Orsini V, 'Tutela dei dati biometrici e prerogative statali: il caso Worldcoin tra GDPR ed eIDAS 2' (2024) Special Issue EJPLT.
DOI:

EJPLT
ISSN 2704-8012



Tutela dei dati biometrici e prerogative statali: il caso Worldcoin tra GDPR ed eIDAS 2

Biometric Data Protection and State Prerogatives: the Worldcoin Case between GDPR and eIDAS 2

VINCENZO ORSINI
Post-doctoral Research Fellow and Contract Professor
University of Salerno

Abstract
Il contributo analizza il progetto Worldcoin alla luce della disciplina europea in materia di protezione dei dati personali e identificazione digitale. Dopo aver illustrato il funzionamento tecnico del sistema, si esaminano i rilievi sollevati dalle autorità garanti, con particolare attenzione alla validità del consenso e ai diritti degli interessati. Si discutono inoltre l'impatto dell'azione regolatoria e le implicazioni istituzionali legate all'emergere di identità digitali autogestite, anche in rapporto al nuovo Portafoglio Europeo di Identità Digitale previsto da eIDAS 2.

The paper examines the Worldcoin project under the European legal framework on personal data protection and digital identity. After outlining the system's technical structure, it addresses the concerns raised by data protection authorities, focusing on consent and data subject rights. It further considers the regulatory response and the institutional implications of self-sovereign digital identities, especially in light of the new European Digital Identity Wallet introduced by eIDAS 2.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Worldcoin; GDPR; consenso condizionato; diritto alla cancellazione; eIDAS 2; identificazione digitale; sovranità statale.

Sommario: 1. Il caso Worldcoin. – 2. Il funzionamento del protocollo informatico. – 3. I rilievi delle autorità di controllo. – 4. Alcune note critiche. – 5. L'impatto dell'azione regolatoria. – 6. Il ruolo degli Stati nel processo di identificazione.

1. Il caso Worldcoin.

Il progetto Worldcoin [1] è emblematico del complesso rapporto tra innovazione e regole, dovendosi sviluppare compatibilmente alle norme in materia di protezione dei dati personali e rischiando, al contempo, di invadere prerogative statali in materia di identificazione dei cittadini[2]. Questo progetto, infatti, nasce con l'ambizione di creare una rete globale di identità digitali univoche basate su dati biometrici e tecnologia a registri distribuiti. A questo scopo, Worldcoin si propone di identificare i propri utenti tramite scansione dell'iride, per poi assegnargli un portafogli, denominato "World ID", da gestire mediante tecnologia a registri distribuiti[3].

Tale progetto, pertanto, costituisce un significativo banco di prova per valutare la portata della tutela offerta dal Regolamento 2016/679/UE (GDPR) nel trattamento, su larga scala, di dati biometrici. Inoltre, collocandosi all'interno del paradigma delle Self-Sovereign Identities (SSI)[4], ossia identità

[1] Nel corso del 2024, il progetto originariamente noto come *Worldcoin* ha ufficialmente cambiato nome in "World Network", abbreviato spesso in "World", per riflettere una missione più ampia che va oltre la semplice distribuzione di una criptovaluta. Il nuovo nome intende rappresentare una rete globale di identità umane verificate, al centro dello sviluppo dell'intelligenza artificiale e delle infrastrutture digitali future (cfr. WORLD, *Hello World: The 5 key announcements from the new world event in San Francisco*, 17 ottobre 2024. Consultabile online: https://world.org/blog/announcements/hello-world-5-key-announcements-from-new-world-event-san-francisco). Tuttavia, per maggiore chiarezza, in questo contesto continueremo a utilizzare il termine "Worldcoin" come riferimento all'intero ecosistema, inclusi i suoi componenti principali: World ID, World App, World Chain e il token WLD. Questa scelta è motivata dal fatto che "Worldcoin" rimane il nome con maggiore capacità distintiva. Pertanto, ogni riferimento a "Worldcoin" in questo testo comprende l'intero progetto, sia nella sua denominazione originale che in quella attuale.

[2] La letteratura giuridica specificamente dedicata al progetto *Worldcoin* è, allo stato, ancora estremamente limitata, soprattutto in ambito italiano. Ciononostante, alcuni contributi stranieri, pur affrontando il tema solo indirettamente, forniscono spunti utili per inquadrare criticamente le implicazioni giuridiche del progetto, in particolare sotto il profilo dell'identità digitale: S. JAIN, C. SPELLISCY, S. VANCE-LAW, S. MOORE, *AI and Democracy's Digital Identity Crisis*, in *Stanford Journal of Blockchain Law & Policy*, 2024, vol. 7, 56-75; V.W. KARIITHI, *Navigating the Web3 Revolution: Regulatory Strategies for Kenya*, in *Journal of Intellectual Property and Information Technology Law*, 2024, vol. 4, 101-165; M. MANNAN, *From Digital Humanitarianism to Crypto-Humanitarianism*, in *International Trade and Business Law Review*, 2024, vol. 24, 121-148; M. ROBLES-CARRILLO, *Digital identity: an approach to its nature, concept, and functionalities*, in *International Journal of Law and Information Technology*, 2024, vol. 32, 1-21; P. OHLHAVER, M. NIKULIN, P. BERMAN, *Compressed to 0: The Silent Strings of Proof of Personhood*, in *Stanford Journal of Blockchain Law & Policy*, 2025, vol. 8, 60-113; J.E. COHEN, *Oligarchy, State, and Cryptopia*, in *Fordham Law Review*, 2025 vol. 94 (in corso di pubblicazione); H.J. ALLEN, *Fintech and Techno-Solutionism*, in *Southern California Law Review*, 2025 (in corso di pubblicazione), 1-68.

[3] Per una descrizione complessiva degli obiettivi, dell'architettura tecnica e dei meccanismi di funzionamento del progetto Worldcoin, si V. WORLD, *A New Identity and Financial Network* (ultimo accesso 12 aprile 2025). Consultabile online: https://whitepaper.world.org/.

[4] Il termine Self-Sovereign Identity è stato coniato nel 2016 dall'informatico americano Christopher Allen, che in un articolo di blog proponeva un modello di identità digitale in cui l'individuo detiene il pieno controllo sulle proprie credenziali, senza dipendere da autorità centrali. Nell'articolo, l'autore ricostruiva l'evoluzione delle identità digitali e definiva dieci linee guida a cui attenersi nella costituzione di un SSI: reale esistenza di

digitali gestite autonomamente dagli utenti, solleva interrogativi sostanziali circa il ruolo tradizionale degli Stati nell'attribuzione delle identità.

Il presente contributo, quindi, si pone l'obiettivo di valutare basi giuridiche e limiti imposti dal quadro normativo europeo per il trattamento dei dati biometrici; e di evidenziare le implicazioni istituzionali e regolatorie legate all'emergere delle SSI, tenendo conto della recente revisione del Regolamento eIDAS. A tal fine, il lavoro prenderà avvio dalla ricostruzione del funzionamento dell'infrastruttura Worldcoin, per poi valutare criticamente i rilievi mossi dalle autorità di controllo e l'impatto di questi ultimi sullo sviluppo della tecnologia. Successivamente, verranno approfonditi i rischi di interferenza con le prerogative sovrane degli Stati, evidenziando come l'adozione su larga scala di sistemi decentralizzati di identità potrebbe ridefinire le dinamiche istituzionali e giuridiche tra pubblico e privato.

2. Il funzionamento del protocollo informatico.

Worldcoin si propone l'obiettivo di risolvere il cd. unique-human problem, che consiste nella difficoltà - sempre più attuale in un'epoca segnata dalla proliferazione di intelligenze artificiali, profili multipli e attività automatizzate - di associare un determinato profilo digitale a una persona fisica e di impedire che ne abbia più di uno[5]. L'iniziativa si fonda sull'idea di attribuire a ciascun individuo un identificatore digitale univoco, World ID, da impiegare in ambiente informatico per dimostrare la propria natura umana senza dover necessariamente rivelare la propria reale identità ("proof of humanity")[6].

Per generare l'identificatore World ID, il protocollo informatico si serve dei dati biometrici dell'individuo, raccolti tramite un dispositivo denominato "Orb"[7]. Tale dispositivo, di forma sferica, cattura immagini ad alta risoluzione e

---

ogni utente, pieno controllo sulla propria identità, accesso ai propri dati, trasparenza dei sistemi, persistenza delle identità, portabilità, interoperabilità, consenso informato, minimizzazione della divulgazione dei dati e protezione dei diritti degli utenti. Cfr. C. ALLEN, *The Path to Self-Sovereign Identity*, 2016. Consultabile online: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/. Si v., inoltre, A. PREUKSCHAT, D. REED, *Self-Sovereign Identity. Decentralized digital identity and verifiable credentials*, 2021, New York. In Europa, l'interesse istituzionale per le SSI si è concretizzato nel 2019 con la creazione dell'European Self-Sovereign Identity Framework (ESSIF) come parte integrante dell'European Blockchain Services Infrastructure (EBSI). Questa iniziativa pubblica mira a sviluppare un sistema di identità digitale interoperabile e decentralizzato, allineato ai principi del GDPR e alle disposizioni del Regolamento eIDAS.

[5] Vitalik Buterin, celebre fondatore del protocollo Ethereum, in un breve articolo del 2023 descriveva il c.d. unique-human problem come l'esigenza di assicurare che ogni identità digitale corrisponda a una specifica persona fisica e che questa non abbia più di un profilo. Cfr. V. Buterin, *What do I think about biometric proof of personhood?*, 24 luglio 2023. Consultabile online: https://vitalik.eth.limo/general/2023/07/24/biometric.html.

[6] Proof-of-Humanity (PoH) e Proof of Personhood (PoP) sono espressioni sostanzialmente equivalenti, utilizzate per indicare meccanismi volti a verificare digitalmente l'unicità e l'umanità di un individuo. La prima è adottata specificamente nell'ambito del progetto Worldcoin, mentre la seconda ha un impiego più ampio e generico nel dibattito sulle SSI.

[7] Gli Orb sono gestiti da World Operators, imprenditori locali indipendenti che collaborano con la Worldcoin foundation, a titolo gratuito, per offrire servizi di verifica. Costoro informano gli utenti, forniscono assistenza durante il processo di verifica e facilitano l'attribuzione di un World ID. Per diventare un operatore, è necessario registrarsi tramite il portale ufficiale di Worldcoin e superare un processo di valutazione. Sempre tramite sito internet, è anche possibile consultare la mappa aggiornata dei punti di verifica attivi e prenotare un appuntamento. Per ulteriori informazioni sul funzionamento del dispositivo, si v. https://www.toolsforhumanity.com/orb.

multispettrali di ciascuna iride, un'immagine dell'occhio e un'immagine del viso. Queste immagini vengono elaborate localmente nell'Orb, utilizzando modelli di intelligenza artificiale per verificare che si tratti di una persona fisica e che sia viva. Sulla base delle immagini raccolte, tramite un algoritmo di cifratura, l'Orb genera un codice alfanumerico. Questo codice, che è un identificatore univoco corrispondente ai dati biometrici raccolti, è chiamato "Iris Code" e viene confrontato in tempo reale con i codici precedentemente raccolti e conservati per verificare se la persona dispone già di un World ID.

Stando alle informazioni rese note dalla Worldcoin Foundation, promotrice del progetto, al termine del processo le immagini catturate (volto e iride) vengono immediatamente eliminate dal dispositivo Orb[8]. L'Iris Code, invece, viene successivamente convertito, tramite avanzate tecniche crittografiche, in una pluralità di frammenti cifrati che vengono archiviati in banche dati gestite da trusted third parties (TTP), connotate dal carattere dell'indipendenza[9]. In questo modo, i singoli frammenti non dovrebbero consentire né l'identificabilità dell'utente, né la ricostruibilità dell'Iris Code[10].

Occorre puntualizzare che il complesso meccanismo ideato da Worldcoin si serve di due tipi differenti di conservazione dei dati raccolti: il primo, reversibile, consiste nella conservazione dei frammenti di Iris Code sui server (tradizionali) gestiti dalle TTP; il secondo, irreversibile, consiste nella gestione dei World ID tramite tecnologia a registri distribuiti (che rende inalterabili le informazioni)[11]. Il primo trattamento, che è più problematico dal punto di vista

---

[8] Invero, gli utenti possono scegliere se autorizzare la conservazione delle immagini acquisite dall'Orb (tramite un meccanismo "opt-in") per migliorare la sicurezza del sistema attraverso l'impiego delle immagini per finalità di addestramento algoritmico e per l'aggiornamento automatico del codice biometrico. Dal punto di vista tecnico, le immagini degli utenti che scelgono di consentire la conservazione sono inizialmente salvate su un disco rigido criptato all'interno dell'Orb e successivamente caricate su server sicuri. In ogni caso, l'utente può in sempre revocare il consenso e cancellare le proprie immagini tramite la World App (cfr. WORLD, *A New Identity and Financial Network*, cit.).

[9] Come si avrà modo di sottolineare nelle pagine seguenti (*infra*, §5), a seguito di interlocuzioni con le autorità di controllo europee, Worldcoin ha modificato in modo sostanziale il meccanismo di conservazione degli Iris Code. Infatti, il 15 maggio 2024, Worldcoin ha introdotto un nuovo sistema di trattamento dei dati biometrici basato sulla tecnologia Secure Multiparty Computation (SMPC). Attraverso questo sistema, gli Iris Code vengono scomposti in "shares", ovvero sequenze numeriche casuali distribuite tra i partecipanti della rete. A partire da gennaio 2025, i partecipanti al sistema SMPC includono Nethermind, l'Università di Erlangen-Norimberga (FAU) e il Center for Responsible Decentralized Intelligence (RDI) dell'Università di Berkeley, con il supporto del Blockchain Center dell'Università di Zurigo. Cfr. WORLD, *Introducing AMPC: Another leap in privacy and performance for World ID*, 17 ottobre 2024. Consultabile online: https://world.org/blog/engineering/introducing-ampc-another-leap-privacy-performance-world-id. Si v., inoltre, R. BLOEMEN, B. GILLESPIE, D. KALES, P. SIPPL, R. WALCH, *Scaling Private Iris Code Uniqueness Checks to Millions of Users*, in *Cryptology ePrint Archive*, n. 705, 2024, 1-22.

[10] Decisamente scettica, in tal senso, si mostra l'autorità di controllo bavarese, la quale rileva che i frammenti, se ricomposti, renderebbero possibile la piena ricostruzione delle scansioni dell'iride. Tale rischio risulterebbe ulteriormente accentuato dal fatto che entrambe le parti coinvolte nel sistema SMPC — inizialmente limitato a due attori — si avvalevano del medesimo fornitore di servizi cloud, Amazon AWS. Cfr. BayLDA, decisione del 13 dicembre 2024, EDPBI:DEBY:OSS:D:2024:1594. Consultabile online: https://www.edpb.europa.eu/system/files/2025-02/decision1594_0.pdf.

[11] Poiché la gestione degli Iris Code non avviene mediante tecnologia a registri distribuiti, bensì attraverso un'infrastruttura centralizzata, viene meno uno degli ostacoli principali che solitamente complicano l'applicazione del GDPR nell'ambito del c.d. Web 3.0. In particolare, l'assenza del carattere dell'immutabilità – tratto distintivo delle blockchain – consente una più agevole individuazione dei soggetti responsabili del trattamento, nonché l'effettiva implementazione dei diritti riconosciuti agli interessati, come il diritto alla cancellazione, alla rettifica e alla limitazione del trattamento. Oltre alle linee guida recentemente elaborate dall'EDPB sul trattamento dei dati personali mediante tecnologie blockchain (2/2025 dell'8 aprile 2025), si v. M. FINCK, *Blockchains and Data Protection in the European Union*, in *European Data Protection Law Review*, I, 2018, 17-35; C. MILLARD, *Blockchain and Law: Incompatible Codes?*, in *Computer Law & Security Review*, IV, 2018,

giuridico, serve al protocollo informatico per verificare che l'utente non disponga già di un Iris Code e, quindi, di un World ID. Il secondo trattamento, invece, serve all'utente per l'accesso a servizi digitali che richiedono la proof of humanity dell'utente.

Lo strumento operativo principale di cui si serve l'utente è la "World App", applicazione mobile che funge da portafogli per la gestione del World ID. L'applicazione consente, oltre alla gestione dei processi identificativi, l'esecuzione di transazioni in criptovaluta, con particolare riferimento al token nativo denominato "WLD". Tale token, conforme allo standard tecnico ERC-20[12], viene attribuito gratuitamente agli utenti che abbiano completato con successo la procedura di verifica, e svolge una duplice funzione: da un lato, rappresenta uno strumento di incentivazione economica, dall'altro, costituisce un mezzo di partecipazione attiva all'interno dell'infrastruttura Worldcoin. Il token WLD può essere impiegato per effettuare pagamenti, interagire con servizi digitali integrati nel sistema e, in prospettiva, consentirà agli utenti di contribuire ai processi decisionali concernenti l'aggiornamento del protocollo, attraverso meccanismi di governance decentralizzata[13].

---

p. 843-846; R. HERIAN, *Regulating disruption: blockchain, GDPR, and questions of data sovereignty*, in *Journal of Internet Law*, II, 2018, 8-16; L. MOEREL, *Blockchain & data protection …and why they are not on a collision course*, in *European Review of Private Law*, VI, 2018, 825-851; L. PIATTI, *"Blockchain", decentralizzazione e "privacy": un nuovo approccio del diritto*, in *Cib. dir.*, I-II, 2018, 179-196; F. RAMPONE, *I dati personali in ambiente blockchain tra anonimato e pseudonimato*, in *Cib. dir.*, III, 2018, 457-478; T. BUOCZ, T. EHRKE-RABEL, E. HÖDL, I. EISENBERGER, *Bitcoin and the GDPR: allocating responsibility in distributed networks*, in *Computer Law & Security Review*, II, 2019, 182-198; A.E. DEKHUIJZEN, *Call for action on the EDPB to provide guidance concerning GDPR and blockchain: is public blockchain sustainable under the GDPR?*, in *Computer Law Review International*, II, 2019, 33-36; A.M. GAMBINO, C. Bomprezzi, *Blockchain e protezione dei dati personali*, in *Dir. inf.*, III, 2019, 619-646; M. Schellekens, *Conceptualizations of the controller in permissionless blockchains*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, II, 2020, 215-227; A. GIANNOPOULOU, *Putting data protection by design on the blockchain*, in *European Data Protection Law Review*, III, 2021, 388-399; M.T. GIORDANO, *Blockchain and the GDPR: new challenges for privacy and security*, in B. CAPPIELLO, G. CARULLO (a cura di), *Blockchain, Law and Governance*, Berlino, 2021, 275-286; C. IORIO, *Legal issues concerning the circulation and processing of data in the digital age*, in *EJPLT*, II, 2022, 153-168. Si consenta inoltre il rinvio a V. ORSINI, *La protezione dei dati personali nell'epoca delle tecnologie a registri distribuiti*, in *Tecnologie e Diritto*, II, 2023, 377-396.

[12] È ormai noto che l'ERC-20 (Ethereum Request for Comment 20) è uno standard tecnico adottato per l'emissione e la gestione di token fungibili sulla blockchain di Ethereum. Esso definisce un insieme uniforme di regole — relative, tra l'altro, al trasferimento dei token, alla registrazione dei saldi e all'offerta totale — con l'obiettivo di assicurare l'interoperabilità tra token, smart contract e applicazioni decentralizzate all'interno dell'ecosistema Ethereum.

[13] Non è questa la sede per affrontare il tema della qualificazione giuridica del token WLD. Stando alle informazioni riportate nel whitepaper di Worldcoin, si tratterebbe di un "utility token" utilizzabile esclusivamente all'interno della piattaforma per facilitare interazioni tra partecipanti e, in futuro, per definire la governance della piattaforma sul piano tecnico. In considerazione dell'assenza di un diritto al rimborso o alla conversione in denaro fiat (o in altri crypto-asset), il token WLD non sarebbe considerabile come moneta elettronica. Inoltre, non attribuendo alcun diritto — né di natura patrimoniale né amministrativa — nei confronti della Worldcoin Foundation o dei suoi soggetti affiliati, non sarebbe qualificabile come strumento finanziario (cfr. WORLD, *A New Identity and Financial Network*, cit.). Resta tuttavia fondamentale precisare che la qualificazione giuridica di un token non può basarsi sul *nomen* attribuito dall'emittente, bensì deve essere desunta dalle sue caratteristiche funzionali ed economiche effettive. Per ulteriori considerazioni in arg. si rinvia ad A. DI AMATO, V. ORSINI, *Beyond Bitcoin: Understanding Legal Boundaries of Blockchain Technology*, in *EJPLT*, I, 2022, 112-121; V. ORSINI, *Della natura giuridica delle criptovalute*, in *Diritto del Mercato Assicurativo e Finanziario*, I, 2021, 15-77. Tra i contributi più recenti in materia, si v. A. MINTO, A. URBANI, *Brevi riflessioni sul coordinamento tra "MICAR" e assetti normativi limitrofi (con particolare attenzione alla disciplina sulla prestazione dei servizi di investimento e a quella relativa ai servizi di pagamento)*, in *Banca impresa,* III, 2024, 351-368; U. MALVAGNA, *"Digital cash" e regolamento MiCA: tra pagamento e intermediazione finanziaria*, in *Banca borsa tit. cred.*, IV, 2024, 583-600; D. SARTI, *La funzione non finanziaria dei token MiCAR*, in *Orizzonti del diritto commerciale*, III, 2024, 764-811; C. SANDEI, *La nuova disciplina*

3. I rilievi delle autorità di controllo.

Come prevedibile, un progetto di tale portata ha sollevato numerosi interrogativi in ordine alla raccolta massiva di dati biometrici e alla loro conservazione, seppur in forma cifrata, da parte di un ente privato. In ambito europeo, diverse autorità di controllo hanno avviato indagini sul funzionamento del progetto Worldcoin[14]. Tra queste, un ruolo di primo piano è stato assunto dalla Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)[15], autorità tedesca competente in qualità di autorità capofila ai sensi

europea delle cripto-attività: un passo avanti (e due indietro)?, ivi, 861-875; M. DE MARI, *"Utility token"*, ivi, 915-929; R. LENER, S.L. FURNARI, *La "decentralizzazione" dei mercati finanziari. Innovazione tecnologica e nuove istanze di regolamentazione*, in *Riv. trim. dir. econ.*, I, 2024, 447-466; G. SCHNEIDER, *Le cripto-attività quali prodotti finanziari: il fine giustifica i mezzi?*, in *Giur. comm.*, VI, 2023, 959-982; F. ANNUNZIATA, *La disciplina europea del mercato delle cripto-attività (MiCAR)*, in *Riv. società*, V-VI, 2023, 923-963; V. TROIANO, *Moneta elettronica e "token" utilizzabili come mezzo di pagamento tra MICAR, proposta di PSD 3 e adattamento dell'ordinamento interno*, in *Riv. trim. dir. econ.*, IV, 2023, 151-174; M. CIAN, *Noterelle su finanziarietà e non finanziarietà nei "crypto-assets": la Suprema Corte sulla natura del servizio di "exchange"*¸ in *Banca borsa tit. cred.*, I, 2023, 3-9.

[14] Oltre alle indagini avviate dalle autorità europee, il progetto Worldcoin ha suscitato preoccupazioni e azioni regolatorie anche in diverse giurisdizioni extraeuropee. Nel Regno Unito, l'Information Commissioner's Office (ICO) ha rilasciato una dichiarazione in cui sottolinea l'importanza di condurre una valutazione d'impatto sulla protezione dei dati (DPIA) prima di iniziare qualsiasi trattamento di dati biometrici, nonché la necessità di una base giuridica valida per il trattamento di simili dati [cfr. ICO, *Statement on WorldCoin*, 31 luglio 2023. Consultabile online: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/07/ico-statement-on-worldcoin/]. A Hong Kong, l'ufficio del Privacy Commissioner for Personal Data (PCPD) ha riscontrato violazioni delle norme sulla privacy da parte di Worldcoin - in particolare riguardo alla raccolta e conservazione eccessiva di dati biometrici e alla scarsa trasparenza del consenso informato - e, di conseguenza, ha ordinato la cessazione di ogni attività di scansione e raccolta di immagini dell'iride e del volto nel territorio [cfr. PCPD, *The Operation of the Worldcoin Project in Hong Kong Contravenes the Personal Data (Privacy) Ordinance*, 22 maggio 2024, R24 - 01335. Consultabile online: https://www.pcpd.org.hk/english/enforcement/commissioners_findings/files/r24_01335_e.pdf]. In Brasile, il Consiglio Direttivo dell'Autoridade Nacional de Proteção de Dados (ANPD) ha recentemente confermato la decisione n. 3/2025/FIS/CGF, in cui intimava la sospensione immediata delle compensazioni finanziarie offerte in cambio delle scansioni iridee, respingendo la richiesta di un'estensione di 45 giorni [cfr. ANPD, *Despacho Decisório PR/ANPD nº 6/2025*. Consultabile online: https://www.in.gov.br/web/dou/-/despacho-decisorio-pr/anpd-n-6/2025-611866801; Id., *Despacho Decisório PR/ANPD nº 18/2025*. Consultabile online: https://www.in.gov.br/web/dou/-/despacho-decisorio-pr/anpd-n-18/2025-619528039]. In Kenya, l'Office of the Data Protection Commissioner (ODPC) ha avviato d'ufficio un'indagine il 2 agosto 2023 ove ha riscontrato numerose violazioni della normativa keniana in materia di protezione dei dati personali, tra cui: l'assenza di valido consenso al trattamento dei dati; l'illiceità del trasferimento transfrontaliero di tali dati; la mancata conduzione di una valutazione d'impatto [cfr. ODPC, *Complaint no. 1394 of 2023*, CONF/1/7/4 vol 1(31). Consultabile online: https://www.odpc.go.ke/wp-content/uploads/2025/01/20230906-SUO-MOTU-WORLDCOIN-FOUNDATION-TOOLS-FOR-HUMANITY-TOOLS-FOR-HUMANITY-GMBH.pdf].

[15] Nell'aprile 2023, su impulso dell'autorità di controllo francese, la BayLDA ha avviato un'indagine sul progetto Worldcoin, chiedendo la produzione di una valutazione d'impatto. Dopo i primi accertamenti, a luglio 2023, in coincidenza con il lancio ufficiale del progetto, è stata avviata una fase ispettiva approfondita, comprensiva di visite presso le sedi delle società coinvolte. Con una nota del 23 dicembre 2023, la BayLDA ha comunicato che le misure di sicurezza adottate non erano conformi all'art. 32 GDPR, spingendo la Worldcoin Foundation a introdurre, nel maggio 2024, un nuovo sistema crittografico (SMPC). Tuttavia, l'autorità ha ritenuto necessarie ulteriori verifiche e ha avviato il confronto con le altre autorità europee. Il 30 aprile 2024, è stata trasmessa alla Worldcoin Foundation una prima bozza di decisione, seguita da una seconda il 6 giugno 2024, alla luce dei commenti ricevuti. La Foundation ha replicato, ma senza fornire nuovi elementi sostanziali. Con la decisione finale, del 13 dicembre 2024, la BayLDA ha ordinato la cancellazione dei dati biometrici, la sospensione del trattamento e l'adeguamento alle disposizioni del GDPR, tra cui il diritto alla cancellazione per gli interessati. Sono state fissate scadenze precise e previste sanzioni economiche in caso di inadempimento, oltre al pagamento delle spese procedimentali. Cfr. BayLDA, *13. Tätigkeitsbericht*, 2023. Consultabile online: https://www.lda.bayern.de/media/baylda_report_13.pdf; Id.,

dell'art. 56 GDPR, in quanto la Worldcoin Foundation opera nel territorio dell'Unione tramite la controllata ZipCode GmbH, con sede a Erlangen (Baviera)[16]. In tale veste, la BayLDA è abilitata ad agire quale principale interlocutore del titolare del trattamento, pur nel rispetto dei meccanismi di cooperazione e coerenza previsti dal Regolamento. Cionondimeno, facendo leva sulla deroga di cui all'art. 66 GDPR, alcune autorità nazionali hanno avviato procedure d'urgenza autonome. In particolare, l'Agencia Española de Protección de Datos (AEPD), con delibera del 26 febbraio 2024, ha ordinato la sospensione immediata delle operazioni di raccolta e trattamento dei dati biometrici (immagini dell'iride, degli occhi e del volto) sul territorio spagnolo, nonché il blocco dei dati già acquisiti[17]. Analogo provvedimento è stato adottato dalla Comissão Nacional de Protecção de Dados (CNPD) portoghese il 25 marzo 2024, in seguito alla raccolta di dati biometrici relativi a oltre 300.000 soggetti[18]. In Italia, pur in assenza di attività di raccolta effettiva, il Garante per la Protezione dei Dati Personali (GPDP) ha rivolto un formale avvertimento alla società in data 21 marzo 2024[19].

I rilievi avanzati dalle autorità di controllo convergono su un punto essenziale: l'interazione problematica tra la conservazione a lungo termine di dati biometrici e la tutela dei dati personali.

In primo luogo, viene messa in discussione la validità del consenso quale base giuridica per il trattamento dei dati biometrici, in quanto ritenuto non sufficientemente libero, specifico, informato e inequivocabile, in violazione dei requisiti di cui all'art. 4, n. 11, del GDPR[20]. Com'è noto, l'art. 9 del Regolamento stabilisce un divieto generale al trattamento dei dati biometrici intesi a identificare in modo univoco una persona fisica, salvo che l'interessato abbia prestato un consenso esplicito ai sensi del paragrafo 2, lettera a)[21]. Nel caso di

---

14. Tätigkeitsbericht, 2024. Consultabile online: https://www.lda.bayern.de/media/baylda_report_14.pdf; Id., decisione del 13 dicembre 2024, cit.

[16] Il 27 giugno 2024 la società ha modificato la propria denominazione in "Worldcoin Europe GmbH" e trasferito la sede legale a Monaco di Baviera, senza che ciò incidesse sulla competenza territoriale dell'autorità capofila. Com'è noto, infatti, l'autorità di controllo dello stabilimento principale (o unico) del titolare o del responsabile del trattamento è competente ad agire in qualità di autorità capofila nei trattamenti transfrontalieri, cooperando con le altre autorità interessate per l'adozione di una decisione condivisa. Nel procedimento a carico di Worldcoin, le autorità coinvolte risultano essere quelle di: Germania, Paesi Bassi, Portogallo, Svezia, Italia, Norvegia, Ungheria, Francia, Irlanda, Estonia, Lussemburgo, Danimarca, Polonia, Croazia, Belgio, Lituania, Romania, Slovacchia, Finlandia, Spagna e Austria.

[17] Cfr. AEPD, *Acuerdo de adopción de medida provisional*, EXP202312448, 26 febbraio 2024. Consultabile online: https://www.aepd.es/documento/co-000297-2023-medida-provisional.pdf.

[18] Cfr. CNPD, *Deliberação/2024/137*, 25 marzo 2024. Consultabile online: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/123142. Si v., inoltre, Id., *Deliberação/2024/279*, 9 luglio 2024. Consultabile online: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/123157.

[19] Cfr. GPDP, *Provvedimento del 21 marzo 2024*. Consultabile online: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9998877.

[20] L'assenza dei presupposti necessari determina l'invalidità del consenso reso dall'interessato. Tuttavia, come evidenzia autorevole dottrina, «sotto il profilo della patologia della figura si segnala un netto distacco rispetto alla disciplina dei vizi del volere in materia contrattuale. L'interessato non deve esercitare un'azione di annullamento ma agire per l'accertamento della illiceità dell'attività relativa ai suoi dati posta in essere nonostante la mancanza di un valido consenso» [cfr. S. PATTI, *Art. 23*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, I, 2007, 551].

[21] La definizione di "dato biometrico", assente nell'impianto della Direttiva 95/46/CE, è il frutto dell'esperienza maturata nei singoli ordinamenti nazionali e in seno al Working Party 29, dettata dalle istanze di protezione sorte nel contesto dell'evoluzione tecnologica [in arg. si v., *ex multis*, C. JASSERAND, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *European Data Protection Law*

specie, tuttavia, la validità del consenso risulterebbe compromessa sotto una pluralità di profili. In particolare, secondo l'analisi condotta dalla BayLDA, gli utenti non sarebbero stati adeguatamente informati circa i rischi connessi al trattamento dei propri dati biometrici, con particolare riferimento alla conservazione a lungo termine degli stessi [22]. Inoltre, il consenso prestato risulterebbe parziale, in quanto limitato alle fasi iniziali del trattamento – segnatamente, la generazione dell'Iris Code a partire dalle immagini acquisite tramite il dispositivo Orb e il successivo confronto "attivo" con i codici già registrati – e non esteso alla fase più invasiva e duratura, rappresentata dalla conservazione degli Iris Code ai fini del confronto "passivo" con i dati acquisiti da nuovi utenti[23]. Di conseguenza, il consenso risulterebbe viziato in quanto fondato su un'informativa lacunosa e poco trasparente, e perché circoscritto alla sola porzione del trattamento meno impattante sui diritti e le libertà fondamentali degli interessati. A ciò si aggiunge che la previsione di un

Review, 3, 2016, 297-311; R. DUCATO, *I dati biometrici*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1285-1322; I. ALAGNA, *Biometria*, in AA.VV., *Codice della Disciplina Privacy*, Milano, 2019, 955-970; L. FEROLA, *Le "misure di garanzia" a tutela dei dati biometrici, genetici e della salute*, in F. PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021, 411-446; A. THIENE, L. SCAFFARDI, *Art 9. Trattamento di categorie particolari di dati personali*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, 239-261]. Il legislatore italiano, ad esempio, pur non qualificando espressamente i dati biometrici come dati sensibili, prevedeva già alcune garanzie specifiche per il trattamento di simili dati (all'art. 37, comma 1, lett. a, ed all'art. 55 del D.lgs. 30 giugno 2006, n. 196 – Codice della Privacy). Il Garante, inoltre, ha rivestito un ruolo fondamentale per la disciplina del trattamento di dati biometrici, non solo attraverso la propria attività autorizzativa e prescrittiva, ma anche normativa (significative, in materia, sono le linee-guida in materia di riconoscimento biometrico e firma grafometrica - 12 novembre 2014, n. 513). A livello europeo, invece, il tema è stato affrontato in diversi pareri del Working Party 29, tra cui il documento di lavoro sulla biometria (1° agosto 2003, WP 80) e il parere sugli sviluppi nelle tecnologie biometriche (27 aprile 2012, n. 3). Oggi, il GDPR definisce i "dati biometrici" «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici» (art. 4, par. 1, n. 14). Cionondimeno, si qualificano come dati sensibili solo i dati biometrici sottoposti a un trattamento tecnico idoneo a renderlo utilizzabile per l'identificazione individuale (art. 9, par. 1). In tal senso, l'EDPB ha chiarito che l'elemento qualificante del dato biometrico non è la mera rappresentazione fisica, come quella resa in un'immagine o una registrazione vocale, bensì la sua finalizzazione all'identificazione mediante procedure automatizzate (cfr. Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, 29 gennaio 2020; Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto, 26 aprile 2023). Proprio in virtù della loro natura fortemente identificativa e difficilmente revocabile, i dati biometrici rientrano tra le categorie particolari di dati personali il cui trattamento è in linea di principio vietato, salvo il ricorrere di specifiche condizioni, tra cui il consenso esplicito dell'interessato (art. 9, par. 2, lett. a). La disciplina europea è completata dalle disposizioni nazionali introdotte dal D.lgs. 10 agosto 2018, n. 101 al Codice della Privacy: l'art. 2-*sexies*, sul trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante; l'art. 2-*septies*, che attribuisce al Garante la facoltà di disporre misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute.

[22] La rappresentazione dell'iride costituisce una delle forme più affidabili di dato biometrico ai fini dell'identificazione individuale. La sua efficacia è accresciuta dalla semplicità di utilizzo e dalla versatilità applicativa, favorita dall'ampia disponibilità di immagini facciali provenienti tanto da contesti pubblici (videosorveglianza urbana, stazioni, semafori) quanto privati (luoghi di lavoro, esercizi commerciali, social network). A differenza delle impronte digitali – che si deteriorano facilmente, possono sovrapporsi ad altre e richiedono un contatto diretto – l'iride può essere verificato a distanza, in modo discreto e non invasivo. Proprio tali caratteristiche, tuttavia, amplificano i rischi per i diritti fondamentali degli interessati, in particolare laddove il trattamento avvenga attraverso l'archiviazione centralizzata di questi codici biometrici in un'unica banca dati, come nel caso del progetto Worldcoin. L'accesso non autorizzato da parte di malintenzionati (hacker o governi stranieri) a una simile infrastruttura potrebbe comportare effetti sistemici difficilmente quantificabili, aggravati dall'assenza di cifratura dei dati biometrici archiviati (cfr. BayLDA, decisione del 13 dicembre 2024, cit., parr. 536-550).

[23] *Ibid.*, parr. 120, 125, 278.

incentivo economico, sotto forma di token WLD gratuiti, si presta a compromettere significativamente la libertà del consenso, orientando la scelta dell'interessato su basi meramente economiche, piuttosto che su una determinazione effettivamente genuina e consapevole[24].

In secondo luogo, le autorità di controllo evidenziano il pericolo che un sistema che fonda la propria stessa realizzazione sulla conservazione dei dati sensibili raccolti possa compromettere, *de facto*, l'esercizio dei diritti fondamentali degli interessati, in particolare quelli di revoca del consenso e di cancellazione dei propri dati personali[25]. Gli interessati, prima dell'intervento delle autorità di controllo, si sarebbero trovati nell'impossibilità di esercitare i propri diritti, in quanto la possibilità di revocare il consenso e ottenere la cancellazione dei dati sarebbe stata esplicitamente negata dalla Worldcoin Foundation[26]. Quest'ultima, infatti, avrebbe invocato a fondamento del trattamento un proprio interesse legittimo a prevenire registrazioni multiple da parte degli utenti. D'altronde, sussiste una significativa discrepanza tra l'interesse del titolare del trattamento e i diritti fondamentali degli interessati: la revoca del consenso e la successiva cancellazione dei dati rischierebbero di minare la sostenibilità dell'intero progetto Worldcoin, basato proprio sulla conservazione dei dati biometrici per risolvere lo unique-human problem. L'impossibilità di esercitare la revoca, oltre a configurare una violazione del diritto alla cancellazione previsto dall'art. 17 GDPR, incide direttamente sulla validità stessa del consenso quale base giuridica del trattamento. Come espressamente previsto dal Considerando 42 del Regolamento, «[i]l consenso

[24] Tale valutazione risulta ancor più significativa se riferita ai Paesi a basso reddito, dove l'incentivo economico legato alla distribuzione di criptovalute può incidere in misura ancora più marcata sulla libertà di autodeterminazione dei soggetti coinvolti. In tale prospettiva, l'autorità kenyota ha osservato che: «TFH and Worldcoin placed themselves in a position of innate economic influence by issuing Worldcoin tokens, a cryptocurrency that is convertible to fiat money/legal tender. This introduced an element of influence upon the data subject's expression of their free will» (cfr. ODPC, *Complaint no. 1394 of 2023*, cit., p. 9).

[25] Com'è noto, il diritto all'oblio attribuisce all'interessato la facoltà di ottenere la cancellazione dei propri dati personali qualora, ad esempio, non siano più necessari rispetto alle finalità per le quali sono stati raccolti o trattati, ovvero in caso di revoca del consenso o di trattamento illecito (art. 17 GDPR). L'elaborazione teorica di questo diritto si inserisce in un dibattito che affonda le radici già negli anni Ottanta, allorché la dottrina sollevava i primi interrogativi sull'opportunità di mantenere accessibili informazioni legittimamente diffuse nel passato ma ormai prive di attualità e non più sorrette da un interesse pubblico (si v. A.T. AULETTA, *Riservatezza e droit à l'oubli*, in AA. VV., *L'informazione e i diritti della persona*, Napoli, 1983, 127 ss.; G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, I, 1990, 801-824). Il diritto alla cancellazione dei dati riveste un'importanza centrale nel contesto digitale, dove la persistenza dell'informazione può tradursi in una lesione permanente della dignità o dell'identità personale. Il suo esercizio, tuttavia, richiede un bilanciamento con altri interessi prevalenti, quali la libertà di espressione, il diritto all'informazione e gli obblighi di conservazione previsti dalla legge (cfr. G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. inf.*, III, 2010, 391-404). D'altronde, come sottolineava autorevole dottrina, il bilanciamento tra tutela della riservatezza e tutela dell'informazione «deve rappresentare un punto fermo di orientamento per l'interprete» [cfr. C.M. BIANCA, *Nota introduttiva I*, in ID., F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, I, 2007, XXXI]. A tal fine, la Corte di giustizia dell'Unione europea ha contribuito in modo determinante a delineare i confini applicativi del diritto alla cancellazione (si v. C-131/12, Google Spain; C-398/15, Manni; C-507/17 e C-136/17, CNIL; C-460/20, Google LLC). In arg., tra gli altri, si v. M. D'AMBROSIO, *Tutela dei diritti della personalità nella rete: ruolo del provider nella fruizione dei servizi online e (a)territorialità dell'ingiunzione di rimozione di contenuti illeciti*, in *Tecn. dir.*, II, 2020, 582-601; M. BIANCA, *Memoria ed oblio: due reali antagonisti?*, in *Media Laws*, 3, 2019, 23-36; V. CUFFARO, *Cancellare i dati personali. Dalla damnatio memoriae al diritto all'oblio*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 219-236; G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

[26] Cfr. CNPD, *Deliberação/2024/137*, cit., par. 37; AEPD, 26 febbraio 2024, cit., 3; BayLDA, decisione del 13 dicembre 2024, cit., par. 279.

non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio». Alla luce di ciò, la mancata predisposizione di strumenti efficaci per esercitare il diritto di revoca – peraltro aggravata dall'atteggiamento ostruzionistico del titolare – avrebbe privato il consenso di uno dei suoi requisiti essenziali, rendendolo inidoneo a legittimare il trattamento di dati biometrici secondo le previsioni del GDPR.

Infine, è stata rilevata l'assenza di meccanismi idonei a prevenire l'accesso alla procedura di registrazione da parte di soggetti minori di 18 anni[27]. Non risulterebbero, infatti, implementati sistemi efficaci di verifica dell'età, né risulterebbe che gli operatori addetti al funzionamento dell'Orb siano tenuti a richiedere un documento identificativo. Eppure, secondo quanto espressamente riconosciuto dal Considerando 38 del GDPR, i minori necessitano di una protezione rafforzata «in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali».

4. Alcune note critiche.

Alla luce dei rilievi delle autorità di controllo, si rende necessario esaminare più nel dettaglio la qualificazione giuridica degli Iris Code e le condizioni poste dal GDPR per la liceità del loro trattamento.

Il primo nodo interpretativo da sciogliere attiene la qualificazione giuridica degli Iris Code. Si tratta di una questione di rilievo fondamentale: dalla qualificazione di tali dati dipende l'applicabilità, o meno, dell'intero impianto normativo a tutela dei dati personali. Come noto, il GDPR trova applicazione unicamente nei confronti dei 'dati personali', ovvero delle informazioni riferibili a una persona fisica identificata o identificabile[28]. Rientrano in tale definizione anche i dati 'pseudonimizzati', ossia trattati in modo tale da non poter essere

[27] Non è questa la sede per approfondire il delicato tema della protezione dei dati personali riferibili ai minori. Si rinvia, di conseguenza, alla più recente produzione scientifica in materia: C. COLAPIETRO, A. IANNUZZI, *I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione*, in *Rivista italiana di informatica e diritto*, 2, 2024, 333-337; S. TROZZI, *La tutela dei minori nel prisma della protezione dei dati personali. I sistemi di verifica dell'età tra personalismo ed esigenze di bilanciamento fra diritti*, *ivi*, 339-354; F. RICCIULLI, *L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti*, *ivi*, 355-370; L. M. LUCARELLI TONINI, *Strumenti di "age verification" alla luce del contributo del Garante privacy e dell'AGCOM [Autorità per le Garanzie nelle Comunicazioni]: il rischio di obsolescenza tecnologica e conoscitiva*, *ivi*, 435-447; G. CAPILLI, *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, in *Media Laws*, 1, 2024, 53-72; E. ADAMO, *L'identità del minorenne nella rete tra istanze di protezione e prospettive rimediali*, in *Dir. famiglia*, 4, 2023, 1677-1709; B. AGOSTINELLI, *Minori in rete: l'illusione del consenso e l'equivoco della "privacy"*, in *Familia*, 3, 2023, 397-415; M. MARTONI, *Sistemi di "age verification". Una prima esplorazione fra salvaguardia dell'interesse prioritario del minore e protezione dei dati personali*, in *Ciberspazio e Diritto*, 3, 2023, 307-322; E. BATTELLI, *Il trattamento dei dati nel prisma della tutela della persona minore di età*, in *Dir. inf. e informatica*, 2, 2022, 267-301.

[28] In base ai criteri indicati dal WP29, un'informazione è personale se, per contenuto, scopo o effetto, risulta collegata a una persona fisica identificabile (cfr. WP29, Parere 4/2007 sul concetto di dati personali, 20 giugno 2007). L'Iris Code soddisfa tutte queste condizioni: è un'informazione intrinsecamente legata a un individuo (per contenuto), è trattato al fine di distinguerlo univocamente dagli altri soggetti (scopo identificativo) e la sua elaborazione produce effetti diretti sull'interessato (ad es. l'ammissione o l'esclusione dal servizio).

attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, da conservarsi separatamente (art. 4, n. 5, GDPR). Sono, invece, esclusi dall'ambito di applicazione del Regolamento i dati resi anonimi in modo tale da non consentire – nemmeno indirettamente – l'identificazione dell'interessato (Considerando 26)[29].

Contrariamente a quanto sostenuto dalla Worlcoin Foundation, l'Iris Code non può essere considerato un dato anonimo, tuttalpiù pseudonimo. Come affermato dalla BayLDA, si tratta di una sequenza binaria generata sulla base di caratteristiche fisiologiche dell'iride, che consente di distinguere in modo univoco una persona fisica da tutte le altre[30]. Pertanto, anche se l'Iris Code non è direttamente collegato a un nome o a un'identità pubblica, permette comunque di identificare una persona rispetto a tutte le altre registrate nel sistema[31]. È del tutto inconferente l'affermazione secondo cui l'Iris Code non può essere qualificato come identificatore perché non consente la ricostruzione dell'immagine originaria dell'iride. Tale argomentazione si fonda su un presupposto giuridicamente errato. La possibilità di ricostruzione del dato biometrico di partenza non è, infatti, né determinante ai fini della qualificazione dell'Iris Code come dato personale, né rilevante ai fini della sua classificazione come dato biometrico ai sensi dell'art. 4, n. 14, GDPR[32]. Inoltre, il disaccoppiamento del codice da altri identificatori non elimina il rischio di re-identificazione, anche dal punto di vista tecnico[33]. L'algoritmo utilizzato per generare il codice – sebbene proprietario – non è tecnicamente irripetibile: anche terzi, impiegando strumenti simili o equivalenti, potrebbero essere in grado di generare codici biometrici comparabili e quindi effettuare un

[29] Il titolare del trattamento è pienamente consapevole delle difficoltà che, ancora oggi, gravano sul processo di anonimizzazione dei dati personali (cfr. World, *A World View: GDPR and anonymization in Europe*, 19 dicembre 2024. Consultabile online: https://world.org/blog/world/world-view-gdpr-anonymization-europe). D'altronde, il dato positivo non chiarisce che procedimento tecnico adottare, ma rimette tale valutazione ai privati, imponendo che i dati personali siano resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Per accertare se una persona fisica è ancora identificabile, allora, bisogna considerare la portata dei mezzi di identificazione da adottare, che devono essere "ragionevoli". Ne consegue che l'impossibilità di re-identificazione non deve essere intesa in termini assoluti, bensì relativi al contesto tecnico e fattuale concreto (si v. EDPB, Linee guida 5/2014 sulle tecniche di anonimizzazione, 10 aprile 2014 – in corso di aggiornamento). La valutazione di ragionevolezza dei mezzi dipende da un insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, e tiene conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici (considerando 26, GDPR). Nel caso in esame, il quantitativo di dati raccolti e l'aspettativa di vita degli interessati impone di valutare anche scenari futuri (ad es., nel 2100), nei quali la re-identificazione potrebbe risultare estremamente agevole (cfr. BayLDA, decisione del 13 dicembre 2024, cit., parr. 419-422).

[30] *Ibid.*, par. 315.

[31] Il Regolamento 2024/1689/UE sull'intelligenza artificiale (AI Act) offre utili chiarimenti in merito alla nozione e agli usi operativi dei dati biometrici, in continuità con quanto previsto dall'art. 4, punto 14 GDPR. Nel Regolamento si chiarisce che tali dati possono essere utilizzati per tre finalità distinte: autenticazione, identificazione e categorizzazione. L'autenticazione (o verifica) implica un confronto uno-a-uno tra un template biometricamente registrato e uno nuovo, allo scopo di confermare l'identità rivendicata da un soggetto. L'identificazione, invece, avviene tramite confronto uno-a-molti: si crea un nuovo template biometrico e lo si confronta con tutti quelli presenti in un database, al fine di riconoscere un soggetto specifico tra una pluralità, senza necessità di conoscerne l'identità civile. La categorizzazione, infine, mira ad assegnare un individuo a una determinata classe (es. età, sesso, caratteristiche fisiche), ma senza effettuare confronti con dati biometrici preesistenti. Il trattamento effettuato dalla Worldcoin Foundation — che utilizza gli Iris Code per escludere registrazioni multiple mediante deduplicazione su vasta scala — deve essere qualificato come identificazione biometrica e, in quanto tale, soggetto alle garanzie rafforzate previste dall'art. 9 GDPR.

[32] Cfr. BayLDA, decisione del 13 dicembre 2024, cit., par. 322.

[33] *Ibid.*, parr. 305-310.

riconoscimento incrociato. Ciò è reso ancor più problematico dal fatto che le informazioni biometriche richieste per attivare il processo di identificazione non si limitano al volto o agli occhi dell'interessato (raccolte in presenza). In molti casi potrebbero essere sufficienti immagini fotografiche, anche estratte da fonti accessibili al pubblico, per generare un codice compatibile e tentare la re-identificazione.

Il secondo nodo interpretativo da affrontare concerne la possibilità, tutt'altro che scontata, che esista una base giuridica idonea a legittimare la conservazione a lungo termine di dati biometrici.

Come già anticipato, il consenso per essere valido deve essere liberamente prestato. La libertà del consenso, tuttavia, risulta compromessa qualora la sua prestazione sia condizionata all'accesso a un servizio o a un vantaggio economico[34]. L'art. 7, par. 4, GDPR stabilisce infatti che, nella valutazione della libertà del consenso, occorre tenere in massima considerazione l'eventualità che l'esecuzione di un contratto sia subordinata al consenso al trattamento di dati non necessari alla sua esecuzione. Ciò mira a evitare che il consenso diventi una controprestazione contrattuale *de facto* per ottenere un servizio quando i dati non sono strettamente pertinenti a quest'ultimo. Tale disposizione, cionondimeno, si riferisce al trattamento di dati non essenziali rispetto alla prestazione contrattuale. Se, al contrario, il trattamento dei dati personali è necessario per erogare la prestazione principale – come nel caso del sistema World ID, che non potrebbe operare senza l'identificazione biometrica – il consenso cessa di essere una base giuridica adeguata al trattamento. In simili circostanze, la base giuridica più appropriata sarebbe, in linea teorica,

[34] Rimane attuale la constatazione secondo cui «non può considerarsi libero il consenso prestato da chi non poteva fare a meno del bene o del servizio offerto dalla controparte» (cfr. S. Patti, *Art. 23*, cit., 548). D'altronde, è ormai chiaro che il consenso al trattamento dei propri dati personali non è equiparabile a una manifestazione negoziale di volontà. I dati personali, infatti, non sono considerabili beni e cedibili in cambio di un servizio, ma costituiscono espressione dei diritti della personalità [per alcune interessanti suggestioni in arg., si v. V. Ricciuto, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 95-136; G. Resta, V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ.*, 2, 2018, 411-440; A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017]. Bisogna considerare che i dati personali: non sono "posseduti" dall'interessato, ma raccolti dal titolare; non sono beni rivali, perché non possono essere trasferiti in esclusiva né alienati in senso proprio; talvolta sono irrinunciabili, perché rientrano in una sfera individuale sottratta alla disponibilità dell'interessato stesso. Affinché il consenso possa dirsi liberamente espresso, devono essere assenti forme di coercizione, condizionamento o pregiudizio a carico del soggetto che rifiuta di acconsentire. La Corte di Giustizia, in tal senso, ha affermato che la posizione dominante del titolare è un fattore rilevante nella valutazione della libertà del consenso e che, in mancanza di necessità contrattuale, gli utenti devono poter rifiutare singole operazioni di trattamento senza perdere l'accesso al servizio, salvo che non venga offerta un'alternativa equivalente, eventualmente a pagamento, ma priva di quei trattamenti (C-252/21, Meta Platforms). L'EDPB, benché si fosse già espressa numerose volte in argomento, ha recentemente chiarito che i modelli "consent or pay", in cui l'accesso a un servizio online è subordinato alla scelta tra il consenso al trattamento dei dati personali per finalità di pubblicità comportamentale e il pagamento di un corrispettivo, raramente soddisfano i requisiti del consenso validamente prestato ai sensi del GDPR. I dati personali, infatti, non possono formare oggetto di controprestazione. Allora, il solo fatto di offrire un'alternativa a pagamento non garantisce di per sé che il consenso sia libero. Affinché si possa parlare di una scelta genuinamente libera, è necessario che l'interessato non subisca un detrimento in caso di rifiuto, che non si configuri uno squilibrio strutturale tra le parti (es. per effetto del potere di mercato del titolare) e che venga fornita, ove possibile, una ulteriore alternativa gratuita, priva di profilazione (EDPB, Parere 8/2024 sul consenso valido nel contesto dei modelli "consenso o pagamento" attuati dalle piattaforme online di grandi dimensioni, 17 aprile 2024).

l'esecuzione del contratto o l'interesse legittimo del titolare[35].

L'Iris Code, tuttavia, rientra nella categoria dei dati biometrici e, in quanto tale, tra le categorie particolari tutelate dall'art. 9, par. 1, GDPR. Ciò comporta che le ordinarie basi giuridiche di liceità del trattamento, quali l'esecuzione del contratto (art. 6, par. 1, lett. b) o il legittimo interesse del titolare (lett. f), non possono trovare applicazione. Nel caso di specie, l'unica deroga astrattamente ipotizzabile al divieto generale di trattamento dei dati sensibili, tra quelle previste dall'art. 9, par. 2, GDPR, è rappresentata dal consenso esplicito dell'interessato (lett. a). In altri termini, per poter trattare le scansioni dell'iride necessarie all'erogazione del servizio, l'unica opzione percorribile resta il consenso esplicito *ex* art. 9, par. 2, lett. a) GDPR. La logica interna al Regolamento, in tal modo, impone un duplice vincolo: da un lato, esclude l'impiego di basi alternative al consenso per i dati sensibili; dall'altro, impone che tale consenso sia effettivamente libero.

Proprio quest'ultimo requisito risulta problematico nel caso in esame, dal momento che la prestazione principale (ossia il rilascio del World ID) – e i vantaggi economici ad essa collegati – risultano subordinati all'accettazione del trattamento dei dati biometrici. Ne deriva un fondato dubbio circa la legittimità della pratica, nella misura in cui il consenso appare imposto come condizione di accesso al servizio, compromettendo la libertà reale di scelta dell'utente. L'European Data Protection Board sembra ammettere la possibilità di condizionare la prestazione principale al consenso esplicito al trattamento di dati sensibili, ma solo in presenza di garanzie molto stringenti[36]. In particolare, l'utente dovrebbe comunque conservare un effettivo margine di scelta (ad esempio attraverso misure alternative meno invasive) e il consenso andrebbe raccolto in forma realmente esplicita e specifica. In mancanza di tali cautele, un approccio "take it or leave it" rischia di svuotare la libertà del consenso, in contrasto con i principi fondamentali di tutela dei dati personali.

5. L'impatto dell'azione regolatoria.

Alla luce delle criticità evidenziate, si impone un bilanciamento particolarmente delicato tra interessi divergenti: da un lato, la libertà d'iniziativa economica e l'innovazione tecnologica promosse da attori privati come la Worldcoin Foundation; dall'altro, l'esigenza di assicurare una tutela effettiva dei diritti fondamentali alla riservatezza e alla protezione dei dati personali. Questo bilanciamento deve essere guidato da criteri di proporzionalità, necessità e adeguatezza, nella prospettiva di garantire il controllo effettivo da parte dell'individuo sui propri dati, in conformità con i

[35] Cfr. EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, 4 maggio 2020, parr. 31-32.

[36] «L'articolo 9, paragrafo 2, non riconosce il trattamento "necessario all'esecuzione di un contratto" come un'eccezione al divieto generale di trattare categorie particolari di dati. Di conseguenza i titolari del trattamento e gli Stati membri che rientrano nel contesto di applicazione di tale circostanza dovrebbero esaminare le eccezioni specifiche di cui all'articolo 9, paragrafo 2, lettere da b) a j). Qualora non si applichi nessuna delle eccezioni da b) a j), l'ottenimento del consenso esplicito in conformità con le condizioni per il consenso valido previste dal regolamento rimane l'unica eccezione lecita possibile per trattare tali dati» (*ibid.*, parr. 99-102).

principi fondanti del GDPR[37].

In tale prospettiva, assume un'importanza centrale la garanzia, per gli interessati, di poter revocare in qualsiasi momento il consenso precedentemente prestato e di ottenere la cancellazione dei propri dati biometrici. Il rispetto effettivo di tali diritti costituisce un indice decisivo della legittimità complessiva del trattamento, soprattutto quando sono trattati dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR. La conservazione a lungo termine di dati biometrici comporta, infatti, un rischio particolarmente elevato per i diritti e le libertà fondamentali degli interessati, rendendo necessarie tutele rafforzate sotto il profilo sostanziale e procedurale. D'altronde, nel provvedimento adottato nei confronti della Worldcoin Foundation, la BayLDA ha espressamente richiesto l'implementazione di procedure idonee a garantire la completa eliminazione degli Iris Code in caso di revoca del consenso, al fine di assicurare l'effettivo esercizio del diritto all'oblio[38].

A ciò si affianca un ulteriore presupposto imprescindibile per la liceità del trattamento: l'adozione di misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR. In presenza di dati altamente sensibili, come quelli biometrici, la sola base giuridica non è sufficiente a rendere lecito il trattamento, se non accompagnata da garanzie concrete in termini di sicurezza. In particolare, la conservazione prolungata nel tempo di tali dati esige la predisposizione di strumenti capaci di assicurare il rispetto dei principi di integrità e riservatezza, come sancito dall'art. 5, par. 1, lett. f), GDPR, nonché di limitarne la conservazione entro limiti ragionevoli, in ossequio al principio di limitazione della conservazione di cui alla lett. e) del medesimo articolo.

In tale contesto, risulta significativo osservare come l'azione regolatoria abbia concretamente contribuito a orientare l'evoluzione tecnologica del progetto[39]. Nel corso dell'istruttoria condotta dalle autorità di protezione dei

---

[37] Vale la pena rimarcare che «l'idea secondo la quale solo ed esclusivamente l'individuo può essere giudice dei suoi interessi non ha più riscontro nella società del nostro tempo. Il riconoscimento della libertà del singolo s'inserisce ormai in una concezione dell'ordinamento che s'ispira al prevalente valore della *solidarietà sociale*, quale valore di fondo della nostra Costituzione» (cfr. C.M. BIANCA, *Diritto civile. 3. Il contratto*, Milano, 2019, 24). In alcune ipotesi – come quelle oggetto del presente contributo – è dunque necessario attribuire adeguato rilievo anche agli interessi non patrimoniali eventualmente coinvolti. Il bilanciamento tra interessi, funzionale alla determinazione della disciplina applicabile, non può esaurirsi in una mera valutazione proporzionale di tipo quantitativo, ma deve fondarsi su un criterio di ragionevolezza, alla luce dei principi generali dell'ordinamento (cfr. P. PERLINGIERI, *Il diritto civile nella legalità costituzionale. IV. Attività e responsabilità*, Napoli, 2020, 124). In questo quadro, la limitazione dell'autonomia e del potere dei privati rappresenta una condizione imprescindibile per il concreto dispiegarsi del modello costituzionale di società, fondato sulla tutela effettiva dei diritti fondamentali e delle libertà individuali. Come ha lucidamente evidenziato Cesare Massimo Bianca, in un'opera che ha segnato un punto di svolta nella riflessione privatistica, il riconoscimento della centralità della persona impone di interrogarsi sul ruolo e sui limiti dei poteri privati, in particolare quando questi si esplicano in forme unilaterali o discrezionali, tali da generare situazioni di soggezione sostanziale (cfr. C.M. BIANCA, *Le autorità private*, Napoli, 1977, *passim*).

[38] Cfr. BayLDA, decisione del 13 dicembre 2024, cit., parr. 686-690.

[39] Non è questa la sede per approfondire il tema della capacità conformativa delle autorità amministrative indipendenti, da intendersi come il potere di influenzare o determinare il comportamento dei soggetti regolati, attraverso l'adozione di atti di carattere generale e particolare. In materia di protezione dei dati personali, tale capacità si rivela essenziale perché il GDPR attribuisce un ruolo determinante al Garante nell'attuazione e nell'implementazione del Regolamento [*ex multis*, si v. L. CALIFANO, *Il ruolo di vigilanza del Garante per la protezione dei dati personali*, in *Federalismi*, 2020, 1-27; G. BUSIA, *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 293-355; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali* in *Contratto e impresa*, 3, 2018, 1098-1119; F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo*

dati, infatti, la Worldcoin Foundation ha avviato una revisione della propria infrastruttura informatica, abbandonando il modello di conservazione integrale degli Iris Code a favore di un sistema basato sulla tecnologia della Secure Multiparty Computation (SMPC)[40]. Questo approccio, almeno in via teorica, consente di frammentare e distribuire i dati biometrici tra più entità, rendendo significativamente più difficile la ricostruzione del dato originario e, quindi, l'identificazione della persona fisica cui esso si riferisce. Contestualmente, in alcune giurisdizioni, la società ha sperimentato l'utilizzo del passaporto elettronico come strumento alternativo per la verifica dell'identità, riducendo così la necessità di trattare dati biometrici[41]. È evidente che tali adeguamenti sono stati adottati in risposta diretta alle sollecitazioni delle autorità di controllo, nel tentativo di rafforzare le garanzie di riservatezza e, potenzialmente, di riconfigurare la natura giuridica dei dati trattati, orientandola verso una possibile qualificazione in termini di anonimato.

L'evoluzione del progetto impone anche considerazioni rilevanti sotto il profilo del rispetto del principio di neutralità tecnologica, acquisito implicitamente dal GDPR e ribadito a più riprese dalla dottrina e dalle autorità europee[42]. Tale principio impone che la regolazione in materia di protezione dei dati non prescriva l'adozione di una specifica tecnologia, ma si limiti a definire obiettivi di tutela, lasciando al titolare del trattamento la libertà di individuare le soluzioni tecniche più idonee per raggiungerli. In questo senso, è importante sottolineare che l'adozione del sistema basato sulla SMPC da parte della Worldcoin Foundation costituisce una libera scelta dell'ente, non una prescrizione normativa o regolatoria. La BayLDA, nel corso del procedimento

---

regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni, in *Media Laws*, 1, 2018, 103-123]. Quest'ultimo, infatti, è fondato su un'architettura "principle-based" che impone ai titolari del trattamento l'obbligo di assumersi la responsabilità di garantire e dimostrare la conformità alla normativa, in ottica di "accountability" [per un confronto con il regime previgente, si v. C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, II, 2007, 1961-2076]. In questo contesto, il Garante esercita la sua capacità conformativa attraverso l'emissione di linee guida, pareri, provvedimenti e sanzioni che orientano e, se necessario, vincolano le condotte dei titolari del trattamento (tra i casi più celebri si segnalano: GPDP, 30 marzo 2023, n. 112 – ChatGPT; 22 luglio 2021, n.285 – Deliveroo). Attraverso tali interventi, il Garante non solo assicura la tutela dei diritti fondamentali degli interessati, ma contribuisce anche a delineare concretamente le modalità di applicazione dei principi del GDPR, rafforzando la cultura della protezione dei dati e promuovendo una maggiore responsabilizzazione dei titolari del trattamento. Del resto, non va trascurato che il ruolo del Garante trova un espresso riconoscimento nell'art. 8 della Carta di Nizza, che sancisce il diritto alla protezione dei dati personali e ne affida la garanzia a un'autorità indipendente, conferendogli così una chiara valenza costituzionale.

[40] *Supra*, nt. 9.

[41] Il 31 gennaio 2025, la Worldcoin Foundation ha avviato il programma pilota del "World ID Passport Credential", che consente agli utenti di associare il proprio passaporto o una carta d'identità nazionale con chip NFC al World ID tramite l'applicazione World App. La nuova funzionalità, inizialmente disponibile in Cile, Colombia, Malesia e Corea del Sud, permette di dimostrare attributi personali – come l'età o la cittadinanza – in forma anonima, senza che i dati vengano condivisi con terze parti. Tutte le informazioni restano criptate e conservate localmente sul dispositivo dell'utente, al quale soltanto è garantito l'accesso (cfr. WORLD, *New World ID Passport Credential pilot launches, with access to WLD tokens*, 31 gennaio 2025. Consultabile online: https://world.org/blog/announcements/new-world-id-passport-credential-launches-access-wld-tokens).

[42] Il principio di neutralità tecnologica fa la sua prima comparsa, in ambito comunitario, nella Direttiva quadro sulle comunicazioni elettroniche (Direttiva 2002/21/CE), laddove si afferma che la regolamentazione deve essere improntata alla neutralità tecnologica, vale a dire non deve imporre l'adozione di una specifica tecnologia né discriminare tra tecnologie diverse (Considerando 18). Da allora, il legislatore europeo sembra aver assunto tale principio come riferimento costante, inteso nel senso che il diritto non dovrebbe interferire nello sviluppo tecnologico, né orientarlo favorendo alcune soluzioni rispetto ad altre, né alterare l'equilibrio del mercato avvantaggiando determinati prodotti o modelli (cfr. G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Dir. inf.*, 4-5, 2018, 833).

istruttorio, ha orientato la valutazione in termini di risultati attesi e di conformità ai principi del GDPR, senza imporre vincoli sull'architettura tecnologica da adottare. In prospettiva di neutralità tecnologica, la regolazione ha dunque svolto essenzialmente un ruolo di indirizzo, senza tradursi in una prescrizione tecnica vincolante, e ha lasciato alla società la responsabilità – e la libertà – di individuare il modello tecnico-organizzativo più adeguato rispetto alle finalità perseguite e ai rischi connessi al trattamento.

Il procedimento condotto dalla BayLDA si è concluso con l'accertamento di plurime violazioni del GDPR, in particolare in relazione al trattamento dei dati biometrici per finalità di confronto passivo[43]. Al termine dell'indagine, l'autorità ha adottato una serie di ordini vincolanti, tra cui la sospensione immediata del trattamento per finalità di confronto passivo (fintantoché non siano rispettate le prescrizioni del GDPR) e la cancellazione degli Iris Code (anche nella versione elaborata attraverso il meccanismo SMPC a partire dal 24 luglio 2023). Alla luce delle modifiche tecniche introdotte dalla società – segnatamente l'adozione del sistema SMPC, ancora in via di sviluppo – l'autorità ha riservato una futura verifica approfondita sull'effettiva idoneità di tale soluzione per il rispetto dei requisiti previsti dalla normativa. Le prospettive future del progetto dipenderanno, pertanto, dalla capacità della Worldcoin Foundation di adeguarsi pienamente al quadro normativo europeo, dimostrando che le nuove modalità di trattamento siano compatibili con i principi del GDPR e non pregiudichino i diritti fondamentali degli interessati.

6. Il ruolo degli Stati nel processo di identificazione.

Oltre ai profili prettamente legati alla tutela dei dati personali, emerge tuttavia una questione di carattere più ampio e profondo, che investe direttamente le prerogative statali in materia di identificazione dei cittadini e dei residenti nello Stato. Worldcoin si colloca, infatti, all'interno del paradigma delle SSI, ossia identità digitali gestite autonomamente dagli utenti, senza l'intermediazione dello Stato o di soggetti privati autorizzati. L'idea di fondo consiste nel conferire agli individui piena autonomia nella gestione e divulgazione dei dati personali, consentendogli di scegliere quali informazioni condividere con i servizi e le applicazioni informatiche[44]. Tuttavia, il modello

[43] Una sintesi dei provvedimenti assunti dalla BayLDA è reperibile nella decisione del 13 dicembre 2024 (cit.) ai paragrafi 2-41.

[44] Un simile approccio si inscrive pienamente nel paradigma del c.d. techno-solutionism, nozione coniata da Evgeny Morozov e successivamente approfondita da Hilary J. Allen, che designa una visione riduzionista della realtà sociale, secondo cui ogni problema, per quanto complesso sul piano politico, economico o istituzionale, può essere tradotto in termini tecnici e risolto attraverso soluzioni tecnologiche (cfr. H.J. ALLEN, *Fintech and Techno-Solutionism*, cit., 5; E. MOROZOV, *To Save Everything, Click Here: The Folly of Technological Solutionism*, New York, 2013, *passim*; H.S. SÆTRA, *The Promise and Pitfalls of Techno-solutionism*, in *Technology and Sustainable Development*, New York, 2023, 1-10). Tale approccio, profondamente radicato nella cultura dell'innovazione della *Silicon Valley*, tende a ignorare la complessità storica, strutturale e normativa dei problemi che intende affrontare, proponendo invece soluzioni ingegneristiche (c.d. "silver bullets") che, spesso, generano nuovi rischi o aggravano quelli esistenti. In questo senso, la promozione delle SSI (come Worldcoin), appare sintomatica della tendenza tecno-soluzionista a risolvere problemi istituzionali complessi mediante meccanismi tecnologici standardizzati e apparentemente neutri, ma in realtà frutto di precise scelte ideologiche e di potere. Il techno-solutionism, infatti, è spesso funzionale ai progetti politici dei cosiddetti "tech oligarchs" (cfr. J.E. COHEN, *Oligarchy, State, and Cryptopia*, cit., 22-28). Questi ultimi, forti

delle SSI – ove implementato su larga scala – solleva rilevanti interrogativi circa la possibilità di interferire con una sfera che rientra tradizionalmente tra le prerogative esclusive degli Stati.

Com'è noto, tra i poteri-doveri che connotano uno Stato sovrano in senso moderno rientra, in via indiscussa, quello di identificare i cittadini e i residenti presenti sul proprio territorio[45]. L'identificazione personale, infatti, costituisce il presupposto imprescindibile per garantire l'effettivo esercizio dei diritti fondamentali: senza un'identità giuridicamente riconosciuta, l'individuo rischierebbe di essere invisibile per l'ordinamento[46]. In questa prospettiva, la Costituzione italiana, tra le altre, sancisce all'art. 22 che «[n]essuno può essere privato, per motivi politici, della capacità giuridica, della cittadinanza, del nome», riconoscendo tali elementi come essenziali per l'appartenenza all'ordinamento giuridico.

---

di enormi concentrazioni di ricchezza e potere infrastrutturale, promuovono una visione tecno-futurista che non mira tanto alla risoluzione dei problemi esistenti, quanto piuttosto alla ristrutturazione dell'intero sistema politico-economico secondo logiche private e deregolate. La spinta alla disintermediazione e alla decentralizzazione — ad esempio attraverso le criptovalute o le SSI — si traduce spesso in una vera e propria espropriazione dell'autorità pubblica, sostituita da meccanismi aziendali opachi, sottratti a qualunque forma di controllo democratico.

[45] Le norme che disciplinano il complesso degli elementi che svolgono la funzione di individuazione della persona tutelano, al contempo, interessi individuali e collettivi [in arg., si v. M. NUZZO, *Nome (dir. vig.)*, in *Enc. dir.*, XXVIII, 1978, 304-311]. In chiave individualistica, tali elementi costituiscono attributi della personalità - inscindibili dal soggetto cui si riferiscono - e vanno tutelati a prescindere da ogni valutazione contingente operata dal legislatore, perché funzionali all'affermazione della propria identità personale. Secondo questa impostazione, «l'ordinamento giuridico vuol tutelare l'interesse 'di ogni persona' alla protezione della propria identità sul piano sociale, valutando come 'bene' la stessa identità personale, in sé e per sé considerata indipendentemente dal grado sociale o dalla virtù della singola persona» (cfr. A. DE CUPIS, *I diritti della personalità*, in *Tratt. Cicu e Messineo*, IV, 2, Milano, 1961, 27). In chiave collettivistica, invece, le norme che disciplinano l'identificazione assolvono a finalità di ordine prettamente pubblicistico, poiché sono necessarie a garantire l'efficienza amministrativa e la certezza nei rapporti giuridici (cfr. M. PLANIOL, *Traité élémentaire de droit civil*, I, 1, Paris, 1928, 156). In tale ottica, la tutela giuridica dell'identità personale risponde a interessi generali, sicché non costituisce un diritto soggettivo, bensì «un diritto alla cessazione del fatto lesivo altrui, consistente nella infondata contestazione o nella pregiudizievole usurpazione» (cfr. F. SANTORO-PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1964, 50). Tuttavia, le norme che disciplinano i singoli profili dell'identità personale non possono essere rigidamente ricondotte né alla sola prospettiva individualistica né a quella esclusivamente collettivistica. Esse vanno piuttosto interpretate come manifestazioni concrete del valore costituzionale della persona umana (cfr. G. GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. e proc. civ.*, 1958, 458-471).

[46] Sebbene l'articolo 6 della Dichiarazione Universale dei Diritti Umani riconosca espressamente che «ogni individuo ha diritto, in ogni luogo, al riconoscimento della sua personalità giuridica», le stime fornite dalle organizzazioni internazionali attestano che circa un miliardo di persone nel mondo risulta privo di un'identità legale formalmente riconosciuta (cfr. UN LIEG, *United Nations Strategy for Legal Identity for All*, giugno 2019, disponibile online: https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf). Tale circostanza comporta rilevanti conseguenze sul piano dell'inclusione sociale e della fruizione effettiva dei diritti fondamentali. L'assenza di riconoscimento giuridico configura una condizione comunemente definita come "legal invisibility", espressione che denota lo stato in cui si trovano gli individui che, non essendo formalmente identificati dalle autorità statali, risultano esclusi dall'accesso a diritti e servizi essenziali, quali l'istruzione, l'assistenza sanitaria, il lavoro regolare e la partecipazione alla vita pubblica. Si tratta di una forma di invisibilità istituzionale che compromette la piena attuazione del principio di uguaglianza e della dignità della persona umana. In risposta a tale problematica, le Nazioni Unite hanno promosso l'elaborazione di una strategia globale volta a garantire l'accesso universale all'identità legale, considerata quale presupposto indispensabile per il riconoscimento della soggettività giuridica e, conseguentemente, per l'effettivo esercizio dei diritti fondamentali. Scopo di tale iniziativa è quello di garantire che ogni individuo — dalla nascita fino al decesso — sia oggetto di registrazione formale mediante strumenti interoperabili, sicuri e rispettosi dei diritti fondamentali, in particolare con riferimento alla tutela della riservatezza e alla protezione dei dati personali. A tal fine, è stato istituito il Legal Identity Expert Group (LIEG), organismo interagenzia che coordina l'attività di enti quali UNDP, UNICEF e UNDESA, con l'obiettivo di sostenere gli Stati nello sviluppo di sistemi integrati di registrazione civile, raccolta delle statistiche vitali e gestione dell'identità personale.

Accanto a questa dimensione individuale, l'identificazione svolge una funzione primaria anche sul versante collettivo, consentendo allo Stato di registrare e documentare la popolazione per finalità di amministrazione, sicurezza e ordine pubblico[47]. La raccolta e la gestione di dati identificativi rispondono dunque a esigenze pubbliche di organizzazione e controllo, ma devono avvenire entro limiti rigorosi. Per evitare derive autoritarie o compressioni ingiustificate della libertà personale, è la stessa Carta costituzionale a definire una cornice di garanzie, entro la quale il potere dello Stato può essere legittimamente esercitato. In sintesi, l'identificazione rappresenta la condizione necessaria per rendere operativi i rapporti tra cittadino e Stato, consentendo di determinare chi sono i soggetti titolari di diritti e destinatari di obblighi, e dunque di assicurare l'effettiva applicazione delle disposizioni normative.

Con l'avvento del digitale, la funzione pubblica di identificazione si è progressivamente estesa all'ambiente informatico, mediante l'introduzione di sistemi nazionali di identità digitale, come lo SPID in Italia[48]. Tali strumenti mirano a semplificare l'interazione tra cittadino e Pubblica Amministrazione, permettendo l'accesso ai servizi pubblici anche in modalità telematica. Alla base vi è l'esigenza di attribuire valore giuridico all'identificazione digitale, a condizione che essa sia accompagnata da adeguate garanzie di sicurezza, affidabilità e controllo pubblico[49]. In questa direzione si colloca il Regolamento

[47] In ragione della sua rilevanza sistemica, la materia è attribuita alla competenza legislativa esclusiva dello Stato, come stabilito dall'art. 117, secondo comma, lett. a), della Costituzione. Nell'ambito di tale riserva rientrano non soltanto le disposizioni relative all'acquisto e alla perdita della cittadinanza, ma anche la disciplina concernente la tenuta dei registri dello stato civile e dell'anagrafe della popolazione residente, unitamente alla regolamentazione del rilascio dei documenti di identità e di ogni altro strumento volto all'accertamento ufficiale dell'identità personale. È opportuno precisare che il Capo III del Codice Privacy, relativo a "stato civile, anagrafi e liste elettorali" [su cui si v. F. BOCCHINI, *Artt. 62 e 63*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, II, 2007, 1042-1057] è stato abrogato dal D.lgs. 10 agosto 2018, n. 101, a seguito dell'introduzione del GDPR.

[48] L'identificazione digitale rappresenta un nodo cruciale per quei servizi che richiedono un accertamento formale dell'identità (quali, ad es., l'apertura di conti bancari o la partecipazione a gare pubbliche). Il Regolamento 910/2014/UE (eIDAS) ha fornito una prima risposta organica a tale esigenza, ponendosi l'obiettivo di rafforzare la fiducia nelle transazioni elettroniche mediante l'uniformazione del quadro normativo europeo in materia di identificazione, autenticazione, firme elettroniche e servizi fiduciari [cfr. G. FINOCCHIARO, *Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione* online*, firme elettroniche e servizi fiduciari*, in *Nuove leggi civ. comm.*, 3, 2015, 419-428]. Il Regolamento, direttamente applicabile negli Stati membri, consentiva a ciascun Paese di notificare i propri sistemi nazionali di identificazione elettronica alla Commissione europea: una volta approvati, tali sistemi dovevano essere riconosciuti dagli altri Stati membri, almeno per i servizi pubblici e a condizione che il livello di sicurezza fosse "sostanziale" o "elevato". In ambito nazionale, tale funzione è svolta, tra gli altri strumenti, dallo SPID (Sistema Pubblico di Identità Digitale), concepito per garantire l'accesso sicuro ai servizi online da parte di cittadini e imprese. In ambito nazionale, tale funzione è svolta, tra gli altri strumenti, dallo SPID (Sistema Pubblico di Identità Digitale), concepito per garantire l'accesso sicuro ai servizi online da parte di cittadini e imprese. Sul piano interno, il quadro tracciato da eIDAS si integra con il Codice dell'Amministrazione Digitale (CAD), introdotto con il d.lgs. n. 82/2005 e successivamente aggiornato. Il CAD rappresenta la base normativa della digitalizzazione della pubblica amministrazione italiana e disciplina gli strumenti digitali, le firme elettroniche, i documenti informatici, l'identità digitale e i diritti dei cittadini nell'ambito digitale. In particolare, il CAD recepisce e sviluppa molti degli istituti previsti da eIDAS, adattandoli al contesto italiano e regolando aspetti pratici legati all'uso di SPID, CIE, PEC e delle firme elettroniche nei rapporti tra cittadini, imprese e amministrazioni (in arg., si v. R. CAVALLO PERIN, D.U. GALLETTA, *Il Diritto dell'Amministrazione Pubblica digitale*, Milano, 2025; C. BOCCIA, C. CONTESSA, E. DE GIOVANNI, *Codice dell'amministrazione digitale*, Milano, 2018).

[49] D'altronde, il concetto giuridico di identità si articola in due dimensioni: oggettiva e soggettiva. La prima corrisponde all'insieme dei dati personali verificabili (es. nome, data di nascita, residenza), che consentono l'identificazione formale della persona nei rapporti giuridici e con la pubblica amministrazione. Su questa dimensione si concentra il Regolamento eIDAS, volto a garantire sistemi di identificazione elettronica

2024/1183/UE (eIDAS 2), entrato in vigore il 20 maggio 2024, che ha istituito il Portafoglio Europeo di Identità Digitale (EUDI Wallet) quale strumento comune per l'identificazione elettronica dei cittadini e dei residenti nell'Unione[50]. Il nuovo portafoglio digitale permetterà agli individui di conservare e gestire sul proprio dispositivo mobile i dati identificativi e gli attestati ufficiali (quali nome, indirizzo, patente, titoli di studio, certificati, ecc.), da utilizzare in tutti gli Stati membri.

Il Regolamento conferma il ruolo centrale degli Stati membri, stabilendo che i portafogli possano essere forniti sia direttamente dallo Stato sia da soggetti privati, purché sotto supervisione pubblica (art. 5-*bis*, par. 2, eIDAS 2). L'obiettivo è promuovere un modello di identità digitale che sia affidabile, interoperabile e conforme ai diritti fondamentali, preservando il presidio pubblico su un ambito essenziale per l'effettività della cittadinanza e la certezza dei rapporti giuridici nello spazio digitale europeo[51]. Si intende così rafforzare la fiducia nell'identificazione online, evitando che i cittadini debbano fornire a ogni accesso i propri dati personali, o che debbano impiegare servizi di identificazione privati (come ad es. Google Sign-in). In linea con tale approccio, la normativa impone alle grandi piattaforme online (le "very large online platforms") di accettare il nuovo Portafoglio Europeo per l'accesso ai propri servizi[52]. Ciò significa che in futuro il cittadino potrà accedere a social network, marketplace o altri servizi digitali utilizzando la propria identità digitale pubblica, anziché credenziali fornite da privati. È un cambiamento significativo, che mira a invertire la tendenza alla "privatizzazione" delle identità digitali da parte di colossi del web[53].

Resta da chiedersi se il potere statale di identificare i cittadini debba considerarsi, oltre che storicamente riconosciuto, anche esclusivo in senso giuridico. Sul piano positivo, non si rinviene, almeno nell'ordinamento europeo, un'espressa riserva in favore dello Stato che impedisca in assoluto a soggetti

---

interoperabili a livello europeo. L'identità soggettiva, invece, riguarda la proiezione sociale dell'individuo, ossia l'immagine che di lui si forma nel contesto delle relazioni interpersonali. Su questa dimensione si concentra la disciplina in materia di protezione dei dati personali [cfr. G. Finocchiaro, *Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione* online*, firme elettroniche e servizi fiduciari*, cit., 420-421].

[50] L'EUDI Wallet sarà rilasciato sotto forma di applicazione mobile dai singoli Stati membri, ma sarà pienamente interoperabile su scala europea, con l'obiettivo di creare un'infrastruttura uniforme per l'identificazione elettronica e l'accesso ai servizi digitali, sia pubblici che privati. A tal fine, esso si fonda su standard tecnici comuni, definiti a livello dell'Unione, e dovrà garantire elevati requisiti di sicurezza, affidabilità e conformità al diritto alla protezione dei dati personali, in linea con il GDPR (per alcune considerazioni critiche, si v. D. Baldini, *The Impact of the Right to Personal Data Protection on the Design of the European Digital Identity Wallet*, in *Italian Journal of Public Law*, 1, 2024, 297-317). Tra le sue funzionalità principali, si annoverano: la possibilità per l'utente di decidere autonomamente quali informazioni condividere, con quali soggetti e per quali finalità; l'accesso semplificato a una pluralità di servizi digitali, quali la sanità elettronica, i pagamenti online, l'amministrazione digitale o la firma elettronica; l'integrazione nativa di certificati digitali e attestazioni elettroniche, rilasciati da soggetti autorizzati, idonei a sostituire documenti fisici o procedimenti cartacei nella vita quotidiana del cittadino europeo.

[51] Cfr. Commissione UE, *Plasmare il futuro digitale dell'Europa*, 19 febbraio 2020; Decisione 2022/2481/UE.

[52] Il Considerando 57 del Regolamento specifica che le piattaforme online di dimensioni molto grandi (*ex* art. 33, par. 1, Reg. 2022/2065/UE) «dovrebbero essere tenute ad accettare l'uso dei portafogli europei di identità digitale su richiesta volontaria dell'utente. Gli utenti non dovrebbero essere obbligati a usare un portafoglio europeo di identità digitale per accedere ai servizi privati e il loro accesso ai servizi non dovrebbe essere limitato o ostacolato per il fatto che non utilizzano un portafoglio europeo di identità digitale».

[53] Giova, ancora una volta, richiamare il pensiero di Cesare Massimo Bianca, il quale, con straordinaria lungimiranza teorica, aveva già colto la necessità di contenere l'espansione di poteri privati in grado di esercitare un'autorità sostanziale su altri soggetti, pur operando all'interno delle coordinate formali del diritto privato (cfr. C.M. Bianca, *Le autorità private*, cit.).

privati di sviluppare sistemi di identificazione personale, purché tali sistemi non pretendano di produrre effetti giuridici equivalenti a quelli riconosciuti alle identità ufficiali. Ne deriva che il carattere esclusivo di tale potere non può ritenersi ontologico, ma si configura piuttosto come una scelta di opportunità politica, volta a garantire la certezza, la coerenza e la legittimità delle relazioni giuridiche. L'attribuzione di un'identità legale da parte dello Stato risponde infatti a esigenze di ordine pubblico, uguaglianza e inclusività, difficilmente perseguibili in un ecosistema frammentato di soluzioni private concorrenti. Tuttavia, in un contesto tecnologico in rapida evoluzione, il confine tra prerogativa pubblica e iniziativa privata si fa sempre più mobile.