



# Who's who

**Iniciativas mal justificadas y oportunistas, como la de escanear el iris humano con misteriosos Orbes por una empresa relacionada con OpenAI a cambio de criptomonedas de dudoso futuro económico como las WorldCoins (WLD<sup>1</sup>), saltaron hace poco más de un año a la palestra informativa por sus diferencias con la Agencia Española de Protección de Datos que les llevaron a retirarse (diciembre 2024). Sin embargo, aquí aparecen de nuevo, tras un “rebranding” poco ingenioso, por lo que deberíamos echarle un vistazo a lo que puede haber detrás de tanta insistencia. No vaya a ser que necesitemos que nuestros gobiernos, autoridades e instituciones civiles, se deban oponer y nos defiendan. O en el peor de los casos, ver qué puede significar esta insistencia en el problema de la Identificación de usuario en la Internet actual.**

Desde mediados del siglo XIX, en Inglaterra, empezó a publicarse anualmente un elenco en forma de libro de tapas rígidas (y que terminó siendo publicado *on-line* en 1999) encargado de listar y dar información de gente alrededor del mundo que influía el estilo británico de vida. La “entradas” de dicha “base de datos” incluía “figuras notables” del gobierno (británico), la política, el mundo académico, empresarial, deportivo y de las artes. La edición de 2025 del Who's Who<sup>2</sup>, es la edición 177 (Oxford University Press) e incluye más de 32.500 personas distintas.

Este prominente trabajo de referencia bibliográfica del Reino Unido es que, supongo, debe tener en mente una reaparecida compañía tecnológica del panorama patrio actual, World<sup>3</sup>, o Worldcoin<sup>4</sup> si nos fijamos en su primera identidad. Informaciones de la prensa española informan de la reaparición de la empresa World. En este caso, World regresa a Barcelona en el 550 de la avenida Diagonal, con el tema del escaneo de iris humano.

Un año y once meses después de que la Agencia Española de Protección de Datos (AEPD) le prohibiera de manera cautelar a la compañía Worldcoin seguir tratando datos personales en España, la retitulada tecnológica anuncia su regreso a nuestro país (¡hay que ver su insistencia! Sin duda, ¡ganan algo con esto!).

La empresa World, también conocida como **World Network**, es un proyecto financiero y proyecto de verificación del **carácter humano**<sup>5</sup> de sus clientes. Originalmente fue lanzada como un proyecto de criptomonedas llamado Worldcoin<sup>6</sup>.

Entre sus principales valedores está la empresa **Tools for Humanity**, compañía fundada en 2019 por Sam Altman, Max No-

vendstern, y Alex Blania. Con la misión de “proveer” un método eficaz y confiable a la vez que anónimo de autenticar humanos en línea que ellos llaman **World ID**.

Después de reunir 250 millones de dólares norteamericanos de diferentes firmas de Venture Capital (como, por ejemplo, Andreessen Horowitz<sup>7</sup>), lanzó una primera versión beta en 2023. El proyecto fue “rebautizado” como World en 2024<sup>8</sup>. Punto en el que la aventura incluye como compañeros a los gobiernos de Taiwan y de Malaysia, preocupados por la verificación de Identidad en redes.

La idea es que para que los clientes puedan utilizar el servicio, deben descargarse en sus teléfonos su app, luego deben permitir que su iris ocular sea escaneado con “el Orbe”<sup>11</sup> plateado, del tamaño de un balón de tamaño pequeño que incluye dentro de sí, el sistema opto electrónico que permite el escaneo del iris mostrado delante de su único orificio. Una vez completo el escaneo, el usuario es incluido en una **base de datos de humanos verificados**, para el que Worldcoin creó un *hash* criptográfico únicamente relacionado con esa persona.



**El iris humano es verificable por cualquiera (humano y no humano), lo cual permite el desvelado público de cualquier identidad en el caso de que le sea necesario (a la empresa) relacionando una determinada identidad con un ente externo no-digital.**

## VERIFICACIÓN BIOMÉTRICA

Para unirse a la red, los candidatos deben completar la verificación biométrica de los mismos ante el artefacto de la compañía conocido como “El Orbe”, en ciertos locales u ubicaciones de la empresa en lugares estratégicos (por ejemplo, en España, en centros comerciales). En su versión inicial, dicha colaboración iba acompañada de la entrega del *digital token* de la empresa<sup>9</sup>, el Worldcoin (WLD), cuyo valor de cambio, en aquellos días, equivalía a unos 80 dólares, lo cual causó furor entre la juventud (criptobros y demás subespecies) y en países pobres como es el caso de Kenia<sup>10</sup>.

El iris escaneado no se almacena en el Orbe, pero el valor *hash* derivado de él podrá ser utilizado posteriormente para “probar” la identidad de su titular de modo anónimo a través de la app de World, que incluye claves privadas relacionadas con una clave pública. Dado que el sistema se ha diseñado para verificar que una persona es realmente un individuo único, si el titular quiere autenticarse, por cualquier razón, pediría al sistema que generase una determinada prueba de conocimiento nulo (**zero-knowledge proof**) que permita a su titular proveer (siempre **a través de World**) sólo la información realmente necesaria a la tercera parte ante la que quiere operar.

Lo que ocurrió tras el primer lanzamien-

to es que varias Agencias de Regulación de Datos Personales, entre ella la española, les pusieron “pegas” al modo en el que ellos recababan esos iris oculares (datos biométricos claramente identificadores) que, además de identificar a cualquier persona, también podría incluir ciertas informaciones sobre la salud de su titular.

### VERIFICACIONES ZERO-KNOWLEDGE

Para esta segunda reaparición, sus promotores decidieron quitar todo lo referido al código de iris, y ahora dicen utilizar un sistema **AMPC**<sup>12</sup> (**Anonymized Multi-Party Computation**) que, según ellos, permite generar verificaciones **Zero-Knowledge** sin almacenar en el orbe ningún tipo de datos. Según **Tiago Sada**<sup>13</sup>, jefe de producto en la empresa **Tools for Humanity**, en la versión actual<sup>14</sup>, todas las fotos del Orbe sólo se encuentran en el móvil personal de cada usuario y nadie tiene acceso a esa información<sup>15</sup>. Quizás con estos

criptográficos desde hace muchas décadas). Lo importante es que **el problema de fondo sigue intacto**.

### UNA AGENCIA DE IDENTIFICACIÓN MUNDIAL

Olvidando todos esos botes de humo, netamente técnicos y criptográficos, de lo que en este caso se trata del **lanzamiento mundial de una agencia de identificación** que pretende reservarse el haber

utilizando SMSs<sup>17</sup> como Segundo Factor<sup>18</sup>) y en los que no necesariamente se ve la voluntad jurídica del usuario.

El objetivo del negocio es la disposición de una base de identidades lo más extensa posible de entes considerados humanos por parte del promotor. Cuando buscaron cómo saber si de un humano se trata, optaron por utilizar lo que estaba muy de moda hace meses, como es y era la biometría<sup>19</sup>. Y de entre todas las posibilidades de **identificación biométrica**,



*Si los objetivos son seres humanos analógicos, éstos contienen tantas debilidades intrínsecas que les convierte en una amplia población de individuos/consumidores fácilmente manipulables, e incluso, los puede hacer “prescindibles”.*



*El establecimiento de una identidad digital sólo requiere de un número secreto suficientemente grande y con suficiente entropía como para ser secreto, aleatorio y único, durante largas porciones de tiempo que, en el caso de los seres humanos, debería ser superior a su longevidad.*

pequeños cambios estéticos adoptados por la empresa promotora puedan levantar las cautelas de las Agencias de Protección de Datos (esperemos que no sea así porque lo de pruebas de Zero-Knowledge es una engañifa técnica que ha estado rondando en el mundo de los protocolos

tenido acceso (voluntario o no) a un humano para apuntarlo en su base de datos **y poder hablar en su nombre a través de la World App**.

eligieron la más futurista y de mayor impacto ante el Gran Público, como es el reconocimiento a través de **reconocimiento de iris ocular**<sup>20</sup>.

El poder discriminante de todas las técnicas de identificación biométrica depende de la cantidad de **entropía**<sup>21</sup> contenida en ella, y utilizar ese **grado de unicidad** en las **verificaciones por coincidencia**. El reconocimiento de iris es excepcional desde este punto de vista porque su entropía es tan alta que hace muy poco probables las “colisiones” o “coincidencias erróneas”, incluso en el caso de poblaciones masivas como sería la **población planetaria presente, pasada y futura**. Su mayor limitación es la adquisición de la imagen del iris de uno o ambos ojos a distancias mayores de uno o dos metros, o incluso sin cooperación por parte del “dueño del iris”. Sin embargo, actualmente, ese pro-

La idea no es realmente tan diferente al ejemplo del **sistema Cl@ve Firma**<sup>16</sup> de la Administración española, en la que el Cuerpo Nacional de Policía firma digitalmente, en nuestro nombre, después de haber verificado la autorización a través de protocolos y canales de menos seguridad (por ejemplo,

<sup>1</sup> Ver <https://coinmarketcap.com/es/currencias/worldcoin-org/>

<sup>2</sup> Ver <https://www.ukwhoswho.com/>

<sup>3</sup> Ver [https://en.wikipedia.org/wiki/World\\_\(blockchain\)](https://en.wikipedia.org/wiki/World_(blockchain))

<sup>4</sup> Ver <https://es.wikipedia.org/wiki/Worldcoin>

<sup>5</sup> Ver <https://world.org/es-es>

<sup>6</sup> Ver <https://techcrunch.com/2023/03/07/worldcoin-cofounded-by-sam-altman-is-betting-the-next-big-thing-in-ai-is-proving-you-are-human/>

<sup>7</sup> Ver [https://en.wikipedia.org/wiki/Andreessen\\_Horowitz](https://en.wikipedia.org/wiki/Andreessen_Horowitz)

<sup>8</sup> Ver <https://www.reuters.com/technology/artificial-intelligence/sam-altmans-rebranded-worldcoin-ramps-up-iris-scanning-crypto-project-2024-10-17/>

<sup>9</sup> Ver <https://world.org/es-es/worldcoin-token>

<sup>10</sup> Ver <https://www.bbc.com/news/world-africa-66383325>

<sup>11</sup> Ver <https://github.com/worldcoin/orb-hardware>

<sup>12</sup> Ver [https://en.wikipedia.org/wiki/Secure\\_multi-party\\_computation](https://en.wikipedia.org/wiki/Secure_multi-party_computation)

<sup>13</sup> Ver <https://www.linkedin.com/in/tiagosada/>

<sup>14</sup> Ver <https://world.org/es-es/blog/announcements/worldcoin-foundation-unveils-new-smpc-system-deletes-old-iris-codes>

<sup>15</sup> Ver <https://support.world.org/hc/es-419/articles/15273885973267--Cómo-funciona-el-Orb>

<sup>16</sup> Acuerdo del Consejo de Ministros español, en su reunión del 19 de septiembre de 2014. Ver <https://sede.seg-social.gob.es/wps/portal/sede/sede/Inicio/ClaveldElectronica/> <https://clave.gob.es/dnin>

<sup>17</sup> Ver <https://en.wikipedia.org/wiki/SMS>

<sup>18</sup> Ver [https://en.wikipedia.org/wiki/Multi-factor\\_authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication)

<sup>19</sup> Ver <https://en.wikipedia.org/wiki/Biometrics>

<sup>20</sup> Ver [https://en.wikipedia.org/wiki/Iris\\_recognition](https://en.wikipedia.org/wiki/Iris_recognition)

<sup>21</sup> Ver [https://en.wikipedia.org/wiki/Entropy\\_\(information\\_theory\)](https://en.wikipedia.org/wiki/Entropy_(information_theory))

blema técnico está superado y esa adquisición puede realizarse incluso a cinco o más metros de la cámara.

## ESTABLECIMIENTO DE UNA IDENTIDAD DIGITAL

En realidad, el establecimiento de una identidad digital sólo requiere de un **número secreto suficientemente grande y con suficiente entropía** como para **ser secreto, aleatorio y único**, durante largas porciones de tiempo (que, en el caso de los seres humanos, debería ser superior a su **longevidad**<sup>22</sup>). Este parámetro secreto que va a ser vinculado y va a actuar como representante de un objeto "externo" al mundo digital. La tendencia a querer relacionar esa identidad digital a un individuo u objeto no-digital con una característica biométrica es problema del verificador, que podría querer en cualquier momento **1) demostrar ante terceros** que su identidad realmente está respaldada por la existencia de dicho objeto, **2) poder estar seguro** (y así venderlo como parte del servicio) de **la unicidad de tal identidad**. Y estas dos son las características principales que quiere vender la empresa World a sus clientes mediante su WorldID.

Como la empresa elige el iris ocular, todos sus representados serán cuerpos (no necesariamente humanos vivos). Los promotores de este sistema alegan el carácter (supuestamente humano) a sus bases de datos de futuros usuarios digitales (es decir de WorldIDs). Sin embargo, todo este razonamiento no está carente de debilidades.

## ¿IRIS HUMANOS?, NO NECESARIAMENTE

Los iris son aceptablemente únicos, pero **no necesariamente de humanos** (ni todos los humanos tienen iris que utilizar). La posesión de un iris no es sinónimo de que su titular **lo ha entregado libre y conscientemente**. Cualquiera puede conseguir los iris de cualquiera si consigue que le mire a la cámara durante uno cuantos milisegundos. El iris humano es verificable por cualquiera (humano y no humano), lo cual permite el desvelado público de cualquier identidad en el caso de que le sea necesario (a la empresa) relacionando una determinada identidad

con un ente externo no-digital.

Otra cosa que hay que plantearse con este tipo de empresas es la Liturgia con la que dicen justificar su existencia y su carácter de potencial unicornio blanco para engañar a los inversores ¿Cuál puede ser la necesidad real de **distinguir seres humanos (analógicos)** detrás de las transacciones y operaciones netamente digitales que realizan en su nombre **sus representantes** (identidades digitales y los que las implementan)?

Si pensamos en una Internet plenamente autenticada en la que tanto servidores como usuarios estas plenamente identificados (y son legalmente responsables), el sistema que persigue World es de una proveedora de identidad basada en pseudónimos (los WorldIDs). Aunque la empresa jurarse y perjurase que jamás desvelaría quien está detrás de cada una



**Al final, el futuro de este tipo de iniciativas, si son reales, es establecer un sistema de identidad planetaria en la que los usuarios sean los pagadores del servicio o, como ocurre con Internet, son simplemente las víctimas, los objetivos de negocio, y su identificación, perfilado, ubicación, y reconocimiento es lo que la empresa vende y lo que sus clientes compran.**

de sus identidades, el uso de seudónimos **1) no elimina la trazabilidad** y el cruzamiento de operaciones con un mismo seudónimo y, sobre todo, **2) que el vínculo existe y puede ser robado u obtenido bajo coacción**<sup>23</sup> (legal o por la fuerza o mediante engaño).

Al final, el futuro de este tipo de iniciativas, si son reales, es establecer un sistema de identidad planetaria en el que los usuarios sean los pagadores del servicio o, como ocurre con Internet, los usuarios son simplemente las víctimas, los objetivos de negocio, y su identificación, perfilado, ubicación, y reconocimiento es lo que la empresa vende y lo que sus clientes compran.

Todo este tinglado no tiene nada que ver con la Inteligencia Artificial, ya que a ésta le importa poco de dónde salen los datos con los que se la entrena. Sin embargo, si los objetivos son seres humanos analógicos, éstos contienen tantas **debilidades intrínsecas** que les convierte en

una amplia población de individuos/consumidores fácilmente **manipulables**, e incluso, los puede hacer "**prescindibles**".

## EL ANONIMATO COMO LA OPCIÓN MÁS INTELIGENTE

Dado que la únicas Inteligencias Artificiales con éxito que hay en el panorama actual son las **Inteligencias Artificiales Militares (Selectores automáticos de objetivos** de eliminación, bombardeo, etc., **la armonización de jaurías de drones suicidas baratos, centinelas automáticos**, colaboración/coordinación de **interceptores antiaéreos** basados en misiles tierra-aire, y algunas más), en ninguna de ellas conviene jugar el papel de persona identificable, por lo que **el Anonimato es la opción más inteligente** para la supervivencia del titular.

Por otra parte, los que sólo ven negocios no son sensibles a ello, pero quienes sí consideran el derecho a una identidad uno de los Derechos Humanos esenciales, la identidad es algo que otorga la sociedad dentro de la que está sumergido el individuo, por lo que privatizas lo que ahora entregan comunidades y Estados, veríamos el éxito de la **identificación digital plena** como un **derecho inalienable** que debería otorgar esa misma sociedad (Policía civil, Registros Nacionales, Ayuntamientos, Censos, etc.) pero esa posibilidad está limitada por las intenciones reales de los gestores de dichas instituciones. Y dado que "*no es oro todo lo que reluce*" en las **sociedades falibles** que vivimos, **el Anonimato vuelve a ser la opción más inteligente** para disfrutar de una vida tranquila y provechosa. ■

**JORGE DÁVILA**  
Consultor independiente  
Director  
Laboratorio de Criptografía  
LSIIS – Facultad  
de Informática – UPM  
jdavila@fi.upm.es

<sup>22</sup> Ver <https://en.wikipedia.org/wiki/Longevity>

<sup>23</sup> Ver [https://en.wikipedia.org/wiki/Duress\\_in\\_American\\_Law](https://en.wikipedia.org/wiki/Duress_in_American_Law)