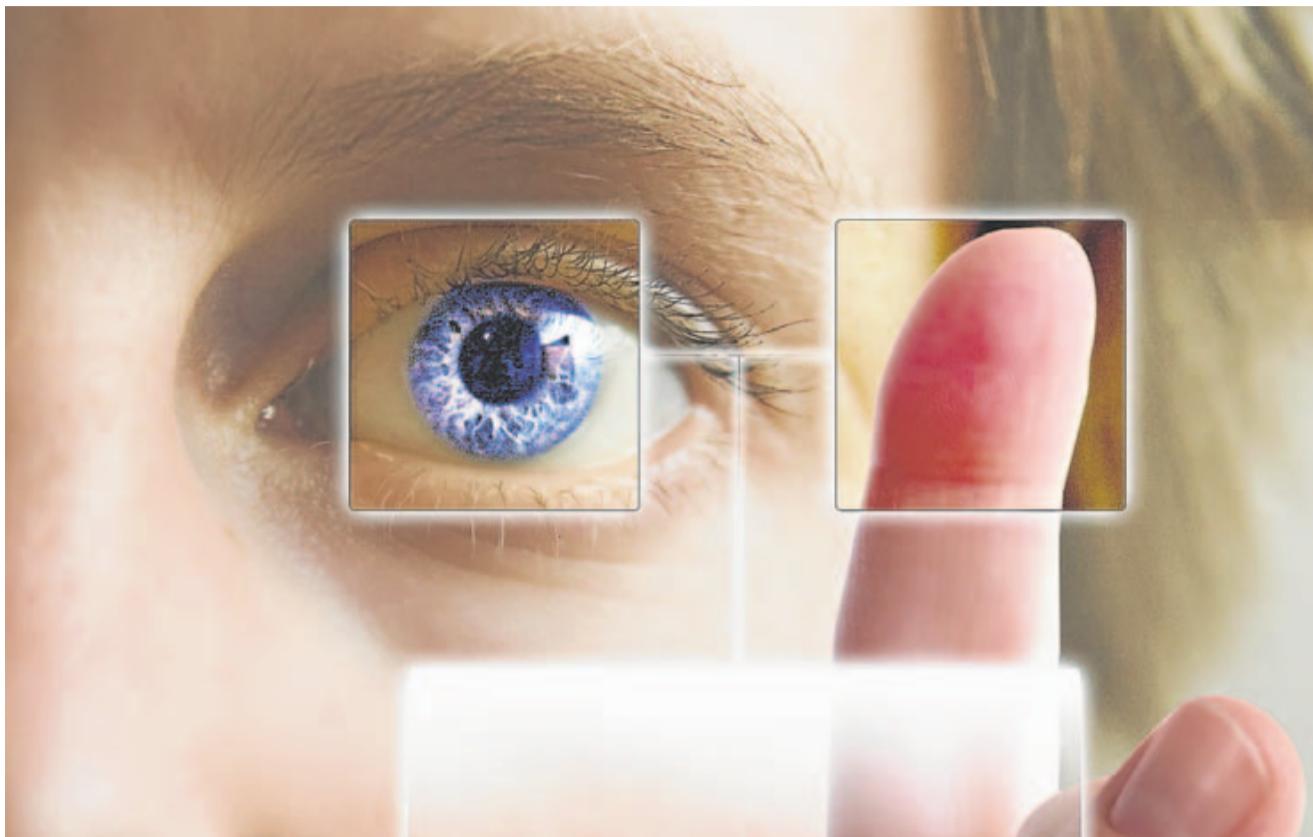


EL ANÁLISIS PROTECCIÓN DE LOS DATOS BIOMÉTRICOS



Escaneo de iris y huella dactilar mediante reconocimiento biométrico. FOTOLIA.

Lo que el ojo cuenta de ti

Escaneo de iris Proyectos como Worldcoin hacen saltar las alarmas por el riesgo de un uso viciado de los datos recogidos, según expertos de UNIR

V. DUCRÓS

Llega un día en el que la ciencia ficción deja de serlo para convertirse en algo real. Películas como 'Minority Report', con escenas tan tecnológicamente futuristas –cabe recordar que se estrenó hace más de dos décadas– y, en apariencia utópicamente replicables, lanzaron el guante que bien han sabido recoger grandes compañías tecnológicas.

Proyectos como Worldcoin han demostrado que ese futuro tan lejano de las películas estaba más cerca de lo que se intuía. Y han sabido atraer a millones

de personas para que, sin ser en muchos casos conscientes de las consecuencias y riesgos que lleva, les cedan su información más valiosa, sus datos biométricos –únicos para cada persona-. Actualmente, la información biométrica brinda una identificación casi perfecta. A diferencia de las contraseñas, no puede modificarse, por lo que esos datos valiosos corren el riesgo de poder sufrir un uso viciado.

En España se estima que cerca de medio millar de personas ya habían escaneado su iris a cambio de criptomonedas antes

de que la Asociación Española de Protección de Datos obligara a Worldcoin a interrumpir, de manera cautelar –porque la suspensión no puede exceder los tres meses–, su actividad en España. Es decir, «impide que siga tratando datos personales y bloquee los que ya tenía recopilados», explica Susana Duro, directora del Máster Universitario de Protección de Datos. «La normativa europea de protección de datos permite que en circunstancias excepcionales se intervenga urgentemente para preservar el derecho a la protección

de datos y el derecho a la intimidad de los ciudadanos de manera provisional», añade.

¿Cuál era el propósito de Sam Altman, CEO de OpenAI y creador de Chat GPT, con su proyecto Worldcoin? «Crear una base de datos biométrica de personas con la que poder entrenar a un software para que sea capaz de reconocer si una persona es real o está generada por inteligencia artificial», desarrolla Manuel Sánchez, codirector del Máster Universitario en Ciberseguridad de UNIR e investigador científico en el Instituto Nacional de

LA FRASE

Manuel Sánchez Rubio
Codirector del Máster en Ciberseguridad de UNIR



«Worldcoin busca enseñar a su software a diferenciar a personas reales de las generadas por IA»

Técnica Aeroespacial del Ministerio de Defensa. «Para poder diferenciar si es una persona real o no, necesita unos patrones o datos biométricos. Cada ojo es único en el mundo».

«A remolque»

El quid de la cuestión reside en el fin último del destino de ese escaneo de iris. Un tema delicado, ya que esos datos recogidos «pueden venderse a personas o países con normativas mucho más laxas», apunta Susana Duro. Pone el ejemplo de Estados Unidos o China, «que albergan las bases de las grandes tecnológicas» y donde esa permisibilidad en las medidas de control les hace ir por delante de la Unión Europea en esta área. «Vamos un poco a remolque, por esa protección mayor de los derechos fundamentales y avanzamos más despacio por tener que conjugar la adaptación de las normativas con evitar la vulneración de derechos fundamentales».

Worldcoin empleaba un sistema biométrico muy similar a los sistemas de vigilancia masiva que utilizan otros estados y que «choca de pleno con nuestras actuales directivas y regulaciones», aclara. Pero reconoce que es algo imparable e «irremediablemente tendrá que regularse sí o sí». Será la Unión Europea la encargada. «Sucedie siempre en Derecho; primero se dan los cambios sociales o tecnológicos y luego es el propio Derecho el que tiene que regular cada situación concreta», subraya Duro.

Una identificación que necesita ser protegida y asegurada

V. D.

LOGROÑO. El iris es como la huella dactilar. Proporciona la identificación de una persona de manera inequívoca y refleja aquellas características físicas, fisiológicas e incluso conductuales de una determina-

da persona que va a conducir a esa identificación en la que no tiene cabida el error.

«Se le está entrenando a un software para poder diferenciar luego si lo que tiene delante es humano o no lo es. Y eso que parece futurista o vanguardista ya ha venido, es real, es

lo que nos ha traído la inteligencia artificial», indica Manuel Sánchez, que alerta de que «aún no sabemos qué cuestiones malintencionadas se puede hacer con ello, que llegarán».

Se muestra confuso por el hecho de que la gente sí es consciente de esa necesidad de asegurar datos como el DNI o de proteger nuestra huella dactilar «y de repente cedemos un dato único como es nuestro iris. Quizá no lo veamos a corto plazo, pero tarde o tem-

prano el delito saldrá», vaticina Manuel Sánchez.

Tanto él como Susana Duro coinciden en señalar que esta tecnología ha llegado para quedarse, de ahí la importancia de tomar medidas en materia de ciberseguridad. «Estamos destinados a que esos avances tecnológicos vayan avanzando al mismo tiempo en la vulneración de derechos fundamentales», opina Susana Duro.

Alega que las tecnológicas «no tienen en cuenta la protección al derecho a la intimidad, al de protección de datos o al secreto de las comunicaciones», derechos que en la Unión Europea están regulados. Aboga por reunir a expertos en diferentes materias, como juristas o tecnólogos, para «poder hacer frente a esta situación tan acuciante para los derechos fundamentales».



Susana Duro