·经济法·

DOI:10.16339/j.cnki.hdxbcjb.2024.03.020

个人金融账户信息的法律界定

尹华容,伍洋宇

(湘潭大学 法学院,湖南 湘潭 411105)*

摘 要:《个人信息保护法》将金融账户信息纳入敏感个人信息的范围,但未作出明确的界定。界定标准的不明确将导致权利主体权益易损、义务主体责任不明、司法裁判依据不清。考察域外立法例,同时结合我国有关立法现状和实践,宜采取"定义+列举+排除"的界定模式,以"信息主体""信息性质"和"信息处理"为定义的考量因素,从立法、实践的综合角度进行列举,并排除通过间接识别才能确认的金融账户信息。基于此,我国出台"金融账户信息"的司法解释可侧重四个方面,以实现个人信息的保护和社会信息利用的动态平衡。

关键词:个人信息保护法;金融账户;个人金融信息;敏感个人信息

中图分类号:DF438;G2 **文献标识码**:A **文章编号**:1003-7217(2024)03-0154-07

一、引 言

2021 年 11 月 1 日起,《中华人民共和国个人信息保护法》(以下简称《个保法》)正式施行,其中第二章第二节规定了敏感个人信息的处理规则,引起学界的普遍关注,这也是我国首次在法律层面对敏感个人信息进行界定。《个保法》将"金融账户"纳入敏感个人信息,金融账户与信息主体的经济、财产关系密切,一旦泄露、滥用,对信息主体将会造成严重的损害。相关数据统计报告显示,2022 年我国境内政府部门和金融贸易行业所遭受的高级持续性威胁(advanced persistent threat,APT)占比高达 43%,其中全球金融商贸所遭受的 APT 达 8%,我国境内金融商贸行业的 ATP 活动占比达 14%,为我国境内受影响行业排名第二[①]。有关 APT 组织意图窃取银行、风投公司等金融机构的敏感信息,从而获取大量非法经济利益。

《个保法》虽有规定"金融账户",但缺乏对其具体界定,实践中出现一系列问题亟待解决:信息权利主体认识权益边界不清晰,产生更高的致害风险;信息义务主体理解规范不准确,导致瑕疵的义务履行后果;裁判机构缺乏具体指引,影响案件审理的公正性、权威性。

在《个保法》发布以前,就金融账户信息而言,有关的规定散见于各类标准和规范之中,其中虽提出"个人金融信息"或"银行账户""金融账户"等概念,但都存在一些问题:在适用范围上有限、界定模糊或者未界定、界定形式和内容多而杂乱。这意味着裁判机构可能在对"金融账户"进行认定时缺乏明确的法律依据。《个保法》颁布以后,学界对个人金融信息、金融账户信息的内涵与外延展开了激烈的讨论,不断做出探索,但现有研究未系统界定金融账户信息,多为论证个人金融信息的相关内容,对《个保法》第 28 条敏感个人信息中"金融账户"的内容针对性不强。伴随着大数据时代的兴起,支付 App、互联网银行等新金融业态不断涌现,个人金融账户信息受到侵害的风险也不断增加。有必要对金融账户信息进行合理、明确界定,确定其保护范围,从而为有关裁判机构在处理案件时提供指引,准确调取金融账户信息的法定范围,并对信息义务主体服务机制进行严格管控,预防冤假错案的发生;帮助解决信息主体与信息处理者之间的信息不平等问题,降低信息主体在金融法律关系中面临的风险;信息义务主体能够以此制定明确的服务规范,更好地保护信息主体的财产安全,平衡多方利益。为此,本文试图通过梳理我国现有的"金融账户信息"及类似概念之界定,考察美国、欧洲地区、澳大利亚等相关立法例,为我国科学界定"金融账户信息"提供参考。

二、界定现状及界定不明导致的问题

个人金融账户信息承载着个人金融经济活动的记录,是信息主体管理自身金融财产、进行金融交易

* **收稿日期**: 2023-10-07; **修回日期**: 2024-03-05
基金项目: 国家社会科学基金重点项目(21ZD&-204)
作者简介: 尹华容(1973—),男,湖南洞口人,博士,湘潭大学法学院副教授,硕士生导师,研究方向:行政法学。

活动的重要保障。我国法律规范中多为对个人金融信息的规定,且不同规范间概念不统一,保护的范围也有所区别。

(一)我国个人金融账户信息的界定现状

我国法律及司法解释均未界定金融账户信息。法律层面,《中华人民共和国民法典》(以下简称《民法典》)第 1034 条规定了个人信息范围,但"金融账户"并未纳入其中。《个保法》第 28 条将"金融账户"纳入敏感个人信息,但缺乏具体的界定。在司法解释层面,2017 年发布的《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》(以下简称《解释》)规定的公民个人信息虽包含"账号密码""财产状况",但并不能将其推导视为"金融账户",因此,《解释》也未对金融账户信息作出规定[1]。

"个人金融信息""个人账户信息""金融账户信息"等概念散见于行政法规、部门规章、相关标准和规范性文件中,其中"个人金融信息"多有涉及。

2013 年,中国人民银行发布的《关于银行业金融机构做好个人金融信息保护工作的通知》对个人金融信息进行了分类,但仅列举了账户信息内容。2017 年,《非居民金融账户涉税信息尽职调查管理办法》(以下简称《管理办法》)中,只是对一些账户做出定义和列举。2020 年,《信息安全技术个人信息安全规范》(以下简称《安全规范》)在关于个人敏感信息的规定中,包含了银行账户、个人财产信息,其指出个人财产信息又包括银行账户、交易和消费记录、虚拟财产等,未对"金融账户"概念单独作出界定。《个人金融信息保护技术规范》(以下简称《技术规范》)和《中国人民银行金融消费者权益保护实施办法》(以下简称《实施办法》)同为 2020 年出台,两者均对个人金融信息进行了定义。《技术规范》对个人金融信息进行了敏感层级分类,并将账户信息作为个人金融信息的一部分对其进行界定,但账户信息在不同敏感层级中均有表述,从而使得界定缺乏针对性;《实施办法》规定账户类信息属于消费者金融信息,未进一步作出界定。2023 年,全国信息安全标准化技术委员会发布的《信息安全技术敏感个人信息处理安全要求》征求意见稿(以下简称《安全要求》)中对金融账户信息作出了初步界定,认为金融账户信息为与账户和交易相关的信息,该界定仍过于模糊,无法确定金融账户信息的保护范围。

(二)界定不明导致的问题

由于我国法律及司法解释均未界定金融账户信息,相关标准和规范性文件更多的是对其上位概念"个人金融信息"作出界定,因此,裁判机构在法律适用以及有关主体履行义务时面临困境。

金融账户信息无明确界定,使我国司法在案件的处理上对与财产、账户有关的信息认定不具备统一标准。如在某民事纠纷案中,法院依据《个保法》认为银行流水属于敏感金融信息,而《个保法》关于敏感个人信息明确规定为"金融账户",法院未对认定的金融信息作出相应解释。在某刑事案件中,法院将银行存款、理财产品明确归为金融账户信息。此外,还有其他不同领域的案件,法院对其金融账户信息的认定标准无具体论证,对与财产、账户等具有关联性的信息直接归类于金融信息或者直接以金融信息表述,这种认定乱象产生的原因在于《个保法》虽然对金融账户信息有所提及,但未作出明确界定,使得法官在认定金融账户信息时自由裁判的空间过大,这明显不利于保护信息主体的权益。

明确金融账户信息内涵与外延对义务主体及时、正确履行义务起到重要的指引作用。《个保法》中规定了"知情-同意"的义务,要求义务主体在处理个人敏感信息时应当取得个人的明确同意,并且要告知其对处理敏感信息的方式、范围和目的,在涉及个人财产有关的情况中,应通过隐私政策来征得信息主体的同意[2]。如果信息的定义、范围和种类缺失,"知情-同意"义务的履行就会失去明确的指引。实践中,互联网企业于《个保法》生效后陆续更新了企业隐私政策,在金融账户信息界定缺失的情况下,这些互联网企业考虑到自身业务的特殊性以及所要面临的法律风险,在各自隐私规定的内容上存在着差异。如,支付宝《隐私权政策》将银行账户信息和银行预留手机号归为敏感个人信息;美团《美团外卖隐私政策》将个人财产信息,包括银行账号、消费和交易记录、信贷记录及虚拟财产信息归为敏感个人信息。具体来说,这些企业通过明确《个保法》中金融账户信息的具体种类,以较小的范围和确定的范围来要求自身,防止义务范围过大而处于不利地位。互联网企业这种通过列举来缩小自身的责任范围的行为,其实也在揭示目前金融账户信息的适用困境。

三、域外金融账户信息界定的相关立法例

我国现有法律规范对个人金融账户信息未有明确界定,因此,可从比较法视角出发,对其他国家的有关法律制度进行分析和梳理,吸取其中可借鉴的做法。本文选择美国、欧洲地区、澳大利亚等国家或地区为考察对象,有三个原因:一是这些国家或地区在早期即对个人数据保护领域立法进行了探索,并在长期实践中积累了宝贵经验,可供借鉴参考;二是这些国家或地区在具备较为强大的经济实力的同时

也注重维护公民的权利,这与我国依法保护人民合法权益的现实需求相符;三是考虑到我国科学技术的迅速发展和国际地位的提升,更深入地研究其他国家与地区的相关规范,有利于构建符合我国国家发展、社会稳定和人民利益的制度。

(一)美国相关立法例

美国相关立法中主要有“ financial account”“financial data”“bank account”等与金融财产有关的概念。这些概念均与信息主体的金融类有关信息存在密切联系。

1.美国各州层面对金融账户信息的立法考察。美国在州层面对于“金融账户”的界定散见于各州对消费者隐私的保护法案或相关隐私、数据保护法案,但大部分州的有关法案在认定个人敏感信息或者敏感数据时,少有将金融账户信息或者金融信息包括在内。弗吉尼亚州 2021 年《消费者数据保护法》(CDPA)关于敏感数据的定义中只包含了身份性个人数据、生物特征数据、儿童个人数据及地理位置数据,未纳入金融有关信息。同样,《华盛顿隐私法案》《田纳西州信息保护法》等也未包含有关金融类信息。而 2020 年《加州隐私权法案》(CPRA)作为美国一个全面的隐私法案,其将“金融账户”纳入敏感数据之中,同时纳入的相关联概念还有“账户登录”“借记卡或者信用卡号码”等,并规定访问账户所必需的凭证,如安全或访问代码、密码等也属于敏感数据范畴[3]。

2.美国联邦层面对金融账户信息的立法考察。2021 年《联邦消费者在线隐私权法》(COPRA)中,对“金融账户”以“列举”模式进行了界定。COPRA 规定金融账号、借记卡号、信用卡号以及允许访问任何此类账户的凭据都属于敏感涵盖数据。2022 年《美国数据和隐私保护法案》(ADDPA)对“金融账户”以“定义+列举+排除”的模式作出了界定,定义部分包括能够描述或者揭示个人收入水平或者银行账户余额的信息,但并未对描述或揭示的方法作出解释;列举部分包括了账户号码、借记卡号、信用卡号。此外,根据 ADDPA 第 28 条第八款的规定,账户或设备的登录凭据以及账户或设备的安全、访问代码也属于敏感涵盖数据,这与 COPRA 的内容基本一致。排除部分针对信用卡和借记卡号,认为这两类卡号码的最后四位不应属于敏感数据。

(二)欧洲地区相关立法例

欧盟《通用数据保护条例》(GDPR)没有特别注重对金融账户的定义,其在特殊类别个人数据的处理中并未规定金融账户信息。在欧洲国家,如德国《联邦数据保护法》、英国《数据保护法》、《法国数据保护法》等有关法律均依照 GDPR 的内容对特殊类别个人数据进行规定,不包含金融账户信息。

2007 年,欧盟颁布的《支付服务指令》(payment services directive,PSD)是关于内部市场支付服务指令的最初版本,PSD 中对“支付账户”作出了定义,即以一个或多个支付服务用户名义持有的用于执行支付交易的账户。此后,为了提升对金融领域数据的利用和保护,2015 年出台了《支付服务指令修正案》(PSD2),其主要目的是应对电子支付出现的安全风险,给支付市场的良好运转提供安全、可靠的支付服务。PSD2 规定了敏感支付数据条款,并以“定义+排除”的方式作出界定,认为其是一种可用于欺诈的个性化安全凭证数据,在排除方面规定支付发起服务提供商和账户信息服务提供商的活动中,账户所有者姓名和账户号码不属于敏感支付数据。

由于欧洲地区各国家同我国社会历史、性质和成员的组成有着较大的差异,它们在敏感个人信息的认定上,对种族(民族)血统、政治观点、工会身份以及性生活或性取向更为重视,这与我国《个保法》的敏感个人信息保护范围有区别。

(三)澳大利亚相关立法例

澳大利亚 1988 年《隐私法》在敏感信息的规定中,不包含“金融账户”“个人金融信息”的有关内容,同欧洲国家的对敏感信息立法相近,但《隐私法》中还规定了“信用信息” “支付信息”“还款信息”等,以此为金融领域秩序的稳定提供重要作用,并对消费者的有关权益作出保护。

澳大利亚 2006 年的《反洗钱和反恐融资法》中有着对账户的规定,以“举例+排除”模式认定账户包含信用卡账户、贷款账户、单位形式持有的货币账户,排除了账户为零以及与账户相关的任何交易。当然,该规定最终适用的范围以该法案为限,在其他领域能否发挥具体作用还有待考察。

(四) 对域外立法的考察和梳理

在对域外有关金融信息、金融账户信息立法观察中,发现部分国家对其的规定碎片化或者无具体规定,但也有如美国、欧盟等以数据、信息的视角对其做出界定,以完善对个人隐私、个人信息的保护。

根据梳理发现,各国对涉及“金融账户”“金融信息”的有关定义有以下界定方式:“单纯列举”“定义+列举”“定义+列举+排除”“定义+排除”“举例+排除”。即对欧盟、美国、澳大利、日本等国家和地区关于“金融账户信息”或类似概念界定模式的经验考察归纳如下:(1)美国联邦的 ADDPA 所采取的“定义+列举+排除”的界定模式,在尽可能明确多种类

型的同时,又考虑了一定的排除范围,能够更好地指导司法适用。(2)美国加利福尼亚州的 CPRA、欧盟 PSD2 采用的“密码”“访问凭证”等,更能体现出“金融账户”若作为敏感个人信息所强调的隐私、私密属性。(3)美国 ADDPA、欧盟 PSD2 及澳大利亚《反洗钱和反恐融资法》中,对一些可供公开或者非必要性内容都认定为可排除信息。美国认为一些号码的后四位可排除;欧盟认为只要名义持有即可,而账户者的姓名、号码为非必要信息;澳大利亚认为金额为零的账户以及账户交易不属于账户类别。

四、我国金融账户信息的界定构想

我国对个人金融账户信息界定可采取“定义+列举+排除”的模式,以“信息主体”“信息性质”和“信息处理”为考量因素,基于社会实践与公众普遍认可度来列举,从“信息识别”的角度确定排除范围。

(一)我国金融账户信息界定适用模式

1.“定义式”。即仅单纯地给出金融账户信息的概念,无法直接对某种信息是否属于金融账户信息作出判断,在此情况下会增加对其适用的难度。

2.“列举式”。即直接逐项列举金融账户信息的种类,如单纯采用这种模式界定,法律所要保护的对象将被具体为特定的类型,并且概念定义的缺乏还将进一步限制个人信息适用的范围。金融账户信息的种类会随着社会资源的更新迭代而不断增加,且类型难以逐一列举。因而,这种方式不宜用于界定金融账户信息。

3.“定义+列举”。即在说明金融账户信息抽象概念的同时列举金融账户信息的种类。此种界定方式能够在一定程度上弥补单纯定义式的不确定性和单纯列举的滞后性,这也是我国立法常采取的界定模式。如《中华人民共和国行政诉讼法》对证据的规定,即是“定义+列举”的模式。前述国外立法中加利福尼亚州 CPRA 与美国 ADDPA 就是采用该界定模式。但对于金融账户信息的界定模式还应当考虑“排除”所发挥的作用,“排除”部分属于应当豁免的信息。《个保法》在对敏感个人信息界定时,已经划定了具体的范围,但金融账户信息作为下级具体分类,与个人金融财产密切相关,应当考虑无法直接识别财产的“低敏感性”信息、“可脱敏性”信息等在不同情形下所产生的影响。因此,为使金融账户信息的界定更加清晰,有必要将“排除”部分纳入金融账户信息界定模式的范围中,采取“定义+列举+排除”的模式来尝试对“金融账户”这一敏感个人信息作出界定。

(二)金融账户信息的明确定义

1.金融账户信息的明确定义界定,可采取“定义+列举+排除”的模式。对“金融账户信息”的定义目前也存在着不同的观点:如“金融账户信息”也即“个人金融信息”[4],未对两者明确作出区分,并且认为《实施办法》对消费者金融信息的界定即为对“金融账户”的界定;个人金融账户信息属于个人金融信息,在讨论金融账户信息时,应该将其置于种属关系下来进行[5]。故此,有必要对二者进行区分和解释。

个人金融信息不应等同于金融账户信息,个人金融信息虽和信息主体有着紧密联系,但并不意味一切个人金融信息都属于敏感信息,《个保法》中也仅将“金融账户”作为敏感个人信息进行规定,并未将所有金融信息作为一个整体纳入敏感信息的范畴。因此,应将金融账户信息独立于个人金融信息之外来作出定义[6]。

界定金融账户信息应充分考虑其所蕴含的敏感性价值。但金融账户信息包含的内容并非全部具有敏感性,如金融账户的号码、信息主体的身份证号码、电话号码等,这些信息本身并不具备敏感性的致害风险。因此,对金融账户进行定义时可以参考场景理论,某些信息在特定的场景下会呈现出敏感特征,同时在特定以外的场景下又不具备敏感性,场景可以对信息的性质产生重要影响。场景隐私理论出自尼森鲍姆教授提出的经典隐私理论,在尼森鲍姆教授的研究中,将场景因素分为五个要素,即信息主体、信息发送者、信息接收者、信息性质及信息传输原则[7]。也有学者根据该理论再结合《个保法》第 51 条中规定的个人信息处理的规范要素,将场景变量归纳为信息主体要素、信息处理要素、第三方要素、信息性质及处理目的。本文借鉴以上理论对金融账户信息的隐私、敏感性进行讨论,即根据信息利用的处境、目的综合判断该金融账户信息是否敏感,将金融账户信息的定义以“信息主体”“信息性质”“信息处理”作为考量因素。

首先是“信息主体”要素。金融账户信息主体的认定强调“可识别性”,即能够识别出享有和掌握金融账户信息的特定人。这与其他敏感个人信息的认定有着相似之处,如对行踪轨迹信息的认定时,是基于真实地理位置,能准确识别个人及其所处的位置;对生物识别信息的认定,强调对人的生物特征进行识别。如今,在互联网金融管理与服务、生物支付(如指纹、刷脸)等互联网业务兴起的背景下,客户、消费者等金融账户信息主体的交易、消费习惯与偏好具有极高的精确性以及潜在的价值[8],掌握这些信息意味着掌握了金融活动的主动权,识别到特定的人就成为关键环节,因此在金融活动中,认定金融账户信息,须具备可识别性以识别到具体的信息主体。

其次是“信息性质”要素。在具有可识别性的基础上,还需要继续探明是否具备作为敏感个人信息的属性。金融账户信息:第一,其应具备敏感性。根据敏感个人信息的内涵,金融账户信息的敏感性体现在两方面:一是“自然人财产受到危害”的致害风险,二在于该风险具有极易发生的可能性[9]。第二,其特有的与个人财产密切相关财产属性。这里的财产应作限缩解释,不能将个人一切财产都纳入金融账户财产属性的范畴中,该财产应是可以作为电子数据来被记录和被识别的财产。第三,金融账户信息往往需要一个载体。金融账户信息是个人在银行、证券公司等金融机构开设的账户相关信息,通常作为账户的内容来帮助信息主体进行相应的金融活动,对载体有着较强的依赖性,需要借助账户这一载体发挥其功能。

最后是“信息处理”要素。该要素是运用场景理论定义金融账户信息最重要的环节,这里分为“信息处理者”和“信息处理目的”来讨论。(1)“信息处理者”。在不同的场景下的金融账户信息处理者及其目的是不同的。在我国《实施办法》中,“信息处理者”被认为是银行、支付机构,它们能通过开展业务或其他合法渠道来处理消费者信息;《技术规范》认为信息的处理者是金融业机构,即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。欧盟 PSD 和 PSD2 中关于对支付账户的处理者包括支付机构、支付发起服务提供商、账户信息服务提供商。支付机构是指欧盟授权范围内提供和执行支付服务的法人,该规定未将信息处理者限定在金融机构,要求获得支付机构资格即可提供相应的服务。澳大利亚的《反洗钱和反恐融资法》中规定,对有关账户信息的处理者包括金融机构、经批准的第三方账单支付系统、信用卡报告机构等。从我国有关标准和国外的立法例可以看出,金融机构是大部分国家和地区普遍规定的信息处理者。结合我国实际,信息处理者可以认定为以银行为代表的金融机构,但不限于此,实践中普遍出现的非金融机构也应可作为一项认定因素。2022 年支付宝、美团等五家机构通过“个人金融信息保护能力”认证,这些机构在个人金融信息的收集、存储、传输、处理、分类分级等方面的处理能力符合相关标准,能对风险实时发现和处理,从而实现用户个人金融信息的全方位保护[10]。因此,可以将“信息处理者”认定为:以银行为代表的国家金融机构以及经授权符合国家关于金融账户信息处理标准的非金融机构。(2)“信息处理目的”。信息处理要求遵循目的特定原则,这是处理敏感个人信息的必要前提,处理目的缺乏合法性、正当性,个人信息的致害风险也将升高[11]。《技术规范》中金融业机构处理用户的有关金融信息,其处理目的是向其提供金融产品和服务;《实施办法》中是以消费者购买、使用金融产品或者服务意图为依据处理信息。美国 ADDPA 对“处理目的”作出解释,即实体或服务提供商收集、处理或传输涵盖的数据的原因;欧盟 PSD2 要求支付机构的处理目的为实现用户的支付交易,保障交易秩序。信息主体不论是通过提供个人信息以获取金融机构、非授权金融机构等的金融产品和服务,还是对第三方主体作出的支付、收款等商业活动,都可能被有关的收集者、传输者以及储存者利用,并作出一定的处理,形成“主体-处理者-第三方/金融机构”的流程[12]。金融账户信息在这个过程中受到处理的最终目的,就是完成相关交易活动。因此,金融账户信息的处理目的可以定义为:给信息主体提供金融有关服务以及记录信息主体运用金融账户进行金融交易、支付交易等交易活动而作出的处理。

通过对“信息主体”“信息性质”“信息处理”三方要素的讨论,对金融账户信息定义可以总结为:金融机构、经授权的非金融机构以提供金融服务、交易服务并作出活动记录为目的所处理的,可以识别到特定用户并能够通过账户记载的财产信息。

(三)我国金融账户信息的列举种类

“列举式”模式包括穷尽式与非穷尽式。以穷尽式列举界定金融账户信息时,能够确定其种类和范围,在一定程度上提升了司法效率。但如今金融账户信息的种类趋于多元化,穷尽式列举其特有的滞后性将令其无法跟上新技术发展的步伐。若采取非穷尽列举,则更能灵活地面对科技发展的新局面[13]。因此,在对金融账户信息列举方面,采用的是非穷尽式列举。

在前述法院对相关案件的审理中,有着多种理解。譬如法院直接将银行存款、理财产品、信用卡信息归为金融账户信息,将银行流水认为是敏感金融信息。不论是在刑事案件中,还是在民事案件中,两者保护的都是个人金融账户信息所承载的个人财产权益。但仅根据对案件的审理来确定金融账户信息的类型,难以在个人信息流转过程中平衡个人信息权利与社会信息之间的关系。故列举金融账户信息应结合实践、相关标准、规定以及立法例综合考量。《安全规范》中将个人财产信息认定为敏感个人信息,其中有银行账号、鉴别信息、存款信息、交易和消费记录以及虚拟财产信息等表述;《实施办法》有财产信息、账户信息、信用信息、金融交易信息等表述;《安全要求》界定金融账户信息为银行、证券账户以

及相应的交易信息;《技术规范》中规定了 C1、C2、C3 三级敏感程度并分别举例。实践中各大互联网企业的规定也值得参考,支付宝《隐私权政策》中的银行账户信息和银行预留手机号;美团《美团外卖隐私政策》中的个人财产信息,包括银行账号、消费和交易记录、信贷记录以及虚拟财产信息等是各企业在与消费者、客户间进行有关交易活动中所确定的敏感信息。综合法院案例,银行账户信息、信用卡信息、交易信息等为高频出现信息,在实践中较为契合公众的认识度,并且能在社会中得到广泛引用,可以作为金融账户信息的列举种类。

美国 ADDPA 规定将借记卡号、信用卡号列为与金融账户同等的敏感数据;COPRA 除 ADDPA 列举的信息外,还明确将账户登录信息与前述信息置于同一行列。值得注意的是,在 ADDPA、COPRA 和 CPRA 中,都将“密码”以及可以访问所列账户的“访问凭证”认定为敏感涵盖数据。欧盟 PSD2 也规定了一种“个性化安全凭证”,认为其易被用于实施欺诈,具备高风险性,因此属于敏感支付数据。我国《技术规范》在个人金融信息敏感级别划分中,将账户的登录密码、交易密码及查询密码划入最高敏感级 C3;中等敏感级 C2 中划入动态口令、短信验证码、密码提示问题答案、动态声纹密码等用户辅助鉴别信息,且规定若能够与账户结合并完成识别,则属于最高级 C3。基于一般公众认识,普通的银行账户或者有关支付账户的泄露并不会对信息主体造成直接损失,而如果通过技术手段破解其密码等鉴别信息,则将在可预见的范围内产生较高的损害可能性[14]。这类“鉴别信息”与美国、欧盟等地的“访问凭证”类似,皆用于验证信息主体是否具备访问和使用账户的权限,虽然不在金融账户之内,但一般能认定具有较高致害风险性,可以作为金融账户信息的列举种类。

(四)我国金融账户信息的排除范围

个人信息的可识别性包括直接识别和间接识别。在个人金融账户信息中,可以将间接识别的信息予以排除。间接识别信息包括:通过与其他信息结合才能识别到特定人财产的信息、通过与其他信息结合产生高致害风险的信息。前者是指一般不能直接识别到特定人金融账户的信息,这类信息在敏感个人信息这一上级分类中已经进行了排除;后者指一些信息单独存在属于无致害风险或者低致害风险的敏感层级,但若与其他信息相关联结合后具备了高度致害风险性,实现了敏感层级的跨越。例如,个人身份证信息和手机号码一般情况下敏感程度低,但当与金融账户账号、用户鉴别信息结合时,在特定服务场景中可以直接识别到特定人的账户财产信息,从而达到高敏感程度[15]。在这里,欧盟与美国立法例的发展值得我们学习:欧盟 PSD2 将账户所有者姓名和账户号码排除于敏感支付数据之外;美国 ADDPA 强调账号号码的最后四位不应属于敏感数据,都根据本国情况将这类“低敏感性”信息予以排除。因此,排除此类信息有助于进一步划定金融账户信息保护范围的边界,增强法律规定的明确性。

我国《技术规范》特别规定了信息屏蔽内容,即对某些敏感信息通过既定规则屏蔽全部或者部分内容,通过这种方法使信息本身在不失去其识别作用的同时降低风险等级。例如,银行卡卡号信息仅显示前六位与后四位,其余部分予以屏蔽,这类信息具备可脱敏性。而对于金融账户信息性质要求应该具备敏感性而不包含可脱敏性,所以,予以排除将更有助于明确金融账户信息的范围。

综上所述,通过间接与其他有关信息结合而产生的敏感性信息不宜构成金融账户信息的一部分,金融账户信息应该指直接识别到个人金融账户财产的信息,并且可脱敏性的相关信息也应予以排除,以避免金融账户信息保护范围的无限扩张。

(五)最终界定

在综合考虑金融账户信息的界定方式和“信息主体”“信息性质”“信息处理”等要素,以及确定列举和排除的范围后,可对金融账户信息作如下界定:金融账户信息是指金融机构、经授权的非金融机构以提供金融服务、交易服务并作出活动记录为目的所处理的、可以识别到特定用户并通过账户记载的财产信息。其包括银行账户、信用卡账户、账户交易及用于访问账户的鉴别凭证等信息,不包括需结合其他信息才可识别个人金融账户财产的信息和可脱敏性信息。

五、结　语

本文针对我国法律对“金融账户信息”这一法律概念未作界定,在相关规范的认定以及实践中也存在着认定标准不统一的问题,通过对这一敏感个人信息进行总结和完善,并借鉴国外立法例及结合我国实际情况进行分析,认为司法解释的制定可侧重以下几个部分:第一,从信息主体上来看,金融账户信息应是可以识别到个人金融账户财产的信息,无

法直接和单独识别的不属于金融账户信息。第二,从信息性质上来看,金融账户信息是用于金融、商业活动等业务的信息,其以账户作为载体,包括银行账户、信用卡账户等,同时以访问账户的密码、验证码等敏感鉴别信息作为保障账户安全的凭证。第三,从信息处理上来看,金融账户信息是以金融机构、授权非金融机构等具备国家认可资质的主体为处理者,包括但不限于银行、保险公司、金融公司及其他具备资质和能力的处理者,以服务信息主体为处理目的。第四,金融账户信息排除了需要与其他信息识别才具备高致害风险的信息,同时排除了可脱敏性质的信息,更加明确金融账户信息的保护范围,避免保护的无限扩张。

注释:

① 数据参见奇安信威胁情报中心:《全球高级持续性威胁(APT)2022 年度报告》,https://www.qianxin.com/threat/reportdetail?report_id=292。

参考文献:

[1] 胡文涛.我国个人敏感信息界定之构想[J].中国法学,2018(5):235-254.
[2] 孙清白.敏感个人信息保护的特殊制度逻辑及其规制策略[J].行政法学研究,2022(1):119-130.
[3] 丁道勤,姜文,等.国外数据保护法律选编[M].北京:中国法制出版社,2021:19.
[4] 程啸.个人信息保护法理解与适用[M].北京:中国法制出版社,2021:263.
[5] 张新宝.个人金融账户信息的强化保护[J].中国银行业,2021,95(11):26-29.
[6] 韩旭至.敏感个人信息的界定及其处理前提——以《个人信息保护法》第 28 条为中心[J].求是学刊,2022,49(5):132-145.
[7] Helen Nissenbaum. Privacy in context:technology, policy,and the integrity of social life[M]. Redwood City:Stanford University Press,2010:140-147.
[8] 邢会强.大数据时代个人金融信息的保护与利用[J].东方法学,2021(1):47-60.
[9] 宁园.敏感个人信息的法律基准与范畴界定——以《个人信息保护法》第 28 条第 1 款为中心[J].比较法研究,2021(5):33-49.
[10] 支付宝等 5 家机构首批通过"个人金融信息保护能力"认证[EB/OL].新华网,http://www.xinhuanet.com/tech/20221122/3452a998efbb4e916168417de8eaodb5/c.html.
[11] 王苑.敏感个人信息的概念界定与要素判断——以《个人信息保护法》第 28 条为中心[J].环球法律评论,2022,44(2):85-99.
[12] 李东方,李耕坤.数字经济时代个人金融信息的经济法分析与对策——从"立法碎片化"到《个人金融信息保护法》[J].中国政法大学学报,2023,93(1):201-215.
[13] 文进宝,肖冬梅.我国行踪轨迹信息保护范围认定困境与出路[J].图书馆论坛,2022,42(7):55-64.
[14] 谢琳,王漩.我国个人敏感信息的内涵与外延[J].电子知识产权,2020(9):4-16.
[15] 朱芸阳.个人金融信息保护的逻辑与规则展开[J].环球法律评论,2021,43(6):56-73.

(责任编辑:铁青)

Legal Definition of Personal Financial Account Information in China

YIN Huarong, WU Yangyu

(*Law School, Xiangtan University, Xiangtan, Hunan* 411105, *China*)

Abstract: The Personal Information Protection Law includes financial account information in the scope of sensitive personal information but does not provide a clear definition. The lack of a clear definition for the standard can lead to potential vulnerabilities in the rights of data subjects, unclear responsibilities for data controllers, and ambiguity in judicial decisions. By examining foreign legislation examples and considering the current legislative situation and practices in China, it is advisable to adopt a definition model that combines "definition and enumeration and exclusion." This model should consider factors such as the "data subject," "nature of the information," and "data processing" in its definition, listing financial account information comprehensively from both legislative and practical perspectives while excluding financial account information that can only be confirmed through indirect identification. Based on this, China can issue a judicial interpretation of "financial account information" focusing on four aspects to attain a dynamic equilibrium between the protection of personal information and the utilization of societal information.

Key words: Personal Information Protection Law; financial account; personal financial information; sensitive personal information