Comunicación Libre

El iris, la contraseña más fiable y peligrosa

The iris, the most reliable and dangerous password

Carla Sánchez Remacha, Cristina Calvo Simón, Luca Manuel Bueno Borghi, Julia Aramburu Clavería

Hospital Clínico Universitario Lozano Blesa
Autora para la correspondencia: Carla Sánchez Remacha, carlasanchezre@hotmail.com

RESUMEN

Recientemente, más de 400.000 personas en España se han inscrito a Worldcoin para escanear su iris a cambio de criptomonedas. La multinacional, liderada por el fundador de ChatGPT, busca asignar a cada persona en la tierra una especie de DNI digital con el que poder identificarte como un humano y diferenciarse de los bots.
Sin embargo, la Agencia Española de Protección de Datos ha prohibido la actividad de forma cautelar afirmando que debe prevalecer el derecho a la protección de datos personales frente al interés económico de la empresa.
El iris, como las huellas dactilares, prácticamente no varía con el tiempo. Sus fibras musculares forman un patrón particular muy complejo, único para cada persona y cada ojo. Refleja datos de salud permitiendo extraer información adicional. Por ello, los expertos avisan de los riesgos de vender tus datos biométricos: cesión a terceros, suplantación de identidad, ciberdelincuencia, condicionamiento profesional, riesgo social y a la propia intimidad.

Palabras clave: iris, escáner, datos biométricos, inteligencia artificial, protección de datos, seguridad.

ABSTRACT

Recently, more than 400,000 people in Spain have signed up for Worldcoin to scan their irises in exchange for cryptocurrency. The multinational, led by the founder of ChatGPT, seeks to assign each person on Earth a type of digital ID with which to identify yourself as a human and differentiate yourself from bots.
However, the Spanish Data Protection Agency has prohibited the activity as a precautionary measure, stating that the right to protection of personal data must prevail over the economic interest of the company.

Artículo basado en la comunicación «Vender tu iris al mejor postor», presentada en la *XXX Reunión Anual del Grupo de Historia y Humanidades en Oftalmología*, en el *100 Congreso de la Sociedad Española de Oftalmología*, celebrado en Madrid en septiembre de 2024.

Conflicto de intereses y cesión de derechos: Carla Sánchez Remacha, autora, y Cristina Calvo Simón, Luca Manuel Bueno Borghi y Julia Aramburu Clavería, como coautores, certifican que este trabajo es original, no ha sido publicado ni está en trámites de valoración para la publicación en otra revista. Asimismo, transfieren los derechos de propiedad (copyright) del presente trabajo a la *Revista Española de Historia y Humanidades en Oftalmología.*

The iris, like fingerprints, practically does not change over time. Its muscle fibers form a very complex particular pattern, unique for each person and each eye. It reflects health data allowing additional information to be extracted. For this reason, experts warn of the risks of selling your biometric data: transfer to third parties, identity theft, cybercrime, professional conditioning, social risk and privacy risk.

Keywords: iris, scanner, biometric data, artificial intelligence, data protection, safety.

Hace pocos meses, cerca de 400.000 españoles y 4 millones de personas alrededor del mundo han escaneado su iris a cambio de dinero. Se ha podido ver en centros comerciales de varias ciudades españolas largas filas de gente, incluyendo menores de edad, accediendo a esta iniciativa. Unas esferas metálicas, llamadas *Orb,* registran los iris y el usuario, a través de una App y un código QR, obtiene criptomonedas por valor de unos 70 euros.

Según la multinacional que hay detrás de esta actividad, «Worldcoin», liderada por el creador de «ChatGPT», este proyecto pretende crear un nuevo dato personal, igual que el nombre o la huella dactilar, como un DNI digital que nos diferencie de la inteligencia artificial (IA), para por ejemplo en el futuro si alguien sube un vídeo, imagen o *fake news* a la red, saber si ha sido realizado por un humano o un robot.

La multinacional privada quiere crear un archivo más personal que el DNI a nivel gubernamental. Las dudas surgen respecto a sus objetivos y el posible uso de nuestros datos. El modus operandi de estas empresas se basa en transformar los datos biométricos en algoritmos con el pretexto de funcionar como un factor de autenticación.

Como todos los algoritmos, necesitan de iris reales para identificar mejor los patrones complejos del iris. Cuantos más casos reales ha leído, el algoritmo detecta de una forma más precisa y adquiere mayor calidad para su venta. Se trata de una razón de competencia entre empresas. Por otro lado, a cada iris escaneado se asocian unos datos personales; información que tiene muchísimo valor en el mercado.

El escáner de iris está diseñado para leer su patrón muscular complejo y correlacionar con los patrones guardados anteriormente. Para escanear el patrón del iris se aplica una radiación cercana al infrarrojo. En primer lugar, permite que el escáner funcione

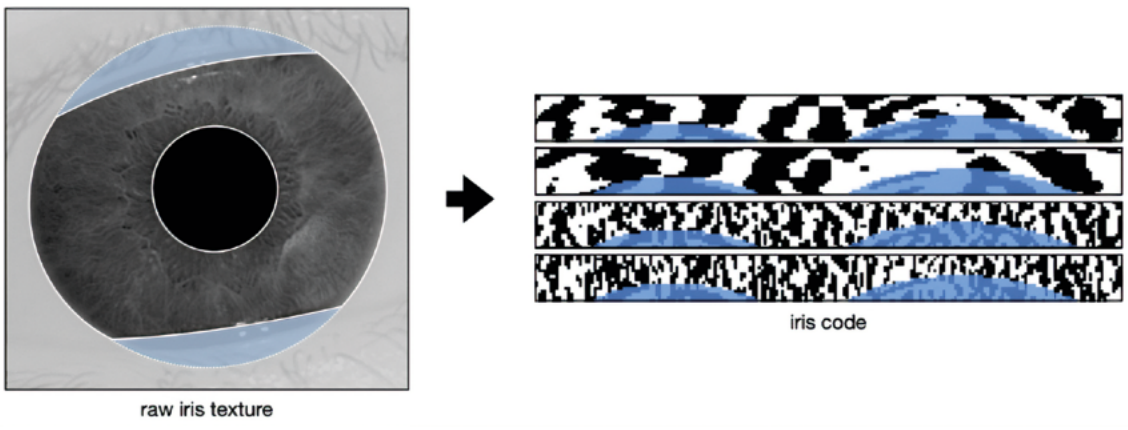

Figura 1: Escáner de iris: se analiza la textura y patrón muscular del iris y se crea un código a partir de esta información.

incluso en la oscuridad, y, en segundo lugar, lee la imagen con mucha más precisión que la radiación del espectro de luz visible. Una vez finalizada la exploración, el dibujo se traduce en un código que se compara con el registro guardado anteriormente buscando la coincidencia.

Las gafas y las lentes de contacto blandas no impiden el paso de los rayos de luz, por lo que no tienen un efecto negativo en la calidad del reconocimiento. Con una dilatación pupilar buena (9 mm) o tras una iridotomía láser, la forma del iris no se altera lo suficiente para dar falsos negativos. Pero hay casos o enfermedades oculares que reducen la precisión del escaneo del iris o impiden directamente que se realice, como el uso de lentes de contacto rígidas, lentillas cosméticas o tras sufrir alteraciones en la disposición y textura del iris por sinequias iridianas en uveítis o como secuela postraumática.

En la actualidad, sobre todo con la IA, nuestros datos biométricos adquieren un valor mayúsculo, porque podemos cambiar, modificar, omitir o mentir sobre un nombre, un término, una contraseña, pero los datos biométricos son únicos y unívocos, nos identifican claramente y nos diferencian del resto de las personas. No hay dos iris iguales, ni siquiera entre ambos ojos de una persona. Además, es un órgano que no se modifica de forma natural con el tiempo.

El principal riesgo asociado es que nos pueden identificar de forma única. La persona ya está marcada y monitorizada prácticamente de por vida. En ese sentido, estamos entrando en una nueva economía, la economía de los sentimientos, en la que la biometría es fundamental para el reconocimiento emocional de las personas y para que nos puedan trazar en función de nuestras reacciones emocionales.

Si nuestros datos se han vendido o compartido con empresas terceras, con objetivos no muy claros, o se *hackean*, la suplantación de identidad es fácil y se pueden atribuir acciones, daños o delitos a la persona identificada. La ciberdelincuencia, el ciberacoso o el condicionamiento que estos datos pueden tener en el presente o futuro próximo a nivel profesional son otros riesgos a tener en cuenta por el usuario.

También podemos perder el control sobre nuestras cuentas bancarias, administrativas y personales. De todo ello depende nuestra vida. Y es que ofrecer nuestros datos biométricos es dar la llave de nuestra intimidad.

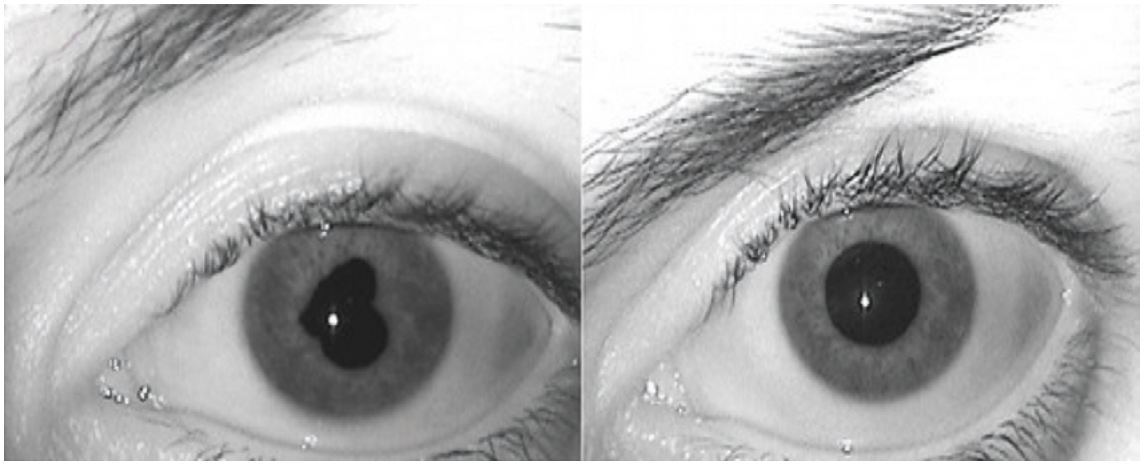

Figura 2: Mismo ojo antes y tras corrección quirúrgica de sinequias iridianas por uveítis anterior. En este caso el sistema dio un falso negativo y no fue capaz de identificar al usuario después del tratamiento.

Hay otro riesgo menor en cuanto a la compensación económica. Y es que, si un grupo de personas desean vender sus criptomonedas al mismo tiempo, su valor se puede igualar a cero, al ser un dinero virtual, una moneda muy volátil, con un valor variable de un día para otro.

El término «compraventa» por nuestro iris ya tiene un componente bastante sensible. El fundamento legal que lo permite se basa en el Consentimiento Informado. Pero para que sea válido, la persona debe ser informada correctamente, con lenguaje sencillo, con información clara y suficiente para que un usuario medio pueda entender lo que se está llevando a cabo. Debe ser otorgado de forma libre, no verse la persona arrastrada por una situación de desequilibrio que vicie la validez del consentimiento. Además de la capacidad de revocación en cualquier momento, que en este caso no se ofrecía a los usuarios. En este sentido, la legislación ampara a los ciudadanos a poder retirar su consentimiento, desistir o arrepentirse y paralizar sus datos en cualquier momento.

El mito de que el consentimiento informado lo puede todo, no es real. Las Agencias de Protección de Datos, nacional y autonómicas, determinan si es suficiente o no un consentimiento informado para el tratamiento de este tipo de información, aunque haya sido brindado de forma correcta.

Entre la legislación que regula este tipo de actividad y nos protege está la normativa de Protección de datos, por ser datos altamente sensibles; la ley de Protección del honor y la intimidad de la persona, también de aplicación en España; y la nueva regulación que llega en materia de IA, que trata de proteger los derechos digitales de los usuarios a la privacidad mental, teniendo mucho que ver con la biometría para dicho reconocimiento de las emociones de las personas. Aportar datos de estas características supone un peligro. De hecho, esta misma ley prohíbe la identificación biométrica en espacios públicos a través de IA, es decir como esa idea de «gran hermano» que nos puedan estar grabando por la calle e identificar con una cámara.

La empresa en cuestión asegura que los datos son anónimos y que el procedimiento es muy seguro. Pero en los «Términos y condiciones» de su propia página afirman que pueden compartir los datos con vendedores y proveedores ajenos a la propia empresa, es decir que los datos pueden circular. Y en caso de que haya algún problema o debilidad en el software, es decir el problema es suyo, o roben estos datos, no garantizan una solución.

Por eso, es nuestra responsabilidad leer las condiciones del documento que se ofrezca al usuario para firmar, donde deben de informar siempre a este respecto, saber cómo usan

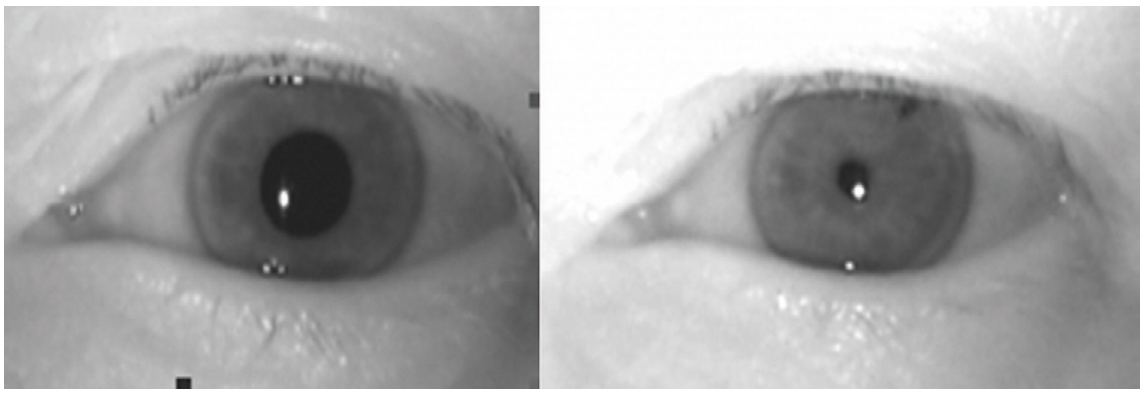

Figura 3: Mismo ojo antes y tras iridotomía. En este caso el sistema de reconocimiento fue capaz de detectar al paciente antes y después del procedimiento.

nuestros datos y si los pueden vender o no ahora y en un futuro. Si pueden cambiar esta política con el tiempo y en qué condiciones.

Hubo varias reclamaciones particulares en las que denunciaban, entre otros aspectos, que los usuarios recibían una información insuficiente, por la captación de datos de menores, o porque no se permitía la retirada del consentimiento inicial. El asunto es de tal importancia que el proyecto ha sido paralizado cautelarmente por la Agencia Española de Protección de Datos y la Audiencia Nacional, siendo la primera vez en la historia que esto se lleva a cabo antes de concluir una investigación y de resolver un expediente. Argumentan que «debe prevalecer la protección de datos personales frente al interés económico de la empresa».

Se puede concluir que las nuevas tecnologías avanzan también en materia de seguridad. En este sentido, el Iris, ese órgano tan preciso, tan precioso para el mundo de la oftalmología y tan preciado para otros, puede convertirse en la contraseña más fiable y peligrosa. Por eso, es importante reflexionar hacia dónde van nuestros datos, quiénes los van a usar y con qué finalidad.

BIBLIOGRAFÍA

1. Girdhar N, Sharma D, Kumar R, Sahu M, Lin CC. Emerging trends in biomedical trait-based human identification: A bibliometric analysis. SLAS Technol. 2024; 29(3): 100136.
2. Samatas GG, Papakostas GA. Biometrics: Going 3D. Sensors (Basel). 2022; 22(17): 6364.
3. Jeon B, Jeong B, Jee S, Huang Y, Kim Y, Park GH *and cols*. A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation. JMIR Mhealth Uhealth. 2019; 7(4): 11472.