文章编号:1671 - 1653(2025)01 - 0072 - 07

开放银行的数据风险及其法律防范

刘辉, 姜莉莉

(湖南大学 法学院,湖南 长沙 410082)

摘 要:开放银行商业模式对传统银行业产生颠覆性的影响,为银行业注入了新的活力。开放银行的核心是数据共享,通过数据共享激活银行内海量金融信用数据的价值,创建共赢的生态体系。但数据共享也带来了数据授权风险、数据安全风险与数据滥用风险。数据风险的主要成因是:知情同意机制失灵;未对接受数据共享的主体设置明确的准入标准;缺少数据共享阶段的信息披露机制导致数据使用的透明度降低。防范开放银行带来的数据风险可从以下方面着手:完善现有的授权机制,保障客户基于自由意志作出授权;建立第三方准入审核机制,阻挡不合规的第三方机构加入数据共享链;强化参与方的信息披露义务,缓解信息不对称。

关键词:开放银行;数据风险;数据共享;法律规制

中图分类号:D922.28 **文献标识码**:A **DOI**:10.7535/j.issn.1671-1653.2025.01.009

Data Risk and Legal Regulations of Open Banking

LIU Hui, JIANG Lili

(Law School, Hunan University, Changsha 410082, China)

Abstract: The open banking business model has a subversive impact on the traditional banking industry and injects new vitality into the banking industry. The essence of open banking is data sharing, which activates the value of massive financial credit data in the bank though data sharing and creates a win-win ecosystem. But data sharing also brings risks of data authorization, data security, and data abuse. The main causes of data risks are the failure of the informed consent mechanism; the lack of clear access standards for the subject receiving data sharing; the lack of information disclosure mechanism in the data sharing stage, which leads to the reduction of transparency of data use. In order to prevent the data risks brought by open banking, it is necessary to improve the existing authorization mechanism and ensure that customers make authorization based on free will, establish a third-party access review mechanism to prevent non-compliant third-party institutions from joining the data sharing chain, strengthen the information disclosure obligations of the participants and alleviate information asymmetry.

Keywords: open banking; data risk; data sharing; legal regulation

---

收稿日期:2023 - 12 - 23

基金项目:国家社科基金一般项目(21BFX122)

作者简介:刘辉(1984—),男,四川绵阳人,湖南大学法学院副教授,博士,博士生导师,主要从事金融法学、数据法学研究;姜莉莉(2000—),女,江苏南通人,湖南大学法学院 2023 级法学专业硕士研究生。

近年来，大数据、人工智能等新兴技术蓬勃发展，给许多传统行业注入了新的生命力。金融业同样投身于科技创新的时代潮流中，在产品服务等方面进行了创新，开放银行这一新兴事物的出现使得银行业步入了全新的发展阶段。开放银行正式在我国亮相可追溯到 2018 年浦发银行推出的 API Bank 开放银行平台，此后，各类银行都纷纷推出了自己的开放平台。中国人民银行在《金融科技发展规划（2019—2021 年）》中提到了要借助应用程序编程接口（API）、软件开发工具包（SDK）等手段深化跨界合作，在依法合规的前提下实现资源最大化利用，构建开放、合作、共赢的金融服务生态体系。[①] 这揭示了开放银行所运用的技术手段和理想的实施效果。有关开放银行的内涵，咨询公司 Gartner 认为开放银行是一种平台化商业理念，通过与商业生态系统共享数据、算法、交易、流程和其他业务功能，为商业生态系统的客户、员工、第三方开发者等其他合作伙伴提供服务，使银行创造出新的价值，构建新的核心能力[1]。开放银行的核心是数据共享，利用技术手段，破除传统银行业天然的“数据孤岛”问题，让数据流动起来，使潜在的经济价值得到充分挖掘[2]。开放银行商业模式在为传统银行业注入新活力的同时也带来了相应的数据风险，我国个人数据保护法律体系尚待完善，在应对开放银行数据风险方面，本文试图在分析各类数据风险成因的基础上，构建适合我国的法律防范制度，推动我国开放银行顺利发展。

一、开放银行的数据风险类型

开放银行可以让以银行为主的传统金融机构的海量信用数据发挥其应有的价值[3]，但新兴事物的出现通常会打破旧有局面，破坏原本的秩序平衡。数据共享意味着接触与处理金融数据的主体增加，不可避免地会产生相应的数据风险。

（一）数据授权风险

开放银行的核心是数据共享。数据共享本质上是个人信息传输与收集的一种方式，是对个人信息的再次利用[4]。在“客户、银行、第三方机构”的开放银行的主体构造中，客户虽然是数据主体，但实际上与银行和第三方机构的关系是不对等的，为了平衡这种不对等，就需要让信息数据的处理建立在数据主体同意的基础上。换言之，数据的收集与处理都需要获得数据主体的授权。数据处理者必须受到数据主体授权机制的约束，如果放任可识别的数据被随意通过技术手段获取，如，新浪微博诉脉脉案中，淘友技术公司与淘友科技公司未经新浪微博用户的授权就获取了其账号信息[②]，那么个人的数据保护就无从谈起，也难以通过数据共享构建开放、共赢的金融服务生态体系。

在开放银行使用客户数据的过程中，数据授权风险是数据未经授权与超越授权范围被收集的风险。在开放银行前期收集数据的阶段，客户面临着银行过度采集其相关数据的风险，由于现行采用的知情同意的授权模式实际上是用格式条款的方式实施的，造成客户实质上丧失了选择权，无法自主决定授权的数据内容与范围。在开放银行处理与共享数据的阶段，数据具有主客体分离的特征，数据主体无从得知数据处理方的具体数据处理行为，面临着数据超范围收集与共享的风险。由于客户的金融数据储存在银行内部系统中，银行未经客户授权擅自对个人金融数据进行处理，或超过授权范围对数据进行处理的情况并不罕见。例如，中国邮政储蓄银行由于违反信用信息采集、提供、查询及相关管理规定等违法行为被中国人民银行实施行政处罚。[③]

（二）数据安全风险

在开放银行所形成的多样化生态系统中，各方主体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，加剧了开放银行的脆弱性[5]。一旦一方主体被攻破，其他主体就会受到牵连。在数据共享中，数据从被收集开始就存在安全风险[6]。国外网络社交平台 Facebook 在 2018 年就曾爆出因系统安全漏洞，导致 5 000 多万网民的信息泄露给英国的一家数据分析公司。[④]

在我国传统银行业，数据安全问题并不突出，一方面经营银行需要相应的资质，且在经营过程中受到严格的监管，另一方面在传统的经营模式下，客户数据被视为银行固有的数据资产，只在银行内部系统流转，不易被侵入。而在开放银行模式下，数据接收方的不确定性增加了数据控制的复杂性，减少了数据主体的控制力[7]。数据的充分共享导致数据存储、传输、使用的链条拉长，链条拉长意味着可能出现更多的防护缺口，增加了数据安全被威胁的风险。银行内存储的客户个人身份数据与个人财务数据等核心数据都可能被泄露或破坏。部分银行可能会为了利益盲目扩大业

务规模,放松对接受数据共享的主体的评估,使其轻易加入数据链。各领域机构的业务重心不同,参与数据共享的主体的数据安全防护意愿及水平参差不齐,以及数据聚合服务的产生,使得数据泄露存在木桶效应及聚集效应[8]。财付通支付科技有限公司就曾因违反消费者金融信息保护管理规定被中国人民银行作出行政处罚。⑤

由于数据共享需要依靠应用程序接口(API)等技术手段,相关的技术风险也构成数据安全风险的一部分。首先,没有毫无漏洞的技术存在,技术设计缺陷会被恶意利用与攻击;其次,大多数情况下,各银行为了尽快加入开放银行市场会委托系统外部的技术人员搭建技术平台,技术外包的风险不容忽视;最后,随着数据科技的进步,以往被认为安全可靠的数据处理及传输标准将可能变得不可靠,脱敏数据可能被逆向还原,引发数据安全隐患[9]。

(三)数据滥用风险

数据处理人的数据滥用行为会造成数据失控,逃离自然人控制的数据会多方面影响到自然人的生活[10]。数据滥用行为是指未经当事人允许,或以当事人不愿意的方式使用其数据的行为[11]。“大数据杀熟”是非常典型的数据滥用行为,且这种数据歧视更不易被发现与证实。开放银行的初衷是希望通过数据共享,让“沉睡”的数据发挥作用,让银行与第三方机构通过对数据的分析,更加了解客户的消费习惯,为其定制更为合适的服务,但现实中数据滥用的行为层出不穷。在胡某某诉商务公司侵权案中⑥,法院确认该商务公司处理消费者个人信息的行为超出了法律允许的范围,属于数据滥用。英国剑桥分析公司曾被指控利用在平台上收集的个人数据,针对性地推送信息,利用大数据技术影响美国选民的政治选择,美国选民被无意识地“操控”,是明显的数据滥用。④

当第三方机构接触到充分的客户资料后,机构内部会利用数据分析技术得到客户的消费倾向等信息,迎合式地推送具有诱导性的服务信息,并针对性地调节价格,利用数据分析结果过度压榨客户资源[12],获取超额利润,使得消费者的权益受到损害。同时,开放银行数据共享后提供的金融服务逐步转向线上[13],这将导致“金融排斥”的发生,金融机构还会对“低价值客户”实施数据歧视。“低价值客户”成为了事实上的数据弱势群体,将损害经济法所追求的实质公平[14]。

二、开放银行数据风险的成因

我国开放银行的发展是自下而上的市场驱动模式[9],其实践始于各家银行自发地与第三方机构共享数据,现行法律并没有专门针对开放银行的规定。开放银行数据风险的产生原因可分类探究如下。

(一)数据授权风险的成因

虽然法律明确规定数据处理者处理信息需要获得被收集者的真实同意,且同意以客户事前对数据处理相关事项充分知情为前提,但由于相关法律规定缺少细化的操作判断标准,知情同意机制失灵导致客户的真实授权意愿无法表达,也使同意有效程度难以判断。法律运用的实际效果与理想效果不匹配,进而增加了数据授权风险。

1. 客户的知情权难以实现

同意必须以知情为基础。不保障客户的知情权,则意味着客户是在信息不对称的情况下对自身事物进行安排,同意是有瑕疵的[15]。但在实践中,客户的知情权极易受到干扰。信息处理者一般会象征性地履行其告知义务,要求客户签订隐私保护政策,但信息处理方的告知并不意味着客户方对相应事项的知情。银行的隐私保护政策通常篇幅较长且重点不突出,这是因为数据处理者不愿背负隐瞒信息所带来的法律上的不利后果,而为了追逐更多的利益,倾向通过信息混杂、行文冗长等方式隐藏重要信息,为其数据处理行为找到最大的合法化可能[16]。这就导致信息过载问题的出现,客户难以在告知文件提供的过量的信息中找到少量的有效信息。且随着大数据等科技的发展,相应的数据处理的条文对于普通的金融客户来说用语晦涩难懂,教育背景不同的客户对同样的条款的认知也会存在偏差,高昂的信息提取成本会使客户无暇顾及协议的实体内容[17],在未得到充分信息进行价值衡量的情况下,作出流于形式的同意[18]。

2. 客户的自决权遭受限制

在客户作出代表私人自治的同意时,现有的授权模式并没有很好地尊重客户的自决权。自决权包括同意与否、同意的程度和同意的有效期限。有关同意与否的问题,《金融消费者权益保护实施办法》(以下简称《实施办法》)规定除金融信息的处理是必须的以外,银行不能因为消费者不作出

授权而拒绝提供相应产品或服务。这一规定看似保护了客户自由选择是否同意的权利，但在现实中隐私保护政策一般以格式条款的形式呈现在客户面前，客户无法与银行协商，个人想要享有正常的基础的金融服务，对于银行提出的收集信息的要求很难表示拒绝，客户的权利空间受到了压缩。同意程度问题其实就是《实施办法》中所规定的“银行、支付机构应当建立以分级授权为核心的消费者金融信息使用管理制度”，客户对于不同敏感程度的数据能否被转移处理的态度是不同的，只有分级处理才能更好地表达客户的真实意愿。但现行有关授权规则明显过于笼统，未根据个人数据的类型作出区分，无论数据公开与否、敏感与否都统一规定，未根据不同的数据分享对象作出不同的授权要求[19]，这就导致了在开放银行实践中出现问题。由于开放银行的核心是数据共享，相关服务必然涉及信息的处理，银行对此的态度亦是同意授权即可使用服务，不同意授权即离开[20]，客户所想享受的服务可能只涉及敏感程度较低的个人数据处理，其也同意该程度的数据共享，却由于现行授权规则无法作出仅同意低敏感信息处理的意思表示，而被迫放弃了本该在分级授权模式下享有的服务。关于同意的有效期限问题，客户一旦对隐私保护政策表示同意后，其同意被视为无期限的，即使隐私保护政策内容发生实质性的变更后，银行也仅是使用弹窗、公告等形式推送给客户，让客户自行承担及时关注隐私保护政策变化的审慎义务。如果客户对修改后的隐私保护政策表示不满意，则被捆绑性地不能使用该行的所有产品与服务。且客户作出授权是十分简便的，但想要变更授权与撤销授权则较为繁琐，需要通过电话、银行网络平台等途径，客户的自决权难以得到保障。

（二）数据安全风险的成因

在传统思维下，银行被视为客户个人金融信息的看守者。传统银行法通过强调商业银行对客户金融数据的保密原则来规制商业银行，未经客户明示或默示的同意，银行不得披露客户的金融状况[21]，将个人金融信息数据安全作为最终目的。此时数据是不流通的。数据共享就意味着数据安全风险的增加，银行要在现有的法律框架下承担责任。但数据流通共享是大势所趋，不能因为过于担心数据安全而因噎废食。银行不再是传统的个人金融数据的最终存储者，更多地是承担类似“数据处理与中转站”的责任，不能再将数据安全保护的责任主要让银行承担，权责不对等将阻碍商业银行选择跨入开放银行阶段，应当以数据保护促进数据共享[22]。然而现有法律缺少对接受数据共享的主体明确的准入标准规定，使不合规的第三方机构加入数据共享链是数据安全风险的主要成因。在开放银行中，接受数据共享的主体通常会因为其薄弱的数据安全防护能力成为风险源头。

拥有足够的实力与意愿维护数据安全的第三方机构的加入，会使影响数据安全风险的技术风险与网络风险随之减少。传统银行业模式下，商业银行只有经批准才能设立，并受到专门的银行业监督管理机构监督，相对具有可信性。参与开放银行数据共享浪潮的第三方机构数量庞大，其相应的数据处理与数据安全防护等能力参差不齐。开放银行发展初期我国并没有对第三方机构设置严格的准入门槛。尽管中国人民银行发布的《商业银行应用程序接口安全管理规范》中专门规定了应用方（包括第三方机构）的准入规则，由商业银行承担对应用方进行多维度考察的审核义务，但因为没有具体可参照的审核指标，使银行难以在实践中对所有申请的第三方机构做到公平审核。完全将审核第三方的监管义务给予了商业银行，这种做法耗时且成本高昂，可能会导致排他性关系从而抑制竞争；相反，标准化流程将降低潜在数据接收者的成本，使得数据接收者按照单一的认证流程向客户提供服务[23]。制定一定的标准化流程既可以便利银行，减少审核的成本，提高审核结果的可信度，又可以对意图争取银行数据共享许可的第三方机构进行指引，还可以让客户对接受数据共享的主体产生基本认知。

（三）数据滥用风险的成因

开放银行使得个人信息数据传递的链条被延长、参与的数据处理主体增加。现有的法律主要是针对原有“客户、银行”的构造制定的，由于客户在这种主体构造中处于被动的弱势地位，所以法律法规所规制的对象主要为银行类的金融机构，而传统的监管体系也主要是针对银行这类金融机构。开放银行模式下已然构成了“客户、银行、第三方机构”的三方构造，传统的监管模式几乎失能[24]。虽然《实施办法》所适用的对象还包括提供支付服务的非银行支付机构，这也是开放银行

框架下的第三方机构,但第三方机构并不局限于支付机构,所以,现有的法律制度与监管体系都缺少了对于开放银行中第三方机构的规制。减少数据滥用风险的关键是确保第三方机构在后续的数据共享过程中合理地利用数据,其中信息披露是数据共享必要措施。

客户授权后,在数据共享过程中陷入被动地位。银行与第三方机构作为数据的实际处理者与控制者,凭借其所处的数据共享链的位置与相对高水平的数据处理专业能力,可以轻易隐瞒客户,对数据进行不正当的使用。数据处理者与客户之间存在严重的信息不对等,只能依赖法律规范对客户进行倾斜保护,让其获取真实信息,与数据处理者进行平等对话[25]。对于银行与第三方机构而言,由于如今数据处理与传输都是通过网络进行的,现有技术实现数据记录的功能并不存在过多障碍,为客户提取记录并予以查询,即信息披露并不会增加许多成本,是具有可行性的。但基于资本本身对于利益的追逐,在没有法律强制性规定的前提下,信息披露就意味着给予客户找到其问题的可能,会造成利益损失,银行和第三方机构没有充分的激励机制促进其保护个人数据,故其不愿向客户进行信息披露[26]。为此,必须强化参与方的数据披露义务。信息披露制度属于信息流动工具,是经济法对信息不对称的有效法律规制措施[27]。信息披露意味着保持透明与开放,既增加信任,又可以明确具体环节的责任人,确保数据正当处理标准的实施[28]。

三、开放银行数据风险的法律防范措施

我国开放银行发展迅速,肩负着推动我国金融开放、金融创新的重要责任。开放银行改变了原有的组织架构与运营模式,目前的立法并没有与开放银行相适配,而市场主体的个人数据保护意识不断增强,开放银行数据风险问题亟待解决。在厘清各类数据风险成因的基础上,法律防范措施如下。

(一)数据授权风险的法律防范措施

数据授权风险存在的主要原因是目前采用的知情同意授权模式并不能表达出客户的真实意愿。应当重新设计数据共享事前的数据授权模式。在遵循知情同意的基本逻辑框架的前提下,更改具体的表现形式,使其更易于保证客户的知情权和自决权。

1. 保障客户的知情权

为了确保客户的知情权,对于银行提供的隐私保护政策信息过载问题,银行需要精简隐私保护政策内容,减少例如“为提升用户体验……”等抽象性描述,对于关键性信息采用加粗字体、标红等方式引起客户的注意。对于隐私保护政策文本复杂难懂的问题,银行方应对专业性术语进行专门的解释,包括但不限于提供更详细解释的链接服务,采取弹出窗口的方式强化告知[29]。最大程度上使银行的告知转化成客户的知情。

2. 保证客户的自决权

为了保证客户基于自决作出同意的授权意向,从外在形式上,由于格式合同的特性使得一方只能作出全部同意或不同意的两种选择,不存在只同意一部分的选择,其不具有协商功能。因此客户与银行签订的数据共享事前条款应当独立,避免成为格式合同的组成部分。银行的隐私保护政策应当逐步由纯粹的阅读文本转变为功能文本[30]。隐私保护政策需要抛弃原有的格式条款形式,转变为具有多项选择的模式,让客户根据自身需求选择同意接受的部分条款,不必为了获取基础性服务而同意过度的信息收集与处理条款。这种模式还可以彻底落实分级的个人数据共享授权制度[31],银行可以参照《个人金融信息保护技术规范》,依据个人金融数据的敏感程度将其要收集与共享的数据进行分类,让客户自由选择愿意被收集与转移的个人数据的敏感程度,客观上起到对接受数据共享主体的筛选作用。

为了满足客户便于更改授权与撤销授权的需求,银行应当在其开放平台上增设专门用于授权的操作板块。该板块应当详细列出客户已经作出的授权的相关信息,包括授权对象与授权内容等,让客户可以随时查看个人金融数据被共享的情况。当客户对接收数据的主体产生不信任后,可以快速变更或撤销授权,减少进一步风险的发生。银行对现有的隐私保护政策进行更新后,可在该板块提示客户对更新内容进行查看,减少客户错过推送内容的可能性。

(二)数据安全风险的法律防范措施

1. 建立第三方准入审核机制

建立第三方准入审核机制是应对数据共享中数据安全风险的重要策略。对于第三方的准入标准制定,监管机构应当细化审核第三方的规则,将服务范围、风险管控能力与数据处理技术水平等

考察内容标准化，为商业银行审核第三方机构提供具有可操作性的标准。结合我国金融市场的现状与开放银行的发展过程，对开放银行数据共享的监管适宜采取一种具有无强制而强干预特质的运行模式[32]——助推型监管模式[8]。不宜让监管机构直接承担对第三方机构进行审核的工作。在细化审核标准后，对第三方机构的具体审核工作仍然交付具体的商业银行，第三方机构通过商业银行的审核后，商业银行要将相关审核内容提交监管机构进行复审，复审通过后第三方机构才具有成为开放银行数据共享主体的资格。第三方准入审核机制既尊重商业银行与数据共享第三方机构之间的交易主体性，不破坏原有的审核流程，还可以发挥监管机构的监管作用，在客观上起到了稳步推进开放银行制度实施的作用[33]。

2. 引入开放银行数据共享认证机制

引入开放银行数据共享认证机制——“白名单”与“黑名单”机制。有些拥有雄厚实力的第三方机构希望且有能力与尽可能多的商业银行达成数据共享的合作，如果每家商业银行都需要对其进行审核并提交监管机构复核，可能导致资源的浪费，因此，可以将通过了大多数商业银行审核与监管机构复核的第三方机构列入“白名单”，那些明显不符合资质的第三方机构则列入“黑名单”，这在客观上可以节省审核资源。需要注意的是，“白名单”与“黑名单”均需动态进出才能发挥作用，这就需要商业银行或监管机构定期进行核查，防止数据造假等问题，也可以给予第三方机构更多机会。

（三）数据滥用风险的法律防范措施

1. 明确数据共享参与方的信息披露义务

为减少数据滥用风险，需强化数据共享参与方的数据披露义务。就我国的信息披露义务的承担主体而言，银行与支付机构等金融机构的披露主体地位在各类金融类规范文件中已被确认，而第三方机构由于涉及范围较广，且我国法律规范的修订速度与开放银行的实践发展进程不相匹配，目前并没有系统规定第三方机构信息披露义务的法律规范出台。开放银行模式下第三方机构的信息披露义务主体的地位要被法律规范文件首先予以确认，信息披露的具体操作细则的法律文件应稳步制定。数据授权阶段，银行在信息披露义务承担中占主要地位，主要是通过信息披露让客户了解数据收集的目的、范围等内容，让客户得以判断数据共享的风险。数据共享阶段，在“银行、第三方机构”的构造中，银行对于数据的掌控力明显弱于第三方机构，此时第三方机构主要承担信息披露的义务，银行承担的是辅助披露等次要义务。

2. 区分不同参与方的信息披露义务

由于不同阶段信息披露义务的主要承担主体不同，其相应的披露内容也有不同侧重。银行的信息披露内容侧重于相关客户授权数据共享前应当知晓的数据流转内容，包括共享的数据范围、共享数据的目的、数据接收方的信息、数据共享的持续时长与可能存在的风险等。第三方机构的信息披露内容应当侧重于共享后的数据后续使用情况，包括获取共享数据的时间、共享数据的目的、是否按照授权约定处理数据与采取了哪些安全保障措施等内容，在最大程度上让客户知晓数据共享的全过程信息。第三方机构的信息披露在很大程度上会因为客户自身对于数据授权的不同选择而不同，对于不同客户而言是特定化的，所以需要银行提供可供客户查询自身有关信息披露内容的渠道，确保信息披露不会成为隐私泄露的缺口。除了这类日常数据处理的信息披露外，在危及信息安全的事件发生后，银行与第三方机构要及时统一地向客户群体通知安全事件的基本情况、安全事件可能造成的影响及已经采取的弥补措施，让客户第一时间知晓安全事件的进展，减少因未知可能产生的恐慌。需要注意的是，如果信息披露过于专业复杂，普通客户无法阅读明白，则信息披露就丧失了一定的功能，所以银行与第三机构在发布信息披露内容前，要将内容通俗化，对关键信息以醒目方式标注，便于客户理解，减少信息过载带来的阅读障碍。

注　　释：

①参见：《中国人民银行关于印发〈金融科技发展规划（2022—2025 年）〉的通知》（银发〔2021〕335 号）。

②参见：北京知识产权法院（2016）京 73 民终 588 号民事判决书。

③详细内容参见银罚决字〔2023〕39-54 号。

④参见：英国介入脸书用户数据泄露案 搜查剑桥分析办公室[EB/OL]. http://www.xinhuanet.com/world/2018-03/25/c_129836753.htm. 2023-12-13。

⑤详细内容参见银罚决字〔2023〕34-38 号。

⑥详细内容参见（2021）浙 06 民终 3129 号。

参考文献:

[1]MOYER K. How to build an open bank[EB/OL].[2023-12-13]. https://www.gartner.com/en/docunmenrs/3746220.

[2]杨东,龙航天.开放银行的国际监管启示[J].中国金融,2019(10):78-80.

[3]梁伟亮.金融征信数据共享:现实困境与未来图景[J].征信,2019(6):14-19.

[4]王利明.数据共享与个人信息保护[J].现代法学,2019(1):45-57.

[5]许可.开放银行的制度构造与监管回应[J].财经法学,2019(5):122-136.

[6]黄茂钦,周坤琳.金融数据治理的激励与规制路径探析[J].中国应用法学,2020(6):111-124.

[7]金励,周坤琳.数据共享的制度去障与司法应对研究[J].西南金融,2020(3):88-96.

[8]张建.我国开放银行数据共享的监管模式选择[J].政法论丛,2023(1):65-76.

[9]宣峨,房燕.我国开放银行数据共享的风险挑战与法律规制[J].征信,2022(7):39-44.

[10]王海明.数智化形塑中个人信息权益的失衡风险与新平衡[J].浙江学刊,2023(6):116-128.

[11]杨洸.数字媒体时代的数据滥用:成因、影响与对策[J].中国出版,2020(12):3-8.

[12]杨东,程向文.以消费者为中心的开放银行数据共享机制研究[J].金融监管研究,2019(10):101-114.

[13]DIMACHKI M E. More data and more data sharing:navigating an open banking world[J]. Journal of Digital Banking,2019,3(3):206-214.

[14]周坤琳.经济法实质公平原则对数字鸿沟的消解与弥合[J].征信,2022(4):57-65.

[15]郑佳宁.知情同意原则在信息采集中的适用与规则构建[J].东方法学,2020(2):198-208.

[16]吕炳斌.个人信息保护的"同意"困境及其出路[J].法商研究,2021(2):87-101.

[17]万方.隐私政策中的告知同意原则及其异化[J].法律科学(西北政法大学学报),2019(2):61-68.

[18]丁晓强.个人数据保护中同意规则的"扬"与"抑":卡-梅框架视域下的规则配置研究[J].法学评论,2020(4):130-143.

[19]赵吟.开放银行模式下个人数据共享的法律规制[J].现代法学,2020(3):138-150.

[20]程啸.论大数据时代的个人数据权利[J].中国社会科学,2018(3):102-122.

[21]谈李荣.银行与客户法律关系[M].北京:中国金融出版社,2004:33.

[22]丁晓东.论企业数据权益的法律保护:基于数据法律性质的分析[J].法律科学(西北政法大学学报),2020(2):90-99.

[23]温树英.开放银行监管的英国经验及启示[J].山西大学学报(哲学社会科学版),2023(2):152-160.

[24]易宪容,陈颖颖,周俊杰.开放银行:理论实质及其颠覆性影响[J].江海学刊,2019(2):86-93.

[25]何颖.数据共享背景下的金融隐私保护[J].东南大学学报(哲学社会科学版),2017(1):85-91.

[26]周汉华.探索激励相容的个人数据治理之道:中国个人信息保护法的立法方向[J].法学研究,2018(2):3-23.

[27]邢会强.走向规则的经济法原理法[M].北京:法律出版社,2015:57.

[28]许可.数据交易流通的三元治理:技术、标准与法律[J].吉首大学学报(社会科学版),2022(1): 96-105.

[29]田野.大数据时代知情同意原则的困境与出路:以生物资料库的个人信息保护为例[J].法制与社会发展,2018(6):111-136.

[30]李延舜.我国移动应用软件隐私政策的合规审查及完善:基于49例隐私政策的文本考察[J].法商研究,2019(5):26-39.

[31]管洪博.数字经济下个人信息共享制度的构建[J].法学论坛,2021(6):106-113.

[32]张力.迈向新规制:助推的兴起与行政法面临的双重挑战[J].行政法学研究,2018(3):88-98.

[33]邢会强.论数据可携权在我国的引入:以开放银行为视角[J].政法论丛,2020(2):14-24.