财经法学 No. 5，2019
pp. 122 - 136

开放银行的制度构造与监管回应

许　可*

内容提要：伴随着金融科技 3.0 与银行 4.0 的迅速迭代，金融机构与金融科技公司合力掀起了开放银行的浪潮。世界各国的经验充分表明：开放银行并非只是企业创新的结果，相反，它始终有赖于国家的有效应对与调适。然而，较诸商业实践的突飞猛进，我国开放银行的法律规则尚付诸阙如。立基于开放银行的技术层、内容层、组织层，以应用程序编程接口、数据共享、网络平台为对象的法律框架得以成型，主体平等监管、助推而非强制、治理科技优位的法律原则得以确立，开放银行发展的风险与阻碍最终有望化解。

关键词：开放银行　数据共享　网络平台　治理科技　大数据

2018 年伊始，一场名为“开放银行”（open banking）的金融变革引爆全球。作为这一概念的引领者，英国开风气之先，包括汇丰银行在内的 9 家机构自 2018 年 1 月 13 日起共享彼此数据，使英国成为首个落地实施开放银行理念的国家。2018 年生效的欧盟《第二代支付服务法令》（Payment Service Directive 2，PSD2），要求银行向第三方机构开放支付接口，以期打造支付领域的全欧盟单一市场。在大西洋的另一边，美国消费者金融保护局（CFPB）2017 年 10 月发布金融数据共享九条指导意见，保障向第三方共享数据时的用户安全。而当我们把目光转到亚太，不论是澳大利亚、新加坡，还是日本或我国香港地区，均相继宣布引入开放银行机制。

在开放银行的浪潮面前，我国亦不甘人后。2018 年 7 月，上海浦东发展银行推出业界首个无界开放银行 API Bank；8 月，中国工商银行提出要打造无所不包的开放银行；9 月，招商银行宣布迭代上线招商银行 App7.0 和掌上生活 App7.0，借此契机开放用户和支付体系，实现金融和生活场景的衔接。在这场商业浪潮中，我们不妨心平气和地问一句：何为开放银行？它又将带来何种法律挑战？基于这一问题，本文将首先解释开放银行的含义和缘起，进而分析其法律架构，并在剖析其风险之后，提出中国的回应之道。

*　许可，对外经济贸易大学法学院助理教授。

一、理解开放银行的兴起

（一）开放银行的层次论

作为一个新兴事物，开放银行尚无权威的定义。咨询公司 Gartner 认为，开放银行是一种开放化的商业模式，通过与第三方开发者、金融科技公司、供应商、用户和其他合作伙伴共享数据、算法、交易、流程和其他业务功能，重构商业生态系统，为银行提供新的价值，增强核心竞争力。〔1〕也有学者指出：开放银行是一种金融服务平台，以用户需求为导向，以场景搭建为载体，通过 API（Application Programming Interface，应用程序编程接口）或 SDK（Software Development Kit，软件开发工具包），在大数据、云计算、物联网等技术支撑下，整合内外部资源，使银行更加便捷、智能、开放。〔2〕显然，上述对开放银行的界定均侧重于经济意义，从法律概念操作性和明晰性出发，本文尝试着从下述三个层面给出描述性定义。

1. 开放银行的技术层：API

开放银行主要由 API 技术驱动。〔3〕所谓 API，即一组标准化的函数设置，用于管理一个应用程序与另一个应用程序进行通讯。简言之，我们可以将 API 理解为双方间的“技术胶水”。供应方将自己特定技术服务以 API 的形式开放给需求方，后者按照参数调用接口，从而使得不同技术基于业务逻辑和数据相互粘合，最终达到数据流通和共享。API 包含着复杂的技术内容：（1）安全、高效、高度兼容的数据传输；（2）精简和快速交互的数据交换；（3）数据访问管理，即通过企业之间的 XML 框架或面向消费者的 OAuth 框架，来决定谁可以访问哪些数据以及如何获取这些数据。〔4〕作为用户与产品的枢纽，API 发挥着“去耦合”和“开放”的作用，它一方面将产品分解为账户、应用和数据，另一方面通过建立广泛的渠道网络，以可扩展和安全的方式提升用户的体验和福祉。

2. 开放银行的内容层：数据共享

开放银行以“数据共享”为本质。〔5〕“银行业务都是由位元和字节所组成的”，〔6〕花旗银行首席执行官约翰·里德的名言充分说明数据在银行业中的重要地位。随着信息技术的发展，金融业务逐步实现了数据集中、业务电子化和数字化，用户数据、交易数据、管理数据、行为数据呈现出爆炸性增长。但是，静态的数据价值有限，只有自由流通和有效共享，才能最大限度地激

〔1〕 See Open Banking: Adoption Increases, but Barriers Challenge Path to Collaborative Openness, available at https://www.gartner.com/en/documents/3869115/open-banking-adoption-increases-but-barriers-challenge-p0, last visited on July 1, 2019.

〔2〕 参见张欢、陆岷峰：《开放银行：历史现状和未来趋势研究》，载《湖南财政经济学院学报》2018 年第 6 期。

〔3〕 尽管开放银行有多种实现路径，但由于 API 支持第三方对他方提供的数据和功能进行安全、可控和低成本的访问，故而被广为接受，以至于开放银行亦称“API 银行”。See Brijesh Sivathanu, An Empirical Study on the Intention to Use Open Banking in India, 32 (3) *IRMJ*, 27 - 47 (2019).

〔4〕 See LendIt Fintech, The State of Open Banking, available at https://blog.lendit.com/whitepaper-state-open-banking/, last visited on July 1, 2019.

〔5〕 See Brodsky, Oakes, Data sharing and open banking, available at https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking, last visited on July 1, 2019.

〔6〕〔美〕克里斯·斯金纳：《互联网银行：数字化新金融时代》，张建敏译，中信出版社 2015 年版，第 35 页。

活数据价值，而这正是开放银行的优势所在。

首先，作为金融机构数字化转型的高级阶段，开放银行以数据为关键生产资料。在大数据时代，立足于海量数据规模和多样数据类型，辅以快速的数据流转和动态的数据体系，数据获得了前所未有的重要性。〔7〕数据的收集、汇聚和流通为金融机构个性化服务和风控模型成熟奠定基础，降低金融服务成本、促进供需精准匹配，显著提升了金融运作效率，并经由数据洞察激发出新业态、新模式，演化出分工更精准、结构更合理、空间更广阔的开放银行，最终驱动实体经济和虚拟经济、区域经济和全球经济的升级转型和创新跨界。〔8〕

其次，数据共享是开放银行发挥协同效应的关键环节。在现代金融业的运作过程中，商业银行、投资银行、证券、保险所必需的生产要素专用性不断弱化，使企业更容易打破组织壁垒、实现规模经济和协同效应。由此，各种金融业务得以在开放银行的统一平台上相互支援，通过销售协同、运营协同和管理协同，提供综合性、一体化的金融服务，提升商业银行效率和用户的体验，最终形成高度协同性和战略性的核心竞争力。

最后，数据共享提升了消费者的便利程度。开放银行以“用户”而非“金融产品”为中心，通过数据的整合和透明化，用户不再需要分别处理多个账户，而能够在一个界面上实时查看所有财务信息，根据自身需要，比较选择产品和管理资产，从而避免透支消费和过度借贷、平衡现金流，做出更明智的金融决策。同时，数据在不同企业之间的流通，使用户得以无缝切换金融服务提供商，这无疑为其提供了更广泛的自由度，并落实了消费者选择权。

3. 开放银行的组织层：网络平台

开放银行秉持“银行服务即平台”（Banking-as-a-Platform，BaaP）的理念，数字经济中一种特殊组织——网络平台由此成为其组织形式。然则，何为网络平台？

从技术维度观察，网络平台是一套信息网络系统，其外在表现为硬件终端、操作系统、应用程序 APP、用户端软件、浏览器、搜索引擎、网站，其内在功能则是允许大量创新和服务实现的底层技术架构。〔9〕从主体维度观察，网络平台是平台经营者、消费者、供应商、劳动者、广告主、物流商、支付机构、债权人、债务人等众多主体所构成的复杂集合。〔10〕从功能维度观察，网络平台是为网络游戏、网络购物、网络社交等各种网络活动提供基础服务的服务提供者，这些基础服务包括技术服务、数据存储/分析、支付/结算、物流、认证、征信、金融服务、纠纷解决、行为管理/调控。从结构维度观察，网络平台是互联网“分布式结构”之中的“再中心化”，是网络的关键节点。

作为网络平台，开放银行具有如下特征：（1）多边性。开放银行作为“媒介者”（match-maker），同时给多方提供产品或服务，并使其在平台中相互交流或交易。〔11〕对于第三方合作

〔7〕 参见〔英〕维克托·迈尔—舍恩伯格、肯尼斯·库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 4 页。

〔8〕 参见许可、尹振涛：《金融数据开放流通共享》，载《中国金融》2019 年第 4 期。

〔9〕 参见胡凌：《从开放资源到基础服务：平台监管的新视角》，载《学术月刊》2019 年第 2 期。

〔10〕 参见张江莉：《互联网平台竞争与反垄断规制——以 3Q 反垄断诉讼为视角》，载《中外法学》2015 年第 1 期。

〔11〕 参见〔美〕戴维·埃文斯、理查德·施马兰：《连接：多边平台经济学》，张昕译，中信出版集团股份有限公司 2018 年版，第 242 页。

者，商业银行通过 API 向其集成开放数据和业务功能；对于消费者，商业银行在不同渠道上布局智慧营销平台，根据其需求定制增强型服务产品，并吸引之前接触不足的客群，在获取外部流量的同时提升存量用户价值。(2) 交叉网络外部性（Cross-group network externalities）。开放银行的产品或服务的价值，不但随着平台参与者数量的增加而增加，其中用户的效用，还会随着其他类型参与者，如金融科技公司的增加而增加，反之亦然，从而具有“交叉”性质。(3) 协同性和生态性。这里的“协同性”既体现为平台产品或服务之间的协调一致和创造性组合，也体现为平台不同参与者之间的相互影响与相互合作。就商业银行而言，其利用云计算、大数据、物联网等新技术提供开放智慧的金融服务，由单一的产品服务输出向嵌入场景的服务模式转型，实现客群生态化。就金融科技而言，其不必实际控制用户账户，就可以提供虚拟财务服务，从而规避了复杂和昂贵的银行合规要求。生态性意味着开放银行以“利他”与“分享”为宗旨，以建构开放、普惠和繁荣的在线生态系统为依归。开放银行不被任何一方所独占，不是给予特定主体的政策倾斜，更非金融机构和金融科技公司零和博弈，而旨在搭建共生共存的金融生态圈，推动金融机构和金融科技公司更深层次的协作和竞争，提升服务的弹性、多样性和普惠性，最终追求用户利益最大化。

（二）开放银行兴起的动因

开放银行在全球范围内的兴起，并非突发事件。早在 2004 年，国际支付巨头 PayPal 就推出了 PayPal API，由此成为开放银行的先声。2011 年，法国农业信贷银行开始提供 SDK 和应用商店服务，第三方开发者借此能够更便捷地构建新的移动程序，更好地管理用户的财务状况。2014 年，英国开放数据研究所（ODI）的研究显示：开放数据后，银行竞争力得以提升，中小企业生产效率也有所提高。在开放银行工作组（OBWG）和英国竞争和市场委员会（Competition and Markets Authority）的推动下，“开放银行计划”在 2015 年应运而生。

1. 金融科技 3.0 的驱动

回溯历史，开放银行是金融科技（FinTech）迭代的产物。2016 年 3 月，金融稳定理事会发布了《金融科技的全景描述与分析框架报告》，把金融科技定义为技术带来的金融创新，通过创造新的业务模式应用流程或产品，深刻影响金融市场、金融机构和金融服务的提供方式。其实，从 18 世纪末的电话下单，到世界上第一张信用卡——大来卡（Diners Club），再到全球银行间金融通信系统（SWFIT），科技与金融的结合由来已久。到了 20 世纪 80 年代，金融服务行业就已成为全球信息技术产品和服务的最大购买方。〔12〕 按照技术的演进及其功能，我们将金融科技大致分为三个阶段。〔13〕 其中，1.0 阶段体现为将通信设施和产品导入金融服务之中；2.0 阶段体现为金融的互联网化，用户得以通过更多样和更便捷的途径获得金融服务；3.0 阶段则是人工智能、区块链、云计算、大数据、物联网等技术主导下的根本变革，金融产品设计、生产、销售和服务的全产业链将与科技深度融合，使得金融成本降低和效率提升成为可能。作为依托于大数据分析、分布式系统和移动互联网的商业模式，开放银行正是在金融科技 2.0 阶段萌生，并在 3.0

〔12〕 参见许多奇：《金融科技的破坏性创新本质与监管科技新思路》，载《东方法学》2018 年第 2 期。

〔13〕 See Ross Buckley, Douglas Arner, Janos Barberis, The Evolution of Fintech: A New Post-Crisis Paradigm? 47 *Georgetown Journal of International Law*, 1271-1319 (2016).

阶段成熟。

2. 银行 4.0 的来临

开放银行也是银行自身变革的关键一步。2008 年，马云在第七届中国企业领袖年会上发出豪言："如果银行不改变，我就改变银行。"而这事实上是比尔·盖茨观点的遥远回声。1994 年，比尔·盖茨看到非洲民众用手机开展金融活动后，就指出："银行业是必要的，但银行却不是。"在时代巨变面前，银行不能再固守公元 1 世纪的实体签名开户规则，必须因时而变，与金融科技同步。著名商业作家布雷特·金恩（Brett King）用 Bank1.0 到 Bank4.0 来描述银行的历史演进。〔14〕

所谓 Bank 1.0，即以银行物理网点为基础的银行业务形态，它是最古老的银行。Bank 2.0 是一个自助服务的时代，ATM 机和网上银行开始出现，以满足用户多样化的需求。到了 Bank 3.0，越来越多的金融交易转移到移动支付、P2P 等互联网功能上，银行意识到必须基于消费者习惯、企业金融需求，改变风险管理模式，降低价值产生和传递过程中的金融成本，减少金融交易的中间环节。而在 Bank4.0 阶段，用户获得了前所未有的主动权，银行将采用数字科技提供内嵌的、无所不在的银行服务，随时随地回应用户所需。最终，银行服务将是即时的、情景式的体验和无障碍的互动，并由人工智能所主导，实体银行将不再必要，这就是"有用户处即有银行服务"的真意。在银行 4.0 的崭新架构下，开放银行是不可或缺的关键要素。

3. 金融机构与金融科技公司的合力

开放银行并非仅仅仰赖金融科技或者银行业的孤军奋战，而是这两种力量共同作用的结果。开放银行并未改变金融的本质，恰恰相反，它让金融业重新回到初心：为用户更好地提供价值储存、货币转移和信用获取的服务。一言以蔽之，即以用户为中心重塑金融业。这一被称为"第一原理"的"功能为王"理念，要求金融机构审视自己的定位，积极采取各种新兴科技将用户的需求和金融服务的初衷无缝对接。这一目标的实现，离不开传统金融机构与金融科技公司的共同努力。

对传统金融机构而言，开放银行将带来前所未有的技术升级、流程再造和风格转变，而这不可能一蹴而就。但时不我待，用户对于高度联通、个性化的金融服务的偏好，让金融机构倍感转型压力。在这个充满挑战、瞬息万变的市场中，闭门造车是不可取的，昔日的竞争对手亦可成为合作伙伴。金融科技公司能够提供成本更低和效率更高的技术解决方案和丰富的业务场景，从而有助于金融机构迅速切入开放银行的庞大市场。在另一方面，金融科技公司欠缺金融机构所搭建的基础服务实施，不掌握关键性的用户信息，尚未深刻理解和管理金融风险，同时面临不确定的监管态势。为此，金融科技公司亦有动力与金融机构跨界合作，通过合作竞争实现双赢。放宽视野观察，开放银行的未来必然是金融机构、金融科技公司以及相关方共建的生态系统，从而为更广范围的用户提供更深度的服务，实现金融的普惠化和智慧化。

〔14〕 参见〔澳〕布雷特·金恩：《银行 4.0》，孙一仕、周韦英、林凯雄译，台湾金融研训院 2018 年版，第 342 页。

二、开放银行的法律架构

商业实践绝非开放银行的全部故事。事实上，从欧盟、英国，到新西兰和澳大利亚，再到日本、我国香港地区和新加坡，世界各个国家或地区的监管机构纷纷通过法律和政策，以期将传统的金融服务市场转变为更具竞争力和创新性的市场，满足不断变化的消费者需求：个性化、安全、便捷、灵活的金融服务。世界各国及地区的经验充分表明：开放银行并非只是企业创新的结果，相反，它始终有赖于国家的有效应对与调适。在此，我们将从开放银行三层次出发，探求开放银行的整体架构。

（一）API 的法律架构

API 不仅仅是技术，它事关开放银行的核心架构。首先是向谁开放。是用户、特定合作伙伴的金融公司或金融科技公司，还是满足一定条件的不特定金融公司或金融科技公司，抑或是所有企业和政府机关？其次，是开放什么。是信息查询业务、新服务申请，还是业务办理，又或者是开放账号？显然，不同的选择，将创设不同的法律关系，塑造不同的开放银行生态系统。正因为如此，英国开放银行工作组（the Open Banking Working Group）、我国香港金融管理局和新加坡，先后出台《开放银行标准框架》（The Open Banking Standard）、《香港银行业 Open API 框架咨询文件》《金融业 API 手册》（ABS-MAS Financial World：Finance-As-A-Service API Playbook），就 API 予以详细规定。

1. API 的开放对象

API 的参与方一般包括 API 提供者、API 消费者、金融科技公司、开发者。〔15〕其中，作为将数据、产品和服务共享给第三方的机构，API 提供者应当在开放性、可用性、交互性的原则下设计 API，并使用 OAuth 2.0、OpenID Connect、TLS v1.2 等标准，满足身份认证、授权、加密的安全要求。作为使用 API 的组织和个人，应当遵循 API 提供者的指导原则，坚守 API 提供者明确的安全标准。作为行业颠覆性技术创新的先锋，金融科技公司须依据 API 的技术格式，避免修改既有定义，开发具有兼容性的创新型应用产品和服务。最后，负责设计模型的开发者，应当实现 API 提供者的相应需求，创建技术说明文件，保证技术的安全性。

2. API 的开放内容

API 适用于产品、市场、销售、服务、支付、监管等多个业务流程，根据相关影响和风险，可以将其大致分为四类，即：（1）产品和服务信息 API。银行提供有关产品和服务详情的“只读”信息，包括账户信息、信用卡、按揭贷款、有无抵押贷款产品信息、投资基金、结构化投资产品、贵金属、股票交易产品详细信息、普通保险、人寿和长期保险产品信息，等等。（2）产品与服务的订阅和申请 API，用户可以在线申请信用卡、贷款和其他银行产品，在线处理投资基金、贵金属、股票账户开户需求以及普通保险、人寿保险申请需求。（3）账户信息 API。查询和更改认证用户账户信息（余额、交易记录、限额、付款日期等）。（4）交易 API，处理认证用户

〔15〕 See ABS-MAS Financial World：Finance-As-A-Service API Playbook.

发起的银行交易、支付或预定付款/转账，处理零售投资基金、贵金属、股票交易指令，处理财产保险保单修改和赔付请求，等等。〔16〕

3. API 的治理结构

为了推动 API 的稳健运行，商业银行应当设立一个独立机构，其职责包括跟踪并监督 API 标准的部署进程，处理用户纠纷，确保数据安全性，维护 API 的可靠性、可拓展性和安全性。此外，在“标准—认证—认可”三位一体的治理架构下，商业银行和金融科技公司的行业组织可以作为独立第三方，通过最佳实践、行业指南和认证措施，推动 API 规则成为企业合规的基本规则，并通过监管机构的法律认可，确保其权威性和可执行性。〔17〕借此，当用户遭遇 API 相关事故时，可以联系 API 提供者解决，若逾期未处置，就可以启动下一轮事故处理流程，交由行业组织处理。

（二）数据共享的法律架构

数据共享是开放银行的灵魂，在某种意义上，开放银行就是开放数据。但另一方面，对用户身份资料、账户信息、交易信息承担保密义务，又是银行业的古老传统。如何在“消费者信息和隐私保护”与“数据共享”之间取得平衡，〔18〕是开放银行的症结所在。围绕这一难题，欧盟《一般数据保护条例》（GDPR）和 PSD2、澳大利亚《消费者数据权利法案》（Consumer Data Right Bill）提出了各自的解决方案。

1. 数据共享的发起

与之前由数据控制者——商业银行和金融科技公司发起的数据共享不同，开放银行赋予了用户发起数据共享的权利，其源于欧盟 GDPR 第 20 条“数据可携带权”（Right to Data Portability）。据此，个人不但有权以一种结构化、通用和机器可读的形式获取其已提供给数据控制者的个人数据（副本获取权），而且有权无障碍地从直接收集数据的数据控制者处将该数据转移至另一个数据控制者（数据移转权）。正是觉察到数据可携带权对市场竞争的正面效应，欧盟 PSD2 第 66、67 条赋予用户对其账户信息的控制权，银行应在用户要求时，向第三方开放用户数据的访问权限，即便该方与银行并不存在任何合同关系。澳大利亚延续这一路径，确立了更全面、彻底的“消费者数据权”。它的权利主体不但包括个人，还包括小企业，权利对象不但涵盖个人数据，还包括“与提供给该消费者的产品或服务相关联”的非个人数据，例如云服务提供商存储的文档。总之，开放银行将金融数据想象为一种资产，而不是受保护的基本权利，这改变了金融数据控制和所有的关系，将权利交给用户，促进其积极利用并允许他人利用其数据，最终促进金融市场的竞争。〔19〕

2. 数据共享的范围

共享的数据并非漫无边际，GDPR 第 20 条第（4）款将“不应影响他人的权利和自由”作为

〔16〕 参见《香港银行业 Open API 框架咨询文件》。

〔17〕 参见许可：《从监管科技迈向治理科技——互联网金融监管的新范式》，载《探索与争鸣》2018 年第 10 期。

〔18〕 参见何颖：《数据共享背景下的金融隐私保护》，载《东南大学学报》2017 年第 1 期。

〔19〕 See Samson Yoseph Esayas，Angela Daly，The Proposed Australian Consumer Right to Access and Use Data：A European Comparison，2 *Eur. Competition & Reg. L. Rev.*，187（2018）.

数据“可携带权”的法定边界。根据欧盟29条工作组（WP29）的指南，这里“他人的权利和自由”可以理解为“第三人数据，企业商业秘密或知识产权，尤其是软件版权”。〔20〕由此可见，共享的数据一般限于如下两类：（1）用户提供的数据，主要是基本资料、身份信息、生物识别信息、存款信息等个人信息，包括姓名、身份证号码、住址、通信通讯联系方式、存款信息、指纹、声纹、虹膜和面部特征等数据。（2）交易数据，如原始交易记录、信贷记录、征信信息、流水记录等。

除此以外，“用户增值数据”（Value-added customer data）和“聚合数据集”（Aggregated data sets）是否属于共享范围尚待进一步辨明。前者指的是“数据处理者对用户基础数据和交易数据进行记录、检索、整理、标注、比对、分析、挖掘等处理后产生的数据”，〔21〕诸如收入/资产核实、用户身份验证、信用分。后者指的是将大量用户数据汇集在一起形成跨用户组的去标识的、汇总或平均化的数据。无论是“用户增值数据”，还是“聚合数据集”，其价值很大程度上由企业付出努力和成本所创造，倘若法律强制分享这些数据可能构成对商业秘密或知识产权的侵犯，甚或将数据价值转移给竞争对手，这显然是不公平和违反商业道德的，因而该等数据不应包括在共享数据的范围内。〔22〕

3. 共享数据的标准

共享的数据要遵循相关数据展现、格式、定义、结构的标准，并应满足可获得性、可存取性、可分析性的最低要求。其中，所谓“数据可获得性”，指可以辨认数据为相关之内部及外部数据；“数据可存取性”，指合法第三方机构经用户授权可存取及使用数据；“数据可分析性”，指从数据中可以获得有价值的信息，并可进一步促进决策制定。〔23〕

（三）网络平台的法律架构

网络平台迄今仍然不是法律概念。随着平台经济的崛起，从劳动法到消费者保护法，从财产法、商法到健康法、金融法，传统公法和私法皆面临着重大挑战，以至于美国学者Orly Lobel大胆提出了“平台法”（law of platform）这一新的法律门类。〔24〕在这里，我们暂且跳脱出不同平台所面临的诸多具体法律问题，而是从更宏观的角度去把握网络平台的规则体系，即谁是网络平台的主导者，如何成为它的参与者，以及各方如何承担法律责任。〔25〕

1. 网络平台的主导者

作为企业和市场的混合物，网络平台本身难以成为规制对象，正因如此，尽管我国《电子商务法》在起草过程中将“电子商务第三方平台”纳入其中，但最终仍然将其细分为“电子商务平

〔20〕 See Guidelines on the right to data portability, 16/EN WP 242.

〔21〕 丁道勤：《基础数据与增值数据的二元划分》，载《财经法学》2017年第2期，第8页。

〔22〕 See Review into Open Banking in Australia-Final Report, available at https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf, last visited on July 1, 2019.

〔23〕 参见陈英惠：《Open Banking对金融业之机会与挑战》，载《彰银资料》2018年第12期。

〔24〕 See Orly Lobel, The Law of the Platform, 101 *Minn. L. Rev.*, 87 (2016).

〔25〕 参见〔美〕杰奥夫雷G. 帕克、马歇尔W. 范·埃尔斯泰恩、桑基特·保罗·邱达利：《平台革命：改变世界的商业模式》，志鹏译，机械工业出版社2017年版，第161页

台经营者”“平台内经营者”。〔26〕那么，对于开放银行而言，谁是平台的经营者？

观察既有实践，开放银行有自建、收购、合伙、参与四种模式。〔27〕其中，“自建模式”即商业银行借助应用程序包构建集合信息系统、客户体验、数据分析、物联网等元素的商业生态系统。在这一模式中，银行是当然的平台经营者。对于那些技术掌控度高、人才资源充足且意欲成为业界先锋的大型银行而言，不论是 BBVA、Barclays、Capital One、HSBC 等国际银行，还是中国银行和中国工商银行，均将自建开放银行作为优先选择。“收购模式”即商业银行兼并收购一家金融科技公司，由其作为平台经营者，快速实现体外拓展。例如，Silicon Valley Bank 于 2015 年收购一家专注于 API 的科技公司 Standard Treasury，成功搭建了开放银行。与上述两种模式不同，在“合伙模式”和“参与模式”中，商业银行不再是平台经营者，凭借着技术和流量优势，金融科技公司往往成为开放银行事实上的主导者，PayPal 以及上海银行与京东金融合作的“上银白条闪付”，就是典型的例子。

在我国“政府管平台经营者，经营者管平台上其他主体”的“国家—平台—用户”线性结构下，〔28〕开放银行的经营者将承担保护个人信息、信息管控、金融风险管理、安全保障、配合执法等一揽子义务以及相应的民事、行政和刑事责任。〔29〕显然，开放银行的不同模式，将深刻影响它的制度安排。

2. 网络平台的参与者

网络平台始终在“由经营者排他控制的封闭”和“任何人均能自由访问和接入、不存在任何使用和开发限制的开放”之间徘徊。这事实上是一种取舍。开放意味着参与者进入门槛和用户被“锁定”而不能迁移的可能性同时降低，这必然加剧了竞争，减少了利润；但封闭也将导致市场隔绝和创新不足。〔30〕因而，网络平台的经营者一般会选择混合战略，将资源尽量投入到具有核心竞争力的产品和服务上，而将其他内容予以开放。开放银行亦是如此，但问题在于如何决定和保持其关键领域。对欧美实践的梳理发现，商业银行一般只是按照特定的条款和条件向某些金融科技公司开放，而向软件服务商或独立科技公司开放的寥寥无几，这意味着几乎不存在“即插即用”的增值服务程序。〔31〕无疑，“如何进一步扩大开放”是开放银行的未来重要方向。

决定谁是平台参与者的，除了商业逻辑之外，还有法律限制。在欧盟 PSD2 中，为了降低用户的风险，第三方支付服务提供商（TPP）和账户信息服务提供商（AISPA）必须获得监管机构的批准，并且，只有在满足用户授权和银行审核其资质的双重条件后才能接入平台。无独有偶，

---

〔26〕《电子商务法（草案）》规定：“电子商务第三方平台，是指在电子商务活动中为交易双方或者多方提供网页空间、虚拟经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者其他组织。”在最终稿中，该条将“电子商务第三方平台”修改为“电子商务平台经营者”。但需要指出，《电子商务法》不涉及开放银行等金融类平台。

〔27〕See Kristin Moyer, How to Build an Open Bank, available at https://www.gartner.com/en/documents/3746220/how-to-build-an-open-bank, last visited on July 1, 2019.

〔28〕参见许可：《网络平台规制的双重逻辑及其反思》，载《网络信息法学研究》2018 年第 1 期。

〔29〕参见周学峰、李平主编：《网络平台治理与法律责任》，中国法制出版社 2018 年版，第 331－343 页。

〔30〕See J. West, How open is open enough? Melding proprietary and open source platform strategies, 32 (7) *Research Policy*, 1259－1285 (2003).

〔31〕See Zachariadis, Markos, Ozcan, Pinar, The API Economy and Digital Transformation in Financial Services: The Case of Open Banking, SWIFT Institute Working Paper, No. 2016－001 (2017).

在澳大利亚，竞争与消费者委员会（Australian Competition and Consumer Commission）负责制定开放银行参与者的认证标准和方法，只有获得认证的相关方才能获得开放银行数据，该标准将采取基于风险的分层认证模式，从而不至于给各方造成不必要的进入障碍。

3. 责任承担机制

金融与风险须臾不可分离，开放银行亦不例外。在用户遭受损失之后，如何在各方之间分担损失成为平台责任的核心问题。对此，存在两种不同的制度设计。一种是各负其责，这意味着由过错方独立承担因其过错导致的欺诈、支付瑕疵、数据泄露责任。但在此情形下，数据提供者仍应确保将个人数据传输给正确接收方，同时，还应评估数据转移的具体风险并采取适当的防范措施。〔32〕另一种是由商业银行承担连带责任，这意味着在发生损害后，用户有权要求银行承担先行赔付责任，若第三方存在过错，银行在赔偿后有权向其追索。〔33〕

三、开放银行的挑战与因应

（一）开放银行的风险与障碍

1. API 标准的统一

创建一套可供所有人使用的 API，对于开放银行而言至关重要。考虑到开放银行参与主体的多样性，创建互操作性和高效的 API 必须通过制定标准来完成。目前，API 标准芜杂，存在组织标准（由银行或金融科技公司单独制定）、团体标准（由合作伙伴或具有共同利益的群体所制定或接受）、行业标准（由银行业或金融科技行业协会制定或接受）、通用标准（在一个国家内或全球范围内被接受）。在欧洲，API 标准的分歧和冲突已经显现，目前，由数十家银行和金融公司组成的柏林集团（Berlin Group）公布了 API 通用框架，各国监管机构亦在纷纷推广国家标准，人们普遍担忧，这不仅会增加第三方的成本，也几乎无助于统一欧洲的金融市场。〔34〕

考虑到金融服务需要安全性、隐私性与合规性，API 标准的制定必须超越技术和功能面向，将法律、操作和管理纳入其中。同时，采纳何种 API 标准，以及由谁来制定标准，不但直接影响由何方承担成本，而且决定了何方在开放银行业务中占据优势地位，因此，API 标准统一必将是长期的博弈过程。

2. 网络安全

网络安全是开放银行的生命线。深度互联互通使得金融机构更容易遭受内部和外部的网络攻击，ICT 系统和流程业务的规划不足以及第三方安全防护的能力和意愿欠缺，加剧了开放银行的脆弱性。欧洲银行管理局（EBA）针对 PSD2 列举了一系列风险：（1）对用于支付的通信渠道保

〔32〕 欧盟 29 条工作组（WP29）认为此类风险防范措施包括：对于用户，可以利用额外身份验证信息，例如共享密匙，或一次性密码，如果怀疑相关账户被盗用，可暂缓或冻结数据传输；对于第三方，可采取强制身份验证措施，例如基于令牌的身份验证。See WP29, Guidelines on the Right to Data Portability.

〔33〕 See Liability and Consumer Protection in Open Banking, available at https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf, last visited on July 1, 2019.

〔34〕 See The slow-burning effects of Europe's new data rules, available at https://www.economist.com/finance-and-economics/2019/01/12/the-slow-burning-effects-of-europes-new-data-rules, last visited on July 1, 2019.

护不足；（2）对应用程序、服务器、用户的支付设备等系统和设备保障不足；（3）用户或第三方机构及其员工的不安全行为；（4）业务环境的复杂性增加；（5）欺诈或恶意攻击。〔35〕

3. 个人信息保护

开放银行共享的大量数据属于用户的个人信息，个人信息的收集、存储、使用、共享和删除由此成为贯穿开放银行业务始终的问题。“有用户处即有银行服务”的理念，使得尽可能满足用户随时随地的需求成为开放银行的首要关切，金融服务的个性化和嵌入化应运而生。矛盾的是，金融服务这种转型是以个人信息流通和用户画像为基础的，如何在开放银行中，落实个人信息权利，防范个人信息泄露、滥用和身份欺诈，成为问题的关键。〔36〕

4. 弥散的金融风险

开放银行意味着风险开放。跨市场、跨行业、跨用户群体的特性，导致金融交易行为、业务模式和风险类型更为复杂。作为银行、其他金融机构、金融科技公司、数据技术公司共同参与的多方交易系统，开放银行因信息不对称引发的信用风险和操作风险大幅提升。同时，技术迭代导致金融交易规模和交易频度呈几何级数增长，监测压力陡增。金融监管的对象面临调整、“风险隔离”等传统金融监管核心原则面临挑战。无论是金融机构，还是金融科技公司往往是单方面承担输入风险、共振效应以及内外部风险叠加形成的新风险，缓释机制和隔离机制的薄弱进一步提升了风险管控的难度。

5. 对竞争的影响

开放银行在数据、用户关系和监管的三个层面上重塑现有竞争格局。就数据而言，银行拥有大量金融资产、负债和交易的数据，金融科技公司则掌握着支付、网购、物流、销售以及电商产品相关联的理财、贷款和保险数据。开放银行所要求的“数据共享”，在经济层面上存在金融机构的强关联小数据和金融科技公司弱关联大数据的公允价值差异，在法律层面上存在数据权属不明的掣肘。就用户关系而言，不论是银行，还是金融科技公司都以获得用户、维持用户、影响用户作为核心诉求。然而，开放银行降低了“进入壁垒”，允许直接竞争对手以及其他金融机构或金融科技公司获得用户信息，从而共享用户。这不但带来“谁拥有用户”的问题，更重要的是，由于开放银行触达用户的方式，还存在“将谁的名字写在商店橱窗”中的问题。中小企业，甚至大型银行都可能被纳入更广泛的金融科技品牌之内，以至于无法有效建立自己的品牌声誉。正如人们所担心的：目前，银行已经不再是客户关系的所有者。想象一下明天谷歌决定创立一个银行聚集系统，我们输入密码登录自己的银行账户，它以一种更加新颖、易于互动和更方便客户的方式呈现我们的信息。就在这时，我们和银行之间的关系也就改变了。〔37〕就监管而言，如果对开放银行各主体采取统一的监管措施，高昂的合规成本必然削弱新型服务的灵活性和创新性，但如果采取因主体而异的监管措施，则可能导致监管规避和监管套利，这是一个两难困境。

---

〔35〕 See Guidelines on the security measures under PSD2, available at https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2, last visited on July 1, 2019.

〔36〕 参见易宪容、陈颖颖、周俊杰：《开放银行：理论实质及其颠覆性影响》，载《江海学刊》2019 年第 2 期。

〔37〕 参见〔英〕杰姆斯·汉考克、肖恩·里奇蒙德：《消失的银行》，王浩宇、杨丽萍译，中信出版社 2018 年版，第 76 页。

（二）开放银行的监管原则

1. 主体平等监管

尽管开放银行政策起源于英国政府对金融科技公司的倾斜性扶持，但我国数字金融市场格局与英国迥然不同，金融科技公司反而是先行一步的领先者。在此背景下，监管者应借鉴《电子商务法》第4条确立的“线上线下平等对待”原则，平等对待开放银行的各主体。基于该原则，开放银行的根本目的在于提升金融资源分配效率，促进金融数字转型，实现金融服务的个性化与普惠化，而非单方面支持金融机构或金融科技公司的发展。为此，监管机构不得对任何一方给予歧视性待遇，不得强制一方向另一方开放业务、数据和账户。同时，根据“功能监管”的原则，监管机构应从金融产品和服务的功能和特性出发，对于同类产品和服务适用同等规则，弥补交叉性金融业务的监管漏洞，避免监管套利。

2. 助推而非强制

由2017年诺贝尔经济学奖获得者理查德·泰勒和美国前信息与监管事务办公室主任凯斯·R·桑斯坦提出的“助推论”（Nudge），是近十年来政府监管领域的开创性理论。该理论旨在通过干预、塑造和制约被规制对象的选择框架或背景线索，相对柔性地改变被规制对象的行为基础。〔38〕与强制性监管迥异，开放银行的助推式监管不要求银行或金融机构必须采用特定行为模式，但它也不完全是放任性或倡导性的。相反，监管机构通过提供程序上、组织上以及能力上的规范，采取默认机制、劝说性和咨询性的战略、基于设计的工具、承诺机制、信息机制、路线图等措施，促成不同主体的自我组织和自我规制，从而在推动开放银行发展的同时，避免破坏市场内在的逻辑。

3. 治理科技优位

“治理科技”（GovernTech）与“监管科技”（RegTech）最大的差异，就在于其强调了“治理”的核心地位。简言之，治理科技以“数据”为资源，以“标准—认证—认可”为三位一体的组织架构，以“机制设计”为运作流程。治理科技源于监管科技，又革新了监管科技。治理科技包含两大要素：其一，数据驱动的治理，其强调监管者和被监管者之间的数据共享，从而将金融机构向监管机构的单向数据传输转化为双向的数据整合。其二，经由设计的治理。当面对开放银行这项颠覆性创新时，监管机构首先要确定待解决的核心问题和利益相关者，设定他们的政策目标；然后召集所有利益相关方共同参与设计解决方案，从中选择最佳解决方案，并征求利益相关方的反馈意见；进一步修改和重新测试解决方案，继续进行反馈循环，直到找到最合适的解决方案；在此基础上，在一定范围内实施上述方案，进行beta测试，再根据beta测试数据多次迭代流程、测试并收集反馈，最终发现最具操作性的和适切性的制度。〔39〕

（三）开放银行的监管规则

1. 推动API国家推荐性标准制定

安全、可控和便捷的API架构是开放银行的基础，从“助推而非强制”和“治理科技优先”

〔38〕 参见张力：《迈向新规制：助推的兴起与行政法面临的双重挑战》，载《行政法学研究》2018年第3期。

〔39〕 See Alice Armitage，Andrew K. Cordova，Rebecca Siegel，Design Thinking：The Answer to the Impasse Between Innovation and Regulation，2 *Georgetown Law Technology law Review*，49（2017）.

的原则出发，国家可以鼓励和协助金融机构和金融科技公司从市场出发形成“最佳实践”。在此基础上，通过企业、学界和政府机构的共同参与，努力就以下内容达成国家推荐性标准：（1）API 的功能和架构；（2）开放的类别，产品、服务、账户信息、交易信息；（3）数据标准格式；（4）安全性等问题。

为了增进 API 最佳实践和标准制定，监管机构鼓励金融机构和金融科技公司在官方网站上公布如何使用每个 Open API 的细节，包括功能、架构、安全性等详细说明，同时可以创建一个专门网站，汇聚和展示提供的所有 Open API，从而确保所有第三方服务提供商可以便捷、灵活地获取数据。最后，监管机构可以通过项目研究和专题论坛的方式，召集金融机构和金融科技公司交流分享 Open API 的案例思路和经验。

2. 建构网络安全系统底线

网络安全是开放银行的底线，监管机构可以以“指引”的方式建立网络安全的底线。该指引包括但不限于如下内容：

其一，开放银行平台的经营者应当建立网络安全治理架构。该架构包括：（1）全面的安全政策、安全目标和措施；（2）明确和分配关键角色和职责，以执行安全措施和管理操作性风险；（3）建立必要的程序和系统，以识别、测量、监测和管理因提供服务而产生的各种风险。

其二，开放银行的主要参与者应具备相关基本资格。（1）业务能力：财务稳健性、声誉、管理质量和业务的适当性操作。（2）风险管理：网络安全和 IT 控制（包括机密性、完整性和可用性），监控和缓解措施和应急计划。开放银行经营者负有对上述资格的审查义务，必要时，可以建立第三方认证评估制度和依法备案制度。

其三，针对开放银行的技术支持机构，银行应按照《银行业金融机构信息科技外包风险监管指引》的规定，健全信息科技外包管理机制，提升外包风险管控水平，对接触敏感数据和承担关键基础设施外包服务的第三方机构，要从国别风险、技术风险、经营风险等方面予以全方位评估，探索建立运用信息化手段加强外包风险管控的机制。

3. 平衡个人信息保护与数据共享

个人信息是开放银行共享的重要内容。在我国法律尚未规定欧盟的“携带权”和澳大利亚的“消费者数据权”的背景下，监管者可以将个人信息保护的重点放在由金融机构和金融科技公司所发起的数据共享上。鉴于个人金融信息兼具隐私性和公共性，对个人金融信息的保护应秉持分类分层的理念，从不同的信息类型出发建构不同的保护规则。

对于一旦泄露、非法提供或滥用可能危害人身和财产安全的敏感信息（特别是个人身份信息、银行账号、鉴别信息、存款信息、交易和消费记录），应当采取严格的保护。具体而言，只要在满足如下条件时，该等数据的收集者才能进行数据共享：（1）在首次收集个人数据时，已经向用户清晰、明了地告知其数据可能与第三方共享，同时告知共享方的类型，共享的目的、频率、范围、保存期限；（2）在与第三方共享时，应以增强式告知的方式提醒用户，并取得用户明示同意；（3）在与第三方共享前，应进行个人信息安全风险评估；（4）每年至少一次以电子形式向用户披露其数据的共享情况；（5）在数据收集者或第三方违规违约使用个人信息时，用户有权停止共享，并要求第三方删除相关信息。对于敏感信息以外的一般个人信息（如网络浏览信息），

可采取相对宽松的授权规则。即如果在首次收集个人数据时，金融机构或金融科技公司已在网站首页或 APP 显著位置向用户清晰、明了地告知其数据可能与第三方共享，告知共享的频率、范围和保存期限，则应当允许用户以默示方式授权数据共享。

科技不但是开放银行问题的制造者，也是问题的解决者。因此，除了法律之外，技术治理不可或缺。就数据共享而言，“多方安全计算”就是在不改变数据实际占有和控制权的情形下，促进数据流通共享的最佳例证。立足于多方安全计算平台，这一技术将计算移动到数据端，致力于建造安全和保护隐私的“数据高速公路”；借助同态加密、混淆电路、秘密分享、零知识证明等尖端的多方安全计算和密码学相关技术，在确保高级别的企业数据安全和个人隐私保护的同时，促进数据共享利用与业务创新。

4. 完善数据权属规则和平台规则

开放银行的最大阻碍是数据价值的分配，而“所有的定价问题都是产权问题”，因此，监管机构应当首先明确金融数据的权属。欧盟“数据生产者权”和“个人数据权利”二分的制度表明：数据财产权应首先分配给首先收集和处理数据的数据生产者，而那些与人格密切相关且界定清晰的“个人敏感信息”相关数据的权利应当由个人享有。〔40〕据此，对于个人敏感信息相关数据以外的数据，金融机构和金融科技公司应有权占有、使用、收益和处分，各方可以按照市场规则就其共享的条件和对价，做出公允安排。而对于个人敏感信息相关数据，则应将选择权交给用户，以便其可以选择在目前持有其个人数据的金融机构或金融科技公司与其他新服务机构之间进行转换或者实现数据共享，并令其可以在保留原有机构数据的基础上，将数据转移到另一新的机构，借此促进竞争和创新。

面对平台经营者与平台参与者的矛盾，首先应认识到在颠覆性创新的数字经济中，平台经营者的地位并不稳固，任何垄断行为都将招致市场的惩罚。故此，监管可以坚持平等对待的原则，保持竞争的中性。在具体责任的分担上，应当避免《电子商务法》第 38 条平台经营者对平台内经营者语焉不详的“相应责任”，以过错原则和补充原则为基础，妥善划定平台经营者的责任边界。另外，监管机构还可以促进平台上各利益相关方的合作与协商，为其平等参与平台规则设计提供助力，并监督规则透明、合理的运行，通过合作治理平衡各方利益并最终让消费者受益。显然，这一目的仅靠自愿方式无法达成，因为平台企业的自然激励与上述职能的实施并不相符。因此，监管机构应采取提供《平台规则示范文本》及其程序规则等更细致的监管措施来解决。

5. 坚持一致性监管并尝试沙盒监管

开放银行大大拓展了金融服务提供的方式和场景，面对金融风险的弥散，监管机构应采取穿透式监管的思路，根据资金来源、最终风险分配和服务实质进行一致性监管，即只要从事相同的金融业务，就接受同样的监管，从而确保监管的有效性，防止监管套利。作为一个新兴领域，开放银行有着之前规则所思虑不及的优势和问题，对此，监管机构可以引入“沙盒机制”，在特定区域选择几家金融机构和金融科技公司进行试验，以便监管机构及时发现金融创新的缺陷与风险，进而决定是否允许其正式进入市场。通过把监管机构和创新企业装进同一个盒子里，“监管

〔40〕 参见许可：《数据权属：经济学与法学的双重视角》，载《电子知识产权》2018 年 11 期。

沙盒”令两者同时在线、同频共振，创建监管者、监管专家、技术开发者以及经理人的知识共享机制和非现场联合办公机制，在防范底线风险的同时，积极调适既有监管措施，最大程度保证开放银行的合规。

四、结　语

在数字经济的剧烈变革中，传统银行业必须积极拥抱变化，向开放、共享的金融生态迈进，否则将不可避免地被边缘化，甚至被挑战者取代。但与此同时，我们又要充分认识到开放银行的复杂性，它绝非口号，而是涉及组织架构、企业战略、业务操作、科技研发、服务方式在内的整体革新。职是之故，就庞大而脆弱的银行而言，这种转变尤其需要制度支持。不论是欧洲、澳大利亚和亚洲部分国家的法律先行，还是美国建基于成熟的法律实践与功能监管之上的市场化创新，都充分说明了对开放银行予以制度回应的重要意义。我国立法者和监管者当以前瞻的眼光，既要适时出台针对性措施，化解开放银行进程中的阻碍和风险，又要秉持体系化的法治思考，围绕 API、数据共享和网络平台，构造立体化制度架构，最终奠定开放银行良善治理和长远发展的法律之基。

Abstract：With the rapid iteration of FinTech 3.0 and Banking 4.0，financial institutions and FinTech companies have jointly launched a wave of open banking. The experience of countries across the world has fully demonstrated that open banking is more than the product of enterprise innovation，and it always depends on the effective response and regulation of the State. However，compared with the rich commercial practices，the law for open banking are still absent in China. Based on technology layer，content layer and organization layer of open banking，the three-dimensional legal framework for application programming interfaces，data sharing，and internet platform will be formed，the legal principles of equal supervision of subjects，nudge instead of compulsion，and the superiority of GovernTech will be established and a series of risks and obstacles in the development of open banking are expected to be resolved eventually.

Key Words：open banking，data sharing，network platform，governance technology，big data

（责任编辑：刘　权　赵建蕊）