僅供委員問政所需參考
不代表本院意見或立場

編號：2419

議題研析

一、 題目：數位法幣之隱私保護問題研析

二、 議題所涉法規

中央銀行法、中央銀行發行新臺幣辦法、個人資料保護法

三、 背景說明

據國際貨幣基金（IMF）總裁 2023[1]年 6 月 19 日於非洲央行會議表示，已有 110 餘個國家研究中央銀行數位貨幣[2]（Central Bank Digital Currency, CBDC）。全球央行數位貨幣之發展情形，以日本為例，其央行計畫啟動數位日圓試點（Pilot Run）測試，設計完整 CBDC 生態系統，預計 2024 年春季解決數位日圓的相關法律問題，最快於 2026 年推出 CBDC。我國中央銀行亦持續研究數位法幣可行性，目前已分別完成第一階段「批發型[3]CBDC 可行性技術研究」及第二階段「通用型[4]CBDC 試驗計畫」，111 年已與五家銀行合作試驗，但要上路的法規、資安等，將是下一波試驗關鍵[5]。央行並於 113 年 3 月初首次向全體國銀進行數位貨幣調查，最快 5 月就會公布調查結果[6]。CBDC 就是法定貨幣的數位化[7]（下稱數位法幣），

[1] 本報告有關年份之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

[2] 顏嘉南，IMF 推動 全球央行數位貨幣平台，工商時報，112 年 6 月 21 日，網址：https://www.ctee.com.tw/news/20230621700088-430701，最後瀏覽日期：113 年 3 月 28 日。

[3] 「批發型（wholesale）」，係指提供金融機構跨行清算使用之數位法幣。參自中央銀行券幣數位博物館網站，網址：https://museum.cbc.gov.tw/web/en-us/story/evolution/digit，最後瀏覽日期：113 年 3 月 20 日。

[4] 亦稱為「零售型（retail）」，係指提供大眾使用之數位法幣。參自中央銀行券幣數位博物館網站，同前註。

[5] 巫其倫，央行推數位貨幣不搶快 配套先做好，工商時報，113 年 3 月 12 日，網址：https://www.ctee.com.tw/news/20240312700010-430301，最後瀏覽日期：113 年 3 月 15 日。

[6] 朱漢崙、陳儷方，發行數位台幣？央行 5 月揭曉，聯合報，113 年 3 月 13 日，網址：

其發行、流通使用等可能涉及之議題眾多，擬以數位法幣所涉隱私問題進行初步研析。

四、 探討研析

（一）數位法幣可能產生之問題與其採取之模式有關

數位法幣以其存在形式上可分為在央行或經央行授權之機構開立個人存款帳戶、與現行數位支付型態類似之「帳戶基礎型（account-based）」，及存放於電子錢包、與現金支付型態類似之「代幣基礎型（token-based）」[8]。其中「帳戶基礎型」需驗證整個交易中所涉及之帳戶所有人資料，因此對隱私與個人資料保護之影響較大；而「代幣基礎型」雖可降低對個人隱私與資料外洩之威脅，但其風險在於，若使用者未妥善保管電子錢包的金鑰，則可能造成財物損失[9]；惟倘若為監管需要，將該代幣設計具有可追蹤性（traceable），則仍有隱私風險[10]。

數位法幣之隱私風險高低與其設計有關，倘若設計不允許央行處理個人資料，或嚴格採行「資料最小化（data minimization）」，將有助於防止或降低隱私風險；反之，若數位法幣之設計係允許央行識別及儲存付款相關個人資料，或銷售過程中所蒐集、可連結至消費者個人之資料時，則將可能提升隱私風險[11]。

（二）造成數位法幣隱私風險之可能情況

---

https://udn.com/news/story/7239/7827035，最後瀏覽日期：113 年 3 月 15 日。

[7] 巫其倫，同註 5。

[8] Ori Freiman, CBDC Governance：Programmability, Privacy and Policies, Centre for International Governance Innovation, fall 2023, p.4。

[9] European Data Protection Supervisor（EDPS）, TechDispatch on Central bank digital currency, p.9，available from：https://www.edps.europa.eu/system/files/2023-03/23-03-29_techdispatch_cbdc_en.pdf。

[10] Ori Freiman, *supra* note 8。

[11] European Data Protection Supervisor（EDPS）,*supra* note 9，p.13。

1、存取憑證（access credential）遺失或遭竊[12]

通常透過使用數位法幣之設備轉帳須透過存取憑證之驗證，該憑證遭竊或遺失，即會導致帳戶及個人資料外洩，常見方式是透過社群引擎、旁路攻擊[13]（side-channel attacks）或惡意軟體等，從使用者之設備端提取憑證。

2、資料中心化（data concentration）吸引網路攻擊[14]

數位法幣使用者資料倘若係以集中方式儲存，則該儲存區域會吸引大量網路攻擊，而可能導致個資侵害之系統性風險，或是導致使用者於進行支付時遭系統拒絕提供服務之風險。

3、增加非法利用個人資料之風險[15]

數位法幣可能使用單一且具持續性之識別碼（user-identifier, 又稱 user ID），透過相關資料進行個人剖析（profiling）將更為容易，亦將加劇非法蒐集個人交易資料進行信用評估、或濫用該資料進行行銷等行為之風險。

（三）可用於提升數位法幣隱私之加密科技[16]

有論者認為，數位法幣透過加密科技之設計，得以大幅提升隱私保護，其建議之加密科技如下：

---

[12] European Data Protection Supervisor（EDPS）,*supra* note 9，p.14。

[13] 旁路攻擊之定義，參考 INSIDE 網站專欄「【Wired】硬塞駭客辭典：什麼是旁路攻擊？」一文之描述為：「旁路攻擊是用電腦不斷散發出來的訊息痕跡，解讀其中各種模式的攻擊手法。例如電腦螢幕或硬碟發出的電輻射，會因為穿過螢幕或被硬碟磁頭判讀的訊息不同，導致發散電輻射的情況也會有些許不同；或者是電腦零組件在執行某些過程中，會消耗不同的電量。又或者是當你打字放開鍵盤時，駭客判讀非常細微的聲音差異後，就能推敲出使用者的密碼。」該原文來自 Wired《Hacker Lexicon: What Is a Side Channel Attack?》，作者 Andy Greenberg。台灣康泰納仕集團授權提供，由 Linden Chen 翻譯並經 INSIDE 編審。網址：https://www.inside.com.tw/article/23299-what-is-a-side-channel-attack，最後瀏覽日期：113 年 3 月 26 日。

[14] European Data Protection Supervisor（EDPS）,*supra* note 9, p.14。

[15] European Data Protection Supervisor（EDPS）,*supra* note 9, p.9。

[16] Ori Freiman, *supra* note 8, p.4-5。

1、零知識證明（Zero-knowledge proofs）

無須揭露即可確認該資料為真實之技術，例如：無須揭露帳戶餘額，即可確認帳戶中尚具有足夠金額可完成交易。

2、同態加密（homomorphic encryption）

相關技術得以在不解密之情況下對加密資料進行計算，例如：無須揭露帳戶餘額，即可計算及支付利息。

3、差異化隱私及匿名（differential privacy and anonymization）

相關技術得以保留利用資料進行研究和分析的能力，同時確保該研究與分析無法從資料集中提取個人資訊，例如：透過添加雜訊或刪除標識碼等方式。

（四）歐盟個資保護監督機關（European Data Protection Supervisor, EDPS）針對數位法幣之隱私保護建議

歐盟之個資保護監督機關於 2023 年提出之數位法幣技術調度報告（TechDispatch on Central bank digital currency），認為於不同之數位法幣計畫階段，應進行個資保護影響評估（data protection impact assessment, DPIA），且於數位法幣設計之初，即應納入「隱私保護始於設計」（privacy by design）或「隱私保護預設」（privacy by default）等規劃，而其監管架構、核心技術決定皆應將隱私與個資保護納入考量，所有有關功能、配置和風險接受度的設計等亦皆應經過適當評估並記錄[17]。

（五）研析與建議

數位法幣之設計，將大幅影響其可能造成之隱私風險，目前央行對於數位法幣之態度亦傾向審慎評估、研究，央行或可參考歐盟個資

[17] European Data Protection Supervisor（EDPS）,*supra* note 9, p.10。

保護監督機關之建議，視規劃階段進行 DPIA，並納入「隱私保護始於設計或隱私保護預設」，採行適當之加密科技技術；又考量我國已設個人資料保護委員會籌備處，籌設未來個人資料保護獨立監督機關，央行於研議數位法幣之隱私保護制度及相關規劃時，宜與該籌備處共同研商，以降低數位法幣之隱私侵害風險。

撰稿人：陳育靖