

此,与其说二维码支付的规范与治理是一个制度建设问题,倒不如说其先是一个技术认知问题。扫码支付依托于二维码,而二维码是一个技术含量高的信息载体,且其技术门槛低,制作与发布简单。由于专业上或消费心理上的差异,普通用户在享受扫码支付带来的福利时,多对其实体与风险缺乏足够的了解与判断,所以只知其然而不知其所以然。二维码信息与知识的不对称就直接影响到扫码支付交易的安全与行业的长远发展。

二维码又被称为QR码(quick response code),其于1994年由日本Denso-Wave公司发明,是在一维条码基础上升级而成的集信息编码、图像处理、信息传递与数据加密等于一体的综合性电子标签技术,是当下信息采集与传递的重要媒介。在设计上,二维码由若干黑白相间的方块组合成一个正方形矩阵,该矩阵被划分为功能图形区和编码区。其中,黑色模块代表二进制“1”,白色模块代表二进制“0”,其符号规格可基于编码数据量自动进行调整,支持的数据类型包括字母数据、数字数据、8位字节数据、汉字数据。二维码支持的信息类型非常广泛,包括图片、文本、视频与音频及网络链接等,且能够对各种类型的信息进行加密处理。在技术上,QR码将数字、汉字、字母及二进制字节这四种标准化编码数据化为二维码图形,其编/译表现为一个“开始→数据分析→信息编码→纠错编码→生成图像→扫描识读→图形定位→纠错编码→信息解码→信息展示→结束”^①的流程。当下,由于二维码的编/译基本上处于开放状态,且对于专业人士而言,其制作比较简便。在法律制度对新技术的治理反应比较迟缓的情况下,在扫码支付^②中,二维码攻击主要表现为以下四种类型。

其一是木马植入。攻击者事先将恶意软件指令编入二维码之中,当用户在不知悉的情况下扫读该类二维码时,用户的智能手机等移动终端系统就会被悄然地植入木马或其他隐性程序。借此,攻击者即可在后台窃取扫码支付用户的支付账户、银行卡、交易记录等信息,从而达到不法侵占他人货币数据资金的目的。

其二是恶意网址诱导。攻击者将钓鱼性质的恶意网址链接伪装成二维码图形。只要用户扫读该类二维码,就会诱导其登录预先植有木马的网站,进而获取用户输入的金融账户、密码、金融交易记录及用户个人的敏感信息等。

其三是二维码的“偷梁换柱”。由于仅凭肉眼难以有效识别二维码之间的差别,而这也无形中给不法之徒达到秘密窃取他人财物提供了可乘之机,如“2016年11月底,佛山市公安局禅城分局接到曾某报案,称其店铺的微信收款二维码被人更换,导致其当天

① 林佳华等:《QR二维码的攻击方法与防御措施》,载《信息安全》2013年第5期。

② 扫码支付可分为主扫(正扫)与被扫(反扫),前者即收款码支付,商家提供收款二维码,而用户使用其手机中载有的App扫码支付。该模式存在二个弊端:一是安全无法保证。由于二维码由商家提供,在扫读中用户的App有可能被插入恶意代码。二是必须借助网络。在网络效果较差时,容易影响消费体验;后者即付款码支付,用户提供付款二维码,商家用扫码枪扫码收款。该模式有二大优点:一是由于二维码由用户本人提供,支付风险被降低;二是不需要网络支持,在结算时,用户提供二维码即可交易。

营业收入6360余元被窃”。^③ 犯罪方式的改变也激发了人们关于此罪或彼罪等的热议,如“该行为对买家构成诈骗罪,对店家则构成盗窃罪,但由于被侵害的法益事实上只有一个,不能被评价为想象竞合犯,因而陷入定性的困境”。^④

其四是信息劫持。为了交易便利,在电子交易中,许多商家会提供在线扫码支付,网络支付平台会根据买家的订单生成支付二维码,以供用户扫码结算。由于交易信息在商家与买家之间传送时存在一定的时差,若攻击者利用网络技术拦截了该类信息,则其可以恶意地修改订单,如篡改收款金额、收货人与托运地址、联系电话等信息,从而给买卖双方带来交易风险。

二维码技术是人类思想的结晶,是人类日益走向文明的标志。然而,由于人根深蒂固的自私自利性,“文明是诅咒,还是福音呢?在过去,文明既是诅咒,又是福音。至于将来怎么样,则取决于人类是将过去文明中积累起来的知识用于破坏,还是用于建设。”^⑤实质上,当我们将二维码技术应用于第三方支付时,其安全性主要系于以下三大隐患:支付指令验证能否得到切实有效的保障、客户端软件的防火墙是否坚实可靠、是否具有完备的纠错处理机制。因此,有专业人士即认为:“存在安全风险不是因为二维码编码技术本身存在问题,而是因为用不好。”^⑥这一评价是合理的,那么与其说扫码支付有风险,倒不如说是人性恶才是风险的真正诱因。二维码与支付风险之间是一种源与流的关系。为了抑恶扬善,唯有从源头上根除与遏制风险,并将相关的二维码清洁措施法律化才是正本清源所在。

(二) 风险规制:二维码清洁的制度化

风险识别与控制关系到交易秩序的稳定、交易模式的市场认可及社会和谐等宏观、中观与微观的价值定向与维系。也正是出于对日渐普及的扫码支付安全的忧虑,2014年3月中国人民银行支付结算司下发了《关于暂停支付宝公司线下条码(二维码)支付等业务意见的函》。对于暂停的原因,文件作了如下解释:线下条码(二维码)支付突破了传统受理终端的业务模式,其风险控制水平直接关系到客户的信息安全和资金安全。目前,将条码(二维码)应用于支付领域有关技术,终端的安全标准尚不明确。相关支付撮合验证方式的安全性尚存质疑,存在一定的支付风险隐患。暂且不论监管者提供的这种理由是否令人信服,但是它毕竟指出了一个问题,即二维码支付存在交易风险,亟须论证与治理。

扫码支付是一个涉及消费者、商家、第三方支付机构与无线通讯运营商等多方主体参与的一个非直接接触式的交易链。在这个循环链中,二维码是作为一个信息中枢而存在,其交易风险释放与扩大的根本原因就在于二维码生成阶段的风险没有得到应有的事前管控。“对消费者而言,自始至终接触的只有二维码,普通用户在扫码前很难鉴

③ 王吕斌:《偷换商家收款二维码 两男子盗刷近百万元》,载《新快报》2016年12月19日。

④ 叶良芳等:《第三方支付环境下非法占有他人财物行为的定性》,载《华东政法大学学报》2017年第3期。

⑤ [美]斯塔夫里·阿诺斯著:《全球通史:从史前史到21世纪》,吴象婴等译,北京大学出版社2012年版,第195页。

⑥ 倪思洁:《二维码藏风险 技术监管有高招》,载《中国科学报》2013年4月4日。

别二维码内容的真伪,也无法了解发布者身份信息是否真实,这使不法分子有机可乘,将两二维码作为植入木马、病毒和非法链接的新通道。”^⑦因此,从源头上加强管理是防控二维码支付风险的症结所在。在借鉴国外经验的基础上,我国早前也推出了两个二维码国家标准,即1997年原国家技术监督局推出的《GB/T 17172 四一七条码》及2000年的《GB/T 18284 快速响应矩阵码》。

为了二维码支付交易的安全,以中国支付清算协会的《条码支付业务规范》(征求意见稿)为蓝本,2017年12月29日中国人民银行发布了《条码支付业务规范(试行)》(银发[2017]296号),该文件对保障条码的“无毒性”作了如下规定:一是设定验证要素。支付机构开展支付业务,可以组合选用下列三种要素,对交易进行验证:仅客户本人知悉的要素,如静态密码等;仅客户本人持有并特有的,不可复制或不可重复利用的要素,如经过安全认证的数字证书、电子签名等;客户本人生物特征要素,如指纹等。当采用数字证书、电子签名作为验证要素时,其过程应符合相关规定,并确保证书的唯一性、完整性及交易的不可抵赖性。二是风险提示。文件第14条规定,支付机构应具备差异化的风控措施和完善的客户权益受损解决机制,在条码生成、识读、支付等核心业务流程中明确提示客户支付风险,切实防范不法分子通过在条码中植入木马、病毒等方式造成客户信息泄露和资金损失。三是软硬件提质要求。支付所涉的业务系统、客户端软件、受理终端等应持续符合监管部门及行业标准,确保条码生成和识读过程的安全性、真实性和完整性。

虽然《条码支付业务规范》的推出缓解了二维码支付所产生的规范供求矛盾,但它还是没有较好地解决二维码自身的安全问题。这主要体现于以下两个方面:其一是没有解决二维码的“出身”与统一管理。“关于二维码的发布权、企业发布二维码的相关资质等没有统一明确的规定和管理。”^⑧虽然由前述的国家质检总局发布二维码技术标准具有一定的合理性,但是支付风险治理并不是该机构的专长,由此就可能造成第三方支付监管者央行与该局之间在这一问题上缺乏深度的协作而各自为战;其二是没有从细节上真正严格二维码的“清洁性”。虽然在“296号”文中,监管者多次重申二维码的安全性、有效性、真实性与完整性,但是如何从规范上实现这些目标呢?对此,文件并不详尽。二维码是支付交易指令传递的介质,是支付风险的源头。如果事前防范是风险法律控制的核心,那么从制度上明确、统一、严格二维码出生标准的“话语权”就是“清洁工程”的首要问题。

在制度设计上,二维码的去伪存真可以着力于以下三点:一是二维码信息加密要求。对此,学者们提出了许多建议,如“基于Ising模型的加密算法”^⑨、“QR二维码的多重融合加密法”^⑩。为了强化对用户的信息保护及达到二维码“清洁”的效果,将加密作

⑦ 苏文君:《二维码支付风险防范分析》,载《金融科技时代》2016年第11期。

⑧ 林安红:《服务定位:科技期刊二维码应用的理性思考》,载《出版广角》2015年第6期。

⑨ 周庆等:《基于Ising模型的QR码加密算法》,载《计算机应用》2013年第10期。

⑩ 于英政等:《基于QR二维码的多级融合加密算法的设计与实现》,载《计算机与数字工程》2014年第12期。

为二维码发布者的法定义务是确保支付安全的必要条件。然而,为了兼顾安全与效率,在法律创新中,必须考虑到加密的适度性,因为“若为了获得信息的绝对保密,则选用加密复杂度极高的密算法,则编译码的应用效率呈几何级数下降;若为了提高编译码效率,忽视加密算法的安全等级,则失去了加密的意义”。^①二是规范认证与管理。伪劣的二维码如同假冒伪劣商品,它不仅会使二维码使用者的资金遭受损失,而且所产生的劣币驱良币的逆淘汰效应也会扰乱正常的二维码支付秩序。因此,通过强化数字签名与数字证书的方式确认交易当事人的真实身份对于保证扫码支付安全具有重要意义。三是加大与强化支付机构对二维码生成的法律责任。“如果一种制度可以从外部得到这样一种可能性的保证,即人们都特别为遵守法规或惩处违法行为的目的而运用强制力(物理的或心理的强制力)的可能性,那么这种制度就可以被称之为法律。”^②因此,在一种可欲的法律秩序构建与维护中,增加行为人对其可能违法成本的预期是一个必需的选项。在扫码支付中,二维码是支付交易的桥梁,而支付机构是收款码与付款码的生产者。由此可见,要求支付机构保证其系统生成的二维码的“清洁无瑕”就是一个理所当然的逻辑。

在朝这一目标迈进中,法定化的二维码防伪管理系统是防微杜渐的关键所在,该系统应由认证、解析与比对、检索三要素构成。对于认证平台,究竟是由第三方认证机构,还是由央行下设的二级机构来承担,人们的看法并不一致。鉴于政府的公共服务更具有中立性与公信力,同时认证也是监管权力的行使,因而由央行来统筹这一职能是一个更好的选择。为了保证认证的有效性与客观性,所有商户都应在认证平台实名登记注册,依照法定的或行业标准生成官方认证且加密过的二维码,而用户则应在官方的认证平台下载二维码译读应用程序,以作为读码工具获取的唯一途径。扫码完成后,识读程序则根据唯一的私钥对扫描信息进行解码,并对解析后的结果进行比对,这是防止二维码被“污染”的第一道防火墙。其后是将确认的结果自动与央行的认证平台进行链接,以对钓鱼信息、恶意代码与内植的非法网址进行拦截、过滤与屏蔽,以达到进一步的净化效果。为了明确责任机制与形成市场约束,央行认证中心应尽快建立支付二维码数据库,要求所涉主体将流通中的二维码(特别是收款码)在中心备案登记,以便于检索与查询,并作为法律责任追溯的依据。

二、扫码支付对货币法律制度的冲击与应对

(一) 对货币法律制度的冲击

货币制度事关一个国家的本位货币、货币流通、货币铸造、货币偿付与币值稳定等核心问题,它直接关系到金融安全、金融效率与金融正义等社会高远目标。由于其重要

^① 张彬等:《二维码的安全技术研究》,载《信息安全与通信保密》2015年第10期。

^② Max Weber, *On Law in Economy and Society*, trans. by E. Shils and Rheinstein (Cambridge, Mass, 1966), p. 5.

性,这一制度的保障与贯彻无不由一国的央行垄断与专享。在纸质货币下,由于央行绝对垄断了货币的发行与回笼,且在长期的监管中,商业银行的业务活动已处于央行等严密、系统的制度网络看守下,所以作为货币制度核心的货币政策在“央行——商业银行”的二元架构中,其运行的可靠性与有效性能得到预期与保障。然而,无卡、无纸化的扫码支付不仅对传统的货币法律制度产生了挑战,而且也对央行职能运行的有效性产生了“革命性”冲击。对此,解析如下。

1. 刷新了传统货币的概念

无论货币在“实物货币→金属货币→银行券→纸币”这一流程中表现为何种形式,在人们的惯性认知中,货币是一种物理有形的有偿证券。虽然在对第三方支付机构的属性定位中,各国的实践并不相同,但一个无可争辩的事实是,数据化与无纸化的支付结算已经宣告了一个货币电子化时代的来临,而这也必将连带性地触发货币法律制度脱胎换骨性的“革命”。早在1998年,巴塞尔银行监管委员会在其《电子银行和电子货币业务的风险管管》中将电子货币定义为:“通过电子设备、或销售终端、或移动电话与因特网等公开网络,基于储值或预付而支付的货币。”^⑬在学术探讨中,人们也提出了一些大同小异的观点,如“电子货币是在法定货币的基础上衍化出来的一种具有流通支付功能,以电子数据为基础存在形式的货币资产。”^⑭

无论人们对电子货币做何种解读,一个胜于雄辩的事实是,现金已开始渐进式地退出流通领域。无论是在线上还是线下的交易中,支付结算更多地体现为电子化。毋庸置疑,包括扫码支付在内的货币资金的数据化异动已从形式至实体对传统货币产生了猛烈的连锁性颠覆效应。货币的表现形式与发行是整个货币法律制度的基石。虽然扫码类的第三方移动支付其本意并非要侵蚀与挑战央行所垄断的货币发行权,但在实际上还是对央行专属的发行权产生了涟漪效应。当第三方支付机构以红包返利或代金券等来激励消费时,那么在法律还没有改变之前,这种僭越就表现得更为明显。“当前电子货币发行主体主要是商业银行等金融机构,还有是些特别发行公司的非银行机构,电子货币发行主体的多元化使中央银行作为发行的银行地位受到挑战。”^⑮

由央行垄断货币发行是服务于安全的需要。为了巩固这一思想,一国多通过立法予以明确,如《中国人民银行法》第18条、20条规定:人民币由中国人民银行统一印制、发行;任何单位和个人不得印制、发售代币票券,以代替人民币在市场上流通。然而,当下,这一规定已面临移动支付的严重挑战。第三方支付自产生之日起,其功能即在于支付结算,以作为对传统商业银行中间业务的补充,并通过和电子商城的“联姻”使消费者产生黏性效应,从而扩大需求。虽然这种业务的开展必须以银行卡的绑定为基础,且交易的额度也受限于支付账户持有人银行卡内的资金余额,但是支付机构主导下的扫码

^⑬ Basel Committee on Banking Supervision, Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision Working Paper, 1998.

^⑭ 刘少军:《金融法原理》,知识产权出版社2006年版,第249页。

^⑮ 谢吉晨:《电子货币对央行及货币政策影响研究述评》,载《上海金融》2007年第6期。

支付直接产生了一个问题,即货币的电子化,支付机构间接地获得了电子货币的发行权。

金融安全是金融治理中不变的主旋律,而大势所趋的货币电子化势必导致对发行权的争论及央行对金融系统风险控制力的降低。作为现代科技进步的产物,电子货币是人类货币史上又一次量变到质变的飞越,它的产生极大地降低了信息成本与交易费用,信息流与资金流的光速传递打破了时空阻隔的障碍,实体货币印刷、发行、运输及盘点等环节的消失也节省了大量的人力与物力成本。科技会弱化人类的选择,并最终使人因屈从而失去选择。而且,随着生产率的飞速提升,在供求矛盾中,人类所面临的已不再是供给不足,而更多的是需求不足问题。与现金消费相比,扫码者在消费心理上会表现得更为“阔绰”与“豪爽”,而这无形中会扩大消费,拉动需求,进而促进就业岗位的增加。因此,利弊相权之下,对于货币电子化,所面临的并不是说“不”,而是如何认识、规范与引导的问题。

2. 对央行货币政策有效性的影响

“货币流通速度的稳定性和可预测性,关系到货币流量的变化能否对宏观经济活动产生稳定的和可预测的影响,从而决定货币政策是否有效。”^{①⑥}电子货币对于货币流通究竟是产生提速或减速作用,这是一个非常重要的问题。当下,人们还没有完全达成共识,但是鉴于货币是服务于市场交易的,那么交易的频率就会自然带动货币的流速。从市场交易量的显著提升看,“电子货币降低了中央银行对基础货币的控制能力,提高了货币流通速度。”^{①⑦}作为电子化与信息化的载体,电子货币不仅具有其独特的货币创造与供给机制,而且也改变了货币数据信息流转的方式,一个可预见的结果是,“电子货币会改变货币乘数,增加中央银行借用传统信用创造理论调控货币供给关系的难度。”^{①⑧}

虽然在发展中,由于正当性与合法性等不可抗拒的因素,初期的电子货币不得不依托于传统通货,并受制于央行的强力管控,但是随着纸币流通的不断溢出,数据化的电子货币便会形成自己的供给创造机制。如有学者认为,“随着移动支付和电子货币网络规模效应的凸显,货币需求形式的改变和电子货币的私人供给,将会使得货币控制的有效性大大降低,这时需要中央银行发明新的货币政策工具来应对这一冲击。”^{①⑨}如果对货币电子化欠缺正确的认知与规范化的引导,则在主流学说影响下,如金融机构等享有电子货币发行权,其不仅会导致社会中货币供给渠道、供给机制与货币乘数的变化,而且也会直接导致央行货币控制能力的下降与货币政策有效性的滑坡。如就公开市场操作活动而言,由于央行的货币发行权被分散,其铸币税收入与资产负债量的大幅缩减将可

^{①⑥} 王亮等:《电子货币、货币流通速度和货币政策有效性》,载《金融理论与实践》2014年第5期。

^{①⑦} Suan M. Sulliva, *Electronic Money and Its impact on Central Banking and Monetary Policy*, Hamilton College Working Paper, No. 02/1, 2002.

^{①⑧} Friedman, *Monetary Policy Implementation: Past, Present and Future-Will the Advent of Electronic Money Lead to the Demise of Central Banking?* *International Finance*, 2000, 3, pp. 221-227.

^{①⑨} 谢平等:《ICT、移动支付与电子货币》,载《金融研究》2013年第10期。

能导致其无力进行大规模的货币吞吐操作。另外,法定存款准备金要求的名存实亡也会节约融资成本,商业银行等也会尽量减少向央行通过再贴现举债,这也会加剧央行货币政策传导功能的失灵。

实际上,货币电子化的辐射效应并不局限于金融法域,其也波及刑法的定罪与刑罚及民法中对物的认定与评价。如在二维码偷换案中,有人认为:“行为人通过秘密手段将商家的财物转移为自己非法占有,完全符合盗窃罪的构成特征,应当成立盗窃罪。”^⑩当货币电子化“一统江湖”时,央行的货币发行权会终结为与国民生产总值相匹配的电子货币核发权,其结果是纸币最终退出流通。当该情形发生时,我国《刑法》所规定的一些罪名也就会形同虚设,如伪造货币罪、持有使用假币罪、变造货币罪等;再者,其也影响到当下民事法律对物的认定。在已有的民法研究中,对于物,学界主流认为:“民法上的物,是指存在人体之外,为人类所支配,且能满足人类社会生活需要的有体物……有体物不仅包括那些能够看得见、摸得着的有形物,也包括无法为人们肉眼所看见或无法为人所触摸的无形物,如电、光、热等。”^⑪无需质疑的是,对于电子化的货币是否属于物,学理上并不存在实质歧义。然而,在实证的法律规范中,物这一关键词却显得有些模糊,如我国《物权法》第2条规定:本法所称物,是指包括不动产和动产。法律规定权利作为物权客体的,依照其规定。对于何谓不动产和动产,该法并没有相关内容。对此,我国1995年的《担保法》第92条的规定是:不动产是指土地以及房屋、林木等地上定着物,动产是指不动产以外的物。由此可见,由于货币形态的变化,在发生争议时,电子货币是否属于物也是一个见仁见智的问题。

(二) 应对之策

虽然法律对稳定性和秩序性的追求给其自身的发展注入了惰性因子,但是法律必须服务于人类文明持续发展的要求。如果法律过度拘泥于安定性而丧失了顺时的成长性,那么其就自然失去了法律所应有的“法性”,而走到法律的对立面。从人类已走过的历程看,一味地固守现状与强调安全,只会导致停滞不前。相反,稳定性与安全性只有通过实时变革才能获得,而拒绝变革则会使社会秩序变得更加脆弱与不可靠。“实在法均具有暂时性和文化多元的特质。暂时性意味着实在法的变化性、非确定性。”^⑫互联网代表着人类科技的进步,其网络与数据革命必然会对既有的法律产生冲击,“从传统走向现代,反映金融信息化的最新动态,成为当前金融法制变革的重要主题。”^⑬承接前文的论述,对此做如下思考。

1. 关于电子货币问题

思想是人类在竞争中优胜劣汰、文明与发展的主宰。以互联网为标志的新技术正如蛛网般影响着人类生活的各个方面,它不仅催生了生活的互联网思维,而且在金融领

^⑩ 周铭川:《偷换商家支付二维码获取财物的定性分析》,载《东方法学》2017年第2期。

^⑪ 王利明等:《民法学》,法律出版社2015年版,第198-199页。

^⑫ 舒国滢等:《法学方法论问题研究》,中国政法大学出版社2007年版,第11页。

^⑬ 冯果等:《社会变迁视野下的金融法理论与实践》,北京大学出版社2013年版,第63页。

域也正自下而上地使得货币的形态与金融治理面临技术性的冲击与挑战。互联网+、云计算与大数据等科技创新的应景不仅促使人们不得不以一种新的思维模式来重新审视市场、产品、价值链、信息交流等整个商业生态圈,而且也直接对货币的表现与流通方式产生了强大的催化效应。互联网时代,数据化已是我们这个时代的标签。“大数据开启了一次重大的时代转型。就像望远镜让我们能够感觉宇宙,显微镜让我们能够观测微生物一样,大数据正在改变我们的生活以及理解世界的方式,成为新发明和新服务的源泉,而更多的改变正在蓄势待发。”^{②4}

货币数据化、电子化已是情景所需。然而,这是否就意味着在货币法律制度的创新中,立法者就必须吸纳主流的观点,“识时务为俊杰”地另起炉灶而将既有的法律全部推倒重来呢?在对电子货币的研讨中,学者们对其发行、交易、流通等环节的制度化提出了诸多建议,如“我国未来立法亦只应允许非银行发行商从事电子货币发行、提供与此紧密相关的金融和非金融服务、数据存储业务。”^{②5}另外,亦有学者建议我国应仿效欧盟的做法将第三方支付机构纳入电子货币机构,而赋予其电子货币的发行权。当下,电子货币是一个比较时髦的词语,但这并不是一个精准、科学的表达,它只是标志着传统纸质货币形态的改变,并没有对传统货币及其关联制度产生致命性的“釜底抽薪”效果。客观上,“电子货币不是一种新的货币形态,只是基于实体货币而诞生的用于电子支付体系的新支付方式。”^{②6}因此,货币电子化才是对现实准确的定位与回应。

没有任何一种创新是无中生有的。对于制度的创新,我们都必须清醒地认识到:“人们自己创造自己的历史,但是他们并不是随心所欲地创造,并不是在他们自己选定的条件下创造,而是在直接碰到的、既定的从过去继承下来的条件下创造。”^{②7}基于此,以下观点无疑是公正且理性的:“从本质上讲,电子货币是一种货币形态的革命,是作为货币的物的形态的革命,而电子支付是支付方式的革命,是债务履行方式的革命。”^{②8}货币不仅是一个经济概念,其更是一个具有法偿性的法律概念。当下,“从目前各国的有关立法来看,并不存在将电子货币确认为法定货币的法律。”^{②9}综合考察,扫码支付等电子支付都没有,也不可能脱离当下运行的货币生态与规范系统,而只是货币资金支付方式的变化。

在电子货币的讨论中,其发行权的确立是一个紧要问题。“欧洲大陆各国,以加强监管为目的,认为电子货币的发行主体原则上应限定在金融机构并作为金融监管的对象。”^{③0}为此,欧盟亦出台了《电子货币指令》(2000/46/EC),并创设了电子货币机构这一

^{②4} [英]维克托·迈尔等:《大数据时代》,盛杨燕等译,浙江人民出版社2013年版,第1页。

^{②5} 钟志勇:《电子货币若干法律问题研究》,载《河北法学》2007年第9期。

^{②6} 张庆麟:《电子货币的法律性质初探》,载《武汉大学学报》(社会科学版)2001年第5期。

^{②7} 《马克思恩格斯选集》(第1卷),人民出版社1995年版,第585页。

^{②8} 刘颖:《货币发展形态的法律分析》,载《中国法学》2002年第1期。

^{②9} 徐冬根:《论法偿货币——兼论电子货币非法律意义上的货币》,载《江西社会科学》2013年第6期。

^{③0} 赵家敏:《电子货币》,广东经济出版社1999年版,第193页。

概念。在研究中,主流的观点认为,如果对电子货币进行严格管控,则可能会抑制创新,因而有必要将金融机构法定为电子货币的发行主体。对此类复古的观点,我们应持怀疑的态度。“中央银行是发行货币的银行、政府的银行、银行的银行之性质与职能并非与生俱生,而是经过数百年的演进才沉淀成的认识。”^⑨现实地看,央行职能的固化是商品经济模式下货币与信用发展的产物,是经济安全、政治稳定与社会和谐等多种因素融合的必然结果。如果在法律创新中,我们基于扫码等电子支付而贸然地将货币的发行权赋予商业银行、第三方支付机构等,那么将是一种退化,它很可能使我们再次面临货币发行市场失灵而无人兜底的系统性金融失控风险。因此,笔者认为,扫码支付只是意味着支付方式与货币的电子化,在整体上,其并不意味着对央行货币职能的篡位,而仅仅意味着职能行使形式的制度化创新。

2. 关于货币政策问题

大数据不会恶化监管,相反,如果善用,它的信息快速传导反倒会促进监管。在各种学理的论战中,人们之所以对央行货币政策的有效性表现得忧心忡忡,其原因即在于货币流通中的数据不完整等。如果央行能解决数据的及时性、完整性、真实性、合法性等问题,那么这种担心自然就会迎刃而解。由于备付金的管理有些失范,二元化的“第三方支付机构——客户”之间清结不仅创造了货币乘数,而且游离于清算体系外的资金循环也衍生了诸多监管风险,造成市场混乱。对于这一问题,我国央行已展开了“收编性”的整饬行动。2017年8月4日,央行支付结算司下发了银支付〔2017〕209号《关于将非银行支付机构网络支付业务由直连模式迁移至网联平台处理的通知》。文件规定,自2018年6月30日起,支付机构受理的涉及银行账户的网络支付业务全部通过网联平台处理。各银行与支付机构应于2017年10月15日前完成接入网络平台和业务迁移相关准备工作。

在央行的指导下成立网联的意义是不言而喻的,其不仅可以通过与银联竞争的方式加速清算行业的创新与有序,更重要的是,它保证了支付机构货币资金流动数据传递的及时性、通畅性与透明性,从而极大地保证了央行的货币政策能在信息充分占有与监测的情形下运行。同时,大数据下货币异动的高度阳光化也能达到对扫码支付中可能存在的洗钱、钓鱼欺诈等可疑交易行为起到及时“消毒”的效果。虽然该文件明晰了时间表,加快了网络版银联的打造,但是该平台的角色与功能定位还欠明确。2016年7月央行发布的《关于二维码支付监管原则及要求的通知》第2条规定:支付机构基于银联卡快捷支付开展条码支付业务的,通过接入中国银联进行处理或在支付清算协会组织筹建的统一清算平台投入运行后,通过统一清算平台转接至中国银联进行处理。由此可见,在目标设定上,网联只是作为银联的前置平台存在。在结果上,与其说支付机构是被央行“收编”,倒不如说是被银联“收编”。

货币电子化会放大货币创造乘数,进而影响传统货币政策的有效性。虽然网联

^⑨ 陈晓:《中央银行法律制度研究》,法律出版社1997年版,第17页。

能缓和这一矛盾,但是它只能解决监管中的信息不对称问题。实际上,有效的货币政策提出一个很现实的问题,即央行必须具有互联网思维。如果在治理中,央行依然故我地停留于传统的货币政策工具运作模式,那么探讨制度创新就是一个伪命题。“为提高货币政策的有效性,中国人民银行要充分考虑电子货币对流通中纸币替代所产生的货币供给创造效应,并且要清楚识别不同类型电子货币对流通中纸币所形成的货币创造机制,进而制定合理的标准和规则来引导电子货币的发展,增强对社会经济中货币供给的控制能力。”^②传统的货币政策工具,如公开市场操作活动、再贴现等都必须基于可依赖的信息。虽然在互联网背景下,这些传统工具仍然是举足轻重,但是货币数据信息的占有是当下央行治理的重点。新语境下,虽然货币的表现形式电子化,但是其存在仍不能脱离于实体经济与传统纸币的发行与调控理念。因此,第三方支付机构的电子化货币运行必须遵守以下原则:一是其总量不得超过支付系统账户内的资金余额,而该资金余额又必须与支付账户绑定的银行卡账户资金余额保持对等关系;二是红包或代金券的发行必须基于支付机构的净资产状况,并设定合理的发行比例。同时,不得违背《中国人民银行法》的禁止性或限制性规定;三是资金循环必须接受央行周期性的动态管理;四是货币电子化数据必须接受央行的现场与非现场检查与监督。

三、未授权扫码支付风险与制度创新的进路

(一) 未授权扫码支付风险

若在网上搜索二维码支付损失,则很容易找到许多相关二维码支付未授权交易损失的案例。此类事件的发生不外乎以下原因:手机遗失被他人盗用二维码进行消费支付,或用户扫读了他人提供的植有病毒的二维码,或二维码支付交易信息被劫持等。为了保证支付安全,当下的支付机构也配置了一些应急措施,如在手机被盗抢或遗失时,用户可以通过事前绑定的邮箱找回密码,或通过手机短信与独立的支付密匙等来保障用户的资金安全。微信支付在支付安全中就做了如下营销说明:银行级别的安全技术、支付密码和手机短信双重验证、中国人民财险全额承保。然而,当智能手机不能处于本人控制时,如果支付验证仅为手机验证码或支付密钥,那么扫码支付就事实上让用户的支付账户及与该账户绑定的银行卡处于不设防状态。上述所谓的保障也只能是中看不中的“花瓶”而已,很难形成有效的救济。

此外,在扫码用户与支付机构的服务协议中,关联的支付机构早已通过“霸王性”的格式条款将未授权交易的法律风险进行事前、全方位性的排除,如《微信支付用户协议》即规定:用户应妥善保管好微信号及其登录密码、微信支付密码、手势密码、手机等移动终端及SIM卡信息、二维码等信息,并确保手机等移动终端设备在安全、无病毒、未被入侵、未被监控、未被非法控制的环境下运行和使用。若泄露了上述信息中的任意一项或

^② 印文等:《电子货币的货币供给创造机制与规模》,载《国际金融研究》2016年第12期。

遗失了上述硬件设备,因此导致的风险和损失由用户自行承担。而且,在支付指令发出后,用户也只能自求多福,如《财付通服务协议》规定:在财付通公司网站或第三方网站、软件、App 上按财付通服务流程所发出的指令或确认的交易状态均为不可撤销的指令,财付通公司将据此提供支付服务。支付宝《快捷支付服务协议》更是以强硬的措辞声明如下:客户发出的指令不可撤回或撤销,支付宝一旦根据指令委托银行或第三方从银行账户中划扣资金给收款人,客户不应以非本人意愿交易或其他任何原因要求支付宝退款或承担其他责任;客户对在使用本服务过程中发出指令的真实性及有效性承担全部责任,由此操作所产生的一切风险由客户本人承担。

为了避免资金损失,虽然用户也可以不厌其烦地在每次扫码支付后开启“暂停使用”之类的设置,但是这种烦琐有悖于二维码支付推出的初衷,因为小额无卡、无密是与支付快捷深度关联的。扫码支付之所以能在极短的时间内风靡于市场,也是源于用户在心理上已接受、认同了其所带来的快捷扫码体验,而安全问题被暂时搁置。由于高度洞察了用户的消费心理,为了提升扫码支付的资金消费量,支付机构还隐性地预设了增加单笔无密支付的内容,如《财付通服务协议》即规定:当任何功能减少或者增加或者变化时,只要仍然使用财付通服务,即视为用户同意本协议或本协议修正后的条款;财付通在其微信支付中阐明:开通微信支付付款码服务后,付款金额不足 1000 元的交易,无须验证支付密码或其他交易指令验证要素;《银联用户服务协议》在陈述与保证部分规定:若在本协议内容公告变更后继续使用本协议下服务,表示已充分阅读、理解并接受修改后的协议内容,也将遵循修改后的协议内容使用本协议下服务;支付宝在这方面则表现得人性化,体现出与用户共治的特点,用户只要点击支付宝应用程序,经过“设置→支付设置→免密支付→小额免密支付→支付密码输入→开启”的操作流程,就可以在“200/笔、500/笔、800/笔、1000 元/笔、2000 元/笔”五档中进行选择设定。对更多佣金回报与市场份额的追求自然会促使支付机构提高单笔扫码支付的金额,这无疑会进一步放大用户未授权扫码支付的风险。

互联网金融的应景下,资金流动的电子数据化已是一种“革命性”的时代潮流。虽然从最密切利害关系看,保证交易资金安全是消费者责无旁贷的责任,但是在技术、信息、人力等非对称关系下,确保交易的非风险性更是涉事支付机构的职责所在。电子交易下,密钥是用户保障资金安全的最后一道有力防线。在扫码支付中,如果这道防线由于支付机构的不作为或营销的需要而被外来者突破,那么由此产生的损失却因为支付机构预设的抗辩权而由弱勢的消费者承担,这显然违背法律的公平与正义。在法哲学研究的掘进中,“虽然我们并不拥有判断正义的肯定标准,但是我们确实拥有一些能够告诉我们何者是不正义的否定标准。”^③随着人类科学技术的发展,生产创造或决定需求而让位于需求决定生产,这一转向必然导致消费者权益保护成为一种政治性与法律性的运动,而这也直接促成了金融治理理念的转向。“在传统上,金融监管以维护金融稳

^③ [英]哈耶克:《法律、立法与自由》(第2、3卷),邓正来译,中国大百科全书出版社2000年版,第65页。

定为主旨,保护‘经营者主权’。20世纪60年代后,消费者保护逐渐进入监管者的视野和金融监管目标体系中,‘消费者主权’也开始取代‘经营者主权’。”^⑭正义是一个动态的概念,当二维码扫码等移动支付被市场青睐时,对未经授权交易的风险合理分切就是一个与正义相关的问题。除此之外,在制度的演化中,还有一个更深层次的问题是值得警惕的,即技术创新似乎意味着人们越来越接近真理与自由。诚如庄子所言:凡有机事者必有机心,凡有机心者必有机心。实质上,包括扫码支付在内的技术正在日益污染人的灵魂,剥夺人们的自由,使人越来越成为技术、规范、标准与习惯的附庸。

(二) 制度创新的进路:以维护消费者权益为导向

虽然各支付机构在其线上或线下协议中通过格式条款对包括扫码支付在内的未经授权交易风险进行了事前规避,但是若发生法律争议,对其效力,法院最终如何判定,这是一个充满变数的解释与博弈问题。对此,我国《合同法》第40、41条规定:提供格式条款一方免除其责任、加重对方责任、排除对方主要权利的,该条款无效。对格式条款的理解发生争议的,应当按照通常理解予以解释。对格式条款有两种以上解释的,应当做出不利于提供格式条款一方的解释。另外,《消费者权益保护法》第26条亦规定:经营者不得以格式条款、通知、声明、店堂告示等方式,做出排除或者限制消费者权利、减轻或者免除经营者责任、加重消费者责任等对消费者不公平、不合理的规定,不得利用格式条款并借助技术手段强制交易。

尽管在未授权扫码支付中,上述相关的内容给支付用户的维权提供了法律依据,但是解释权毕竟掌握在法院手中。实质上,在契约自由精神下,无论对条文作何种扩张性的解释,其都不可能完全游离于语词的核心要义。当支付服务协议白纸黑字地约定未经授权交易风险由用户承担时,争议双方力量的悬殊也决定了法院的解释空间是非常狭窄的。如果当事人意图借用显失公平来行使其合同的变更权或撤销权,则由于显失公平本身的含糊其词性,在实践中法院多持比较谨慎的态度,而且这两种权利的行使还受除斥期间的限制。因此,在既有的法律框架下,发生未授权扫码支付时,用户的维权之路并不那么顺畅与平坦。当“市场失灵导致单纯依靠市场力量无法给金融消费者提供完全有效的保护”^⑮时,增加法律公共产品的注入以缓解规范供求的失衡就成为一种必然。为了实现利益的公平保护及对扫码支付这种新金融形式提供必要的支撑,我国的法律可从以下几个方面进行革新。

1. 举证责任的重新配置

为了支付安全,微信支付引进了由中国人保承保的“24小时极速理赔”机制。然而,这很有可能只是一种“摆拍秀”,因为相关的理赔条款并没有在支付服务协议中得到体现,这就导致一个效力认定问题。同时,微信支付声明,为保证成功赔偿,用户应积极配合提供相关资料以核实情况,但是被骗问题,不在该反馈的受理范围。要求用户保证

^⑭ 吴弘等:《金融消费者保护的法理探析》,载《东方法学》2009年第5期。

^⑮ 孙天琦:《金融业行为监管与消费者保护研究》,中国金融出版社2017年版,第8页。

资料的真实性,这是非常困难的。“当消费者和支付者之间就某一特定支付是否经过授权发生争议时,如果沿用传统的‘谁主张,谁举证’的举证责任配置规则,显然对消费者不利,因为有关支付授权的所有记录和数据都掌握在支付机构手中。”^③欲速则不达的警世格言在某种程度上也表明快捷是不安全的代名词。如果我们意图将一种本质上还不安全的支付模式变成一种安全的支付模式,其出路就是事前确定好未授权交易的责任配置。

证明是诉讼的脊梁,其直接关系到实体权利在程序中的兑现。虽然从诉讼程序启动与诉权分配公平的角度看,谁主张、谁举证是比较合理的,但是互联网金融下,当交易数据、方式、身份识别等都被平台方垄断或操控时,如果还强势要求支付用户等消费者去证明支付机构等存有过错,这确实有些强人所难。当新技术已实质上改变了资源控制的平衡,并在事实上导致资源越来越集中时,如果法律还固守传统的证据观念与规则,那么其只会加剧强弱失衡的“马太效应”。在这一点上,欧盟的做法是值得称道的,其关于内部市场支付服务的 2007/64/EC 指令第 59 条即规定:若消费者认为其并没有授权某个支付交易,或其发出的交易指令没有得到准确的执行,那么则应由支付服务商来证明交易的真实性、交易未受技术故障或其他因素的影响。因此,在面对扫码支付引发的法律僵局时,立法者应审时度势地对支付机构等创立举证责任倒置的原则,以克服传统举证规则形式公平而实质不公平的呆板。如此,不仅可以迫使支付机构研发、升级其杀毒软件,规范商家的收款行为,同时也可以促进大数据背景下证据规则的适时更新。

2. 交易限额的正当性考察

为了控制风险,《条码支付业务规范》根据支付机构的风险防范能力分别设定了日交易上限,如 A 级(采用包括数字证书或电子签名在内的两类以上有效要素验证者),可与客户约定单日累计限额;B 级(采用不包括数字证书或电子签名在内的两类以上有效要素验证者),同一客户所有支付账户单日累计交易金额不超过 5000 元;C 级(采用不足两类要素验证者),同一客户所有支付账户单日累计交易金额不超过 1000 元;D 级(使用静态条码者),同一客户所有支付账户单日累计交易金额不超过 500 元。虽然“央妈”这种限额交易的做法能起到未授权扫码支付交易止损的效果,但是却给人一种因噎废食之嫌。作为一种公共服务,金融治理必须反应与迎合民意,必须与科技发展保持同步。

金融治理必须立于经济发展矛盾的缓解或解决,必须在保守与激进之间保持动态的平衡。内需不足是我国经济发展中的一大瓶颈,限定静态扫码日交易额不仅不利于商家业务的发展,而且也不益于我国就业岗位的创造。另外,“官为民做主”的“善意”也彰显了对公民私产的干预与不尊重。公民对其合法财产具有处分权,这是公理,亦是法理。是故,不从风险源、技术优势等角度来思考风险控制,而将未授权的扫码支付交

^③ 任超:《网上支付金融消费者权益保护制度的完善》,载《法学》2015 年第 5 期。

易风险防范归结为交易上限,这既是治标不治本,同时也是顾头不顾尾的短视之举。正确的态度是,我们的目光应更多地盯住第三方支付机构,而不是拉动需求的扫码支付使用者。

3. 金融教育义务的强化

未授权交易风险的管控不单是政府强力介入的“独舞”,它更需要市场、交易主体等的全体协作。因此,金融知识的普及与提升是风险整体控制中不可缺少的一环。在这一方面,美国的经验值得借鉴。早在2003年美国就颁布了《金融扫盲与教育促进条例》,将金融教育要求正式纳入国家法案,现已形成了课堂教学、网站浏览、游戏互动等多种形式融合的教育模式。为此,美国还专门成立了金融扫盲和教育委员会(FLEC),其主要责任包括:“鼓励政府和私营部门努力促进金融扫盲、协调联邦政府的金融教育工作、建立一个全国性的金融教育网站、建立一个免费热线电话等。”^⑤

有知是防范与消灭未授权交易风险的消毒剂。为了实现有知,我国也应考虑将适度的金融扫盲教育纳入金融机构合规管理的范围,如就扫码支付而言,应通过线上或线下等多元化方式对用户进行二维码支付知识的普及,其内容可包括二维码的构成知识、潜在的支付安全风险、正扫与反扫的利弊、金融隐私信息的保护、扫码支付应用程序的正规下载、木马病毒的防范、常态化的系统升级等。

4. 确立消费者在未授权扫码支付中的有限责任制度

在操作流程上,扫码支付实质上是对银行POS刷卡收单流程的模仿,所不同的是POS机是一个只具有支付功能的闭环性智能终端。为了保证资金安全,银行已为该系统确立了严格的安全认证与密钥机制。虽然扫码支付软件也具有加密功能,但是除了Android、IOS系统存在被Root、木马等病毒攻击感染的可能性外,底层数据被打通后,也会滋生信息外泄,甚至是被拦截风险。我们基本上可以下一个这样的判断:为了迎合市场,扫码支付实际上是将一个还不能满足支付安全需求的技术投放到了一个应用广阔的应景中。在本质上,快速、便捷的资金流动天然地排斥严格的安全要求。在此现状下,承认支付协议中的免责条款,要求消费者全额为未授权交易的损失买单,其公正性昭然若揭。

未授权交易风险之所以发生其因更多地在于客户身份识别手段没有跟上技术的发展。对于这一问题,《非银行支付机构网络支付业务管理办法》第6条规定:支付机构应当遵循“了解你的客户”原则,建立健全客户身份识别机制。该法第24条规定,支付机构应承诺无条件地对采用不足两类有效要素进行验证的单个客户所有支付账户单日累计金额不超过1000元的交易承担全额赔付责任。故而,要求扫码支付用户全额承担未授权交易风险,也有欠公允。在产品推介中,支付机构认为小额无密支付是国际实践,我国应与国际接轨。那么,在责任配置上,我国也应与国际接轨。在这一点上,美国的立法经验是值得借鉴的,如其《电子资金划拨法》与《监管E条例》就将未授权的资金划

^⑤ 徐雅萍:《美国金融教育国家战略:促进金融成功》,载《西部金融》2013年第10期。

拨定性为:由消费者以外的未获消费者本人授权所发起的,从该消费者账户划出资金而该消费者并未从该划拨中受益的资金异常流动。对于此类交易,该法规定:“如消费者在得知该交易后2个工作日内报告,则其承担的责任不超过50美金;如在2个工作日之后至60个工作日之间报告,则承担的责任不超过500美金。”^③

为了引导我国第三方支付业健康、规范地发展,及迫使支付机构研发可靠的客户身份识别技术,如指纹识别、虹膜识别等,我国有必要确立支付用户未授权交易损失承担的有限责任制度,如5%或10%的损失承担比例。当下,在扫码支付的强大压力下,同时为了扩大银行卡的使用,商业银行也对小额无密支付表现出了深厚的兴趣,如中国银行已与一些卖场合作在客户还没有授权的情况下,着力推广300元以内的消费可持卡无密免签的结算。因此,在更广泛的意义上,明确未授权交易下用户的有限责任也能对商业银行等具有结算业务资质的主体在推介与开办该类业务时起到示范性的警示作用,从而促使其从内部的软硬件上做好事前的风险防控与评估,而不是轻率、霸气地通过所谓公正协议的方式将风险向处于弱势地位的用户全部转嫁。

四、扫码支付用户信息保护面临的挑战与法律改良

(一) 支付用户信息保护面临的挑战

如果用户打算开通扫码支付功能,那么其就必须注册支付账户,并将该支付账户与其持有的银行卡关联,在这一过程中,其必须输入个人身份证号、银行卡号、联系方式等私密信息。诚如前文所述,虽然在设计上二维码比较简单,但是对于非专业人士而言,它可能被嵌入木马等程序,从而达到窃取他人信息的目的。数据化的时代,信息已被市场化与商品化,而这无疑给支付机构提供了“近水楼台先得月”的商机。由于支付机构本身就留存了大量的客户个人基础信息与交易信息,而这更加剧了客户信息被泄露的风险。对于客户信息的获取、存储等,支付机构预设了诸多利己的规则,如支付宝《快捷支付服务协议》就对客户要求如下:在使用本服务期间或本服务终止后,客户应授权支付宝有权保留其在使用服务期间所形成的相关信息数据,同时该项授权不可撤销。除此之外,支付宝还专项制定了《信息授权协议》,如其规定,本协议中的个人信息包括但不限于身份信息、账户信息、银行卡信息及其他必要信息。客户同意授权支付宝查询客户的个人银行账户信息,包括但不限于卡号/账号、户名、余额、用卡时间、频次及金额等。“包括但不限于”的措辞使得支付机构能掌控的信息范围变得无所不包。

为了防止可能的信息泄露风险,央行在相关文件中已做了安排。《支付业务管理办法》第20条规定:支付机构应当依照有关客户信息保护的规定,制定有效的客户信息保护措施和风险控制机制,履行客户信息保护责任。支付机构不得存储客户银行卡的磁道信息或芯片信息、验证码、密码等敏感信息,原则上不得存储银行卡有效期。在客户

^③ 唐琼琼:《第三方支付中的消费者权益保护问题研究》,载《河北法学》2015年第4期。

信息的采集、使用、存储与传输中,支付机构应遵守“最小化”原则,并告知客户相关信息的使用目的与范围。同时,应当通过协议约定禁止特约商户为上述行为,并采取定期检查、技术监测等必要监督措施;《条码支付业务规范》第18条规定:条码信息仅限于当次支付相关信息,不应包括任何与客户及其账户相关的支付敏感信息。除此之外,早前的《侵权责任法》已将隐私权作为一项具体的人格权加以保护。虽然在思想认知与制度建设上,我国的个人信息保护已有所增进,但是其仍远远地落后于大数据发展所提出的诉求,这主要表现在以下几个方面。

其一是核心概念不明确。虽然隐私权已被记载于《侵权责任法》的民事权益中,但是通观全文,该法对于何谓隐私权、其内涵与外延等基本范畴并没有只言片语的表述。概念是我们认识与把握事物的起点,更是规范与调整社会关系必不可少的工具。隐私权这一基础概念的缺位所暴露的不仅是我们对隐私权保护意识与观念的乏善可陈,而且更严峻的是,这种缺位也直接导致在金融隐私权、信息权保护上的立法与实践难有较大的作为,而只能停留于象征意义的宏大话语,因为毕竟“隐私权→金融隐私权→信息权”之间是一种继往开来的衍生关系。

其二是支付机构的属性定位不能适应信息保护的要求。金融机构并非一个恒定不变的概念,其边界与内涵必须顺应金融在特定时代下发展的需求。互联网技术的推动下,资金供求之间的流动形式与介质已发生了革命性变化。第三方支付机构等已在事实上突破了商业银行、证券公司等传统金融机构的含义,并挑战这些传统金融机构的地位。如果当下的法律不能因时制宜地对金融机构做出时代性的阐释,则不仅不利于经济金融的创新性发展,而且也不利于包括金融消费者隐私权在内的权益保护,如早在2005年我国的《电子银行业务管理办法》第52条规定:金融机构应采取适当措施,保证电子银行业务符合相关法律法规对客户信息和隐私保护的规定。由于第三方支付机构不属于金融机构,那么其自然就被排除在该文件所述的隐私权保护合规要求之外。

其三是与互联网金融的时代格局存在严重不匹配现象。金融隐私具有浓厚的人权性与价值性,它直接关系到消费者的核心利益。在某种程度上,保护这种利益就是在保护、规范市场与保障金融安全。在互联网技术欠发达的过去,由于信息传播、收集、储存、复制等的效率相对低下,且公众的关注度也不太高,金融隐私权保护问题还显得不那么迫切与紧急,但是随着大数据时代的来临,这一切都发生了翻天覆地的变化,因为“大数据是在新一代信息基础设施的支撑下,物理空间运动过程加速向网络空间映射的结果,具体表现为规模巨大、种类多样、内在关联的数据集中,趋向于无限接近真实世界。”^③

共享与协作是大数据时代的特征,这似乎昭示着隐私权保护的不再或衰落,但是“它并不意味着以金融消费者为代表的主体不再对自身的信息享有任何权利,而是这种权利的核心不再拘泥于私密性和隐秘性,正是在这些背景下金融信息权理论开始

^③ 王达:《美国互联网金融与大数据监管研究》,中国金融出版社2016年版,第181页。

崛起。”^⑩虽然移动性的扫码支付创新了人类的支付模式,但是它也使得隐私权保护面临一种塌崩性的风险,因为网络化的时代,“我们正处于一种不断变化但却日趋精密的被监视状态中。事实上,现在我们的一举一动都能在某个数据库中找到线索。”^⑪时下,扫码支付以点带面地抛出了一些值得深入探讨的问题,如互联网金融背景下,隐私权是否过窄?是否应以金融信息权来取代金融隐私权?金融信息权的边界何在?信息公开与保密之间应如何协调?

其四是话语权的失衡问题。虽然财付通与支付宝等都高调地出台了隐私权政策或在协议中内置了相关条款,但是对于信息的公开与使用等,在格式化协议与扫码支付之间,消费者只能作是或不是的取舍时,支付用户并不享有多少话语权。同时,与其说相关的隐私政策是在保护消费者的隐私权,倒不如说是支付机构通过形式正义的协议为其占用、存储、使用、收集、公开用户的信息获得正当性与合法性,如《财付通隐私政策》就开宗明义地表明:当客户同意《财付通服务协议》时,或访问财付通公司网站及其相关网站,或是下载、安装、使用财付通公司客户端时,或使用其提供的任一服务时,即表示客户已同意其可按照该政策收集、储存、使用和分享信息。除非客户已阅读并接受本政策所有条款,否则其无权使用财付通服务。在权利的配置不公允时,理论上,作为公共产品的法律是对这种失衡进行矫正的有力补充。

(二) 法律改良的路径:以确立信息权为中心

大数据时代,信息已在事实上成为社会中至关重要的财富与资源。互联网、云计算与大数据在缩短信息传送的时空距离的同时,也衍生了一些新的问题,如信息越来越不受信息主体的控制、信息被商品化、信息更易于被不法使用及传统信息保护观念与模式的失灵等。凡举事必循法以动,变法者应因时而化。法律的成长性决定了,对个人秘密的保护也必须紧随互联网时代所提出的演进诉求。对于这一点,法人类学者霍贝尔曾言:“实际上法律是一个动态的过程,在其中没有哪一种解决问题的方法可以永世长存。因此,法律的第四个功能就是,关系的重新规定和期望的重新定向。”^⑫对扫码支付所触发的金融隐私权保护问题,做如下思考。

其一是确立信息权,并兼顾平衡保护。在目前的司法实践中,我国对侵犯个人信息保护更多地表现为一种人格权的隐私权保护路线。虽然与传统相比,这已是进步,但是其仍严重滞后于时代的发展。大数据时代,“通过获取、汇集和整合人们在日常生活中所留下的种种生活痕迹,数据技术完全能够在短期内描摹出于个人的实际人格相似的数字人格,从而使私人图像一览无余地暴露于他人的窥视之下。”^⑬网络技术的更新扩展了信息公开的空间,但是与此同时也扩张了人们对信息保护诉求的范围。为了通过市场消费对扫码支付、大数据等创新提供回馈,并消除消费者的顾虑与观望心态,有必

^⑩ 张继红:《论我国金融消费者信息权保护的立法完善》,载《法学论坛》2016年第6期。

^⑪ [美]艾伯特—拉斯洛·巴拉巴西:《爆发》,马慧译,北京联合出版公司2017年版,第12页。

^⑫ [美]霍贝尔:《原始人的法》,严存生等译,贵州人民出版社1992年版,第249页。

^⑬ 赵宏:《从信息公开到信息保护:公法上信息权保护研究的风向流转与核心问题》,载《比较法研究》2017年第2期。

要与时俱进地在法律中创设信息权概念,并厘定信息权与传统隐私权两者之间的关系。

隐私权的关注点更多地在于信息的秘密性与敏感性,即“个人不愿向外透露的与公共利益无关的信息,并且不被他人知晓和支配的权利。对于隐私权的侵害主要表现为非法披露和骚扰。”^④由此可知,并非公民未公开的所有信息都属于隐私权保护的范畴,大数据时代,这就自然造成大量的信息因法律概念的裹足不前而得不到应有的法律保护。虽然在知识传承中,我们将法律贴上了规律、理性、科学的标签,但是归根结底,法律注定都是它那个特定时代的产儿。扫码支付大场景下的大数据时代,确立信息权是理论正确与时代正确。“信息权所涵涉的范围已远远超越了隐私权,除了与隐私权所保护的敏感及私密信息外,还有一部分信息所体现出的是个人公开信息,这部分信息并不在隐私权的保护范围内,但信息主体仍享有对该信息的收集、处理、更正及删除的权利。”^⑤信息是信息权中的关键词,其指“能为人所支配的,来自人自身、能满足们生产和生活需要的数据资料,具有传播性、不可消耗性、价值性和确定性等特征。”^⑥个人信息权即信息决定权,指个人依据法律的规定对其线上与线下的个人信息所享有的控制,并决定是否允许他人收集、公开、复制与利用的权利。虽然在探索中,有学者提出了隐私权与信息权并举的主张,但是“个人信息这一概念已远远超出了隐私信息的范围”^⑦,在这种被包容下,是沿袭传统而保留“二张皮”,还是将隐私权囊括进信息权中,这是一个传统与当下博弈的问题。

由于消费者已不仅是一个法律概念,同时其更与民主政治深度关联,所以在国际上,尊重消费者,加强对其个人信息的保护已是一种通行的做法。如美国早在1974年便出台了《隐私权法》,以规范政府采集、使用和披露个人信息的行为;1978年又推出《金融隐私权法》,以禁止政府不法获取个人的金融信息;1999年的《金融服务现代化法》确立了隐私权保护的四大原则,即通知原则、退出选择原则、禁止市场公开原则及安全保护原则;在这一点上,欧盟的实践更加贴近时代的气息,其在措辞上直接援用了“数据”,而非传统的“隐私”,如1995年的《关于个人数据处理与自由流动的保护指令》(95/46/EC),其目的在于“成员国有义务确保个人信息得到公平、合法的处理,信息的采集必须符合特定的、明确的、合法的目的,数据不得过度加工。”^⑧2009年通过的《欧盟Cookie指令》(2009/136/EC),则在于对电子商务中cookie的使用加以规范及对信息披露强化管理;2015年12月通过的《一般数据保护条例》则进一步确定与提升了对个人数据的保护原则与监管方式,以避免使公众在信息时代遭受“裸奔”的尴尬。这些数据保护意识、保护与公开之间的平衡、保护的前瞻性、严格的内控与管理都具有很好的启迪性。

^④ 王利明:《论个人信息权的法律保护》,载《现代法学》2013年第4期。

^⑤ 齐爱民:《大数据时代个人信息保护法国际比较研究》,法律出版社2015年版,第192页。

^⑥ 齐爱民:《界定法律意义上的信息》,载《社会科学家》2009年第3期。

^⑦ 李晓辉:《信息权研究》,知识产权出版社2006年,第118-119页。

^⑧ 郭雳等:《信用征信法律框架研究》,经济日报出版社2008年版,第64页。

在学理上,权利即限制,因为“每个社会秩序都面临着分配权利、限定权利范围、使一些权利与其他权利相协调的任务。”^④虽然信息权延展了隐私权的边界,但是其也并非一个无所不包的概念。“在个人信息日益受到重视的今天,一方面固然从国家立法、行业自律、多元化纠纷解决途径等诸方面予以规制,另一方面也要恰当地划定其界限,使其尽量不与在先的或之后的其他权利发生冲突。”^⑤互联网时代,在利益保护上,物化的信息已是一个非常棘手的法律问题。在信息保护与公开上,它牵涉到自由、安全、效率、秩序等多种法律价值。如果我们认可公共利益与秩序是法律的基础,那么国家安全与整体利益就必然优于信息保护;如果从市场效率原则出发,就必然会淡化对信息权的保护,而强调信息的公开与共享,毕竟“消费者数据的交换可以减少商人的调查成本,促进买家和卖家的供求平衡,从而增强市场的效率。”^⑥虽然时代的发展已将信息权提上了法律的日程,但是没有一种权利是绝对的,对该种利益的保护也必须在克减的基础上,与国家安全、市场效率等保持必要的平衡。

其二是还原第三方支付机构的金融属性。随着社会分工的日益复杂与社会连带关系的增强,金融监管专业化已是势在必行。然而,在目前的规范体系下,第三方支付机构仍被排除于金融机构的属类外。在数字金融的时代,财富日益被数据化与电子化,而这直接促使政府在金融监管中,日益强化与贯彻安全、秩序、稳定的价值倾向。同时,在学理研究中,对于名正言顺的金融机构治理,人们所形成的学术成果已是汗牛充栋。如对银行与客户的隐私保护义务,在长期的研讨中,人们已形成了较系统的学说,并对立法与司法产生了深远影响,如保护的信息范围应包括“有关账户的信息、有关客户交易的信息、银行因保管客户账户而获得的与客户有关的任何信息。”^⑦而且,这种保密义务并不因账户清结或停止使用而终止。在包括扫码支付在内的各类协议中,支付机构以霸王条款来架空用户的信息权就与其非金融属性的定位及学术探讨的相对不足存在一定的关联。因此,还原第三方支付机构的金融属性不仅是出于对事物“本真”的追求,而更是出于对处于弱势地位的消费者提供强有力的公权力保护。

其三是强化信息权保护的财产性、专业性与责任性。虽然在功能上,法律表现为指引、评价、预测、教育与强制,但是从社会秩序和谐的成本与效率评判,法律更多地在于张扬知有所禁而不犯的理念。虽然在隐私权保护上,我国已有所建树,但是其仍不能与大数据时代保持同步,如在保护模式上,仍然比较笼统、粗放,而没有紧跟时代的步伐而体现出专门化与分领域的特点。同时,在保护的时段上,也体现出强烈的“亡羊补牢”性,如其法律依据要么是最高人民法院“补丁”式的相关司法解释,要么就是仅提及隐私权的《侵权责任法》。此外,对隐私权的保护,也更多地侧重于事后性的精神损害赔偿等,而不具有事前性。

^④ [美]博登海默:《法理学——法律哲学与法律方法》,邓正来译,中国政法大学出版社1999年版,第298页。

^⑤ 李延舜:《个人信息权保护的法经济学分析及其限制》,载《法学论坛》2015年第3期。

^⑥ 张民安主编:《隐私权的比较研究》,中山大学出版社2013年版,第372页。

^⑦ 谈李荣:《银行与客户法律关系》,中国金融出版社2004年版,第50页。

大数据已开启了一个重大的时代转型,我们所在的社会也必将经历类似地壳式的运动,在改变人类基本的生活与思维方式的同时,大数据也必将推动人类信息管理范式的嬗变与重新定位。大数据背景下,我们的法律也应作以下几点改变:一是认识到信息的财产性,进而在法律上强化其财产性保护。“因社会经济活动的扩大,科技的发展,特定人格权已进入市场而商业化,具有一定经济利益的内涵,应肯定其具有财产权的性质。”^{⑤③}二是保护的法律专业性。在规律上,信息权保护应体现一个“一般法律保护→专门隐私权法律保护→信息权法律保护”的轨迹。作为大数据中的一环,扫码支付也对我国信息权保护的法律创制提出了大同小异的要求;三是强有力的责任机制。“惩罚之值在任何情况下,皆须不小于超过罪过收益之值。”^{⑤④}从民事、行政与刑事责任方面增加侵犯信息权的成本,特别是民事赔偿额度是立法优化的重点所在。

结 语

在世界的探求中,一种主流的认识是,我们越接近真理,人类就越自由、越幸福。然而,一个吊诡的现实是,狂飙突进的科学技术不仅使人类面临着自我毁灭的危险,而且更严重的是,代表真知的科学技术也改变了人类的言说方式。当技术性语言篡位占统治地位的时代,人面前的世界就不再是一个丰富多彩和灵性的世界,人类也不可能再沉醉于荷尔德林所言的“人充满劳绩,但还诗意地安居于这块大地之上”^{⑤⑤}的诗情画意中。在一个被高度技术化、标准化、规范化的世界中,一切都被机械地决定着。在造就这样的历史中,事实上,人类已身不由己地陷入了一个二律背反,即“人是生而自由,却无所不在枷锁之中。自以为是其他一切的主人,反比其他一切更是奴隶。”^{⑤⑥}大数据、云计算、扫码支付等似乎再次彰显人定胜天。“表面上看,当下的人类较以往任何时候都更富足和强大,但实际上,我们又可以说它比任何时候都更匮乏和孱弱。”^{⑤⑦}

很久以前,洛克曾言:法律的目的并不是要废除或限制自由,而是保护和扩大自由。现实是,在权力与权利的二元角力中,虽然我们赞成公共利益与私人利益、自由与控制之间的分界,但是当一项技术被开发出来而被应用到社会中时,出于公共秩序与公共利益的维护,我们又不得不请求政府出来维持公道。如此之循环就必定导致国家权力的不断跟进式扩张、私人权利的被蚕食与缩小。因此,新技术最大的难题不是扩大自由,而是限制与剥夺自由。在这些变迁中,许多是不可预测的。历史经验的启示是,技术创新造就社会新问题的速度远比解决旧问题的速度迅猛。虽然技术发展为法律的变革、政府权力的强大提供了正当性与现实性,但是技术也一步步地将法律带入一个无法轻

^{⑤③} 王泽鉴:《民法总则》,中国政法大学出版社2001年版,第134页。

^{⑤④} [英]边沁:《道德与立法原理研究》,时殷弘译,商务印书馆2000年版,第225-227页。

^{⑤⑤} [德]海德格尔:《人,诗意地安居》,郅元宝译,广西师范大学出版社2000年版,第73页。

^{⑤⑥} [法]卢梭:《社会契约论》,李平沅译,商务印书馆2011年版,第4页。

^{⑤⑦} [美]伯尔曼:《法律与宗教》,梁治平译,中国政法大学出版社2003年版,第9页。

易摆脱的死胡同中。大数据下的扫码支付只是证明人类成功与卓越的冰山一角,但是在这种法律的演变中,它使我们窥探到了整个法律的世界。在货币电子化、未授权交易、信息保护等提出挑战时,我们尽可以殚精竭虑地为之创制新的法律规则,但是其结果究竟是自由还是奴役?这是一个左右为难的人类问题。

Abstract: As the product of further development of human science and technology, the two-dimensional barcode payment greatly improves the efficiency of the circular capital and meets the needs of people's fast consumption. However, the other side of civilization often implies admonition, slavery and restriction. The payment of two-dimensional barcode has realized the combination of information flow and money flow. Compared with the traditional money legal system, control and assumption of transaction risk and protection of financial privacy, it produced revolutionary effect. Innovation is creative destruction under certain circumstances. In the context of the Internet, big data and cloud computing, it is the focus to innovate related systems caused by electronic currency, unauthorized transaction risk, information right from the payment of two-dimensional barcode. Meanwhile, nationwide financial literacy education is also an indispensable part of the comprehensive management of financial risks.

(责任编辑:王莉萍)