PROYECTO WORLDCOIN Y PROTECCIÓN DE DATOS BIOMÉTRICOS EN LA UNIÓN EUROPEA

Análisis jurídico de las acciones de la AEPD y la BayLDA ante el tratamiento masivo de datos biométricos. Implicaciones para la gobernanza europea de la identidad digital

Informe de Investigación Jurídica

Marzo de 2026

ÍNDICE

CAPÍTULO I. INTRODUCCIÓN Y CONTEXTO DEL PROYECTO WORLDCOIN

El ecosistema digital atraviesa una fase de transformación caracterizada por la irrupción masiva de la inteligencia artificial y por la emergencia de proyectos que pretenden redefinir los fundamentos de la identidad y la actividad económica en la red. En este contexto nace Worldcoin, un proyecto de alcance global impulsado por Tools for Humanity Corporation (TFH) —cuya fundación se vincula a figuras de relevancia en el sector tecnológico, entre ellas Sam Altman— y la Worldcoin Foundation. Su objetivo declarado consiste en instaurar una red financiera y de identidad global denominada World Network, articulada sobre el concepto de Proof of Personhood —prueba de humanidad— materializado en la denominada World ID. La premisa técnica es la garantía de que cada actor en la red sea un ser humano único, lo que requiere la captura y el procesamiento masivo de datos biométricos de carácter ocular.

Desde una perspectiva jurídica, el modelo de captación desplegado por Worldcoin presenta tensiones estructurales con el marco europeo de protección de datos. El incentivo principal para la incorporación de usuarios ha consistido en la entrega de criptomonedas (WLD) a cambio del escaneo ocular, práctica que sitúa el tratamiento de datos biométricos —identificadores inalterables de la persona física— bajo una lupa regulatoria que suscita interrogantes de la mayor gravedad en relación con la licitud, la transparencia y la protección de colectivos vulnerables.[1] La noción de mercantilización de la biometría que subyace al modelo de negocio de Worldcoin constituye el núcleo del conflicto regulatorio analizado en este informe.

[1]Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 [en adelante, RGPD], DO L 119, 4 de mayo de 2016, art. 4.1.

La gobernanza del caso se articula sobre el mecanismo de ventanilla única previsto en el Reglamento General de Protección de Datos (RGPD),[2] toda vez que TFH tiene su establecimiento principal europeo en Baviera, lo que atribuye a la autoridad de control de dicho estado federal alemán —la BayLDA— el liderazgo de la investigación transfronteriza. No obstante, la gravedad de los hechos detectados en España motivó una intervención autónoma de la Agencia Española de Protección de Datos (AEPD) mediante medidas cautelares de urgencia, posteriormente avaladas por la Audiencia Nacional. La dualidad de acciones regulatorias —nacional y europea— configura el objeto central de este análisis.

El informe adopta un enfoque metodológico multidisciplinar que combina el análisis técnico de la arquitectura de procesamiento biométrico con la hermenéutica jurídica del RGPD, la doctrina española y comparada, y la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE). El objetivo final es valorar si el marco normativo vigente resulta suficiente para afrontar los retos que plantea el tratamiento masivo de biometría con fines de identidad digital global, y formular propuestas de *lege ferenda* allí donde se detecten lagunas.

CAPÍTULO II. ARQUITECTURA TÉCNICA Y PROCESAMIENTO DE DATOS BIOMÉTRICOS

II.1. El dispositivo Orb y la generación del Iris Code

La comprensión del conflicto jurídico exige examinar previamente la arquitectura tecnológica que lo origina. El dispositivo Orb actúa como primer y más crítico eslabón de la cadena de tratamiento: se trata de un sensor de imagen de alta resolución que integra un sistema de inteligencia artificial diseñado para verificar la presencia de un ser humano vivo y para descartar tentativas de suplantación mediante lentes de contacto cosméticas u otros medios técnicos.[3] Una vez verificada la presencia humana, el sistema procede a la generación del denominado Iris Code: una representación numérica binaria derivada de los patrones únicos del iris mediante versiones modificadas del algoritmo de Daugman.[4] El Iris Code se vincula a continuación a un código QR que transforma la aplicación móvil del usuario en un pasaporte digital que funciona simultáneamente como monedero de criptomonedas.

La empresa ha sostenido públicamente que el proceso de generación del Iris Code es irreversible y que no permite reconstruir las imágenes originales del iris. Sin embargo, la BayLDA ha señalado que, bajo determinadas condiciones técnicas, podría ser posible reconstruir fragmentos de imagen capaces de revelar información de naturaleza sanitaria —como la presencia de melanomas oculares—,[5] lo que confirma el carácter de dato de categoría especial del Iris Code y la necesidad de aplicar las garantías reforzadas previstas en el artículo 9 RGPD.[6]

---

[3]ISO/IEC 30107-3:2023, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting, International Organization for Standardization, Ginebra, 2023.
[4]DAUGMAN, John, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, núm. 1 (2004), pp. 21-30.
[5]RAMÓN FERNÁNDEZ, Francisca, "Datos de salud, datos especialmente protegidos: el caso de los datos biométricos y su comercialización", Universidad Politécnica de Valencia, 2024, p. 12.
[6]Art. 9.1 RGPD.

II.2. Los dominios operativos: comparación activa y comparación pasiva

El sistema de procesamiento se articula en torno a dos dominios operativos diferenciados que resulta imprescindible no confundir. La comparación activa se produce en el momento del registro inicial: la biometría captada se coteja con la base de datos existente para validar la identidad del nuevo usuario. La comparación pasiva o deduplicación, en cambio, implica el almacenamiento permanente del Iris Code y su cotejo continuado contra cada nuevo intento de incorporación a la red, con el fin de prevenir registros duplicados. Es precisamente la persistencia de los datos en el backend de la compañía lo que ha concentrado la mayor parte de las objeciones regulatorias, por cuanto supone un tratamiento continuado de datos biométricos cuya base jurídica la empresa no ha acreditado con suficiencia.[7]

II.3. El sistema SMPC y la distinción entre seudonimización y anonimización

En respuesta a las críticas regulatorias, Worldcoin migró hacia un sistema de Computación Segura de Múltiples Partes (SMPC): el Iris Code original ya no se almacena en texto plano en una base de datos centralizada, sino que se fragmenta en porciones o shares distribuidas entre entidades diferenciadas —fundamentalmente Tools for Humanity GmbH y Worldcoin Europe GmbH—, de modo que ninguna de ellas posea, en teoría, la información completa.[8]

No obstante, la BayLDA y la doctrina especializada han descartado que esta fragmentación constituya una anonimización en el sentido jurídico del término.[9] Conforme al artículo 4.5 RGPD y al Dictamen 05/2014 del Grupo de Trabajo del Artículo 29, la anonimización requiere que la

[7]BayLDA (Bayerisches Landesamt für Datenschutzaufsicht), Comunicado de prensa y resolución de órdenes correctivas contra la Worldcoin Foundation, 19 de diciembre de 2024 [en adelante, Resolución BayLDA 2024].
[8]Resolución BayLDA 2024, op. cit., sección IV (análisis del sistema SMPC).
[9]Grupo de Trabajo del Artículo 29, Dictamen 05/2014 sobre técnicas de anonimización, WP216, op. cit., pp. 3-10 (distinción entre anonimización y seudonimización).

reidentificación resulte técnicamente imposible para el responsable del tratamiento y para cualquier tercero.[10] En el presente caso, ambas entidades están estrechamente vinculadas y operan sobre la misma infraestructura en Amazon Web Services (AWS), lo que significa que el responsable del tratamiento conserva los medios técnicos razonables para reconstruir el Iris Code original a partir de sus fragmentos.[11] El sistema SMPC no constituye, en consecuencia, sino una seudonimización en los términos del artículo 4.5 RGPD, con los plenos efectos jurídicos de protección que dicha calificación implica.

[10]Art. 4.5 RGPD (seudonimización). Véase también: Grupo de Trabajo del Artículo 29, Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014, WP216, pp. 20-25.
[11]STJUE de 19 de octubre de 2016, Breyer c. Bundesrepublik Deutschland, C-582/14, EU:C:2016:779, párr. 43-49 (identificabilidad mediante medios razonables).

CAPÍTULO III. CARACTERIZACIÓN JURÍDICA DE LOS DATOS Y EL MARCO DEL RGPD

III.1. Calificación como datos personales y biométricos

La controversia sobre la naturaleza jurídica del Iris Code constituye el eje en torno al que gira toda la arquitectura regulatoria del caso. Worldcoin ha sostenido en diferentes foros que el Iris Code no es un dato personal por no estar vinculado a un nombre o a una identidad civil directamente identificable. Este argumento no puede ser aceptado desde la perspectiva del RGPD. El artículo 4.1 define como dato personal toda información que permita identificar, directa o indirectamente, a una persona física, ya sea por referencia a identificadores específicos o a elementos propios de su identidad biológica.[12] El estándar determinante no es la identificación directa por nombre, sino la singularización: la capacidad de distinguir a una persona concreta entre una multitud.[13] El Iris Code cumple este estándar de forma paradigmática: al ser el resultado de un tratamiento técnico específico aplicado a características biológicas únicas del ojo humano, es un identificador que permite singularizar al individuo con un nivel de precisión superior al de cualquier otro dato de identificación convencional.

La calificación adicional como dato biométrico en el sentido del artículo 4.14 RGPD[14] resulta igualmente incontrovertible: el Iris Code es el producto de un tratamiento técnico específico —la aplicación del algoritmo de Daugman a imágenes del iris— que permite la identificación única de una persona física. Su nota característica más relevante desde la perspectiva del riesgo es la inmutabilidad: a diferencia de una contraseña o de un

[13]Considerando 26 RGPD: "Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física."
[14]Art. 4.14 RGPD.

número de cuenta bancaria, el iris no puede ser modificado ni sustituido en caso de compromiso. Esta circunstancia determina que la lesión del derecho a la protección de datos que un tratamiento ilícito de Iris Codes podría generar sea, por naturaleza, de carácter irreversible.[15]

III.2. El régimen de protección reforzada del artículo 9 RGPD

Calificado el Iris Code como dato biométrico destinado a identificar de forma unívoca a una persona física, le resulta de aplicación la prohibición general de tratamiento establecida en el artículo 9.1 RGPD,[16] que solo admite excepción en los supuestos taxativamente enumerados en el artículo 9.2 RGPD.[17] Worldcoin ha invocado, esencialmente, el consentimiento explícito del interesado como base jurídica habilitante [art. 9.2.a) RGPD]. La BayLDA ha concluido, sin embargo, que dicho consentimiento no cumplía los requisitos de especificidad e información previa suficiente que exige el considerando 43 del RGPD para que el acto de aceptación pueda considerarse libre y genuinamente voluntario.[18]

La cuestión de la base jurídica es especialmente aguda en relación con la comparación pasiva: el tratamiento permanente del Iris Code con fines de deduplicación se produce de forma continuada e independiente de cualquier acto de voluntad del interesado tras el registro inicial. La empresa no ha logrado identificar una base jurídica válida —ni consentimiento específico para esta finalidad, ni interés legítimo que pueda prevalecer sobre los derechos del interesado tratándose de categorías especiales de datos— lo que determina la ilicitud del tratamiento con arreglo a los artículos 6 y 9 RGPD.[19]

III.3. El consentimiento libre como requisito de licitud

[15]Considerando 75 RGPD, sobre riesgos para derechos y libertades derivados del tratamiento de datos biométricos.
[17]Art. 9.2 RGPD (lista taxativa de excepciones a la prohibición de tratamiento de categorías especiales).
[18]Comité Europeo de Protección de Datos (CEPD), Directrices 05/2020 sobre el consentimiento en virtud del Reglamento (UE) 2016/679, versión 1.1 adoptada el 4 de mayo de 2020, WP259 rev.01, pp. 11-15.
[19]Art. 6.1 RGPD (bases jurídicas del tratamiento). Art. 9.2 RGPD (excepciones para categorías especiales).

El empleo de incentivos económicos —entrega de criptomonedas WLD— como contraprestación por el escaneo ocular plantea interrogantes de primera magnitud sobre la libertad del acto de consentimiento. El considerando 43 del RGPD establece con claridad que el consentimiento no puede considerarse libre cuando exista un desequilibrio claro entre el interesado y el responsable, en particular cuando este último sea una autoridad pública o cuando el interesado sea un particular que se encuentra en una posición de vulnerabilidad.[20] Las Directrices 05/2020 del Comité Europeo de Protección de Datos precisan, a este respecto, que la prestación de servicios —o la entrega de incentivos— condicionada al consentimiento para el tratamiento de datos no esenciales vicia la libertad del acto.[21] La mercantilización de la biometría que caracteriza al modelo de negocio de Worldcoin constituye, a juicio de la AEPD y de la BayLDA, un supuesto paradigmático de consentimiento estructuralmente viciado.

La problemática se agudiza en los supuestos de captación de datos de menores de edad. El artículo 8 RGPD, en relación con el artículo 7 de la Ley Orgánica 3/2018 (LOPDGDD),[22] fija en España la edad mínima de consentimiento autónomo en catorce años.[23] Las denuncias recibidas por la AEPD señalaban que Worldcoin había captado datos biométricos de menores sin el consentimiento de sus tutores legales, situación que eleva el nivel de riesgo del tratamiento a una dimensión que supera el daño patrimonial para adentrarse en la lesión de derechos fundamentales de personas especialmente vulnerables.[24]

[20]Considerando 43 RGPD: el consentimiento no puede considerarse libre cuando exista un desequilibrio claro entre el interesado y el responsable.
[22]Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [LOPDGDD], BOE núm. 294, 6 de diciembre de 2018, arts. 7 y 8 (tratamiento de datos de menores).
[23]Art. 8 RGPD, en relación con el art. 7 LOPDGDD: edad mínima de consentimiento fijada en 14 años en España.
[24]AEPD, Resolución de adopción de medida provisional contra Tools for Humanity Corporation, EXP202312448, 26 de febrero de 2024 [en adelante, Resolución AEPD 2024].

CAPÍTULO IV. ACCIONES DE LA AEPD Y CONTROL JURISDICCIONAL EN ESPAÑA

IV.1. La medida provisional de urgencia (art. 66.1 RGPD)

Mediante su Resolución de 26 de febrero de 2024 (EXP202312448), la Agencia Española de Protección de Datos adoptó medidas provisionales de urgencia contra Tools for Humanity Corporation, ordenando el cese inmediato de la recopilación y del tratamiento de datos personales en territorio español, así como el bloqueo de todos los datos ya captados a través de los dispositivos Orb desplegados en centros comerciales.[25] El fundamento jurídico de esta actuación se asienta en el artículo 66.1 RGPD, que faculta a las autoridades de control afectadas para adoptar medidas provisionales en caso de que exista una necesidad urgente de proteger los derechos y libertades de los interesados en su territorio, con independencia de cuál sea la autoridad principal competente.[26]

La AEPD fundamentó su decisión en tres pilares: la opacidad del tratamiento frente a los interesados, que impedía el ejercicio efectivo de sus derechos; la captación de datos de menores de edad sin las garantías exigidas por la LOPDGDD; y la naturaleza del incentivo económico en criptomonedas, que viciaba la libertad del consentimiento al crear un condicionamiento entre la obtención de un beneficio económico y la entrega de datos biométricos irreversibles.[27] La Agencia activó asimismo el mecanismo de urgencia previsto en el artículo 66.2 RGPD para informar al Comité Europeo de Protección de Datos de las medidas adoptadas, dado el carácter transfronterizo del tratamiento.[28]

IV.2. El control judicial de la Audiencia Nacional

[26]Art. 66.1 RGPD.
[27]Resolución AEPD 2024, op. cit., fundamento jurídico III.
[28]AEPD, Nota de prensa: "Worldcoin se compromete a paralizar su actividad en España", 4 de junio de 2024.

Tools for Humanity Corporation recurrió la medida provisional ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, solicitando su suspensión cautelarísima. La empresa argumentó, *inter alia*, que la AEPD carecía de competencia por no ser la autoridad principal en virtud del artículo 56 RGPD, y que la medida le generaba perjuicios económicos y reputacionales de difícil reparación.

En su Auto núm. 00241/2024, de 11 de marzo de 2024, la Audiencia Nacional desestimó el recurso de TFH con argumentación de notable solidez jurídica.[29] El Tribunal razonó, en primer lugar, que el artículo 66.1 RGPD otorga expresamente a las autoridades de control afectadas —y no solo a la autoridad principal— la facultad de adoptar medidas provisionales ante situaciones de urgencia, por lo que la AEPD actuó dentro de su competencia legalmente atribuida. En segundo lugar, y con mayor trascendencia doctrinal, el Tribunal afirmó con precisión que los perjuicios económicos son, por naturaleza, reparables mediante indemnización, en tanto que la pérdida de control sobre datos biométricos irreversibles puede ocasionar daños de imposible reparación,[30] lo que inclina el juicio de ponderación cautelar inequívocamente a favor de la tutela de los derechos fundamentales.

Esta doctrina judicial resulta de singular relevancia para la hermenéutica del artículo 66.1 RGPD en el marco de tratamientos de datos biométricos, al consagrar el principio de que la irreversibilidad del daño potencial sobre identificadores inalterables de la persona física constituye, *per se*, un criterio determinante en el juicio de ponderación cautelar. La Resolución de la AEPD y el Auto de la Audiencia Nacional han sentado, en este sentido, un precedente de notable valor para la interpretación coordinada

[29]Audiencia Nacional, Sala de lo Contencioso-administrativo, Auto núm. 00241/2024, de 11 de marzo de 2024, razonamiento jurídico II.
[30]Auto AN 00241/2024, op. cit., razonamiento jurídico III: "los perjuicios económicos son, por naturaleza, reparables mediante indemnización, en tanto que la pérdida de control sobre datos biométricos irreversibles puede ocasionar daños de imposible reparación."

del artículo 66 RGPD y del artículo 9 de la Carta de los Derechos Fundamentales de la Unión Europea.[3132]

Como resultado del procedimiento cautelar, Worldcoin asumió el compromiso jurídicamente vinculante de no reanudar sus operaciones en España hasta finales de 2024 o hasta que la autoridad bávara dictaminara de forma definitiva,[33] poniendo de manifiesto la eficacia de las medidas nacionales de urgencia como instrumento de tutela preventiva en el régimen del RGPD.

[31]Carta de los Derechos Fundamentales de la Unión Europea, DO C 326, 26 de octubre de 2012, art. 8.
[32]BOLDOVA MARZO, Daniel Miguel, "La Audiencia Nacional avala la medida cautelar de la AEPD que prohíbe la recopilación de datos biométricos a cambio de criptomonedas", Universidad de Zaragoza, 2024, pp. 8-14.

CAPÍTULO V. INVESTIGACIÓN DE LA BAYLDA Y EL MECANISMO DE VENTANILLA ÚNICA

V.1. El liderazgo de la autoridad principal bávara

El artículo 56 RGPD atribuye a la autoridad de control del establecimiento principal del responsable del tratamiento la condición de autoridad principal y, con ello, el liderazgo de cualquier investigación transfronteriza.[34] Dado que Tools for Humanity GmbH y Worldcoin Europe GmbH —entidades europeas del grupo— tienen su domicilio social en Múnich y Erlangen respectivamente, la BayLDA (Bayerisches Landesamt für Datenschutzaufsicht) asumió la dirección de la investigación coordinada, iniciada en abril de 2023 a raíz de consultas formuladas inicialmente por la autoridad francesa.[35] La complejidad técnica del expediente y la escala global del tratamiento —Worldcoin operaba simultáneamente en decenas de países— determinaron que la investigación se prolongara hasta diciembre de 2024, fecha en la que la BayLDA dictó su resolución definitiva con órdenes correctivas de eficacia erga omnes en el territorio de la Unión Europea.

V.2. Infracciones del artículo 32 RGPD y ausencia de base jurídica

La resolución de la BayLDA identificó dos bloques de infracciones de distinta naturaleza, cuya concurrencia revela una quiebra sistémica del cumplimiento normativo en el núcleo del modelo de negocio de Worldcoin.

El primer bloque, de carácter técnico, se concreta en la infracción del artículo 32 RGPD, que impone al responsable del tratamiento la obligación de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo el cifrado de los

[34]Art. 56 RGPD (mecanismo de ventanilla única).
[35]Resolución BayLDA 2024, op. cit., antecedentes (inicio de la investigación en abril de 2023 a raíz de consultas de la autoridad francesa).

datos personales.[36] La BayLDA constató que, desde julio de 2023 hasta mayo de 2024, Worldcoin almacenó los Iris Codes de sus usuarios en texto plano en una base de datos centralizada gestionada sobre infraestructura de Amazon Web Services (AWS), sin aplicar cifrado a nivel de dato.[37] Esta circunstancia resulta tanto más grave cuanto que el tratamiento recaía sobre datos de categoría especial en el sentido del artículo 9 RGPD, cuya inmutabilidad convierte cualquier exposición no autorizada —ya sea por intrusión externa o por requerimiento estatal— en un daño de reparación imposible.[38]

El segundo bloque de infracciones, de naturaleza jurídica, se articuló en torno a la comparación pasiva o deduplicación. La BayLDA concluyó que el tratamiento permanente de los Iris Codes con la finalidad de cotejar cada nuevo registro contra la base acumulada carecía de base jurídica válida.[39] Worldcoin no logró demostrar que el consentimiento prestado por los usuarios en el momento del escaneo inicial abarcara, con el grado de especificidad e información previa exigido por el RGPD, esta finalidad de tratamiento continuado e independiente.[40] La autoridad bávara descartó asimismo que el interés legítimo del artículo 6.1.f) RGPD pudiera constituir una base jurídica habilitante para el tratamiento de categorías especiales de datos en ausencia de una excepción expresa del artículo 9.2 RGPD.

V.3. Órdenes correctivas y efectos transfronterizos

La parte dispositiva de la Resolución BayLDA de 19 de diciembre de 2024 incluyó órdenes correctivas de obligado cumplimiento con eficacia en toda la Unión Europea.[41] Entre las más relevantes se encuentran: el borrado inmediato de todos los Iris Codes recabados durante el período en que el almacenamiento en texto plano infringió el artículo 32 RGPD; la obligación

[36]Arts. 25 y 32 RGPD.
[37]Resolución BayLDA 2024, op. cit., sección III.1 (almacenamiento de Iris Codes en texto plano desde julio de 2023 hasta mayo de 2024).
[38]Art. 32.1.a) RGPD: obligación de cifrado de datos personales.
[39]Resolución BayLDA 2024, op. cit., sección III.3 (comparación pasiva y ausencia de base jurídica válida).
[41]Resolución BayLDA 2024, op. cit., parte dispositiva, órdenes correctivas 1.ª a 4.ª.

de implementar un procedimiento efectivo y accesible para que los interesados puedan ejercer su derecho de supresión conforme al artículo 17 RGPD[42] —derecho que, de forma llamativa, no estaba garantizado en la arquitectura original del sistema—; y la prohibición de continuar el tratamiento con fines de comparación pasiva en tanto no se acredite una base jurídica válida y conforme con los artículos 6 y 9 RGPD.

La Resolución de la BayLDA tiene, además, una dimensión prospectiva de singular importancia: al descartar que el sistema SMPC constituya una anonimización en sentido jurídico y al calificarlo como mera seudonimización, la autoridad principal ha establecido un estándar interpretativo que condiciona la arquitectura técnica de cualquier sistema de identidad digital basado en biometría ocular que pretenda operar en el espacio europeo de protección de datos.[43]

[42]Art. 17 RGPD (derecho de supresión o "derecho al olvido").

CAPÍTULO VI. SÍNTESIS MULTIDISCIPLINAR Y CONCLUSIONES

VI.1. Implicaciones para la gobernanza europea de datos biométricos

El caso Worldcoin constituye un hito en la jurisprudencia administrativa europea sobre el tratamiento de datos biométricos con fines de identidad digital, y su análisis pone de manifiesto varias tensiones estructurales que el ordenamiento jurídico vigente debe abordar con precisión.

En primer lugar, el caso confirma que la mercantilización de la biometría mediante incentivos económicos es incompatible con el concepto de consentimiento libre exigido por el artículo 7 RGPD en relación con el considerando 43 de la misma norma.[44] La entrega de criptomonedas como contraprestación por el escaneo ocular crea un condicionamiento que vicia la autonomía del acto de consentimiento, transformando la privacidad en un bien transaccionable sometido a las dinámicas del mercado. Esta conclusión tiene implicaciones más amplias para todo modelo de negocio que ofrezca servicios o beneficios a cambio del tratamiento de datos personales, en particular cuando se trate de categorías especiales de datos.

En segundo lugar, el pronunciamiento coordinado de la AEPD, la Audiencia Nacional y la BayLDA ha validado la eficacia del mecanismo de cooperación previsto en el capítulo VII del RGPD, aunque con la matización de que la actuación paralela de la autoridad de control afectada —mediante el procedimiento de urgencia del artículo 66— puede resultar imprescindible cuando la magnitud del riesgo y la irreversibilidad del daño potencial no admiten dilación.[45] La doctrina del Auto AN 00241/2024 sobre

[45]STJUE de 13 de mayo de 2014, Google Spain SL y Google Inc. c. AEPD y Mario Costeja González, C-131/12, EU:C:2014:317 (derecho al olvido como manifestación del control sobre datos personales).

la prevalencia de la tutela de los datos biométricos irreversibles sobre los intereses económicos del responsable ha aportado un criterio hermenéutico de primera magnitud para la aplicación coordinada del artículo 66 RGPD.

En tercer lugar, el expediente evidencia la necesidad de aplicar los principios de privacidad por diseño y por defecto del artículo 25 RGPD[46] a los sistemas de identidad digital desde su fase de concepción arquitectónica. La circunstancia de que el derecho de supresión del artículo 17 RGPD no estuviera garantizado en la arquitectura original de Worldcoin revela una quiebra fundamental del cumplimiento normativo *by design*, cuya corrección no puede quedar diferida a la intervención *ex post* de las autoridades de control.

VI.2. Propuestas de lege ferenda

El análisis del caso Worldcoin pone de relieve que el marco normativo vigente, si bien ha demostrado suficiencia para responder a las infracciones concretas documentadas, presenta lagunas que justifican propuestas de *lege ferenda* orientadas a reforzar la protección preventiva.

Primera propuesta: la adopción, en el marco del Reglamento (UE) 2024/1689 o en una norma sectorial específica, de una prohibición expresa del condicionamiento biométrico: cualquier práctica que haga depender la entrega de bienes, servicios o incentivos económicos del consentimiento para el tratamiento de datos biométricos debe ser calificada como consentimiento estructuralmente viciado y, por tanto, jurídicamente ineficaz como base del tratamiento.[47]

Segunda propuesta: la introducción de un estándar mínimo de seguridad obligatoria para el tratamiento de datos biométricos que exija, con carácter imperativo y no meramente orientativo, el cifrado de los identificadores

[47]Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 [AI Act / RIA], DO L, 12 de julio de 2024, considerando 58 y arts. 9 y 10 (datos biométricos en sistemas de identificación).

biométricos a nivel de dato —con independencia de las medidas de seguridad perimetral adoptadas—, conforme a lo previsto en el artículo 32.1.a) RGPD y en la norma técnica ISO/IEC 30107-3:2023.[48]

Tercera propuesta: la clarificación, en el seno del Comité Europeo de Protección de Datos, de los criterios que distinguen la anonimización de la seudonimización en el contexto de los sistemas SMPC, con especial referencia a los supuestos en que el responsable del tratamiento controla directa o indirectamente a las entidades que custodian los diferentes fragmentos del identificador, adoptando directrices vinculantes que actualicen el Dictamen 05/2014 del Grupo de Trabajo del Artículo 29.[49]

Cuarta propuesta: la articulación, en el Reglamento (UE) 2024/1689,[50] de un régimen específico de evaluación de impacto (*DPIA*)[51] obligatoria ex ante para todo sistema de identidad digital global que implique el tratamiento masivo de datos biométricos con fines de singularización de personas físicas, con publicación obligatoria del resultado de la evaluación como condición previa al inicio del tratamiento.

[50]Reglamento (UE) 2024/1689 [AI Act], op. cit., art. 26 (obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo).
[51]CEPD, Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, adoptadas el 29 de enero de 2020, versión 2.0, pp. 30-35 (evaluación de impacto en tratamientos de alto riesgo).

BIBLIOGRAFÍA

I. Normativa

Carta de los Derechos Fundamentales de la Unión Europea, DO C 326, 26 de octubre de 2012.

Constitución Española de 1978, BOE núm. 311, 29 de diciembre de 1978, art. 18.4.

Convenio 108+ del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, modernizado en 2018.

ISO/IEC 30107-3:2023, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting, International Organization for Standardization, Ginebra, 2023.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [LOPDGDD], BOE núm. 294, 6 de diciembre de 2018.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [RGPD], DO L 119, 4 de mayo de 2016.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial [AI Act / RIA], DO L, 12 de julio de 2024.

II. Jurisprudencia y decisiones administrativas

Audiencia Nacional, Sala de lo Contencioso-administrativo, Auto núm. 00241/2024, de 11 de marzo de 2024.

BayLDA (Bayerisches Landesamt für Datenschutzaufsicht), Resolución de órdenes correctivas contra la Worldcoin Foundation, 19 de diciembre de 2024.

AEPD, Resolución de adopción de medida provisional contra Tools for Humanity Corporation, EXP202312448, 26 de febrero de 2024.

AEPD, Nota de prensa: "Worldcoin se compromete a paralizar su actividad en España", 4 de junio de 2024.

AEPD, Resolución de archivo de actuaciones respecto a Sideline Ventures, S.L., EXP202312448-B.

STJUE de 19 de octubre de 2016, Breyer c. Bundesrepublik Deutschland, C-582/14, EU:C:2016:779.

STJUE de 13 de mayo de 2014, Google Spain SL y Google Inc. c. AEPD y Mario Costeja González, C-131/12, EU:C:2014:317.

III. Doctrina

BOLDOVA MARZO, Daniel Miguel, "La Audiencia Nacional avala la medida cautelar de la AEPD que prohíbe la recopilación de datos biométricos a cambio de criptomonedas", Universidad de Zaragoza, 2024.

DAUGMAN, John, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, núm. 1 (2004), pp. 21-30.

RAMÓN FERNÁNDEZ, Francisca, "Datos de salud, datos especialmente protegidos: el caso de los datos biométricos y su comercialización", Universidad Politécnica de Valencia, 2024.

IV. Documentos institucionales

Comité Europeo de Protección de Datos (CEPD), Directrices 05/2020 sobre el consentimiento en virtud del Reglamento (UE) 2016/679, versión 1.1, adoptadas el 4 de mayo de 2020, WP259 rev.01.

Comité Europeo de Protección de Datos (CEPD), Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, versión 2.0, adoptadas el 29 de enero de 2020.

Grupo de Trabajo del Artículo 29, Dictamen 05/2014 sobre técnicas de anonimización, WP216, adoptado el 10 de abril de 2014.

GLOSARIO DE TÉRMINOS TÉCNICO-JURÍDICOS

Algoritmos opacos
Sistemas matemáticos de procesamiento cuya lógica interna y criterios de decisión no resultan transparentes para el interesado ni para las autoridades de supervisión, dificultando la auditoría de sesgos o imprecisiones. En el contexto del RGPD, la opacidad algorítmica puede vulnerar el principio de transparencia del artículo 5.1.a).

Anonimización
Proceso irreversible mediante el cual los datos personales son transformados de forma que el interesado no pueda ser identificado por el responsable del tratamiento ni por ningún tercero, empleando todos los medios razonables disponibles. A diferencia de la seudonimización, los datos anonimizados quedan fuera del ámbito de aplicación del RGPD. Véase Dictamen 05/2014 del Grupo de Trabajo del Artículo 29, WP216.

Comparación activa
Proceso técnico que ocurre durante el registro inicial del usuario, en el que la biometría captada se coteja con la base de datos existente para validar la singularidad de la nueva incorporación.

Comparación pasiva (deduplicación)
Almacenamiento permanente de los códigos de iris y cotejo continuado de estos contra cada nuevo intento de registro en la red, con el fin de prevenir duplicidades. La BayLDA ha concluido que este tratamiento carece de base jurídica válida en el modelo original de Worldcoin.

Datos biométricos
Categoría especial de datos personales [art. 4.14 y art. 9 RGPD] obtenidos mediante un tratamiento técnico específico relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o

confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Iris Code
Representación numérica binaria (0/1) generada por el dispositivo Orb a partir del análisis algorítmico de los patrones únicos del iris ocular, conforme al algoritmo de Daugman. Constituye el identificador biométrico primario en la arquitectura del sistema Worldcoin.

Lege ferenda (de)
Locución latina que designa el derecho tal como debería ser creado o reformado, por contraposición a la lex lata o derecho positivo vigente. Utilizada en este informe para encuadrar las propuestas de reforma legislativa orientadas a colmar las lagunas normativas detectadas.

Orb
Dispositivo sensor de imagen de alta resolución diseñado por Worldcoin/TFH para la captura de datos biométricos oculares y faciales y su transformación en Iris Codes.

Proof of Personhood (prueba de humanidad)
Concepto técnico y de negocio que designa el mecanismo mediante el cual Worldcoin pretende certificar que cada actor de su red es un ser humano único y no un sistema automatizado o una identidad duplicada.

Seudonimización
Tratamiento de datos personales de manera que ya no puedan atribuirse a un interesado concreto sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos no se atribuyan a una persona física identificada o identificable [art. 4.5 RGPD]. Los datos seudonimizados siguen siendo datos personales y están sujetos al RGPD.

SMPC (Secure Multiparty Computation / Computación Segura de Múltiples Partes)

Protocolo criptográfico mediante el cual el Iris Code se fragmenta en porciones (shares) distribuidas entre diferentes entidades, de modo que ninguna de ellas posea individualmente el identificador completo en texto plano. La BayLDA ha calificado este sistema como una técnica de seudonimización, no de anonimización.

Ventanilla única (One-Stop-Shop)

Mecanismo previsto en el artículo 56 RGPD que atribuye a la autoridad de control del establecimiento principal del responsable del tratamiento el liderazgo de las investigaciones transfronterizas, sin perjuicio de la facultad de las autoridades afectadas de adoptar medidas provisionales de urgencia conforme al artículo 66 RGPD.

World ID

Identidad digital global —denominada por la empresa pasaporte de humanidad— generada por el sistema Worldcoin como resultado del proceso de escaneo ocular. Certifica que el titular es un ser humano único registrado en la red y funciona simultáneamente como monedero de criptomonedas.