 [J]. 社会科学 2018,(4).
[5] 黎四奇 , 苗羽亭 . 大数据背景下金融隐私权的保护 [J]. 财经理论与实践 , 2019,(4).
[6] 李晓安 . 开放与安全 : 金融安全审查机制创新路径选择 [J]. 法学杂志 , 2020,(3).
[7] 时吴华 . 金融国策论 [M]. 北京 : 社会科学文献出版社 , 2015.
[8] 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).
[9] 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).
[10] 张可法 . 个人金融信息私法保护的困境与出路 [J]. 西北民族大学学报 (哲学社会科学版), 2019,(2).
[11] 张郁安 . 欧盟非个人数据流动监管新进展 [N]. 人民邮电 , 2019-10-11.
[12] 周念利 , 陈寰琦 . 基于《美墨加协定》分析数字贸易规则“美式模板”的深化及扩展 [J]. 国际贸易问题 , 2019,(9).
[13] Meltzer, Joshua Paul. The Internet, Cross-border Data Flows and International Trade[J]. Asia and the Pacific Policy Studies, 2015,(2).
[14] Sharman, J. C. Privacy as Roguery: Personal Financial Information in an Age of Transparency[J]. Public Administration, 2009,(87).

Research on the Risk and Regulation of Cross-border Flow of Financial Data in Digital Age

PENG Delei　ZHANG Zilin

Abstract: In the digital age, economic and social development has put forward new requirements for the cross-border flow of financial data. Financial data is the carrier of financial information, and it is related to personal privacy, financial institutions' own interests, financial security, and even national security. In practice, if there is a lack of effective regulations on the cross-border flow of financial data, it will not only be difficult to discover the potential value of financial data, but will also cause various risks. Currently, the United States and Europe have adopted different regulatory models for cross-border flows of financial data. The United States has increasingly relaxed restrictions on the cross-border flow of financial data; the EU's regulation of cross-border flows of financial data is based on the GDPR and more emphasis on the protection of individual rights. In order to cope with the risk of cross-border flow of financial data, it is necessary for China to further improve the regulatory measures for the cross-border flow of financial data, and form a regulatory approach for the classification and supervision of cross-border flows of financial data. At the same time, it is necessary to strengthen the protection of personal financial information, actively carry out bilateral and multilateral cooperation, and effectively utilize the value of financial data.

Keywords: financial data; cross-border flow; risk regulation

（责任编辑：梁丽华）