

# 数字人民币跨境支付中的 个人信息规制 ——以数字欧元为鉴\*

谢迪扬

**摘 要：**数字人民币跨境支付中的个人信息跨境流动，不同于“个人信息跨境提供”的一般情形，其特殊性在于提供者和境外接收方都是政府机构，需要多次境外传输以及境内外公私主体协同处理。上述特殊性我国现行个人信息规则体系存在不契合之处，导致个人信息保护与反洗钱监管的平衡困难、境外央行作为接收方的合规困境、境外次接收方的监管缺失以及多主体间责任划分混乱等问题。为应对这些挑战，我国可参考欧盟《关于建立数字欧元的提案》，对个人信息保护与反洗钱监管的平衡机制进行法制化升级，对境外央行合规机制进行“模块化”升级，对境外次接收方监管机制进行灵活性升级，对多主体责任划分机制进行体系化升级，并提出多边合作框架，以坚实的个人信息法治基础，助力数字人民币跨境应用的稳妥推进。

**关键词：**数字人民币；跨境支付；个人信息；跨境流动；数字欧元

**作者简介：**华东理工大学 法学院 讲师 上海 200237

**中图分类号：**D996.2

**文献标识码：**A

**文章编号：**1005—4871(2025)04—0088—22

---

\* 本文系国家社会科学基金青年项目“粮食安全视域下种业知识产权惠益分享机制研究”(项目编号：22CFX082)的阶段性研究成果。

## 一、问题的提出

数字人民币是中国人民银行发行的法定数字货币,其“跨境支付”指的是不同国家或地区之间,由跨境贸易、投资等因素引起的,需借助数字人民币与其他货币的合作安排来实现资金跨境转移的支付行为。<sup>①</sup> 数字人民币颇具发展潜力,截至2024年6月,其累计交易金额达7万亿元。<sup>②</sup> 数字人民币的跨境支付也日益频繁:双边层面,数字人民币系统已实现与香港“转数快”快速支付系统的互联互通(下文简称“转数快项目”)。<sup>③</sup> 多边层面,中国与泰国、阿联酋等共同建设的多边央行数字货币桥(multi-Central Bank Digital Currency Bridge,下文简称“mBridge”)已进入最小可行化产品阶段,完成对公汇款、信用证支付结算等多类真实交易。

数字人民币跨境支付语境下的个人信息是指,跨境支付过程中以电子或其他方式记录的、与已识别或可识别的自然人有关的各种信息。分析《中国数字人民币的研发进展白皮书》(下文简称《白皮书》)等公开资料可知,数字人民币跨境支付涉及手机号、身份信息、面部生物信息、金融账户等个人信息。其中,根据《个人信息保护法》(下文简称《个保法》)第28条,金融账户信息应属于敏感个人信息。对此,《个人金融信息保护技术规范》又依照敏感程度将金融账户信息分为三类(详见表1)。此外,根据《个保法》第4条,匿名化处理后的信息,如钱包昵称等,不属于个人信息。

表1 数字人民币跨境支付涉及的个人信息类目表

钱包等级	个人信息类别	具体项目	
四类钱包	通讯信息	手机号	
三类钱包新增	身份信息	姓名、性别、民族、出生日期、住址、身份证号	
一类、二类钱包新增	生物信息	人脸照片、视频	
	金融账户信息 (敏感个人信息)	C1类别	开户时间、开户行等金融机构内部信息
		C2类别	钱包ID、交易金额、交易流水等金融产品与服务信息
		C3类别	硬钱包磁道或芯片数据、交易密码等用户鉴别信息

注:在实践调研中,笔者使用“数字人民币APP”开立二、三、四类钱包,并在数字人民币运营机构现场开立一类钱包。

来源:资料由笔者整理公开信息与实践调研所得。公开信息详见中国人民银行数字货币研究所:《数字人民币APP使用指南》, <https://www.pbcdci.cn/userguide/index.html>, 访问日期:2025-08-09。

① 吕昊旻、赵雪情:《全球跨境支付特征、问题及前景》,载《人民币国际化观察》,2022年第5期,第1-13页,这里第2-3页。

② 穆长春:《稳妥推进数字人民币研发应用》,载《时事报告》,2024年第10期,第30-31页,这里第30页。

③ Hong Kong Monetary Authority, “Expanding the Cross-boundary E-CNY Pilot in Hong Kong”, 2024-05-17, <https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/05/20240517-3>, 访问日期:2025-06-13。

为防范洗钱等金融犯罪活动,数字人民币用户的个人信息将伴随支付指令一同跨境流动(详见图1)。在数字人民币跨境支付中妥善规制个人信息,是各国用户对数字人民币建立信任的基础,也是《中共中央关于进一步全面深化改革 推进中国式现代化的决定》提出的“稳妥推进数字人民币研发和应用”<sup>①</sup>的应有之义。

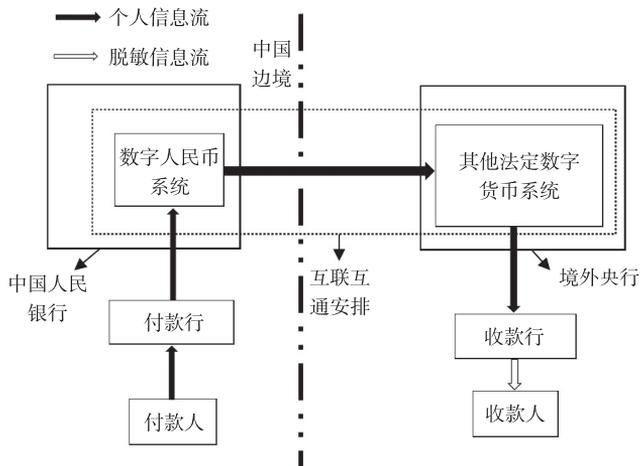


图1 数字人民币跨境支付中个人信息流动的典型路径图

来源:作者自制。

然而,在中国现行规则体系下,数字人民币跨境支付面临个人信息规制困境。虽然《数据安全法》《个保法》等法律规章可适用于数字人民币跨境支付场景,但现有规则预设了“处理者与境外接收方均为私人主体的单次跨境传输”情形,而数字人民币跨境支付与此存在显著差异:其一,处理者(中国人民银行)与境外接收方(境外央行)均具有公权力属性;其二,个人信息跨境后还须进行多次境外传输;其三,境内外公私主体需协同处理个人信息,各主体间的责任划分不清晰。正是上述三个特点导致了现有规则的规制困境。这不仅将削弱用户对数字人民币的信任,<sup>②</sup>还不利于实现反洗钱、反恐怖融资(下文简称“反洗钱”)等公共目标。可见,研究完善数字人民币跨境支付中的个人信息规制,在现阶段具有重大现实意义。

目前学界已对央行数字货币的个人信息问题进行了一定研究,认为其构成了

<sup>①</sup> 《中共中央关于进一步全面深化改革 推进中国式现代化的决定》,载《人民日报》,2024年7月22日,第1版。

<sup>②</sup> 笔者于2025年5月开展的问卷调查结果显示,对数字人民币跨境支付中的个人信息安全状况,持“不信任”或“不知道”态度的用户占47%,认为境外央行、境外商业银行和境内商业银行可能存在个人信息安全漏洞的用户,分别占53%、73%和63%。本次问卷调查采取便利抽样法,在“问卷星”平台对94名数字人民币用户线上发放问卷(共10题),回收有效问卷78份(回收率83%)。

央行数字货币研发和推广的重要挑战。<sup>①</sup> 原理上,部分学者指出央行数字货币的个人信息规则应强调衡量公私利益,<sup>②</sup>兼顾效率导向。<sup>③</sup> 主体上,部分学者认为应由专门机构(如中国人民银行等)专职履行个人信息保护义务。<sup>④</sup> 风险研判上,部分学者认为央行数字货币存在监管权滥用、个人信息保护义务薄弱等问题。<sup>⑤</sup> 匿名程度过低<sup>⑥</sup>或过高<sup>⑦</sup>都可能降低用户使用意愿,加强隐私政策宣传有助于提升用户信任。<sup>⑧</sup> 此外,技术局限被视为引发个人信息风险的重要原因。<sup>⑨</sup> 对此,有观点主张引入新兴隐私增强技术以消减风险;<sup>⑩</sup>另有观点主张将匿名性保持在较低水平,以打击洗钱并提升社会总体福利。<sup>⑪</sup> 然而,学界更多地关注央行数字货币在同一国家或地区境内支付的个人信息问题,对跨境支付场景下的同类问题缺乏系统研究。

2023年6月,欧盟发布《关于建立数字欧元的提案》(Proposal for a Regulation on the Establishment of the Digital Euro,下文简称《提案》),针对个人信息跨境流动提出了细致的规制方案。作为个人信息法治高地,欧盟的《提案》有望为相关实践提供有益启示。对此,本文首先揭示现有规则的规制困境;其次剖析数字欧元个人信息规制方案,并结合数字人民币发展现状,分析欧盟方案的可借鉴性;最后围

① Cheng-Yun Tsang/Yueh-Ping Yang/Ping-Kuei Chen, “Disciplining CBDCs: Achieving the Balance between Privacy Protection and Central Bank Independence”, *Northwestern Journal of International Law & Business*, Vol. 43, No. 3, 2023, pp. 235–289, here p. 235.

② 柯达:《基于公私利益衡量:论我国法定数字货币的个人信息保护》,载《南京社会科学》,2023年第5期,第80–93页,这里第80页。

③ 赵玲:《消费者个人金融信息权益的法律保护研究——基于数字人民币的视角》,载《金融论坛》,2022年第12期,第38–47页,这里第38页。

④ 李建星:《数字人民币安全保障论》,载《苏州大学学报(哲学社会科学版)》,2023年第5期,第116–127页,这里第116页。

⑤ 柯达:《数字人民币智能合约的风险规制》,载《山东大学学报(哲学社会科学版)》,2024年第2期,第180–192页,这里第186页。

⑥ Hiroshi Fujiki, “Central Bank Digital Currency, Crypto Assets, and Cash Demand: Evidence from Japan”, *Applied Economics*, Vol. 56, No. 19, 2024, pp. 2241–2259, here p. 2241.

⑦ Adekemi Omotubora, “Same Naira, More Possibilities! Assessing the Legal Status of the eNaira and Its Potential for Privacy and Inclusion”, *Journal of African Law*, Vol. 68, No. 2, 2024, pp. 245–262, here p. 245.

⑧ Frederic Tronnier/David Harborth/Patrick Biker, “Applying the Extended Attitude Formation Theory to Central Bank Digital Currencies”, *Electronic Markets*, Vol. 33, No. 1, 2023, pp. 1–21, here p. 13.

⑨ 岳平、杨晶晶:《风险与防控:数字人民币反洗钱功能的建构与展望》,载《上海大学学报(社会科学版)》,2023年第4期,第29–40页,这里第29页。

⑩ 王炜炫:《数字人民币发行和流通中的个人信息保护》,载《南方金融》,2023年第6期,第86–99页,这里第86页。

⑪ Zijian Wang, “Money Laundering and the Privacy Design of Central Bank Digital Currency”, *Review of Economic Dynamics*, Vol. 51, 2023, pp. 604–632, here p. 604.

绕前述困境,在借鉴欧盟经验的基础上提出完善个人信息规制的建议。

## 二、现有规则对数字人民币跨境支付场景的规制现状与困境

中国个人信息规则体系已初步建成,能对数字人民币跨境支付场景产生一定规制效果。然而,其与数字人民币跨境支付架构不契合的特点,造成了规制困境。本部分将从法律和规章两个层面入手,分析现有规则对数字人民币跨境支付场景的规制现状,并在此基础上指出具体的规制困境。

### (一) 现有规则在数字人民币跨境支付场景下的规制现状

根据数字人民币跨境支付架构,商业银行收集的个人信息须汇总至央行,由央行发起对其他央行的跨境传输。因此,中国人民银行构成个人信息跨境提供方(即处理者),境外央行构成境外接收方,境外商业银行构成“出境数据再转移”<sup>①</sup>的接收组织(下文简称“次接收方”)。依照不同效力层级,可将现有规则分为以下两类。

#### 1. 法律层面:《网络安全法》《数据安全法》与《个保法》的协同规制

《网络安全法》《数据安全法》与《个保法》均可适用于数字人民币跨境支付场景。三者对个人信息的规制视角不同,但具体要求有所重合,综合来看主要有以下三项。一是安全评估。中国人民银行属于《个保法》中的“国家机关”,向境外提供个人信息前应进行安全评估。此外,“数字货币发行库”和“数字货币商业银行库”(详见图2)均属于《网络安全法》中的“关键信息基础设施”,中国人民银行只有通过国家网信部门的安全评估后,才能向境外提供个人信息。二是单独同意。一方面,基于跨境提供个人信息的高风险性,《个保法》要求个人信息处理者告知用户境

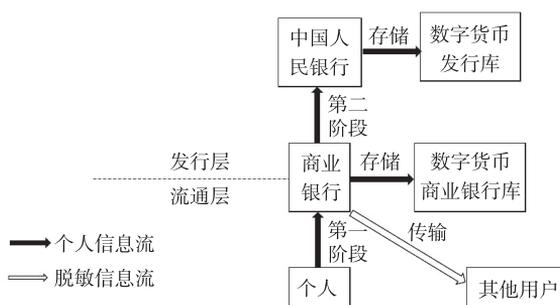


图2 数字人民币双层运营体系中的个人信息流动路径

来源:作者自制。

<sup>①</sup> 国家互联网信息办公室:《数据出境安全评估办法》,第9条,2022-07-07, [https://www.gov.cn/jzhengce/zhengceku/2022-07/08/content\\_5699851.htm](https://www.gov.cn/jzhengce/zhengceku/2022-07/08/content_5699851.htm), 访问日期:2025-08-09。

外金融机构的基本信息与维权方式,并取得用户的单独同意。另一方面,数字人民币跨境支付涉及金融账户等敏感个人信息,《个保法》要求处理敏感个人信息前应取得个人的单独同意。三是境内外保护标准持平。《个保法》要求中国人民银行(处理者)采取必要措施,确保境外合作机构的个人信息保护标准与中国大陆持平。

## 2. 规章层面:围绕安全评估、应急措施、监督管理的细化规定

《网络数据安全条例》(下文简称《数据条例》)也可适用于数字人民币跨境支付场景。其采纳分级管理机制,要求处理1000万人以上个人信息的处理者遵守有关“重要数据”的规定。据中国人民银行数字货币研究所(下文简称“数研所”)统计,数字人民币个人钱包已累计开立1.8亿个。<sup>①</sup>可见,中国人民银行处理的个人信息数量远超上述标准,无法适用《数据条例》第35条对安全评估的简化规定,只有通过国家网信部门组织的评估后,才能向境外提供。

此外,网信、金融部门也发布了可适用于数字人民币跨境支付场景的部门规章。其一,《促进和规范数据跨境流动规定》提出了更细致的个人信息保护要求,如进行个人信息保护影响评估、采取技术措施和补救措施、及时报告安全事件等。其二,《数据出境安全评估办法》(下文简称《评估办法》)细化规定了安全评估的重点事项,包括数据出境的目的、范围、方式是否合法、正当、必要,接收方网络安全情况是否与中国大陆持平,出境后的风险是否可控,处理者是否与接收方约定了安保义务等。其三,《个人金融信息保护技术规范》要求与境外机构签订协议,通过现场核查等方式监督数据保密、数据删除、案件协查等职责义务的履行情况。其四,出于反洗钱监管需要,《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》要求向境外完整传递发起人和受益人的姓名、账号、住所等个人信息,还规定了个人信息的保存期限和方式。

### (二) 规制困境:结合典型案例与实践访谈的分析

数字人民币跨境支付架构具有特殊性,与现行个人信息规则体系并不契合。本部分将结合典型案例与实践访谈,揭示现有规则的规制困境。

#### 1. 个人信息保护与反洗钱监管的平衡问题

数字人民币跨境支付既要求保护个人信息,又要求开展反洗钱监管,但现行规则难以平衡这两个要求。首先,反洗钱金融行动特别工作组(Financial Action Task Force on Money Laundering,下文简称“FATF”)制定的“旅行规则”可能与《个保法》的“最小必要原则”产生冲突。“旅行规则”要求数字人民币跨境支付附带全面且准确的发起人与受益人信息,包括姓名、账号、住址、出生日期等,同时建议

<sup>①</sup> 穆长春:《稳妥推进数字人民币研发应用》,第30页。

各国确定“简易规则”的实施限额,允许在小于限额时仅传输姓名和账号。<sup>①</sup>但“旅行规则”在各国国内法下的转化不一致,如何协调各国法律和标准已构成一大实务难点。<sup>②</sup>例如,“简易规则”实施限额不统一,在未达中国限额(即四类钱包限额)但已超他国限额时,是否应全面传输个人信息,目前尚无定论。若按他国要求全面传输,则可能违背“最小必要原则”。其次,中国人民银行同时具有个人信息处理者和反洗钱监管者的双重身份,可能造成监管中立性缺陷。例如,在转数快项目中,香港快速支付系统与数字人民币系统的对接端口均为“央行端”;<sup>③</sup>在 mBridge 项目中,各方均以“央行端”作为个人信息的出境枢纽。<sup>④</sup>这表明,在实践中向境外提供个人信息的主体是中国人民银行,其身份符合《个保法》中所界定的“处理者”。同时,中国人民银行还承担对其他处理者的监管职责。这种“既当裁判又当运动员”的角色定位,不利于保障监管中立性,也难以在个人信息保护与反洗钱监管之间实现有效平衡。

## 2. 境外央行作为接收方的合规困境

现有规则对处理者提出了有关境外接收方的合规义务,要求其“采取必要措施”保障接收方以不低于中国大陆的标准保护出境个人信息,并对接收方实施监管。但境外央行属于政府机构,其作为个人信息接收方时,处理者可能面临合规困境。因为根据主权平等原则,主权国家有权自主决定本国的货币政策,包括法定数字货币跨境流通中的个人信息保护标准不受其他任何国家、组织或个人的干涉。<sup>⑤</sup>同时,《中华人民共和国香港特别行政区基本法》以及一系列金融法例赋予了香港在金融领域的高度自主权和独立性,香港金融管理局具有独立于中国人民银行的法律地位,可自主决定货币金融政策。由此可见,在维护主权平等、香港金融自主性及促进对外友好交往的大前提下,保障境外接收方的个人信息处理活动符合中国大陆的相关标准,这一目标难以仅依靠中国人民银行“采取必要措施”来实现,更难以对境外接收方实施监管。还有专家指出,考虑到发展中国家的网络安全风险,

<sup>①</sup> Financial Action Task Force, “The FATF Recommendations”, 2025-06-18, <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf>. coredownload.inline.pdf, 访问日期:2025-08-10。

<sup>②</sup> 根据笔者2025年5月对中国建设银行浙江省分行杭州吴山支行公司部职员、中国银行绍兴市分行运行管理部职员的访谈。

<sup>③</sup> 勾明扬:《数字人民币试点再进一步》,载《经济日报》,2024年5月31日,第7版。

<sup>④</sup> BIS, “Project mBridge Reached Minimum Viable Product Stage”, 2024-11-11, [https://www.bis.org/about/bisih/topics/cbdc/mcbdc\\_bridge.htm](https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm), 访问日期:2025-06-13。

<sup>⑤</sup> [英]伊恩·布朗利(Ian Brownlie):《国际公法原理》,曾令良、余敏友等译,北京:法律出版社,2002年版,第319页。

应对其开展必要的技术援助,这也难以由中国人民银行独自完成。<sup>①</sup>因此,现有规则对处理者设置的有关境外接收方的合规要求,并不契合数字人民币跨境支付实践,且将对中国人民银行造成合规困境。

### 3. 境外次接收方的监管缺失

个人信息伴随数字人民币支付指令出境后,还将经历多次境外传输。例如,在mBridge项目中,收款方央行收到支付指令后,将支付指令转送其境内的收款方商业银行,此时转送的信息也包含个人信息,<sup>②</sup>构成了个人信息的境外“再转移”<sup>③</sup>。转数快项目也存在类似情况,只不过数字人民币系统与香港转数快支付系统对接的“总端口”(类似“央行端”)由香港银行同业结算有限公司运营,因此该公司需要将接收到的个人信息再次转送至香港零售银行,这也构成个人信息的境外“再转移”。然而,现有规则缺乏对此类境外“再转移”以及境外次接收方义务的规定。只有《评估办法》第9条要求数据处理者与境外接收方订立法律文件,并涵盖“对于境外接收方将出境数据再转移给其他组织、个人的约束性要求”。<sup>④</sup>银行界实务人士指出,现有规则在技术标准、合作门槛、安全审计、央行间的联合审查等方面,都缺乏细化规定,导致实操性欠佳。<sup>⑤</sup>可见,现有规则对境外次接收方存在监管上的缺失。

### 4. 多主体间的责任划分混乱

当存在多个处理者时,《个保法》设置了详细的责任划分规定,但这并不契合数字人民币跨境支付架构,从而导致多主体间责任划分混乱。

一方面,要求中国人民银行与境外央行承担连带责任缺乏合理性。《个保法》将“两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式”的情形,认定为个人信息的共同处理。造成损害时,由所有共同处理者承担连带责任。<sup>⑥</sup>在实践中,中国人民银行与境外央行一般以签署国际协议的方式共同决定个人信息处理的相关事项,如何通过条款设计合理分配责任,是实务中的难点问题。<sup>⑦</sup>按照《个保法》的上述规定,mBridge项目中的中国人民银行、泰国银行、阿联

<sup>①</sup> 根据笔者2025年5月对中国人民银行技术专家的访谈。

<sup>②</sup> BIS, “Project mBridge: Experimenting with a Multi-CBDC Platform for Cross-border Payments”, [https://www.bis.org/innovation\\_hub/projects/mbridge\\_brochure\\_2311.pdf](https://www.bis.org/innovation_hub/projects/mbridge_brochure_2311.pdf), 访问日期:2025-06-13。

<sup>③</sup> “再转移”的提法出自《数据安全评估办法》第9条,参见国家互联网信息办公室:《数据出境安全评估办法》,第9条。

<sup>④</sup> 国家互联网信息办公室:《数据出境安全评估办法》,第9条。

<sup>⑤</sup> 根据笔者2025年5月对中国工商银行深圳市分行运行管理部经理的访谈。

<sup>⑥</sup> 《中华人民共和国个人信息保护法》,第20条,中国人大网,2021-08-20, [http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820\\_313088.html](http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html), 访问日期:2025-08-09。

<sup>⑦</sup> 根据笔者2025年5月对中国工商银行深圳市分行个人金融部副总经理的访谈。

酋中央银行、沙特阿拉伯中央银行与香港金融管理局五方主体,以及转数快项目中的中国人民银行与香港银行同业结算有限公司两方主体,将分别构成共同处理,须承担连带责任。但是,《个保法》属于中国国内法,无法直接将连带责任赋予外国(或地区)的政府机构。而且从法理上看,连带责任源自共同侵权。至于何为“共同”,主观说认为各加害人之间须有意思联络以及行为分担,客观说则认为须数人行为在客观上发生同一结果。<sup>①</sup>然而,当仅存在境外央行的不当处理行为时,中国人民银行与其既无意思联络,也未参与侵害行为,因此并不构成共同侵权。即便认定中国人民银行存在监管上的过失,其也仅应承担过失范围内的责任,况且其对境外央行不具监管权。由此可见,要求中国人民银行与境外央行承担连带责任缺乏合理性。

另一方面,央行与商业银行之间的责任划分模糊。由于商业银行不能独立于央行擅自决定与数字人民币相关的个人信息处理目的和方式,因此根据《个保法》,商业银行与央行并非两个完全独立的处理者。那么二者构成《个保法》第20条规定的共同处理,还是第21条的委托处理,目前难以判断。尽管大型商业银行也参与数字人民币研发,由此可能导致其与中国人民银行构成共同处理并承担连带责任,但需要指出的是,《白皮书》中“共同探索”的表述不等同于《个保法》中的“共同决定”,而且新近开通或未来将开通数字人民币服务的商业银行,并未参与决定个人信息的处理目的与方式,因此二者也可能构成委托处理。对此,学界存在两种观点:一种观点主张中国人民银行承担委托人替代责任,即作为受托人的商业银行不对个人直接负责。<sup>②</sup>还有一种观点认为中国人民银行仅须承担定作人责任,即原则上由商业银行承担责任,中国人民银行只有在定作、指示、选任行为存在过错时,才承担相应的责任。<sup>③</sup>银行界实务人士则认为,按“谁泄露、谁承担”或“谁运行、谁负责”的原则划分责任更加合理。<sup>④</sup>可见,现有规则下央行与商业银行的责任划分存在争议。

### 三、数字欧元跨境支付中的个人信息规制方案及其可借鉴性

虽然欧盟对央行数字货币的态度相对谨慎,但自2019年欧洲中央银行

<sup>①</sup> 王泽鉴:《侵权行为》,北京:北京大学出版社,2009年版,第352页。

<sup>②</sup> 阮神裕:《个人信息委托处理中受托人的地位、义务与责任》,载《当代法学》,2022年第5期,第110-119页,这里第117页。

<sup>③</sup> 程啸:《论〈民法典〉与〈个人信息保护法〉的关系》,载《法律科学(西北政法大学学报)》,2022年第3期,第19-30页,这里第26页。

<sup>④</sup> 根据笔者2025年5月对交通银行浙江省分行国际部总经理、中国工商银行浙江省分行运行管理部副总经理的访谈。

(European Central Bank, 下文简称“ECB”)宣布成立央行数字货币工作组以来,数字欧元项目进入稳步推进阶段。在此期间,个人信息安全问题被视为建立数字欧元的重大法律挑战,<sup>①</sup>得到欧盟的重点关注。2023年,欧盟发布的《提案》包含细致的个人信息规制方案,涵盖数字欧元跨越欧盟成员国边界的支付交易,以及跨越欧盟边境、与非欧盟国家主体进行的支付交易,能够为中国提供有益的参考。

### (一) 数字欧元跨境支付中的个人信息规制方案

中国当前面临的规制困境,本质上源于央行数字货币跨境支付架构所具有的特殊性,数字欧元跨境支付架构也具有类似特征。《提案》是针对数字欧元跨境支付场景专门制定的,因而其涵盖了上述困境的解决方案。

#### 1. 个人信息保护与反洗钱监管的平衡机制

为平衡个人信息保护与反洗钱监管的双重目标,《提案》一方面要求签署国际协议,令其他合作方承诺对标欧盟规则来转化 FATF“旅行规则”,采纳欧盟的“简易规则”实施限额,实现个人信息传输范围的协调。另一方面,为防止 ECB 与欧盟各成员国央行(the national central banks, 下文简称“NCBs”)出现处理者与监管者身份重合的情况,《提案》设置了个人信息有限访问机制,规定 ECB 与 NCBs 只能访问为实现系统监控和货币政策分析所必要的脱敏聚合数据,不能访问个人信息与具体的交易数据。《提案》要求商业银行采取假名化(pseudonymisation)、散列化(hashing)和加密化(encryption)等技术手段,仅将用户的脱敏信息传输给货币主管机关,确保后者无法识别特定个人用户。<sup>②</sup>此外,《提案》还授权 ECB 制定有关数字欧元的运营管理标准,依照《关于内部市场支付服务的指令》明确 ECB 和 NCBs 的监管主体地位。<sup>③</sup>这说明《提案》选择剥离货币主管机关的个人信息处理者<sup>④</sup>身份,强化监管者身份,以保障监管中立性。

#### 2. 境外央行作为接收方的合规机制

为确保境外央行的个人信息保护水平与欧盟一致,欧盟并未直接要求 ECB“采取必要措施”,或履行对境外央行的“监管义务”,而是提出了国际协议的制定与签署义务,间接保障境内外个人信息保护标准的统一。具言之,《提案》要求欧盟与合

<sup>①</sup> Sime Jozipovic/Marko Perkusic/Nina Mladinic, “A Comparative Review of the Legal Status of National Cryptocurrencies and CBDCs: A Legal Tender or Just Another Means of Payment”, *Pravni Vjesnik*, Vol. 40, No. 1, 2024, pp. 77–96, here pp. 77–78.

<sup>②</sup> European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro”, article 34, 2023–06–28, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369>, 访问日期:2025–08–10。

<sup>③</sup> 同上, article 6。

<sup>④</sup> 在 GDPR 体系下应称为“控制者”(controller)。

作方签署的国际协议涵盖以下内容。<sup>①</sup> 其一,各方央行将完全遵守 ECB 发布的规则、指导方针、指示与要求,并在 ECB 需要时向其提供关于该国使用数字欧元的所有信息(包括个人信息)。其二,除欧盟外的其他缔约方还应制定或修改国内法,使其完全符合欧盟法规定的个人信息保护要求,包括《通用数据保护条例》(General Data Protection Regulation,下文简称“GDPR”)等。其三,缔约方应保证央行受国内法监管,监管标准也须与欧盟水平保持一致。其四,国际协议须涵盖必要的执行措施和程序,以及协议面临限制、暂停或终止时的应对方案。因为根据欧盟《反洗钱条例(草案)》(COM/2021/420),欧盟可能认定缔约方的反洗钱制度存在重大缺陷或合规弱点(compliance weaknesses),此时国际协议应被限制、暂停或终止实施。<sup>②</sup> 因此,国际协议还应纳入相应的限制、暂停或终止使用数字欧元的程序规则。

### 3. 境外次接收方的监管机制

与数字人民币跨境支付架构类似,数字欧元交易指令附带的个人信息进入非欧盟国家后,也将经历多次境外传输,即从境外央行传输至境外商业银行等数字欧元的支付服务提供者。对这类境外次接收方,《提案》采纳的监管机制同样建立在国际协议的基础上。具言之,《提案》要求其他缔约方在国际协议中承诺依照欧盟标准修改国内法,约束其境内所有支付服务提供者,这种约束应与欧盟境内的支付服务提供者受到的约束一致。<sup>③</sup>

### 4. 围绕处理目的的多主体责任划分机制

在数字欧元跨境支付中的责任划分问题上,《提案》主要涉及两类主体:一是支付服务提供者,包括各类商业银行、电子支付机构等。二是货币主管机关,即 ECB 和 NCBs。《提案》根据个人信息处理目的,逐一罗列了上述二者构成“个人信息控制者”的活动类型。换言之,在同一交易中,二者先后或同时处理同一个人信息的行为,并未构成“共同处理”,仅对各自作为控制者的处理活动负责。具体而言,支付服务提供者作为控制者的处理活动包括支付限额控制、存取款登记、数字欧元分发、依法惩处特定用户、配合调查或阻止用户的违法犯罪行为。<sup>④</sup> 货币主管机关被

<sup>①</sup> European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro”, article 19.

<sup>②</sup> 欧盟《提案》第 19 条参照欧盟《反洗钱条例(草案)》(COM/2021/420)规定。参见 European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing”, article 14, 2021-07-20, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420>, 访问日期:2025-08-10。

<sup>③</sup> 同注<sup>①</sup>。

<sup>④</sup> 同上, article 34。

认定为控制者的情形则包括提供数字欧元结算基础设施的访问权限、辅助支付服务提供者之间的信息交换、在线交易结算、基础设施安全维护、账号是否重复申请的查询、特定账号的支付服务提供者变更等。<sup>①</sup>《提案》还特别规定，当 ECB 与 NCBs 在上述目的下共同处理个人信息时，将被视为共同控制者。<sup>②</sup> 由于参与数字欧元跨境支付的非欧盟国家将受到相应的国际协议约束，因此其也须遵守《提案》规定，<sup>③</sup>这意味着境外央行将被欧盟监管主体视同 NCBs，可能与 ECB 一道被认定为共同控制者。同时，境外央行可与 ECB 以书面形式自主确定责任的内部划分方案。

## （二）欧盟方案的可借鉴性分析

尽管《提案》对数字欧元跨境支付场景下的个人信息规制具有较强针对性，但其仍存在缺陷，不能完全契合数字人民币跨境支付的现实环境。因此，深入探讨《提案》的可借鉴性是十分必要的。

### 1. 个人信息保护与反洗钱监管的平衡机制：技术滞后的隐患

《提案》主要通过签署国际协议、限缩央行个人信息访问权的方式，促进个人信息保护与反洗钱监管的平衡。《提案》将欧盟标准强制植入国际协议的做法将带来一些弊端，下文将对此详述，本部分主要分析央行个人信息有限访问机制。欧盟借助个人信息隔离技术，禁止央行处理未脱敏的个人信息，以此保障 ECB 与 NCBs 的监管中立性。这能够凸显数字欧元在隐私保护上的优势，是《提案》的长处所在。<sup>④</sup> 而在数字人民币架构中，中国人民银行与境外央行均可获取具体的个人信息。为分析欧盟有限访问机制的可借鉴性，首先须权衡央行获取个人信息的利弊，再研判对央行隔离个人信息的可行性。

有观点指出，应允许中国人民银行获取数字人民币交易的全过程数据（包括个人信息），因为这不但有助于精准调节货币政策，<sup>⑤</sup>还能高效反洗钱。但对于前者，中国人民银行在调节货币政策过程中所需的信息，实质上与具体的个人信息关联较弱，其使用脱敏信息通常也能实现较为理想的数据分析和决策效果。对于后者，反洗钱目标的实现并不意味着中国人民银行须实时掌握所有个人信息。

<sup>①</sup> European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro”, article 35.

<sup>②</sup> 同上，article 35(5)。

<sup>③</sup> 同上，article 19。

<sup>④</sup> Sime Jozipovic/Marko Perkusic/Stjepan Gadzo, “Tax Compliance in the Era of Cryptocurrencies and CBDCs: The End of the Right to Privacy or No Reason for Concern?”, *EC Tax Review*, Vol. 31, No. 1, 2022, pp. 16–29, here pp. 16–17.

<sup>⑤</sup> 李瀚琰：《数字人民币试点中的个人信息法律监管》，载《财经理论与实践》，2024年第1期，第152–160页，这里第155页。

例如,欧盟方案就是在启动反洗钱调查后,由 ECB 等执法部门要求掌握个人信息的商业银行限时提供。可见,设置央行个人信息隔离机制,与反洗钱的目标也不矛盾。此外,由于数字人民币跨境支付应遵循主权平等原则与对等原则,<sup>①</sup>如果境外央行同意中国人民银行收集个人信息,那么境内个人信息也应被传输至境外央行。当前 mBridge 采用的正是上述方案,即个人信息可由交易所涉央行获取,这带来了境内外多重安全风险。综上,个人信息向央行完全开放的制度设计弊大于利。

那么,对央行隔离个人信息的做法,在中国的技术条件和法律环境下是否可行?诚然,隔离个人信息的技术手段存在滞后性。<sup>②</sup> ECB 在 2024 年《数字欧元准备阶段的第一份进展报告》中坦言,其仍在专家支持下探索隔离个人信息的技术方案,<sup>③</sup>并致力于使用最新的隐私增强技术,继续评估可能、可行和有效的新措施。<sup>④</sup>可见现有加密技术并非无懈可击,需要及时更新迭代以巩固安保能力。对此中国可采取法制化途径,细化央行义务,防范技术滞后的隐患,这在中国现有的技术条件和法律环境下较为可行。一方面,我国可在法律上明确央行对个人信息的“有条件处理”,即规定一般情形下仅处理脱敏信息,只有在特定情形下(如启动反洗钱调查时),才能对脱敏信息进行还原操作。另一方面,我国还应赋予央行持续研发、应用最新加密技术的法定义务。

## 2. 境外央行合规机制:协议模板的弊端

《提案》设置了国际协议的签署义务,形成了对境外央行个人信息处理行为的约束。这较为充分地维护了国家主权平等原则,有效化解了处理者对境外央行的合规难题。此外,中国《个保法》已纳入与国际协议相衔接的规定,在认定向境外提供个人信息的条件时,国际协议具有适用上的优先性。可见,欧盟这种围绕国际协议展开的规制路径,与中国的法律环境具有一定兼容性。如果中国法律也明确规定相关国际协议应涵盖境外接收方的个人信息保护义务,并发展出契合数字人民币的国际协议模板,那么将有助于实现多法域间个人信息保护标准的衔接与稳定。

虽然模板化的思路值得借鉴,但照搬欧盟的国际协议模板并不明智。其原

<sup>①</sup> 贾济东、胡扬:《论我国反洗钱法域外适用的困境与出路》,载《华中科技大学学报(社会科学版)》,2021年第2期,第116-126页,这里第122页。

<sup>②</sup> 何培育、王潇睿、林颖:《论大数据时代个人信息盗窃的技术手段与应对机制》,载《科技管理研究》,2018年第7期,第195-199页,这里第195页。

<sup>③</sup> ECB, “First Progress Report on the Digital Euro Preparation Phase”, [https://www.ecb.europa.eu/euro/digital\\_euro/progress/html/ecb.deprp202406.en.html#toc2](https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202406.en.html#toc2), 访问日期:2025-06-13。

<sup>④</sup> ECB, “Digital Euro and Privacy”, [https://www.ecb.europa.eu/euro/digital\\_euro/features/privacy/html/index.en.html](https://www.ecb.europa.eu/euro/digital_euro/features/privacy/html/index.en.html), 访问日期:2025-06-13。

因在于，一方面，《提案》凸显了欧盟的核心地位，<sup>①</sup>几乎没有为非欧盟国家设置灵活变通的制度空间，相当于提出了一份“格式合同”。这种对其他国家差异化国情的忽视可能会增大国际协议的签署难度。而“稳慎扎实推进人民币国际化”是中国在金融领域的重要发展目标。作为人民币的数字化表现形式，数字人民币的国际化能够为中国经济的高质量发展、扩大金融高水平开放提供重要保障。<sup>②</sup>可见，中国在制定相关国际协议时，应从合作对方的视角考虑协议的可接受性。

另一方面，《提案》规定非欧盟国家须对标欧盟规则，实施与欧盟水平一致的个人信息保护标准，这同时也对合作对象的技术能力提出了较高要求，而目前许多发展中国家难以达到。因此，这种制度设计可能导致技术水平较低的国家长期无法融入数字欧元经济圈，加速了数字鸿沟问题向贫富分化问题的转化。<sup>③</sup>而数字人民币是赋能共建数字“一带一路”的重要金融工具。中国提出“一带一路”倡议，崇尚的是互利共赢，其旨在打造共同发展合作的平台、实现“世界版共同富裕”，让广大发展中国家不再是全球化浪潮下“被遗忘的角落”。因此，数字人民币跨境支付的合作对象不能仅限于经济实力较强、科技水平较高的国家和地区。当前，尼泊尔、菲律宾、印度尼西亚等“一带一路”沿线的发展中国家已成为 mBridge 的观察员，这也预示着数字人民币的合作网络将进一步向不发达地区拓展。因此，有必要在模板化的国际协议中增设配套制度，如技术援助、信息交换、过渡期等，在安全的基础上增强协议的灵活性，以便更契合对方的经济社会发展水平，助力实现“一带一路”倡议的共同发展愿景。

### 3. 境外次接收方的监管机制：严格对接欧盟标准的问题

中国现有规则借助处理者与境外接收方的协议，间接实现对境外次接收方的监管。与此不同的是，欧盟方案设置国际协议的签署义务，要求其他缔约方承诺依照欧盟标准修改国内法，从而依托国内法直接实现对该国境内所有次接收方的监管。这种方案具有以下优势：第一，境外次接收方所受监管的约束力更强，因为这种约束源于缔约方的国内法，而非私法属性的跨境传输协议。第二，欧盟方案能够实现缔约方国内法对境外次接收方的直接约束，而中国现有规则只能通过境外接收方对次接收方施加间接约束，效果不如前者。此外，中国签署

<sup>①</sup> Iulia Monica Oehler-Sincai, “The Digital Euro Project: A Preliminary Assessment”, *Romanian Journal of European Affairs*, Vol. 22, No. 1, 2022, pp. 50-68, here pp. 50-51.

<sup>②</sup> 周光友：《数字人民币国际化的机制与实施策略》，载《人民论坛》，2023年第22期，第32-35页，这里第32页。

<sup>③</sup> 杜振华：《构建和谐和谐社会必须解决数字鸿沟问题》，载《毛泽东邓小平理论研究》，2007年第6期，第46-49+83-84页，这里第46页。

的部分国际协议已要求缔约方承诺其国内法对个人信息提供一定程度的保护。虽然此类条款还较为笼统,但表明欧盟方案对中国法律环境具有一定契合性。例如,《区域全面经济伙伴关系协定》第12章第8条要求缔约方公布其保护电子商务用户之个人信息的法律,包括个人应如何寻求救济、企业应遵守何种要求等。<sup>①</sup>《中国-柬埔寨自由贸易协定》第10章第6条也要求缔约方“采取或维持国内法律和其他措施,以确保电子商务用户个人信息得到保护”。<sup>②</sup>但与上述境外央行合规机制类似,欧盟对境外次接收方的监管机制也存在欧盟中心主义的弊病,其要求对方完全对接欧盟标准的强硬态度,可能阻碍欧盟与其他国家和地区开展合作。

#### 4. 围绕处理目的的多主体责任划分机制:立法方式的缺陷

欧盟在处理目的相关责任划分机制方面,主要遵循责任法定主义,这种规制路径具备与中国法律环境相兼容的可能性。例如,《民法典》中“责任主体的特殊规定”也采取了法定主义的规制路径。其规定了在网络用户致人损害、第三人在经营场所内致人损害等特殊情形下,侵权责任在多主体间的法定分配方案。因此可借鉴《提案》,将数字人民币的个人信息安全事故视为一种特殊侵权情形,并根据不同主体的处理目的,在中国人民银行、境外央行、境内外商业银行等主体间,规定具体的责任分配方案。同时,欧盟方案也允许共同责任人自主决定内部责任的划分。在数字人民币跨境支付场景下,为尊重各方金融主权,也可借鉴这种意定主义的思路。一方面,中国人民银行与境外央行之间的责任分配,可在双方签署的国际协议中规定。另一方面,境外央行、商业银行等境外主体间的责任分配,则应满足透明度要求,相关国际协议可规定各缔约方应公布的法律内容、方式和时限。<sup>③</sup>

然而,欧盟《提案》穷尽罗列处理目的的立法方式有待商榷。从立法理论上,罗列处理目的的条款应属于“例示规定”。在科学立法的要求下,例示规定应在抽象程度上实现具体与概括的统一,以起到补救立法缺陷的作用。<sup>④</sup>特别是在立法者无法预知所有拟规范事项时,<sup>⑤</sup>例示规定内部同时包含典型事例与上位概念,能

<sup>①</sup> 《区域全面经济伙伴关系协定》,第12章第8条,中国自由贸易区服务网,2020-11-15, [https://fta.mofcom.gov.cn/rcep/rceppdf/d12z\\_cn.pdf](https://fta.mofcom.gov.cn/rcep/rceppdf/d12z_cn.pdf), 访问日期:2025-08-10。

<sup>②</sup> 《中华人民共和国政府和柬埔寨王国政府自由贸易协定》,第10章第6条,中国自由贸易区服务网,2020-10-12, [https://fta.mofcom.gov.cn/cambodia/xieyi/xieyizw\\_cn.pdf](https://fta.mofcom.gov.cn/cambodia/xieyi/xieyizw_cn.pdf), 访问日期:2025-08-10。

<sup>③</sup> 马忠法、王悦玥:《论经贸条约中知识产权透明度规则的扩张及中国应对》,载《知识产权》,2022年第12期,第66-86页,这里第66页。

<sup>④</sup> 刘风景:《例示规定的法理与创制》,载《中国社会科学》,2009年第4期,第93-105+206-207页,这里第93-94页。

<sup>⑤</sup> 屈茂辉:《类推适用的私法价值与司法运用》,载《法学研究》,2005年第1期,第3-19页,这里第7页。

够兼顾条款的周严性和可操作性,较为契合数字人民币这类新兴议题。因此,有必要在罗列处理目的的条款中,根据央行和商业银行处理活动的特点,增设上位规定,以更好地适应数字人民币跨境支付的未来发展变化。

#### 四、数字人民币跨境支付中个人信息规制的完善:欧盟方案的本土化升级

上文已阐述了数字欧元跨境支付中的个人信息规制方案,并对其可借鉴性展开了批判性分析。本部分则将结合数字人民币跨境支付之现实,提出升级欧盟方案的具体建议。

##### (一) 个人信息保护与反洗钱监管之平衡机制的法制化升级

为实现平衡个人信息保护与反洗钱监管的双重目标,《提案》一方面要求签署国际协议,统一 FATF“旅行规则”在各方法律中的转化与适用,但其对标欧盟规则的强制要求存在弊端;另一方面,《提案》设置央行个人信息有限访问机制,旨在保障央行的监管中立性,但该机制存在技术滞后的隐患。本文建议升级该平衡机制的法制化水平,以缓解负面影响。

##### 1. 合作各方规则的灵活衔接

FATF“旅行规则”允许各国在其提出的最低标准之上,自行制定反洗钱规则,这导致各国标准衔接不畅。例如,当境外标准严于中国时,如果按境外标准传输个人信息,就可能与“最小必要原则”产生冲突。此时不宜参照《提案》,要求其他合作方对标中国规则修改国内法。本文建议参考 mBridge 的反洗钱机制,以促进各方规则的灵活衔接。mBridge 允许交易各方实施本土反洗钱规则,在商业银行完成反洗钱审查后,mBridge 平台将对该交易进行加密标记,相当于授予一项合规认证证书。当对方反洗钱规则较严时,平台可在上述标记中运用“零知识证明”(zero-knowledge proof)、动态加密等技术手段。这种做法可在不泄露更多信息的前提下,满足对方的认证需要,有助于达致个人信息保护与反洗钱监管的平衡。<sup>①</sup>我国可在适当的时机将上述技术方案转化为国际协议中的条款,以增强反洗钱合作的灵活性。

##### 2. 有限访问之技术效果的法律确认

个人信息有限访问机制可在平时限制央行访问个人信息,仅允许其查阅脱敏信息;特殊状态下可授权央行还原脱敏信息,实现反洗钱等法定目的。在法律上确认这种有限访问的技术效果,有助于我国在技术能力尚不完善的阶段,制裁干扰或颠覆上述技术效果的行为人。对此,我国可制定以下规则:一是规定商业银行的个

<sup>①</sup> BIS, “Project mBridge: Connecting Economies through CBDC”, <https://www.bis.org/publ/othp59.pdf>, 访问日期:2025-06-13。

人信息脱敏义务。我国应要求商业银行以至少达到行业一般水平的加密技术对个人信息完成加密处理后,再传输至央行。二是规定央行的个人信息隔离义务。我国应注重防范内部人员监守自盗,要求央行及其工作人员除法律规定外,不得还原脱敏信息。三是紧急情况下央行可以扩大个人信息访问权。相关法律可授权央行在发生下述情形时还原个人信息:第一,开展反洗钱调查时;第二,司法机关依法调取涉案个人信息时;第三,境外公权力机构基于国际司法协助条约、跨境执法合作协议,或以外交途径申请调取个人信息时。

### 3. 央行技术风险防控与持续研发义务的设置

数字人民币的技术研发与风险防控工作主要由数研所负责。其采取的部分举措已取得较理想的实践效果,<sup>①</sup>可转化为法律以实现常态化。数研所采取的举措主要有以下几项:一是新技术的研究与应用。例如,数研所逐步引入量子加密、非对称加密、零知识证明等最新技术,成功实现 mBridge 技术升级。本文建议在法律中规定数研所的技术更新义务,以保障数字人民币跨境支付技术的前沿性。二是安全漏洞的自查与修复。例如,数研所测试发现,网络不稳定可能构成安全隐患,因而改用弱证书技术,此举提升了网络波动下的安全性能。可见,有必要增设数研所的定期风险自查义务,通过组织技术测试等方式,主动识别并修复潜在的安全漏洞。三是第三方审查。例如,数研所可聘请第三方机构审查代码,为安全开源做足准备。由第三方机构开展独立审查并出具专业意见,可对数研所的工作形成有益补充。因此,本文建议增设第三方审查制度,要求数研所在重大项目实施前聘请第三方机构开展审查,并出具评估意见。

#### (二) 境外央行合规机制的“模块化”升级

欧盟的模板化国际协议虽然有利于约束境外央行,但可能阻碍与发展中国家和地区的跨境支付合作。因此,我国在制定境外央行合规机制时,可对欧盟的机制进行“模块化”升级,产生适当的去模板化效果。“模块”是指具有特定功能、能与其他子系统组合的半自律子系统。<sup>②</sup>将一个系统分解为若干模块,或将若干模块整合成一个系统的过程就是模块化。模块化的方法常用于法学领域,如权利的各项权能可视为模块,<sup>③</sup>规制对象的各组成部分也可视为模块等,<sup>④</sup>从而实现复杂系统

<sup>①</sup> 常佩琦:《中国人民银行数字货币研究所所长穆长春:从三方面系统提升货币桥技术》,载《上海证券报》,2024年10月24日,第4版。

<sup>②</sup> 孙泽南、庄晋财:《模块化理论视阈下的乡村产业融合:本质内涵与实现机制》,载《农业经济问题》,2024年第9期,第82-93页,这里第83页。

<sup>③</sup> 时诚:《数据权利的模块化设计》,载《东方法学》,2024年第5期,第157-173页,这里第157页。

<sup>④</sup> 张欣:《论人工智能体的模块化治理》,载《东方法学》,2024年第3期,第129-142页,这里第129页。

的精密治理。在数字人民币跨境支付中，我国可将国际协议的基准模板与配套制度视为不同“模块”，根据不同合作方的客观状况进行动态调整与组合。

### 1. 个人信息保护基准模块的设计

本文建议参考欧盟国际协议模板设计个人信息保护的基准模块，涵盖以下方面：一是《个保法》中的衔接规则，其应明确要求数字人民币跨境支付架构中的境外主体确保个人信息保护标准原则上不低于中国境内的监管水平。二是中国人民银行与境外央行对个人信息安全的联合监管机制。相关法律可规定在平等协商的基础上，由各央行共同确定对商业银行等主体的监管标准及实施方案。三是发生特殊情况时国际协议的暂停或终止规则。当合作对方境内发生战争或恐怖主义等恶性事件时，中国人民银行判断不宜向其境内传输个人信息的，应及时发出正式通知，按既定程序停止提供数字人民币服务，并要求对方按约封存或删除以往合作涉及的个人信息。

### 2. 基于配套制度模块的动态调整机制

我国可借助配套制度模块，形成国际协议的动态调整机制。这种动态调整机制可使国际协议契合不同合作方的法律、技术和经济发展水平。本文建议设计以下几种配套制度模块：一是技术援助制度模块，该模块可明确规定援助的技术名称、时间与方式，以及到期后受援方应具备的能力标准，要求中国人民银行协同其他政府部门和企业按约执行援助。二是信息交换制度模块，该模块可要求各央行定期交换法定数字货币在各自境内的脱敏交易信息，以辅助调节宏观政策，并定期开展监管经验与最佳做法的交流。三是过渡期制度模块，在对方达到基准模块规定的标准之前，该模块可采取特殊的个人信息保护安排，例如允许境外央行或商业银行在中国大陆设置临时个人信息存储中心等。在实际运用时，我国可根据对方的个人信息保护能力，灵活组合配套制度模块，确保最终形成的国际协议条款具备适应性与可操作性。事实上，mBridge的法律架构已运用了类似的模块化立法技术，其将支付、外汇、资本管理等规则模块化后，允许各方灵活组合所需模块。<sup>①</sup>这说明即便在同一货币桥内，合作各方承诺遵守的规则也可以是差异化、动态化的。

### （三）境外次接收方监管机制的灵活性升级

欧盟方案旨在借助缔约方国内法，实现对境外次接收方的全面、直接监管，但其要求缔约方完全依照欧盟标准修改国内法，可能阻碍数字欧元跨境支付的推进。本文建议在欧盟方案的基础上，寻求境外次接收方监管机制的灵活性升级。

<sup>①</sup> 穆长春：《央行数字货币跨境支付原则与实践》，2023-11-29，[https://www.thepaper.cn/newsDetail\\_forward\\_25467834](https://www.thepaper.cn/newsDetail_forward_25467834)，访问日期：2025-06-13。

## 1. 对接中国大陆标准的原则性规定

本文建议原则上依照中国大陆标准监管境外次接收方。具体而言,我国可借鉴欧盟方案,将对接中国大陆标准的个人信息保护规则融入中国人民银行与境外央行签署的各类国际协议,例如与香港金融管理局签署的《关于在粤港澳大湾区深化金融科技创新监管合作的谅解备忘录》(2021年),与新加坡、阿联酋等“一带一路”沿线国家签署的双边金融合作备忘录等。我国还可通过签署国际协议,要求对方承诺修改国内法,使其中的个人信息保护标准与中国大陆一致。中国目前签署的部分国际协议已涵盖个人信息保护规则,但这些个人信息保护规则仍须细化。我国可依照《个保法》的核心规则,在国际协议中建构针对境外次接收方(主要是商业银行)的监管体系(详见下文“多边合作框架”),包括确立个人信息处理的合法性、正当性、必要性原则,以“单独同意”为基础的个人信息跨境提供规则,以及个人信息在多主体间传输的约束性规定等内容。国际协议还可要求境外次接收方定期开展安全审计,并接受中国人民银行与境外央行的联合监管。

## 2. 依托协议的监管机制变通

对少数短期内难以达到中国大陆个人信息保护标准的合作伙伴,我国可变通监管机制以提升灵活性。例如,我国可沿用现有规则的间接监管路径,依托处理者与境外接收方订立的法律文件,要求后者对境外次接收方展开间接监管。虽然这种监管路径在约束力和直接性等方面不如欧盟方案,但考虑到参与数字人民币跨境支付的境外商业银行数量相对可控,如果规则设置得当,也能对其起到良好的规制效果。因此,本文建议依照《个保法》细化《评估办法》第9条第3款,要求中国人民银行在与境外接收方订立的法律文件中,规定境外次接收方在过渡期结束后应达到的个人信息保护标准,以及中方提供的技术援助承诺和过渡期期间的个人信息保护安排。

### (四) 多主体责任划分机制的体系化升级:构建多边合作框架

《个保法》在数字人民币跨境支付场景下的适用,将导致中国人民银行与境外央行承担不合理的连带责任,同时产生央行与商业银行责任划分模糊的问题。对此,欧盟提出了“法定为主、兼采意定”的责任分配方案,该方案较契合数字人民币跨境支付实践,但各方主体的责任内容仍须细化。本部分将跨境支付的运行过程分为三阶段,探讨每个阶段所涉主体的权利(或权力)、义务与责任(详见表2),以及如何协调不同国家和地区的监管要求,由此构建体系化的多边合作框架(可类推适用于双边合作)。

表 2 多边合作框架下各主体权利(或权力)、义务、责任对照表

阶段	主体	有关个人信息的权利(或权力)、义务与责任
境内阶段	中国人民银行	个人信息传输权、特殊情形下的解密与使用权、对商业银行的监管权;安全评估、标准协调、技术援助、信息共享、反洗钱、与境外央行的联合监管、安全审计等义务;对处理不当、监管不力造成的安全事故承担责任(法定)
	商业银行(付款行)	个人信息收集权、传输权、使用权;反洗钱审查、出境告知、同意征求、加密处理、保密存储、删除、安全审计、配合监管与调查等义务;对处理不当造成的安全事故承担责任(法定)
跨境传输阶段	理事会	资金来源决定权;总括性的个人信息安全保护义务,其决策应与个人信息保护需求相适应
	职能部门	履行各自职责范围内的义务,如基础设施安全维护义务等
	各方央行	平等协商权、共同决策权,摊额较大的央行还可享有决策优先权;费用摊额的缴纳义务;按协议约定对安全事故承担责任(意定)
境外阶段	境外央行	与中国人民银行基本保持一致(对等原则)
	境外商业银行(收款行)	个人信息使用权;解密、反洗钱审查、保密存储、删除、安全审计、配合监管与调查等义务;对处理不当造成的安全事故承担责任(意定)

来源:作者自制。

### 1. 境内阶段

个人信息位于境内系统时,商业银行(付款行)负责收集发起人与受益人的个人信息,记录支付指令的生成时间、金额等,并开展反洗钱审查。商业银行(付款行)还须履行用户告知义务,征求出境事项的单独同意。传输前,商业银行应完成加密处理;传输后,其还须在法定期间内存储个人信息,并在到期后删除。上述处理活动中的安全事故,应由商业银行负主要责任(法定),并由中国人民银行监督。根据现行规定,中国人民银行与国家网信部门应分别开展个人信息出境安全评估。未来,我国可修订相关规则,将两个部门的安全评估合并或简化为主要由中国人民银行负责。通过评估后,个人信息可由中国人民银行上传至跨境支付基础设施。如因评估或处理不当而引发或扩大安全事故,则中国人民银行应承担相应的责任(法定)。

协调各方监管标准对上述处理活动的顺利开展尤为重要。本文建议重点协商个人信息传输范围,明确普通交易和适用“简易规则”的交易应分别传输哪些个人信息,尽可能地实现标准统一。现阶段,若对方要求的传输范围较小,本文建议仅传输对方要求的信息,以符合“最小必要原则”;若对方要求的传输范围较大,则可运用“零知识证明”等技术手段,实现个人信息“可用不可见”,以满足对方的反洗钱要求。此外,在反洗钱标准、加密标准、存储与删除标准等方面,我国可通过技术援助、经验交流、共享数据库(例如重点关注用户名单)等方式,促进各方法律与标准的协调。

## 2. 跨境传输阶段

在跨境传输阶段,我国应重视跨境支付基础设施的安全维护,可参照国际货币基金组织(International Monetary Fund,下文简称“IMF”)的法律架构,明确责任主体和资金来源。在主体方面,本文建议在多边框架下设置专门的职能部门,负责基础设施安全保障。在资金方面,本文建议参考IMF理事会的制度设计,由合作各方财政部长或央行行长担任理事,组建跨境支付理事会,由其决定资金来源。例如,该理事会可决定收取跨境支付手续费用于维护基础设施,或由各合作方按比例分摊费用,并赋予出资比例较高的合作方相应的决策优先权。合作各方应签署国际协议,以增强上述制度的稳定性和透明度,并协商确定该阶段的安全事故责任主体(意定),例如由合作各方共同承担。

## 3. 境外阶段

个人信息到达境外系统后,还须由境外央行传输至境外商业银行(收款行),并由后者解密、开展反洗钱审查、存储与删除。这也需要各方监管标准的协调,因上文已讨论,此处不再赘述。中国人民银行还可与境外央行及商业银行签署国际协议,详细规定该阶段安全事故的责任主体。若事故由境外央行的传输行为引发,建议由境外央行承担责任(意定);若由境外商业银行操作不当引发,则建议由该商业银行承担责任(意定)。此外,为改进欧盟方案中“穷尽罗列处理目的”的立法弊端,我国相关法律还可在罗列责任承担的典型情形后,分别设置相应的上位概念。央行处理活动的特点体现为统筹性、全局性,因此上位概念可表述为“以统筹跨境支付为目的的处理活动”;商业银行处理活动的特点体现为个案性、服务性,因此上位概念可拟为“以服务用户为目的的处理活动”。这种“典型情形+上位概念”的立法范式,将有助于提升国际协议的周严性和体系化水平。

## 4. 辅助性职能部门的设置

为深化跨境支付合作,本文建议借鉴IMF的组织架构,在多边合作框架下设置以下几类辅助性职能部门。一是信息交流部,负责合作各方的信息传递,交换最新数字货币政策、个人信息保护要求、反洗钱监管标准等。二是能力建设部,负责对发展中合作方的技术援助,在各方经济、技术条件差异较大时,辅助协调监管标准。三是研究部,负责更新技术,确保多边框架的技术前沿性。当前,mBridge已设置合规、技术、法律、政策四个委员会,<sup>①</sup>说明这类辅助性职能部门的作用已得到认可。未来,我国可与合作伙伴继续完善职能部门的法律架构,逐步细化跨境支付合作。

<sup>①</sup> BIS, “Project mBridge Reached Minimum Viable Product Stage”.

## 五、结 语

妥善规制数字人民币跨境支付中的个人信息流动，是推进数字人民币国际化并以此赋能共建数字“一带一路”的重要前提。我国应积极运用国内法、国际协议等法律工具，为数字人民币跨境支付架构营造安全、可信的隐私环境。为此，我国可借鉴欧盟为数字欧元专门打造的个人信息规制方案，并根据数字人民币的现实情况进行本土化升级。数字人民币跨境支付架构中个人信息规制的完善，不仅能够为数字人民币打造“隐私保护”和“反洗钱”的双重法治名片，提升中国国际金融话语权和影响力，还有助于维护“一带一路”倡议下各国的金融主权和区域金融安全，在为民众带来更多跨境支付便利和福利的同时，让民众享有充分的个人信息安全感。未来，本议题仍存在若干重点问题有待学界进一步探索。一是针对 mBridge 运营架构的多边个人信息规则建构与实施，应探讨如何在保证个人信息安全的基础上，进一步提升 mBridge 的反洗钱能力，完善相应的跨境执法合作机制。二是在中国国内法中关于数字人民币所涉个人信息规则的专门化和国际化问题上，应着重探讨如何借助数字人民币的跨境支付架构，推动中国的个人信息规制理念、制度设计和标准体系在更大程度上被国际社会所接受，进而逐渐成为国际通行准则。

责任编辑：郑春荣