區塊鏈身分層驗證與個人資料保護之衝突－

以「 World ID」之虹膜數據蒐集為中心

黃裕恆 撰

壹、摘要

區塊鏈科技與人工智慧的迅速發展，使「人」與「非人」的界線日益模糊；新興科技在提升效率的同時，也動搖數位空間中「身分真實性」的基礎，進而威脅數位治理秩序與民主參與。為回應「一人一帳」之需求，World 項目以專用硬體進行虹膜掃描，生成 World ID，建立人格證明（Proof of Personhood），並主張可用於反濫用、治理與普遍基本收入（UBI）。然而，虹膜屬不可逆之生物特徵，一旦被蒐集、留存與比對，其風險具有長期性與不可回復性，因而引發重大法律與倫理爭議[1]。且自 2025 年，官方亦在台啟用 World ID 之現場驗證計劃，相關風險與合規疑義遂由抽象討論轉變為亟待回應之本地監理議題[2]。

本文以 World 項目為案例，透過技術機制與治理設計的拆解，檢驗其在我國個人資料保護法與憲法資訊自決層面之合規可行性；並以歐盟、美國、韓國與若干採行暫停或限制之法域為比較基準，輔以數位倫理視角，分析「真同意」、弱勢保護與人格尊嚴等爭點。在此先行提出本文的中心判斷：以不可逆生物特徵建立一般性身分層，原則上難以通過我國法上比例原則的「必要性」審查；除非符合嚴格的例外許可條件（含撤回即失效與刪除可驗證、模板最小化與本地化、跨境強管、硬體可信鏈稽核、脆弱族群保障等），否則不宜作為常態化之制度選擇。本文據此提出「原則禁止—例外許可」的政策路徑與具體修法建議[3]。

關鍵詞：World ID、Proof of Personhood、個人資料保護法、GDPR、比例原則、數位倫理

Abstract

The rapid advance of blockchain and artificial intelligence has increasingly blurred the boundary between human and non-human actors. While such technologies improve efficiency, they also erode the foundation of identity authenticity in digital spaces, with attendant risks for governance and democratic participation. To meet the "one-person-one-account" demand, the "World" project uses dedicated hardware for iris scanning to generate a World ID and thereby offer a Proof of Personhood, promoted for anti-abuse, governance, and even universal basic income. Because the iris is an irreversible

---

[1] Worldcoin, Worldcoin Whitepaper (2023); Jonas Lutz et al., Compressed to Zero: The Silent Strings of Proof of Personhood (2023)

[2] World Foundation(2025),〈World Proof of Human now available in Taiwan〉,載於:https://world.org/blog/announcements/world-launches-in-taiwan(最後瀏覽日:2025 年 9 月 11 日)。

[3] 比較 Vitalik Buterin, What do I think about biometric proof of personhood? (2023)，其指出 PoP 設計需在「隱私—可及性—去中心化—安全」間尋求平衡。

biometric, however, the collection, retention, and matching of such data create long-lived and difficult-to-remedy risks, raising significant legal and ethical concerns. In 2025 the project also launched in-person World ID verification in Taiwan, turning what had been abstract debates into urgent, local regulatory questions.

Using the "World" project as a case study, this article unpacks the technical mechanisms and governance design and evaluates compliance under Taiwan's Personal Data Protection Act (PDPA) and the constitutional right to informational self-determination. It further situates the analysis in comparative perspective by drawing on the European Union, the United States, Korea, and other jurisdictions that have paused or restricted similar deployments, and incorporates a digital-ethics lens on genuine consent, protection of vulnerable groups, and human dignity.

The central judgment is as follows: building a generalized identity layer on irreversible biometrics presumptively fails the necessity prong of proportionality under Taiwan law. Unless strict, verifiable conditions are satisfied—including withdrawal-triggered invalidation and verifiable deletion, template minimization and localization, strengthened cross-border governance, independent audits of the hardware trust chain, and enhanced safeguards for vulnerable groups—such a design should not be normalized. Accordingly, the paper advances a "default prohibition with narrowly tailored exceptions" policy pathway and offers concrete legislative recommendations.

Keywords: World ID; Proof of Personhood; Personal Data Protection Act (PDPA); GDPR; proportionality; informational self-determination; digital ethics.

貳、World 項目概述

一、項目背景與目的

World 項目由 Tools for Humanity Corporation 推動，其核心構想在於建立全球通用之 Proof of Personhood（PoP, 人格證明）機制，以解決數位環境中「一人一帳」的難題。該項目主張，生成式人工智慧與自動化系統可能造成身分真實性危機，若無有效 PoP，將導致治理與數位資源分配遭嚴重侵蝕。World 以分配 World ID 自許為此一問題的解方，並宣稱能藉由生物特徵驗證確保「一人一帳」[4]。

二、技術架構與運作流程

World 項目採專用硬體 Orb 進行虹膜掃描，生成獨特的「虹膜碼」（iris code），並與使用者的公私鑰配對，以產生 World ID。此 World ID 可於後續應用

[4] Worldcoin, Worldcoin Whitepaper (2023), p. 4.

情境中透過零知識證明（ZK-SNARK）方式，證明其為「獨一無二的人類使用者」，而無需揭露真實身分或原始影像。並藉由 World ID 作為基礎分發項目代幣 Worldcoin($WLD)予已驗證使用者。官方白皮書另載明，系統不會保存完整虹膜影像，僅存放去識別化的雜湊碼，並計畫逐步導入安全多方計算（MPC），以降低資料集中化風險[5]。

三、官方主張與外部批評

World 團隊在白皮書中強調，其制度設計具備三大保障：

（一）、透過零知識證明與去識別化處理，避免直接留存虹膜影像，以確保隱私保護；惟只要長期保有可再比對之模板與雜湊，即構成個資處理，且於撤回後仍可推動比對時，將與我國個資法第 3 條請求停止與刪除權發生結構性衝突。

（二）、雖然初期由單一組織營運，但承諾將隨時間推動治理權下放，最終交由去中心化自治組織（DAO）管理；

（三）、藉由 World ID 作為基礎分發 Worldcoin($WLD)，未來可進行更公平的空投、投票與資源分配，甚至推動普遍基本收入（UBI）[6]。然而，學理與實務上對此模式仍提出重大疑慮。首先，虹膜屬不可逆的生物特徵，一旦外洩即無法更換，對資訊隱私構成永久風險[7]。其次，在部分低收入地區，居民可能因經濟誘因而交出虹膜，致「自願同意」的真實性存疑。此外，Orb 為專用硬體，其製造與驗證權限集中於單一組織，顯示結構性集中化問題。最後，多國監管機關已採取限制措施，尤以西班牙資料保護機關（AEPD）於 2024 年 3 月依 GDPR 第 66 條第 1 項下令停止蒐集與處理，理由包括涉及未成年與同意不可撤回，進一步突顯其合規挑戰[8]。

四、小結

World ID 技術設計結合密碼學與區塊鏈，試圖回應身分驗證之困境，並以去中心化理念正當化其制度。然而，以虹膜作為基礎之敏感個資蒐集，已引起歐盟與多國高度關注，並顯示其在合規與倫理上的潛在衝突[9]，正是本文後續分析的焦點。

---

[5] Ibid., pp. 7–9; Jonas Lutz et al., Compressed to Zero: The Silent Strings of Proof of Personhood (2023).

[6] Worldcoin, Whitepaper, pp. 12–16.以當前價值計算每位經過驗證用戶可領取約相當 100 美金之世界幣，用戶分享註冊鏈接給新用戶註冊後可領取更多世界幣。

[7] Vitalik Buterin, What do I think about biometric proof of personhood?(2023).

[8] Agencia Española de Protección de Datos (AEPD), Press Release (6 March 2024).

[9] Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Press Release (19 December 2024); EDPB, Decision (2025).

參、研究動機

一、問題背景：生物特徵作為身分驗證之法律風險

生物特徵如虹膜因具唯一性而被導入身分驗證；惟其不可替代性使一旦遭不當蒐集、外洩或濫用，即對資訊隱私與人格權造成難以回復之侵害。World 團隊計畫以專用硬體進行虹膜掃描以產生 World ID，雖宣稱回應「一人一帳」之需求，卻同步引發高度風險[10]。2025 年起，官方「Find your nearest Orb」已將台灣列為可進行實體驗證之地區，並出現多個可預約掃描之據點[11]；多家媒體亦報導「虹膜掃描」在台灣啟用與運作流程。是以，相關法律效果與合規問題已非抽象爭議，而屬迫切的本地監理議題，亟需就《個人資料保護法》、跨境傳輸與比例原則等面向提出系統性分析與政策回應。

二、高風險預警與倫理脈絡：

歐盟監管實務已對生物特徵作為身分驗證提出即時警訊。西班牙資料保護機關（AEPD）即依 GDPR 第 66 條第 1 項採取臨時措施，理由涉及資訊揭露不足[12]、未成年資料保護及同意可撤回性不足，顯示監管者將此類處理視為高度風險領域。葡萄牙 CNPD 亦因未成年蒐集與刪除權不可行使等因素，採取暫停措施[13]。德國 BayLDA 與歐洲資料保護委員會（EDPB）更在 2024–2025 年的調查中，針對「虹膜碼」是否構成敏感個資處理、刪除與撤回是否具可驗證性，陸續下達限期刪除與禁止「被動比對」等命令[14]。

在數位倫理層面上，若以經濟誘因交換不可逆的敏感資料，形式同意可能淪為「被迫選擇」；要求以身體特徵證明存在，更可能導致弱勢群體被工具化為可交易之數據資產，形成「數位殖民」的疑慮[15]。此種設計也引發人格尊嚴的侵蝕風險，因其將「人」本身的存在條件化為技術可操控的資源。前述風險，要求本文在國內法規範分析之外，亦以倫理原則作為比例審查中「必要性」與「衡量性」之評價素材[16]。

---

[10] Jonas Lutz et al., Compressed to Zero: The Silent Strings of Proof of Personhood (2023).

[11] World 官方網站(2025),〈Find your nearest Orb | Verify your World ID〉,載於:https://world.org/zh-tw/find-orb?country=TW(最後瀏覽日:2025 年 9 月 11 日)。目前全台已有 33 地點可藉由 orb 驗證 World ID 身分

[12] Agencia Española de Protección de Datos (AEPD), Press Release (6 March 2024).

[13] Comissão Nacional de Proteção de Dados (CNPD), Deliberação/2024/137.

[14] Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Press Release (19 December 2024); European Data Protection Board (EDPB), Decision (2025).

[15] Vitalik Buterin, What do I think about biometric proof of personhood? (2023).

[16] Federal Trade Commission (FTC), Policy Statement on Biometric Information (2023).

三、我國法制缺口：敏感個資與跨境傳輸

我國《個人資料保護法》第六條雖列舉特定敏感資料，惟未明文涵蓋「生物特徵」；跨境資料移轉規制亦未與 GDPR 完整接軌。倘若類似項目在地運作，現行架構可能難以充分回應風險[17]。

肆、研究目的

一、檢驗台灣法制對生物特徵蒐集之適用性

本研究首要目的，在於分析 World ID 所採取之虹膜掃描模式，是否符合我國《個人資料保護法》之規範，並藉由釋字第六○三號、六八九號及六九六號之憲法見解，探討資訊隱私與人格尊嚴在憲法層次之保障。

二、比較國際監管經驗之異同

其次，透過蒐集歐盟、西班牙、葡萄牙、德國、美國、韓國及其他直接禁止或暫停 World 項目之國家之案例，觀察各法域在敏感個資處理與跨境資料傳輸上的立場，並歸納監管強度與政策取向之差異。

三、評估數位倫理爭議之規範意涵

再者，從數位倫理角度切入，檢視「同意之真實性」、「數位殖民」與「人格尊嚴」等爭點，分析其對我國基本權保障之啟示，並思考法制是否應將倫理原則轉化為具體規範。

四、提出台灣未來政策與制度建議

最後，本文將結合前述分析，提出我國在面對類似 PoP 項目時，應如何透過修法、監管機制或國際合作，以兼顧科技發展與基本權保障。

伍、研究方法與過程

一、文獻分析法

本文以官方文件、監管機關新聞稿、學術期刊論文及評論性文獻為基礎，掌握 World 項目及 Proof of Personhood 之核心爭點，並輔以台灣個資法、憲法解釋與國際法規進行分析。

---

[17] 《個人資料保護法》第 6 條。

二、規範分析法

透過條文解釋與體系分析，檢視我國《個資法》第六條對敏感資料之規範，並與 GDPR 第九條及跨境傳輸條款相對照，釐清法律位階與適用問題。

三、比較法方法

選取歐盟、美國、韓國及其他國家對 World 或類似項目之監管案例，分析其法律依據、監管措施與政策考量，並比較各法制間之異同。並聚焦於西班牙 AEPD、葡萄牙 CNPD、德國 BayLDA 與歐洲資料保護委員會（EDPB）等監管行動，藉由具體案例呈現法律適用之實務操作。

四、倫理分析法

以數位倫理理論為基礎，確認事實與倫理衝突，評估 World ID 所涉及之「真同意」、「數位殖民」與「人格尊嚴」問題，並探討其規範化的可能性。

陸、比較法分析

一、歐盟之整體取徑

歐盟法制對生物特徵資料向來採取高度保護之立場。就規範結構觀之，生物特徵被定位為敏感個人資料，原則上不得處理，僅得在嚴格例外與充分保障措施下方可進行。此外，歐盟設有緊急干預機制，賦予監管機關在例外情形下得即時採取臨時措施，以防止難以回復之損害。此一體系性安排，反映歐盟對於人格尊嚴與資料自決之核心價值，亦使會員國對高風險蒐集情境能迅速介入[18]。

二、西班牙之即時禁止措施

西班牙資料保護機關對於以虹膜建立「一人一帳」之驗證模式，採取臨時禁止。其所以採取明確積極之監管態度，主要係基於三層考量：其一，資訊揭露之充分性不足，致使同意之真實性難以確認；其二，涉及未成年者資料之蒐集，風險顯著；其三，同意撤回機制與資料刪除路徑未臻完整，難以確保資料當事人能有效行使權利。此案突顯監管者以「先保護、後評估」之思維，優先確保基本權不受不可逆侵害[19]。

三、葡萄牙之暫停決定

葡萄牙資料保護機關就同類型蒐集行為，同樣採取暫停措施。其核心關切在於，使用不可替代之生物特徵作為身分驗證基礎，是否具備足以對抗風險之合法性

[18] Regulation (EU) 2016/679 (GDPR), art. 9(1); art. 66(1).

[19] Agencia Española de Protección de Datos (AEPD), Press Release (6 March 2024).

基礎與必要性證成；再者，關於資料最小化、保存期限、權利行使與監督稽核之設計，是否足以達到敏感資料之「實質可控制」[20]。

四、非歐盟法域：肯亞之「先嚴後鬆」

肯亞政府初期基於資安、未成年保護與社會秩序之考量，採取全面暫停之政策；俟主管機關完成調查與補救承諾後，方允其恢復活動。此一模式，反映該國法域在面對外來高風險技術時，傾向以公共利益為優先，並以程序監理與承諾機制交換創新空間[21]。

五、美國：聯邦政策指引與州法強監管

美國在聯邦層級缺乏一部統一之一般個資法，監管多仰賴聯邦貿易委員會之不公平或欺騙性行為框架與政策聲明，對生物特徵濫用提供合規指導與執法基礎。州法方面，以伊利諾州之生物特徵資訊隱私法為最具代表性的強監管範例：要求事前明確同意、用途告知、保存與刪除政策，以及對違反者科以民事責任。惟隨著近年判例與修法調整，賠償與計算方式更趨收斂，雖仍具嚇阻力，但整體強度較早期稍緩[22]。

六、韓國：高標準之敏感資料保護與國家主導之數位身分

韓國個資保護法對敏感資料之處理採高門檻之合法性基礎與明確同意要件，並強調目的限制與資料最小化。近年政府推動行動身分制度，藉由官方基礎設施與授權框架，建立可監督、可稽核之身分驗證路徑。此一模式以國家主導確保安全性與權利行使的可近性，惟亦須留意避免形成公權力對個資過度集中之風險[23]。

七、比較小結

綜合上開法域觀察，可得數項趨勢。其一，歐盟體系對生物特徵採最高度保護，並透過緊急措施與一致性機制，確保跨境活動不致游離標準之外。其二，美國以政策聲明與州法並行，形成訴訟風險與合規成本並重之環境，對於市場實務具有行為調整效果。其三，韓國以國家級基礎設施與高標準規範推動數位身分，展現「安全、可監理、可追溯」之導向。其四，新興法域如肯亞，採取「預防性暫停、附條件復航」的彈性監管。整體而言，各國對以虹膜為基礎之驗證機制，普遍聚焦於同意之真實性、未成年保護、刪除與撤回權之可行性、跨境移轉之控制，以及將

---

[20] Comissão Nacional de Proteção de Dados (CNPD), Deliberação/2024/137.

[21] 報導整理，參見肯亞政府有關 Worldcoin 初期暫停與後續附條件復航之政策聲明（2023）。

[22] Federal Trade Commission (FTC), Policy Statement on Biometric Information (2023); Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14.

[23] 韓國《個人情報保護法》（Personal Information Protection Act, PIPA），第 23 條關於敏感資訊之處理限制。

「去識別化結果」仍視為敏感處理之風險評估。此等觀察，對我國後續之合規審查與制度設計，具有直接之參照價值。

柒、我國法之合規分析

一、爭點與法源

以虹膜碼作為持續性身分識別基礎，性質上屬於可識別個人之資訊，應受個人資料保護法（下稱個資法）規範（第 2 條第 1 款）。雖個資法第 6 條對「敏感個資」採列舉，未明載「生物特徵」，但基於其高度可辨識性與不可替代性，實務審查宜比照敏感資料之嚴格標準，並以資料當事人權利為核心（第 1 條、第 3 條）。同時，憲法層次之資訊隱私與資訊自決已受司法院釋字第 603 號、第 689 號肯認，行為若以不可逆特徵作為條件，應受比例原則之嚴格審查。

二、合法性與比例原則

非公務機關蒐集、處理、利用個資，須具合法性基礎並受「特定目的、必要範圍」拘束（第 19 條、第 20 條）。若以「同意」作為基礎，應符合特定、明確、知情、自由，且得以相同之便利撤回（第 7 條、第 8 條；並由第 3 條第 4、5 款之「請求停止與刪除」權落實）於證立必要性時，提出替代方案不可行之技術治理層證據，應為申請者之舉證。就比例原則而言應符合：

(一)、適合性：以唯一性特徵防杜重複註冊，與防機器人目的具有關聯。

(二)、必要性：應先評估是否存在侵害較小之替代方案，如裝置端活體偵測、多因素（行為）驗證、社交圖譜佐證、押金或分級信任機制等；若同等效果可由較低侵害手段達成，即不符必要性。

(三)、衡量性：不可逆特徵一經外洩無法更換，其對人格權之長期風險，須與平台治理之增益加以權衡；未成年人或經濟弱勢之「同意」尤易失衡，宜從嚴（第 3 條、釋字第 689 號）。

三、資料治理與跨境移轉

基於生物特徵屬高度敏感且不可逆之個人資料，凡涉此等高風險處理，法制上之最低門檻應是「可理解且可稽核」。是以，控制者無論直接蒐集或間接取得，均負具體化之透明告知義務，須明確揭示身分、目的、資料類別、利用期間與方式、當事人權利及不提供之效果等事項（第 8 條、第 9 條）。又為使風險可控，必須建置與運行相稱之資安與內控體系，落實技術與組織措施之選擇、驗證與持續改進（第 27 條），並以「目的拘束」與「時間拘束」治理資料生命週期：當特定目的

已消失或保存期間屆滿，控制者即負主動刪除或停止處理、利用之義務（第 11 條第 2、3 項），不得以技術名目迴避。蓋即便不保存原始影像，長期留存可再比對之模板與雜湊，仍屬個資之處理行為，必須踐行資料最小化、保存期限限制與「可驗證刪除」；實務上並應提供撤回同意後即時停用比對的機制、出具刪除憑證並留存稽核軌跡，以昭公信。

涉跨境移轉時，非公務機關並受第 21 條之拘束：倘受入國之保護水準不足，或足以損及當事人權益者，主管機關得為限制或禁止。故合規路徑宜採本地化處理優先；確有跨境必要者，應以強化契約條款、端到端加密與嚴格密鑰治理、以及受任者之獨立稽核與持續監督等補強措施，證成整體風險可接受（第 21 條、第 27 條）。此外，控制者與受委託者間須以書面明確界定處理範圍、資安標準、次委託限制、違規通報與稽核權責，以避免外包環節成為合規破口（第 8 條第 1 項第 6 款、第 27 條）。

綜上所述，在生物特徵驗證的場景中，合規的關鍵不在於形式上「不存原檔」，而在於能否於全生命週期中證成必要性、排除較低侵害之可替代方案，並確保刪除可驗且可受監督；否則即難符合個資法之目的拘束、最小化與安全維護之要求。

四、初步結論與具體建議

綜合《個資法》第 3、7、8、11、19、20、21、27 條及釋字第 603 號、第 689 號之要求，以不可逆生物特徵作為長期身分識別，如未同時達成下列條件，合規性即存重大疑義：

(一)、權利可行使：資料主體請求時，能即時停止比對並提供可驗證刪除證明（第 3 條、第 11 條）。

(二)、必要性證成：提出影響評估與技術說明，說明無同等效果之較低侵害替代方案（第 19 條、第 20 條；釋字第 603 號）。

(三)、模板最小化：避免或嚴格時限保存可再比對模板與雜湊，並以技術方式確保「撤回即失效」（第 27 條）。

(四)、脆弱群體保障：建立年齡驗證、冷靜期、經濟誘因上限與家長（或法定代理）同意規範（第 3 條、釋字第 689 號）。

(五)、跨境控管：明確資料流向與受入地法制，若屬保護不足情形，依第 21 條採限制或改以本地化方案；如仍需移轉，落實強化契約與技術控制（第 21 條、第 27 條）。

捌、數位倫理分析

一、「真實同意」之倫理疑慮

以個人之不可替代身體特徵作為身分驗證前提，首涉個體自主之保障。所謂「同意」，應同時具備自由、知情與特定之內涵，且得以相同之便利撤回。然若以經濟誘因作為主要交換條件，對經濟弱勢或資訊弱勢者，實際效果常呈現「形式上同意、實質上被迫」之狀態。再者，撤回後倘仍保留可再比對之模板與雜湊，或技術上無法停止往後比對，則「可撤回性」難謂符合倫理上對自主的最低要求[24]。

二、「人格尊嚴」之倫理疑慮

將「是否為獨立人類個體」之判斷，建立於虹膜等不可逆資料之長期保存與比對，確有將人之存在工具化、數據化之傾向[25]。雖然生物特徵驗證在現代科技應用中已屢見不鮮，如實務上蘋果公司即以臉部辨識技術作為裝置解鎖機制，但其特徵資料原則上留存在使用者端，並非集中保存於第三方資料庫[26]。倫理評估上，仍須以比例原則檢驗：在可達成同等治理效果的前提下，是否存在侵害更小之替代措施（例如裝置端活體偵測、行為式或社交圖譜輔助、多因素機制、或以可替換憑證取代不可逆特徵等）[27]。如替代方案足以達標，仍選擇仰賴不可逆資料，即有逾越必要與侵害人格尊嚴之虞。

三、「數位殖民」之倫理疑慮

在弱勢社群或未成年族群中，以代幣或小額補貼誘使其交付高度敏感且不可逆之生物特徵資料，構成明顯不對等交換，已被批評為新型態的「數位殖民」。以當下完成生物特徵驗證後可獲取之 WLD 代幣折算，約相當於 164.5 美元之誘因[28]，即足以驅使部分人群參與；此種手段可能以未來長期不確定風險換取當下報酬，難

---

[24] European Data Protection Board (EDPB), Decision (2025)（要求撤回與刪除必須具備可驗證性）。

[25] 司法院釋字第 603 號解釋理由書，指出指紋等不可逆生物特徵屬於資訊隱私權保障範圍，若作為「身分證」發放前提，欠缺比例原則之正當性。

[26] Apple Inc.，〈Face ID security〉（2023），說明臉部特徵資料僅儲存在使用者裝置的「Secure Enclave」，不會上傳至 Apple 伺服器或進行集中保存，藉以降低隱私風險。官方資料：https://support.apple.com/en-us/HT208108（最後瀏覽日：2025 年 9 月 10 日）。

[27] Jonas Lutz et al., Compressed to Zero: The Silent Strings of Proof of Personhood (2023)。

[28] 本數據係作者依 2025 年 9 月 9 日 WLD 市價折算（82.25 WLD × 2 美元／顆＝164.5 美元），惟加密貨幣價格浮動甚鉅，僅供研究當下論證之參考。

免迎來剝削弱勢人群之質疑。實務上，自 2023 年以來，肯亞、奈及利亞、菲律賓等地多次出現排隊進行虹膜掃描以換取加密代幣之現象，反映補貼誘因對經濟脆弱族群之吸引力[29]。依世界銀行 2023 年人均美元 GDP 觀之：奈及利亞 1,596.6、肯亞 1,952.3、菲律賓 3,804.1，相較美國 82,304.6，差距懸殊；在此脈絡下，「補貼換取生物特徵」極易淪為全球南方弱勢者承擔風險、而北方資本與科技企業獲取利益的不平等格局[30]。

玖、問題討論

首先，就目的正當性與手段選擇之關係而言，防杜數位濫用、區別人與機器固屬正當目的，惟目的之正當並不必然導出手段之合理。若以不可逆的生物特徵建構單一且終身唯一的識別基礎，將形成『一次蒐集、長期暴露』的高度風險結構；相對之下，若改採可替換憑證並結合多元驗證方式，雖然治理上較為繁複，卻能降低資料一旦外洩即無從補救的危害[31]。

其次，就「去識別化」的角度觀之，僅以模板與雜湊取代原始影像，並不當然謂風險完全消失；在仍可再比對與鏈結的情況下，其性質更接近於降低風險，而非完全無風險，故本文認為仍應依敏感資料標準嚴加檢驗。

再者，功能外溢（function creep）與目的轉移的現實壓力亦不容忽視：一旦在未來建立可廣泛調用的唯一性身分層，在金融、就業或公共服務等領域被擴張使用，往往會形成制度慣性，屆時再透過個案審查加以抑制，勢必成本高昂且成效有限。更進一步而言，若僅以「同意」作為唯一的正當化依據，則在校園、社福、醫療等脆弱場域，或伴隨強誘因的設計下，極易淪為將人格權出讓作為對價之倫理困境。

---

[29] Reuters, 'Verified human': Worldcoin users queue up for iris scans, 2023-07-25（報導世界各地排隊以換取免費加密貨幣之情形）。

[30] World Bank, World Development Indicators（GDP per capita, current US$，2023）：Philippines 3,804.08；Kenya 1,952.30；Nigeria 1,596.64；United States 82,304.62。

[31] U.S. Government Accountability Office（GAO），Biometric Identification Technologies: Considerations to Help Address Stakeholder Concerns（建議以分級風險管理與差別影響為基礎；可作為替代、防錯與多因子治理之政策參照）

拾、研究結果與建議

一、研究結果

本文認為，以虹膜等不可逆生物特徵作為一般性、持續性之身分識別，有違反我國《個人資料保護法》之虞。並在憲法資訊自決保障脈絡下，原則上難以通過比例原則審查，理由如下：

現代真人驗證之替代方案存在且成熟，如裝置端活體偵測、行為式驗證、多因素組合、社交圖譜佐證或分級信任機制，均可在較低侵害下達成相當之治理效果[32]，在比例原則「必要性」審查方面容有疑義。

其次在權利實效性與可驗證性層面，即便項目團隊宣稱不留存原始影像，但若仍長期保存可供比對之模板與雜湊碼，則資料當事人依個資法第三條所享有之請求停止或刪除權便難以具體落實。且當事人於撤回同意後，該資料仍可被用於比對或辨識，實質上即構成持續處理，即與司法院釋字第 603 號解釋所揭示之資訊隱私保障意旨相背[33]。

再者，跨境比對與集中儲存使監管落差、救濟不可近性與雲端供應鏈風險成為結構性問題；專用硬體「Orb」之可信度與反竄改驗證若非由第三方持續稽核，也難以消解安全疑慮。最後，同意之真實性不足，加以強經濟誘因、資訊不對稱與未成年脆弱性之交互作用，使同意易流於形式，未能反映自由意思之實質形成。

綜上所述，在缺乏刪除可驗證、替代方案排除、跨境監管、硬體稽核及弱勢保障等配套下，以虹膜碼作為一般性身分識別制度，除非滿足嚴格例外條件，不宜以不可逆生物特徵作為一般身分層之政策選擇[34][35]。

二、建議

最後，從政策效果觀察，隨組合式低侵害驗證技術成熟，以不可逆特徵所能帶來之治理增益已呈邊際遞減；與其以高風險技術換取有限增益，宜採「替代方案優

---

[32] U.S. GAO, Biometric Identification Technologies: Considerations to Help Address Stakeholder Concerns (2024)，建議優先採用多因素與替代方案。

[33] 司法院釋字第 603 號解釋，確認「資訊隱私權」屬憲法第 22 條保障之隱私權內涵，人民得自主決定是否、何時、在何範圍與以何種方式向何人揭露個資，並對個資之使用享有知悉與控制及更正等權利。

[34] ZeroDayDispatch，Privacy, Surveillance, and Data Exploitation in the Global South（強誘因與資訊不對等使同意失真；全球南方之監管落差與剝削風險）；參見 Blockworks Opinion 對「以金錢誘因換取虹膜」的倫理批評。

[35] ZeroDayDispatch, Privacy, Surveillance, and Data Exploitation in the Global South (2023)，分析經濟誘因下同意的脆弱性。

先」與「附條件例外」之路徑，以兼顧治理與權利。本文主張：作為一般規範，採「原則禁止—例外許可」；僅於提出「無同等效果之較小侵害替代方案」之可反駁證據，並完成本地化處理、第三方稽核、撤回即失效與刪除可驗證、禁止目的外使用，以及獨立申訴與事故通報等嚴格條件，且設定明確功能邊界、限期與限域、公開稽核摘要並納入定期回顧與可被叫停機制時，方得試行。此一路徑與多國監管對高風險技術之「預防性暫停」[36]與比例原則之審查邏輯一致。

[36] Reuters，Spain temporarily bans Worldcoin（AEPD 命令立即停止蒐集與使用已得資料；法院維持暫禁）；葡萄牙 90 天暫停決定（高風險預防性介入）。

拾壹、參考文獻

一、中文資料

（一）法規與解釋

中華民國《個人資料保護法》。

司法院釋字第 603 號解釋。

司法院釋字第 689 號解釋。

司法院釋字第 696 號解釋。

（二）政府／機關文件與報告

國家發展委員會，《個資法執行現況與 GDPR 適足性認證》，2019。

國家發展委員會，《GDPR 之國際傳輸》，2019。

二、外文資料

（一）法律與規範文件

Agencia Española de Protección de Datos (AEPD), Press Release on provisional measures under GDPR Art. 66(1), 6 March 2024.

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Press Release on Worldcoin, 19 December 2024.

Comissão Nacional de Proteção de Dados (CNPD), Deliberação/2024/137, 2024.

European Data Protection Board (EDPB), Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, 2021.

European Data Protection Board (EDPB), Binding Decision concerning Worldcoin, 2025.

Federal Trade Commission (FTC), Policy Statement on Biometric Information, 2023.

Government Accountability Office (GAO), Biometric Identification Technologies: Considerations to Help Address Stakeholder Concerns, 2024.

Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14.

Information Commissioner's Office (ICO), How do we process biometric data lawfully? (Biometrics guidance page), 2024.

Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council on Artificial Intelligence, 2019.

Office of the Victorian Information Commissioner (OVIC), Biometrics and Privacy – Issues and Challenges, 2018.

Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).

（二）學術／技術文件與白皮書

Buterin, Vitalik, What do I think about biometric proof of personhood?, 2023.

Lutz, Jonas; Albrecht, Martin R.; et al., Compressed to Zero: The Silent Strings of Proof of Personhood, 2023.

Patel, V. et al., Cancelable Biometrics: A Review, 2025.

Worldcoin, Worldcoin Whitepaper, n.d.

（三）政策評論、新聞與專欄

Access Now, Bodily Harms: Mapping the Risks of Emerging Biometric Tech, 2023.

Blockworks (Opinion), Worldcoin isn't as bad as it sounds: It's worse, 2023.

GDPR Advisor, Biometric Data & GDPR Compliance, 2024.

Reuters, Spain temporarily bans Worldcoin / Scrutiny of iris-scanning Worldcoin grows, 2024.

The Block, Vitalik Buterin expresses concerns over Worldcoin, 2023.

The Wall Street Journal, Worldcoin Is Battling With Governments Over Your Eyes, 2024.

Troutman Pepper, ICO's Biometrics Guidance: Lawful Basis and Proportionality, 2024.

ZeroDayDispatch, Worldcoin: Privacy, Surveillance, and Data Exploitation in the Global South, 2023.