主题研讨

个人金融信息保护的逻辑与规则展开

朱芸阳

内容提要:个人金融信息在我国法律体系内始终颇受重视,但又长期定位不清。个人金融信息处于个人信息保护与金融市场监管的交叉领域,信息之于金融行业至关重要。兼具双重属性的个人金融信息承载着不同等级位阶的价值利益,法经济学的分析范式在金融领域的应用,以及国际视域下金融信息共享机制的规则趋同,都为促进金融信息共享提供了正当性理由。个人金融信息保护与促进信息共享两大目标的耦合和平衡,取决于如何配置和协同在事前授权、事中赋权和事后追责等环节的不同规则。我国《个人信息保护法》在适用于金融领域之时,个人金融信息不宜都被视为敏感个人信息,应为处理个人金融信息提供更为周延的合法性事由,同时应强化金融机构的告知义务,实现信息共享机制下个人信息主体的知情权保护。

关键词:个人金融信息　敏感个人信息　信息共享　注意义务　侵权责任

朱芸阳,中央民族大学法学院副教授。

一　问题的提出

伴随着大数据技术在金融领域的广泛应用和迅速迭代,金融业作为高度信息化的行业,不断产生和处理着大量的个人信息。信息、市场和风险紧密相关,个人金融信息保护处于个人信息保护与金融市场监管的交叉领域,关注个人信息保护和信息安全、尊重和保护金融消费者的权益保护已经成为金融监管的共识。但是,金融行业高度重视市场效率,以鼓励创新、挖掘信息价值为其内在驱动,客观上也催生了信息共享利用的迫切需要。在我国法律体系内,个人金融信息始终颇受重视,但又长期定位不清。我国法律法规体系中散落着很多与个人金融信息保护、信息安全、金融数据治理相关的具体条款,人民银行等金融监管部门更是通过部门规章、国家标准、规范文件等举措落实个人金融信息保护。我国《个人信息保护法》经多年酝酿终于在 2021 年出台,成为个人信息保护领域的基本法律,旨在兼顾实现个人信息权益保护与个人信息合理利用这两大立法目标。其中,第 28 条

第1款将“金融账户”纳入敏感个人信息的范畴,适用更为严格的处理规则。该规定无疑为强化保护个人金融信息提供了重要法律基础,但是也衍生出若干法律适用问题。本文将基于法经济学的视角,观察国际视域下金融领域的个人信息保护体系,对下列问题逐一探讨:

第一,个人金融信息实际上是一个概括与庞大的信息群,除了《个人信息保护法》列举的“金融账户”之外,我国现行法律、法规、规范性文件中有与其相类似的表述,例如银行账号、银行账户、支付账户、账户信息等等,而对个人金融信息中的其他子类别信息也有所涉及,包括交易信息、信用信息、财产信息等等。现行《个人信息保护法》并没有明确“金融账户”的内涵意蕴,那么它与前述不同类别的信息之间是何关系仍待阐明;进而,其他个人金融信息是否也有必要被认定为敏感个人信息?

第二,在个人信息保护法的立法过程中,关于是否应当将个人金融信息纳入敏感个人信息的范畴,一直存在争议。有学者肯定金融信息的敏感性,建议将其纳入敏感个人信息,〔1〕但也学者认为,各国对于敏感信息的范围界定并不完全一致,但通常并不会将金融信息认定为敏感信息。〔2〕欧盟、日本、韩国、我国台湾地区也区分敏感和非敏感信息,但均未将金融信息纳入敏感个人信息的范畴。学者欧姆(Paul Ohm)提出确立敏感个人信息的四大因素,即伤害的可能性、伤害概率、特定信任关系、公众关注度,指出基于特定社会事件的发生,公众对某种信息的敏感性提高,从而获得立法采纳,其中包括金融信息。〔3〕实践中存在着大量需要处理个人金融信息的应用场景,个人金融信息的阈值宽泛,实务界长期呼吁要充分考虑金融行业和个人金融信息的特殊性,认为将个人金融信息纳入敏感个人信息范畴,于金融业并无裨益;相反,为了提升服务效率和满足客户需求,更需要促进个人金融信息的共享利用。因此,需要反思个人金融信息和《个人信息保护法》中“敏感个人信息”之间的关系,以及它们在我国现行立法体系中的定位。

第三,《个人信息保护法》作为我国个人信息保护领域的基本法律,具体到金融领域,存在多元化的金融信息应用场景,应当如何正确适用和延展相应的个人信息处理规则,真正协调实现保护“个人信息权益”和“促进个人信息合理利用”这两大立法目标,也是当下亟待解决的问题。

二 个人金融信息保护的成因与逻辑推演

(一)个人金融信息的法律规范群

不同于以美国为代表的采用单独立法模式的国家,针对金融领域的个人信息保护,我国并未形成单独的立法规范,与个人信息保护相关的条款散落在《中国人民银行法》《商业银行法》《证券法》《保险法》《反洗钱法》《征信业管理条例》等法律法规中。中国人民银行多次通过发布规范性文件在个人金融信息的收集和使用、商业银行的报告义务和法

〔1〕 参见胡文涛:《我国个人敏感信息界定之构想》,《中国法学》2018年第5期,第248-249页。

〔2〕 参见王敏:《大数据时代个人隐私的分级保护研究》,社会科学文献出版社2018年版,第146页。

〔3〕 See Paul Ohm, Sensitive Information, 88 *Southern California Law Review* 1125, 1161 (2015).

律责任等方面作出明确规定。央行规范性文件《关于银行业金融机构做好个人金融信息保护工作的通知》首次使用“个人金融信息”的定义。[4] 2020 年修订的《中国人民银行金融消费者权益保护实施办法》(下称“《金融消费者保护办法》”)专设第三章“消费者金融信息保护”,对消费者金融信息的定义、信息收集、信息出境、信息安全义务等内容作出规定。现将相关法律法规、规范性文件中个人金融信息的不同表述归纳如下:

表 1 法律、法规、规范性文件中的不同表述

颁布时间	法律法规、规范性文件	不同表述
2000 年 3 月	国务院《个人存款账户实名制规定》	个人存款账户
2003 年 4 月	中国人民银行《人民币银行结算账户管理办法》	银行结算账户信息
2006 年 10 月	《反洗钱法》	客户身份资料、交易信息
2007 年 6 月	中国人民银行等四部委《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》	客户身份资料、交易记录
2011 年 1 月	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》	个人金融信息
2013 年 1 月	国务院《征信业管理条例》	个人信息、信用信息、信贷信息
2014 年 6 月	中国人民银行《关于 2013 年个人金融信息保护专项检查情况的通报》	个人金融信息、客户信息
2015 年 12 月	中国人民银行《非银行支付机构网络支付业务管理办法》	支付账户、交易信息、敏感信息、客户信息
2016 年 8 月	最高人民法院《关于人民法院在互联网公布裁判文书的规定》	银行账号
2016 年 11 月	《网络安全法》	个人信息、重要数据
2016 年 12 月	证监会《证券期货投资者适当性管理办法》	财务状况、投资经验
2017 年 5 月	最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	账号密码、财产状况;征信信息、财产信息、交易信息
2018 年 5 月	银保监会《银行业金融机构数据治理指引》	个人信息、业务信息
2020 年 2 月	中国人民银行《个人金融信息保护技术规范》	个人金融信息(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、衍生信息等)

〔4〕 该文件第一点规定:个人金融信息是指银行业金融机构在开展业务时,或通过接入中国人民银行征信系统、支付系统以及其他系统获取、加工和保存的以下个人信息:个人身份信息、个人财产信息、个人账户信息、个人信用信息、个人金融交易信息、衍生信息以及在与个人建立业务关系过程中获取、保存的其他个人信息。

（续表1）

颁布时间	法律法规、规范性文件	不同表述
2020年3月	国家市场监督管理总局、国家标准化管理委员会《信息安全技术 个人信息安全规范》	个人敏感信息（列举了银行账户、征信信息、交易信息）
2020年9月	中国人民银行《金融控股公司监督管理试行办法》	客户信息
2020年9月	中国人民银行《金融消费者权益保护实施办法》	消费者金融信息（个人身份信息、财产信息、账户信息、信用信息、金融交易信息）
2021年8月	《个人信息保护法》	金融账户

从个人金融信息的概念表述与体系解释来看，其大致可从以下两方面理解与建构：

其一，部门规章、行业标准通常采取概括、列举相结合的方式来界定个人金融信息。个人金融信息属于个人信息的子概念，但其范围相当宽泛，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他衍生信息。尤其是衍生信息的边界并不清晰，其包括对原始数据进行处理、分析后形成的能够反映特定个人某些情况的信息，例如个人消费或者投资意愿、支付习惯、风险偏好等等。就内涵而言，其必须与信息主体获得金融产品或者服务具有关联性。原则上，为信息主体提供金融产品或者服务所必需的个人信息属于个人金融信息。

其二，《个人信息保护法》第72条第1款规定，该法不适用于自然人因个人或者家庭事务处理个人信息的场景，个人金融信息处理者主要是指包括银行、支付机构在内的、由国家金融管理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，例如个人征信公司。但是，个人金融信息又不限于金融机构通过开展金融业务获取的信息，而是还包括从其他合法渠道处理的个人信息。这里强调个人信息获取渠道的合法性，是与《个人信息保护法》中规定的信息处理的合法性事由相匹配的。

（二）个人金融信息的双重属性

个人信息的产生、处理过程离不开信息主体，个人金融信息通常由信息主体主动提供给金融机构，或者是产生于金融机构提供金融服务或者产品的过程中。我国学界有观点认为，个人信息权益属于不同于隐私权、名誉权等具体人格权的一种新型人格权益，〔5〕个人金融信息以自然人的人格利益为其内核，具有强烈的私人属性。同时，也有学者关注到个人信息的公共性价值，〔6〕数据的互惠分享是互联网赖以生存的基础生态规则，〔7〕指出

〔5〕 参见王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，《现代法学》2013年第4期，第69页；程啸：《论我国民法典中个人信息权益的性质》，《政治与法律》2020年第8期，第10－11页。

〔6〕 参见高富平：《个人信息保护：从个人控制到社会控制》，《法学研究》2018年第3期，第95页。

〔7〕 参见梅夏英：《在分享和控制之间——数据保护的私法局限和公共秩序构建》，《中外法学》2019年第4期，第855页。

西方个人信息的保护直接服务于消费者权益和公法目的。[8] 较之其他个人信息，个人金融信息的公共性属性尤为突出。

1. 个人金融信息的应用场景

美国学者尼森鲍姆教授（Helen Nissenbaum）提出“场景完整理论”，[9] 认为隐私保护与具体场景相关联，[10] 同一信息的敏感度在不同场景中并不确定，隐私类别和敏感程度高度依赖于场景。[11] 但该理论由于适用模糊、无法清晰界定何为场景、缺乏实质性判断标准，也受到部分学者的质疑。[12] 何为场景确实很难完全抽象提炼出标准，但是，场景化确实在实践中具有广泛适用性，法律规范越复杂，规则制定、事前遵从和事后裁决就越困难，因此成本也就越高。[13] 类型化可以成为降低复杂性成本的手段，[14] 而并不会造成认识上的混淆或混乱。个人金融信息也是强调“场景化”适用的信息，不同类型的个人金融信息基于不同的应用场景，其保护力度存在差异，甚至同一信息在不同的服务场景中也可能具有不同的敏感度。因此，正确理解个人金融信息的保护理念和具体规则离不开对具体应用场景的剖析。

首先，金融机构处理个人信息，是开展金融业务的客观需要。金融机构开展金融业务以个人信息为要素，以处理个人信息为前提条件。即，“金融隐私披露或者说消费者对自身金融隐私的让渡是金融契约得以建立的前提。”[15] 在金融机构提供金融服务或者产品的过程中，新的个人金融信息不断产生和留存，例如交易信息、账号信息、信用信息与金融机构提供的金融服务和产品内容直接关联。并且，各国和地区通常将金融控股公司作为信息共享的特殊场景加以规制，金融机构混业经营是国内金融市场发展的大势所趋，中国人民银行 2020 年颁布《金融控股公司监督管理试行办法》已经开始关注通过共享客户信息来实现业务协同。此外，金融机构作为国家金融设施的组成部分，其开展金融业务也具备准公共机构的服务属性，这也迫切需要实现金融信息的共享流通，来实现识别有效融资需求、优化风险管控的目标。

第二，征信行业是个人金融信息处理的重要场景之一，金融机构处理个人金融信息，是各国征信体系建设的普遍做法。个人征信与个人金融信息紧密相关，个人征信报告是信贷信息的集合，甚至被视为金融领域的“第二身份证”。为获得信贷融资机会，借款人必须让渡部分个人信息，供放贷人评估其还款能力、意愿和风险定价。同时，由于借款人

---

〔8〕 参见丁晓东：《个人信息私法保护的困境与出路》，《法学研究》2018 年第 6 期，第 195 页。

〔9〕 See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

〔10〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Washington Law Review* 101, 137 (2004).

〔11〕 See Kirsten E. Martin, Helen Nissenbaum, Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables, 18 *Columbia Science and Techology Law Review* 176, 177 (2016).

〔12〕 参见谢琳、王漩：《我国个人敏感信息的内涵与外延》，《电子知识产权》2020 年第 9 期，第 6 页；胡凌：《功能视角下个人信息的公共性及其实现》，《法制与社会发展》2021 年第 5 期，第 178 页。

〔13〕 参见［德］克里斯托弗·布施：《个性化经济中的算法规制和（不）完美执行》，《环球法律评论》2019 年第 6 期，第 9 页。

〔14〕 See Louis Kaplow, A Model of the Optimal Complexity of Legal Rules, 11 *Journal of Law Economics & Organization* 150, 161 (1995).

〔15〕 朱宝丽、马运全著：《个人金融信息管理：隐私保护与金融交易》，中国社会科学出版社 2018 年版，第 2 页。

未来履约与否，会间接影响他人的信贷消费机会和金融稳定这一公共利益，因此征信体系是一个国家重要的金融基础设施，对提升信贷风险管理水平、维护金融稳定、促进经济增长有着重要的意义，具有一定的公共性。〔16〕

第三，金融机构处理个人信息，是为了满足金融监管所必须履行的法定义务。一是，各国针对反洗钱领域的法定义务虽有所差异，但总体而言，金融机构需要通过客户身份识别和客户尽职调查来履行其反洗钱、反恐怖融资等法定义务，发现异常和可疑资金，增进经济金融交易的规范化和透明度。我国《反洗钱法》第16条第1款规定，“金融机构应当按照规定建立客户身份识别制度。”客户身份识别并非一次性完成，而是分为初次识别、持续识别和重新识别，需要金融机构持续关注客户业务，对客户的基本信息进行定期审核。并且，实施穿透式监管，需要金融机构追踪实际受益所有人。二是，在财富管理领域，作为保护投资者利益的重要举措，信托公司、证券公司、私募基金等从业机构需要履行认定“合格投资者”的法定义务。三是，在证券投资领域，证券期货经营机构开展证券期货业务，需要履行账户实名制、投资者适当性管理的监管要求。评估投资者风险承受能力以处理投资者个人信息为前提条件，客观上也对其处理投资者个人信息提出了新的要求。〔17〕四是，随着金融科技的蓬勃发展，金融监管机构为了精准识别、防范和化解跨行业、跨业态、跨市场的交叉性金融风险，针对商业银行、保险公司、证券公司、金融控股公司等各领域都提出了穿透式监管要求。

2. 场景论下的价值等级位阶

个人金融信息本身具有公共性属性，在上述不同的应用场景中，依次承载着不同层次的利益，包括信息主体自身获取金融消费信贷的机会、他人获取信贷消费的机会、金融机构反欺诈的风险控制利益、金融市场乃至跨行业、跨市场的金融风险，甚至国家安全等逐层递进的不同利益，其背后蕴含着巨大的公共利用价值。美国著名法学家庞德构建的价值等级秩序对此具有借鉴意义。相互冲突的利益中哪一利益应该获得保障、哪一利益应该牺牲，其标准应为选择何种利益可以使整个利益纲目内的最多数利益获得保障。〔18〕

个人金融信息保护与实现信息共享两大目标如何耦合，取决于个人金融信息利用规则的设计配置。个人金融信息的应用场景不仅涉及到信息主体个人权益的实现保障，而且也涉及到信息在不同权利位阶中的效能发挥，包括个人信息保护利益与个人其他利益、个人利益与社会公共利益等不同利益之间的冲突、调整和兼容。因此，提供适度的个人金融信息利用和共享规则，实际上是完成在信息主体、金融机构以及共享信息的第三方之间权利和义务的配置。

（三）法经济法学的解释框架与逻辑展开

数字经济以数据为关键要素。法经济学代表人物科斯认为，作为市场上除了劳动和资本以外的重要资源，信息也是交易成本的要素。另外，波斯纳认为，隐私的经济尺度是

〔16〕 参见个人信息保护课题组：《个人信息保护国际比较研究》（第2版），中国金融出版社2021年版，第129页。

〔17〕 参见朱芸阳：《大数据技术在投资者适当性管理中的应用》，《金融博览》2020年第1期，第52页。

〔18〕 参见［美］庞德著：《法理学》（第3卷），廖德宇译，法律出版社2007年版，第244－251页。

“信息隐藏”,“通过减少买者可获得的信息量……就降低了那个市场的效率”。[19] 基于理性经济人的立场,消费者为了获取交易而受益,在信息披露的主动性上会根据自己要开展的业务种类而有不同选择,包括不披露信息、仅披露部分信息(正面或者负面信息)或者完全披露信息。而且声誉机制的存在,使得消费者更倾向于披露有利于自己的信息,隐藏不利于自己的信息。而信息隐藏会带来额外的调查、错误匹配等社会成本。因此,处于信息强势地位的人能获取超额收益,而信息弱势的人则付出了超额成本,这就会导致市场交易的公平性缺失,同时也增加了交易成本,最终使得市场效率大大降低。

信息之于金融行业至关重要,法经济学的分析范式、信息不对称理论研究被广泛应用于金融市场。在金融行业的不同细分领域,金融产品或服务的供给方与接收方之间普遍存在着金融信息不对称的现象。罗斯柴尔德(Michael Rothschild)和斯蒂格利茨(Joseph E. Stiglitz)关于信息不对称研究的基础性文献,开创了金融市场信息不对称研究的领域。[20] 威斯(Andrew Weiss)和斯蒂格利茨(Joseph E. Stiglitz)将信息不对称研究拓展至银行信贷市场,认为借款人与银行之间存在广泛的信息不对称,而借款人普遍存在逆向选择和道德风险,会导致信贷配给的数量约束及价格约束。[21] 以个人信息为基础构成的征信体系能很好地克服信贷市场的信息不对称,解决逆向选择问题和道德风险问题,起到传递信号、惩罚失信者和激励守信者的作用。随着大数据技术的发展,市场和交易跨越传统的时空限制,传统的信息识别成本有效降低,信息不对称也可得到缓解。

在有交易成本的世界里,法律的作用是至关重要的。法经济学上的“卡—梅框架”给法律规则作了类型划分,当交易成本较低时,采取财产规则是有效率的,反之则选择责任规则是最优的。[22] 因此,就个人金融信息的规则配置而言,在法经济学的视角下衍生出以下的归因公式:当信息的“产权”得到很好的界定时,信息共享就会得到有效配置。不同国家在产权规则方面的设计也不尽相同,如果将赋权视为一种产权分配,那么在美国金融信息保护立法中,“选择退出”模式实际上将信息的“产权”分配给了金融机构,而“选择加入”则将“产权”授予消费者,因此,“选择退出”模式更有可能实现信息共享的有效配置。[23] 而在我国,立法者建立以“知情 - 同意”为核心的个人信息处理规则,赋予信息主体控制个人信息的具体权利,实质上将信息的“产权”分配给了信息主体。

(四)美欧个人信息保护实践的趋同

联合国于 2015 年 12 月通过了 70/186 项决议,对其准则性文件《联合国消费者保护准则》进行修订,在总则第 5 条中明确将“保护消费者隐私”和“全球信息自由流动”并列

---

〔19〕 Richard A. Posner, *The Economics of Justice*, Harvard University Press, 1981, p. 405.

〔20〕 See Michael Rothschild, Joseph E. Stiglitz, Equilibrium in Competitive Insurance Market: An Essay on the Economics of Imperfect Information, 90 *Quarterly Journal of Economics* 629, 648 (1976).

〔21〕 See Andrew Weiss, Joseph E. Stiglitz, Credit Rationing in Markets with Imperfect Information, 71 *The American Economic Review* 393, 393 (1981); 王作功等:《数字金融的发展与治理:从信息不对称到数据不对称》,《金融理论与实践》2019 年第 12 期,第 26 页。

〔22〕 See Guido Calabresi, A. Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of The Cathedral, 85 *Harvard Law Review* 1089, 1110 (1972).

〔23〕 See Financial Privacy: An Economic Perspective, CRS Report for Congress RL31758, 2003, https://epic.org/privacy/glba/RL31758.pdf, 最近访问时间[2021 - 08 - 01]。

对待，作为第四项准则。从美国、欧盟的立法实践来看，其都已经关注到个人金融信息的公共性属性，在具体规则配置上遵循上述准则，兼顾实现保护消费者隐私和全球信息自由流动这两大目标。

1. 美国：共享基础上加强个人权利

就个人信息保护立法模式而言，以美国为代表的国家采取了各行业领域单独立法的模式。对于隐私保护与信息共享，主要呈以下特点。

一方面，从其立法理念来看，促进信息共享利用始终是金融领域立法的首要目标，在特定的金融领域中还在逐步放宽与其他机构共享金融信息的范围和前提条件。《金融服务现代化法案》（*The Gramm-Leach-Bliley Act*，*GLBA*）是一项旨在促进整个金融服务业信息有效共享的联邦立法尝试，[24] 其立法目标是通过消除“银行、保险和证券业之间的联营壁垒”，以便于用户获取“一站式”金融服务，从而提升行业效率，降低机构交易成本，提高行业利润。[25]

基于促进信息共享的立法思路，具体规则主要是围绕如何实现金融机构与其他机构高效共享信息而展开，主要体现在：一是，采取关联方“无需同意”以及非关联方“默示同意”的授权模式。金融机构与其关联机构之间，以及与其专门设立进行数据处理的公司之间，[26] 无需获得个人授权，即可自由共享非公开个人信息；在金融机构向消费者发出“选择退出”通知（opt-out notices），并对如何行权进行说明的前提下，金融机构可以与非关联方共享非公开个人信息。[27] 值得注意的是，《金融服务现代化法案》允许各州单独制定比联邦标准更高的隐私保护标准，[28] 各州立法的分歧正是主要集中于是否需要采用“选择加入”（opt-in）的授权模式。[29] 二是，规定金融机构无需提供“选择退出”权利的例外情形，客观上又促进了信息共享，弱化了信息主体的选择退出权利。例如，基于“共同营销行为”，[30] 即出于为用户提供服务所必需，或者金融机构本身或与其他机构共同营销的需要，以及在立法规定的例外情形下，[31] 金融机构可直接向非关联方披露消费者的非公开信息。

---

〔24〕 See Steven R. Roach, William R. J. Schuerman, Privacy Year in Review: Recent Developments in the Gramm-Leach Bliley Act, Fair Credit Reporting Act, and Other Acts Affecting Financial Privacy, 1 *I/S: A Journal of Law and Policy for the Information Society* 385, 390 (2005).

〔25〕 See Julia C. Schiller, Informational Privacy v. The Commercial Speech Doctrine: Can the Gramm-Leach-Bliley Act Provide Adequate Privacy Protection?, 11 *CommLaw Conspectus* 349, 355 (2003).

〔26〕 美联储颁布的《Y 监管条例》（12 CFR Part 225 - Bank Holding Companies and Change in Bank Control, Regulation Y）扩大了金融控股公司的业务范围，该条例第 28 条规定了金融控股公司“允许从事的非银行业务清单”（List of permissible nonbanking activities），范围包括“数据处理”公司，即银行控股公司及其子公司可以设立专门进行数据处理、数据存储和数据传输活动的公司。

〔27〕 15 U. S. C. §6802 (a) (b). 非公开个人信息包括：金融机构收集的、与个人提供金融产品或服务有关的、任何可识别个人身份的金融信息，不包括金融机构有合理依据认为合法“公开”的信息。另外，金融机构可以合法取得但消费者选择不公开的信息也属于非公开个人信息。

〔28〕 15 U. S. C. §6807 (b).

〔29〕 See Financial Privacy: Status of State Actions on Gramm-Leach-Bliley Act's Privacy Provisions, United States General Accounting Office Report 02 - 361, April 2002, https://www. gao. gov/assets/gao - 02 - 361. pdf, 最近访问时间 [2021 - 08 - 01]。

〔30〕 15 U. S. C. §6802 (b) (1).

〔31〕 15 U. S. C. §6802 (e).

另一方面,在遵循促进信息共享的整体宗旨之上,该法案第五章关于“非公开信息披露”的规定,回应了社会对金融隐私保护存在的担忧。[32] 联邦执法机构在执法实践中发展出了金融机构在处理非公开个人信息时应当同时遵守的两套规则体系:信息安全保障规则[33]和隐私保护规则。其中,隐私保护规则主要体现在以下三个方面:一是,信息主体有权获取隐私政策通知(privacy notice),并对隐私政策通知的内容及其方式作出明确规定。[34] 二是,赋予信息主体的选择退出权利。在金融机构与非关联方共享信息之前,信息主体享有“选择退出”的权利。三是,对共享信息进行限制,包括限制信息的再次重复共享,即除非另有规定或者金融机构直接合法授权,否则非关联方不能再将其从金融机构获取的信息提供给其他第三方;限制金融机构仅为了营销目的而与非关联方共享消费者的信用卡账户、存款账户或交易账户(account numbers)、类似的访问号码或代码。[35] 概言之,在金融领域中个人享有的信息控制权利是相对有限的,促进信息共享利用仍然是个人信息处理的首要原则。

2. 欧盟:严格保护个人数据基础上的“开放银行”模式

作为个人信息保护领域统一立法模式的代表,欧盟《通用数据保护条例》(*GDPR*)是适用于各行业领域的基本立法,同样适用于金融领域。基于提升金融科技发展的宏观愿景,欧盟意图在通过《通用数据保护条例》提升整体个人信息保护水平的同时,也通过修订《支付服务指令修正案》(*Payment Service Directive 2*, *PSD2*,下称“《支付指令》”),[36]增强对金融业特别是银行业数据的开放利用,这为传统金融机构与金融、支付领域的新兴参与者之间加强合作和便于操作奠定了基础。《支付指令》于 2016 年 1 月 12 日开始生效,采取了“开放银行”(opening bank)的思路;开放银行作为一种新的金融发展理念发端于英国,引发了全球银行业的新一轮转型浪潮。

从开放银行的理念以及《支付指令》的具体规则来看,其包括以下内容:第一,“开放银行”本质上是加强金融机构与第三方机构的金融信息共享。即强制要求金融机构通过应用程序编程接口(API),对第三方支付服务提供者开放用户账户信息权限;第三方支付服务访问客户的支付行账户及获取交易信息,为其提供支付启动、账户信息查询和资金确认这三种服务。第二,个人数据处理应当遵守欧盟关于个人数据保护的指令,第三方支付服务提供者访问、处理和留存为用户提供服务所需的个人信息,原则上以用户明确同意(explicit consent)为前提条件。同时,为了防止、调查和发现支付欺诈,允许支付系统和支付服务提供者在必要时处理个人信息。第三,采取信息安全措施是实现信息共享的前提条件。根据《支付指令》第五章的规定,欧盟进一步颁布了《关于强客户身份验证和通用

〔32〕 See Eric Poggemiller, The Consumer Response to Privacy Provisions in Gramm-Leach-Bliley: Much Ado About Nothing?, 6 *North Carolina Banking Institute Journal* 617, 618 (2002).

〔33〕 15 U. S. C. §6801 (a) (b).

〔34〕 See FTC, How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act, https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm,最近访问时间[2021-08-01]。

〔35〕 15 U. S. C. §6802 (c) & (d).

〔36〕 Directive (EU) 2015/2366.

安全开放通信标准的监管技术标准》(*Supplementing Directive with Regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication*,下称"《监管技术标准》"),[37]该标准包括强客户身份验证、安全通信技术标准、风险管理等内容,[38]以保障用户的资金和个人信息的安全。

3. 殊途同归:金融信息共享的规则趋同

不难发现,随着科技与金融行业的不断融合,为了满足金融行业提升效率和鼓励革新的需求,促进整个金融行业的信息高效共享成为各国立法的共通选择。美国《金融服务现代化法案》作为法经济学理论在金融领域的一次践行,在财产规则上采取金融机构与关联方信息共享"无需同意"、与非关联方信息共享需"默示同意"的授权模式,以及"共同营销行为"豁免等具体规则,实际上将金融信息的"产权"分配给了金融机构。同时,在联邦执行执法过程中,衍生出信息安全保障规则和隐私保护规则这两套规则,不断优化金融机构的告知义务,其本质上也是促使处于信息优势地位的金融机构持续性地进行信息披露,以降低双方在信息共享过程中的信息不对称问题,力图实现个人信息保护与促进信息共享的平衡。

欧盟严格保护个人数据基础上的"开放银行"模式有异曲同工之处。从法经济学的视角分析,《通用数据保护条例》为信息主体提供了普适性个人信息保护规则,用户"明示同意"仍然是支付服务提供者等为其提供服务的前提条件。虽然开放银行的思路没有改变信息"产权"归属消费者的本质,但是通过"消费者赋权"的路径,强制要求金融机构开放用户账户信息权限,同样有利于进金融信息的共享利用。

纵观之,促进个人金融信息的利用共享,并不意味着放松个人金融信息保护。国际视域下金融信息共享机制的规则趋同表明,是否能够实现个人金融信息保护与促进信息共享两大目标的双赢,取决于个人金融信息共享规则的设计配置。

三　个人金融信息保护的体系解释与规则延展

我国《个人信息保护法》的整体立法思路并不限制个人金融信息的利用和共享,而是通过体系化的制度安排勾勒出完整的个人信息保护义务和利用规则。同时,我国在个人信息保护立法过程中注重借鉴和吸收域外立法的先进经验,具备后发优势。但就其具体规则在金融领域的延展适用而言,仍有必要结合我国金融行业的常见应用场景,基于体系化解释论的视角,逐条考量和阐明如何通过包括事前授权、事中赋权和事后追责等不同环节的规则设计、配置和协同,来消融个人金融信息保护与促进信息共享这两大目标之间的抵牾。

(一)个人金融信息不宜都归为敏感个人信息

《个人信息保护法》在第二章第二节专门规定"敏感个人信息的处理规则",意图与处

〔37〕 Commission Delegated Regulation (EU) 2018/389.

〔38〕 主要规则包括:基于安全要求,发布和使用强客户身份认证(strong customer authentication)解决方案,允许授权与具体金额和收款人动态关联,通过最大限度地减少错误或欺诈攻击的风险来进一步保护用户;提供交易和设备监控,以识别不寻常的支付模式;以及为支付帐户提供一个标准化和可靠的访问接口(即应用程序编程接口,API),使其能够以安全的方式识别第三方支付服务提供商,并确保所有相关方之间的相关通信。

理非敏感个人信息的“一般规定”相区别。较之非敏感个人信息,立法上对处理者处理敏感个人信息作出更严格的规定,要求只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下方可处理,并且应当取得个人的单独同意、向个人告知处理该等信息的必要性以及对个人权益的影响。

在个人信息保护立法过程中,是否将个人金融信息全部纳入敏感个人信息范畴存在争议。诚然,个人金融信息与信息主体紧密相关,但并不意味着所有的个人金融信息都应作为敏感个人信息对待,不同的个人金融信息类型具有不同的敏感性。《个人信息保护法》将个人信息区分为敏感个人信息与非敏感个人信息两大类,第 28 条第 1 款“敏感个人信息”的列举包括金融账户,彰显出我国个人信息保护立法对金融账户重要程度的关注和伤害风险概率较高的担忧,即其“容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害”。但是鉴于个人金融信息的范围之广,既不能将其他类型的个人金融信息都排除在敏感个人信息之外,也不能将金融账户不加辨识地按照敏感个人信息处理,这是一种“得形忘意”的做法。本文认为,有必要借鉴场景理论,结合《个人信息保护法》中敏感个人信息的内涵意蕴,来理解和厘清哪些个人金融信息属于敏感个人信息的范畴:

第一,个人金融信息不等同于金融账户,我国立法没有将个人金融信息都视为敏感个人信息的做法具有合理性,值得肯定。美国、欧盟均没有将个人金融信息作为敏感个人信息加以保护,金融领域的信息共享是大势所趋。美国是行业单独立法模式的代表,促进金融行业信息共享是美国联邦立法的首要目标,其保护对象即“非公开个人信息”的具体类型与我国《金融消费者保护办法》的“个人金融信息”的定义颇为相似,包括金融账户在内。〔39〕 对非公开个人信息的共享不以获取个人同意为前提条件,金融机构与关联机构之间,无需获取个人同意即可自由地进行非公开信息的共享。而欧盟《通用数据保护条例》采取统一立法模式,同样没有将个人金融信息与其他个人信息区别对待。

第二,我国《个人信息保护法》并没有对金融账户作出明确定义,纳入敏感个人信息的“金融账户”应当是指具有敏感性的金融账户。从敏感个人信息的内涵来看,敏感个人信息的“敏感”要素体现在两个方面:一是存在“自然人的人格尊严受到侵害或者人身、财产安全受到危害”的高致害风险;二是风险概率高,即“容易导致”上述风险。

从金融行业标准《个人金融信息保护技术规范》的定义来看,“账户信息”指账户及账户相关信息,包括但不限于支付账号、银行卡磁道数据(或芯片等效信息)、银行卡有效期、证券账户、保险账户、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等。根据可能产生的影响和危害,将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三个类别,不同的金融账户信息具有不同的敏感程度,例如,银行卡磁道数据(或芯片等效信息)、银行卡有效期为 C3 类别,支付账号、账户余额为 C2 类别,账户开立时间、开户机构仅为 C1 类别。

国外立法不约而同对“账户”作出了特别规定。其中,美国联邦立法上禁止仅基于营销目的与非关联方共享信用卡、银行账户等交易账户或类似的访问号码或代码;但同时又

〔39〕 15 U. S. C. § 6809 (4), 12 C. F. R. § 1016.3 (p) & (q).

进一步解释,该交易账户是指第三方可以向其发起收费的任何账户,如果接收信息的第三方无法对其进行解码,则不禁止共享加密的帐号。[40] 而欧洲《支付指令》也区分“支付账户”(payment account)和“敏感支付数据”(sensitive payment data),两者含义不同。前者是指以一个或多个支付服务用户的名义开立的用于执行支付交易的账户,后者是指可用于实施欺诈的包括个人安全凭证的数据。同时又特别指出,就支付启动服务提供者及账户信息服务提供者的活动而言,帐户持有人的姓名及帐户号码并不构成敏感支付数据。

国外立法对“账户”的关注重点与我国对于敏感个人信息的定义相类似,都需要考虑该个人信息是否有较高概率的致害风险。我国立法将“金融账户”纳入敏感个人信息的范畴,但是没有对“金融账户”的定义和类型进行细化。本文认为,应当首先将需要纳入敏感个人信息的“金融账户”进行限缩解释,不能将金融行业标准《个人金融信息保护技术规范》中全部的“账户信息”都纳入敏感个人信息的范畴,因为其列举的“账户信息”并非都具有敏感性。在此可以借鉴场景理论,根据信息处理的情境、目的来判断该信息是否敏感。即使是同一个信息,在不同的服务场景中也可能具有不同的敏感度。[41] 例如,信息主体的账户余额、金融账户的开立时间、开户机构等信息需要与其他信息相结合才能识别到特定个人,不具有较高概率的致害风险,应当被排除在敏感个人信息范畴之外。但是,两种或两种以上的低敏感程度类别信息经过组合、关联和分析后可能产生高敏感程度的信息,如前述账户余额、账户开立时间、开户机构等低敏感程度的不同金融信息的组合、关联和分析等,可以识别到特定信息主体,则具有更高的敏感性,应当按照敏感个人信息的处理规则来对待。

第三,由于第 28 条第 1 款采取不完全列举,个人金融信息中能被纳入敏感个人信息范畴的也不应当只限于金融账户。针对不同的个人金融信息类别,应当结合敏感个人信息的认定标准,即“致害风险=风险概率”标准来判断是否属于敏感个人信息。在判断时应当采取客观标准,即根据一般公众的认知常识、习惯,来判断该信息是否通常具有敏感性。例如,欧盟《支付指令》对“敏感支付数据”有特殊限制,包括:要获得授权成为支付机构,应当提交关于存储、监控、跟踪和限制访问敏感支付数据的流程说明;支付启动服务提供者不存储用户的敏感支付数据;账户信息服务提供者不得要求与付款帐户相关联的敏感支付数据。我国《个人金融信息保护技术规范》中规定的“鉴别信息”与其相类似,即用于验证主体是否具有访问或使用权限的信息,例如登录密码、查询密码、验证码或口令、密码提示问题答案等,虽然不在金融账户之内,但通常会被认定具有较高概率的致害风险,应当属于敏感个人信息。此外,广义的个人金融信息还包括个人生物识别信息(个人身份信息),此类信息同样应该适用敏感个人信息的处理规则。

第四,即使个人金融信息未能全部列为敏感个人信息,也并不影响该等信息同样受到法律保护。不同于私法教义学上对科学规范体系的要求,《个人信息保护法》既不是《民

〔40〕 详见美国 FTC 官方网站,https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#exceptions,最近访问时间[2021-08-01]。

〔41〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Washington Law Review* 101, 120-121 (2004).

法典》的特别法，也不是不同法律保护体系的简单叠加。该法通过公法与私法相结合的方式，为个人信息的处理过程提供不同的保护重点。依据《民法典》第 1034 条第 3 款的规定，个人信息分为私密信息和非私密信息，两者的区分在于民事权益的类型与保护方法的差异，私密信息既受隐私权的保护，也受个人信息保护规则的保护。与《个人信息保护法》划分为敏感个人信息和非敏感个人信息的模式相比，两种分类的划分标准和规范目的存在明显差异。因此，根据《民法典》第 1033 条的规定，除非法律另有规定或者权利人明确同意，否则任何处理他人私密信息的行为都将构成对他人隐私权的侵害。例如，个人财产信息、交易信息、借贷信息通常是信息主体不愿为他人知晓的私密信息，也可以通过《民法典》加以保护。

（二）个人金融信息处理的合法性事由

我国《个人信息保护法》处理个人信息的正当化事由分为两个层次。首先，确立以“告知—同意”为核心的个人信息处理规则，要求处理个人信息应当在事先充分告知的前提下取得个人同意，并且个人有权撤回同意；重要事项发生变更的应当重新取得个人同意；不得以个人不同意为由拒绝提供产品或者服务。其次，考虑到经济社会生活的复杂性和个人信息处理的不同情况，在“取得个人同意”的传统模式基础上，第 13 条第 1 款第 2 项至第 7 项对无需取得个人同意即可合法处理个人信息的六种情形作了规定，为个人信息的处理提供了更为广泛的正当化事由。

反观之，在《个人信息保护法》出台之前，我国《金融控股公司监督管理试行办法》《金融消费者保护办法》于 2020 年相继颁布；作为金融机构处理消费者金融信息的特别规范，其局限性体现在：第一，《金融消费者保护办法》第 29 条明确规定，金融机构处理消费者金融信息需要经金融消费者或者其监护人明示同意。与域外欧美立法例中加强个人金融信息共享、普遍采用“同意”而非“明示同意”为信息处理事由的做法相比，该办法没有根据不同个人金融信息的敏感程度区分对待，仍然以“明示同意”统一作为其正当化事由，个人信息处理规则更为严苛。第二，作为例外情形的“但书”条款范围狭窄，客观上也不有利于金融领域的信息共享利用。该条但书“法律、行政法规另有规定的除外”，如果仅指履行法定职责或者法定义务所必需情形，例如前述《反洗钱法》《证券投资基金法》《证券法》《证券公司监督管理条例》等法律、行政法规中对金融机构需要履行的实名制、反洗钱、投资者适当性管理、穿透式监管等法定义务已经明确作出规定的相关条款，方可作为取得信息主体明示同意的例外情况，同样难以满足我国金融行业实践中实现个人金融信息共享利用的业务需求。第三，虽然《金融控股公司监督管理试行办法》初步确立了金融控股公司“共享客户信息”的业务协同框架，但其同样以“经客户书面授权或同意”作为信息共享的前提条件，且没有规定例外情况或但书条款，此种相对保守的做法也与欧美立法中在特定机构之间加强信息共享的发展趋势相去甚远。

现实中存在着大量需要处理个人金融信息的场景，个人金融信息具有公共属性。延续法经济学的分析路径，衡量金融领域中处于不同位阶的利益保护价值，本文认为，应当允许金融机构适用《个人信息保护法》第 13 条规定，基于其他合法性事由合法处理个人金融信息。第一，为订立、履行个人作为一方当事人的合同所必需。在金融领域中，金融

机构为了履行通知义务而需要使用金融消费者的个人信息，例如通过邮箱或者手机向信息主体发送账单、消费提示信息、验证码等等；或者是持卡用户享用签约银行在机场的贵宾室服务，需要核验持卡人信息是否真实有效、与本人一致。第二，为紧急情况下为保护自然人的生命健康和财产安全所必需。如前所述，金融场景中存在着不同位阶的利益保护价值，在同一位阶中也包含不同主体的利益保护。基于保护自然人的生命健康和财产安全（无论是信息主体本人还是其他自然人的法益），例如为保护消费者的财产安全而进行反诈骗所必需、为核验是否为本人消费而收集用户信息等，可以不经金融消费者的同意而处理相关信息。上述信息处理的合法性事由表述中均强调“必需”二字，即应当遵守第 5 条规定的必要原则，该原则是比例原则在个人信息保护立法中的体现。其要求对合同目的的实现、不同位阶的利益保护价值等因素予以综合考虑，判断该信息的处理是否是向用户提供服务或者保护自然人利益所必不可少的。

另外值得注意的是，在个人信息处理的特殊领域即征信业实践中，大部分国家强调征信的公共性、实行强制征信机制，征信机构从信贷机构采集借款人的信用信息，一般以告知原则取代本人同意（例如，德国、法国、意大利等国家多数强制数据上报至信贷登记系统，作为获取本人同意处理个人信息规则的例外情形），个人同意成为例外规则（例如美国 1998 年《消费者征信就业澄清法》（*Consumer Reporting Employment Clarification Act*）规定，如果没有消费者的明确同意和书面授权，任何人不能出于就业目的获取信用报告）。而我国现行《征信业管理条例》第 13 条第 1 款以及《征信业务管理办法》第 12 条规定，征信机构采集个人信息都应当经信息主体同意。本文认为，在现行规章没有改变之前，在获取信息主体授权时采取“选择退出”的同意模式，不失为一种有效的折中做法；而从长远来看，征信业务的本质就是信息共享，通过专门立法的制定豁免征信机构须获取个人授权同意的要求，更有利于通过信息共享机制来化解信息不对称难题、防范信用风险。

此外，依据《民法典》第 1036 条的规定，已经公开但是信息主体明确拒绝个人信息处理者处理的个人信息，也落入个人信息保护法的保护范围。因此，不能仅仅因为信息公开就直接认为处理该信息具有合法性事由，此时同样需要根据个人信息处理的正当化理由来判断是否有权处理。

（三）信息共享机制下信息主体的知情权保护

加强个人金融信息保护是金融领域部门立法的目标之一，《金融消费者保护办法》明确金融信息保护是金融消费者权益保护的重要组成部分，其中知情权是金融消费者信息保护权利体系的起点和基石。我国《个人信息保护法》对于以信息主体知情权为核心的权利体系作出了原则性规定，知情权并非一个完全仅靠公法管制或对个人信息处理者提出数据治理要求的权利，而是充分保障信息主体权益的基础。只有在信息自决与知情同意的基础上，才能进一步衍生出查阅权、复制权、更正权与删除权等，这些权利并非简单的程序性权利，而是信息自决、知情权与决定权等基础权利的外在表现。[42]

〔42〕 参见姚佳：《论个人信息处理者的民事责任》，《清华法学》2021 年第 3 期，第 52 页。

1. 强化金融机构的告知义务

金融机构在提供金融服务的场景下，特别是在提供网上银行服务时，往往倾向于采用“捆绑式”的方式列出内容冗长繁琐的隐私政策条款。〔43〕 如果个人信息主体缺乏对相关内容的知情，则其同意即缺乏合法的基础。〔44〕 金融消费者作出真实、明确、有效同意的前提是信息处理者充分、及时、真实地告知个人信息将被如何处理；为了弥合这种“告知义务”与“知情权”的断层，需要对金融机构履行告知义务的方式、内容作出进一步规制。强化金融机构的告知义务，从本质上而言，就是促使处于信息优势地位的金融机构通过信息披露的方式来降低个人信息处理过程中存在的信息不对称现象。

在金融实务中，银行、支付机构等金融机构通常通过格式条款来取得信息主体同意以获得其关于个人信息的授权。《金融消费者保护办法》第 31 条第 2 款认可以格式条款的方式进行告知，《个人信息保护法》第 17 条也明确规定应当告知的内容和方式，即“以显著方式、清晰易懂的语言真实、准确、完整地”向个人告知，告知内容包括个人信息处理者的信息，以及处理目的、处理方式、信息种类和保存期限等。本文认为，现有立法侧重于信息处理的事前授权阶段（包括向其他个人信息处理者提供的情形），缺乏贯穿个人信息处理全周期不同阶段的定期告知。个人金融信息商业价值的实现在于事中共享阶段，而共享一旦失控，对信息主体权益损害的危险性更大。因此，信息共享的事中、事后阶段更应是重要保护阶段。同时，保障信息主体知情权、判断金融机构的告知是否充分，应侧重于告知内容是否包括处理个人信息的实质性信息，以及是否贯穿信息处理的全生命周期。

综合借鉴域外立法的相关规定，金融机构告知义务的适当履行，体现在以下方面：一是，告知义务应当贯穿信息处理的全生命周期，不仅包括信息共享的事前授权阶段，同时包括信息共享的事中阶段和事后追责阶段。二是，不同阶段的告知内容和方式可以有所区别。在信息共享的事前授权阶段，金融机构在格式合同中使用简洁易懂的语言，罗列影响信息主体是否同意的实质性信息，包括信息处理对信息主体会造成何种影响尤其是不利后果、采取的信息安全保护措施等，并采取特殊手段使用户更易于发现和理解服务条款的内容，例如加粗标记关键条款、将关键条款列于协议明显位置等。在信息共享的持续阶段，在信息主体同意的情况下以电子方式定期发送相关信息，或者以清晰、显眼的方式在其网站上持续发布相关信息。值得注意的是，虽然信息共享涉及到金融机构外的第三方，但是信息处理的目的往往是为个人提供金融服务，而个人通常难以辨识信息共享的形式（属于与他人共同处理、委托他人处理、向其他个人信息处理者提供信息中的何种情形），因此在信息共享的场景下，应推定金融机构仍然是告知义务的责任主体。在事后追责阶段，我国就侵权责任的承担采取过错推定的归责原则，由金融机构承担举证责任，证明其已经适当地履行告知义务以保障信息主体的知情权。三是，告知内容可以采取简明版、完整版两种版本，以满足不同主体的需求，并且避免冗长的信息披露而使告知义务流于形式。

2. 自动化决策场景下的知情权实现

《个人信息保护法》首次对利用个人信息进行自动化决策作出规定，这在金融领域中

〔43〕 参见范为：《大数据时代个人信息保护的路径重构》，《环球法律评论》2016 年第 5 期，第 93 页。

〔44〕 参见万方：《个人信息处理中的“同意”与“同意撤回”》，《中国法学》2021 年第 1 期，第 172 页。

尤其重要。自动化决策改变了传统信贷领域的信用评估基础,广泛存在的各类信用评分产品和服务,是金融领域中自动化决策的常见应用场景。用于自动化决策的基础信息是个人金融信息,其产生的衍生信息如果具有可识别性,则也属于个人金融信息的范畴。两大问题随之产生:一是,随着大数据时代的个人信息更加离散化、碎片化和数据化,基础信息的真实性、准确性、完整性如何保证。二是,无论是作为基础信息的个人金融信息可能缺乏准确性和完整性,还是深度学习等多元化算法技术和数据模型的应用可能存在"算法黑箱",由此产生的"衍生信息"的准确性和公平性如何得以保障。不同于央行征信中心提供的个人征信报告(基础信息的类型和内容清晰可见,包括个人基本信息、信用交易信息和个人公积金信息等),此类信用评分产品呈现给信息主体的往往只有最终的征信评分结果,何种个人信息在信用评分产品的数据模型中如何被应用无从知晓,更遑论如何行使查询权、更正权、删除权等等权利。因此,信息主体的知情权对于其他权利的实现而言尤为重要。在以自动化决策方式作出对个人权益有重大影响的决定时,例如不当的信用评分可能会使得信息主体在求职、信贷、保险及其他重要的市场机会方面受到不利影响时,个人信息处理者必须承担更加明确告知的义务。自动化决策涉及应用算法处理个人信息和产生衍生信息两个不同的环节,但是,由于自动化决策技术本身存在着"算法黑箱",自动化决策的不利影响是否能构成对人格权益或者财产权益的侵害也存在争议,[45]因此,在以自动化决策处理个人信息之前适用《个人信息保护法》第17条的规定,由个人信息处理者履行事先告知义务,更为妥当。信息处理者应当以清晰、易懂的方式明确向信息主体告知与处理个人信息相关的内容,特别是可能影响信息主体是否同意通过自动化决策方式处理其个人信息的其他实质性信息,包括特定自动化决策技术的基本原理和应用逻辑、自动化决策决定的后果尤其是应用缺陷以及信息主体应当如何行使法定权利等。

(四)信息主体的民事救济途径

美国《金融服务现代化法案》备受争议的重要缺陷是缺乏有效的执行和补偿机制。该法的执行权力在于联邦政府机构,并没有赋予信息主体私人诉权,当金融机构违反该法规定时,消费者无权向其直接提起民事赔偿诉讼,而是需要向监管机构进行申诉,由金融监管机构依照其职权来执法,消费者无法通过司法途径获得民事救济。相比较而言,我国《个人信息保护法》立法的后发优势体现在,其为信息主体提供了较为完备的民事救济途径。

第一,信息主体在主张权利遭受拒绝时有权提起诉讼。依据第50条第2款规定,当信息主体向金融机构请求行使知情权及其衍生出来的查阅权、复制权、更正权与删除权等各项权利,个人信息处理者无正当理由予以拒绝时,个人有权向法院提起诉讼。这能够在促进信息共享的同时,为信息主体提供事后救济的途径。

第二,信息主体可以主张金融机构承担违约责任。其一,个人信息处理者如果通过用户协议、格式条款方式对个人信息权利行使进行限制,或者扩张自身处理个人信息的授权,例如不可撤销、任意转授权等,信息主体都可以依据《民法典》第497条请求权确认格式条款无效。其二,金融机构履行信息安全保障义务,既是法定义务也是合同义务。金融

〔45〕 参见姚佳:《论个人信息处理者的民事责任》,《清华法学》2021年第3期,第48页。

机构与客户缔结服务合同之时就会产生相应的保密义务，即金融机构负有保护客户所提供的个人信息的合同附随义务。无论是根据美国执法实践中形成的数据安全规则，还是根据欧盟《监管技术标准》中的强客户身份验证和通用安全开放通信标准，金融机构共享信息时，都负有保障个人信息安全性、机密性的法定义务。我国《个人信息保护法》第 51 条也规定了信息处理者需要承担采取安全技术措施来保障个人信息安全的法定义务。此时，可能会产生侵权责任和违约责任的竞合，信息主体可以选择主张权利。

第三，处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。金融机构承担侵权责任以造成损害为其构成要件之一；且《个人信息保护法》采取了过错推定为归责原则，由信息处理者来证明自己没有过错。如果个人信息处理者能够证明严格按照《个人信息保护法》等法律的规定来处理，包括遵循前述信息安全保障义务、保障信息主体合法权益的义务等等，则不存在过错，也无需承担侵权责任。在信息共享的场景下，个人金融信息共享的方式多元化，包括与他人共同处理、委托他人处理、向其他个人信息处理者提供信息等不同情形，因此而产生的法律关系不同，个人信息处理者需要承担的侵权责任亦不同。

关于个人信息处理者共同处理个人信息的侵权责任承担问题，应基于体系化解释路径，认为《个人信息保护法》将共同处理和向其他个人信息处理者提供信息区分处理。第 20 条第 2 款“依法承担连带责任”应当理解为单独的请求权基础，只要共同处理个人信息的个人信息处理者中有任何一方存在过错即需要承担连带责任，这更有利于保护信息主体的信息权益。而个人信息处理者向其他个人信息处理者提供其处理的个人信息需要取得个人的单独同意，因此，不同信息处理者与信息主体之间因处理其个人信息而分别存在单独的法律关系，就其是否存在过错各自承担相应的侵权责任。

就个人信息处理者委托他人处理的情形而论，不同于一般的委托合同关系，受托方是按照个人信息处理者委托处理的目的、期限、处理方式等来处理个人信息，因此，金融机构作为委托方应当依法对个人信息的整个处理过程（包括委托他人）尽到更高标准的注意义务。一是，依据《金融消费者保护办法》第 34 条第 1 款规定，金融机构保护消费者个人金融信息安全的义务不因其与外包服务供应商合作而转移、减免，这就强调了金融机构需要更谨慎地履行选任义务，需要充分审查、评估外包服务供应商保护个人金融信息的能力。二是，金融机构还需要证明自身适当地履行了《个人信息保护法》第 21 条规定的指示义务、持续监督义务，以及按照《金融消费者保护办法》第 34 条第 2 款，采取了必要措施保证外包服务供应商履行保护个人金融信息的职责和保密义务。只有当个人信息处理者举证证明自身已经依法履行上述各项义务，方可免于承担侵权责任。

四 结 语

通过考量我国《个人信息保护法》的具体规则在金融领域的延展适用，本文总体认为，通过事前授权、事中赋权和事后追责等不同环节的规则设计、配置和协同，能够尽可能实现金融领域内个人信息共享与信息保护的双重目标。基于个人金融信息兼及个人权益

和公共利益的双重属性,为了充分发挥信息共享的资源配置作用,我国不宜采取将个人金融信息都作为敏感个人信息加以保护的方式。我国《个人信息保护法》确立了以“告知—同意”为核心的个人信息处理规则,并设置了信息处理的六项合法性事由,实质上是将“产权”分配至信息主体,以充分保障信息主体控制信息的权利,又很大程度上有利于拓展个人金融信息在不同应用场景下合法化共享利用的情形。并且,现行立法对于以信息主体知情权为核心的权利体系以及相应的民事救济途径作出了原则性规定,通过体系化解释,其包括强化金融机构的告知义务、金融机构在信息共享下的注意义务以及可能的侵权责任等等,在相当程度上能够消弭信息共享可能带来的风险忧虑。但是从远期来看,信息在数据要素市场上扮演着越来越重要的角色,无论是美国坚持信息共享的金融隐私保护理念,还是欧盟从“开放银行”过渡至“开放金融”的潮流走向,都显示借助科技力量实现金融创新在客观上已经成为不可逆转的趋势。从金融创新发展的大局出发,基于增强我国金融行业国际竞争力的驱动,需要尊重金融行业和个人金融信息的特殊性,回归金融数据治理的基本逻辑,通过金融领域的专门立法来实现个人金融信息保护和共享利用的双赢目标仍然是大势所趋。

[本文为作者主持的2017年度国家社会科学基金一般项目“创新驱动发展战略下新兴资本市场监管机制的理论与制度构建研究”(17BFX102)的研究成果。]

[**Abstract**] In China's legal system, personal financial information has always been valued, but its position has been unclear for a long time. Located in the overlapping area of personal information protection and financial market supervision, personal financial information is of great importance to the financial industry. Personal financial information has dual attributes, and carries values and interests of different levels. Both the application of analytical model of law and economics to the finance industry and the convergence of the rules of financial information sharing mechanism from international horizon provide justification for promoting financial information sharing. The balance between the two goals of personal financial information protection and information sharing depends on how to configure and coordinate different rules in the links of *ex ante* authorization, in-process empowerment and *ex post* accountability. In the application of the Personal Information Protection Law to the financial industry, we should not treat all personal financial information as sensitive personal information, but provide more comprehensive and legitimate reasons for dealing with such information. To protect the right to know of the subjects of personal information under the information sharing mechanism, the obligation of financial institutions to disclose information or give notices to consumers should also be strengthened.

(责任编辑:余佳楠)