

¿Qué esconde la venta del iris a cambio de criptomonedas?



La campaña mundial de Worldcoin ha recorrido 120 países, incluyendo Chile, AGENCIA UNO

[Worldcoin](#), empresa impulsada por Sam Altman, director del **sistema de inteligencia artificial ChatGPT**, está dedicada a [comprar el iris de las personas](#) a cambio de 25 criptomonedas.

A través del **escaneo de los globos oculares**, la compañía busca crear identificaciones digitales para la recopilación de datos.

La campaña mundial de **Worldcoin ha recorrido 120 países, incluyendo Chile**, y ya cuenta con más de 4 millones de registros, una cifra sigue creciendo a tasas de 400 mil por semana.

En medio de la alerta mundial por este tipo de prácticas, **España ordenó la prohibición temporal del escaneo del iris de Worldcoin** durante los próximos tres meses.

En ese sentido, una abogada y un Ingeniero Civil Electrónico, explicaron a *EL DÍNAMO* lo **perjudicial que resulta la venta del iris** y por qué es importante que los países regulen la protección de los datos.

¿Qué información recopila la empresa Worldcoin con el escaneo del iris?

David Ruete, Ingeniero Civil Electrónico y director de la Escuela de Ingeniería UNAB, Sede Viña del Mar, indicó a *EL DÍNAMO* que, a través de la compra del iris, Worldcoin se recopilan "imágenes que se utilizan para crear un IrisCode, que es básicamente una **representación matemática del iris**. Además, estas se pueden utilizar para verificar que la persona que se escanea es real y no una imagen, y se pueden **recopilar datos adicionales como la edad, el sexo y la etnia**".

¿Por qué es perjudicial la venta del iris?

El académico de la UNAB precisó que **la venta del iris puede ser dañino ya que "afecta directamente a la privacidad** porque podría permitir a las instituciones que **tengan datos únicos en su poder** con el fin de rastrear y monitorear a las personas sin su consentimiento".

En ese sentido, añadió que **"los datos biométricos como el iris son muy sensibles y podrían ser robados o hackeados**. Si los datos del iris se roban, podrían ser utilizados para **suplantar la identidad de las personas o para cometer otros delitos**. Si bien la clonación del iris es muy compleja, la efectividad de la clonación dependerá del sistema de reconocimiento con que se interactúe".

Junto a ello, el directivo aseguró que **la venta de iris puede aumentar las discriminaciones en general**, ya que "el uso del iris para la identificación podría llevar a la discriminación de las personas por **motivos de raza, género, etnia o discapacidad**".

Prohibición del escaneo del iris en España

La Agencia Nacional de España de Protección de Datos (AEPD) prohibió el escaneo del iris, por lo que la empresa **no podrá seguir captando nuevos usuarios** y tendrá que bloquear toda la información personal que ya tiene en su poder, impidiendo que se use.

Érika Tribaldos, abogada española – Itzi, reveló a *EL DÍNAMO* que "el consentimiento que dan las personas al vender su iris, es un consentimiento que **no está asociado a una información transparente por parte de la empresa**, ya que ellos deben explicar en qué se utilizarán los datos obtenidos, cuánto tiempo se van a conservar y cuál es el uso que se le dará a los datos obtenidos, pero acá no sucede esto".

"El problema radica en el desconocimiento que hay detrás de todo esto. Hay que entender que la compensación económica que nos están dando como interesados, con el tiempo será un dato mucho máspreciado y que va a aumentar su valor, pero todo lo que hay detrás va a ser un beneficio todavía más mayor para estas empresas", alertó Tribaldos.

"Con los avances tecnológicos se crean nuevos escenarios en los que se pueden **vulnerar los derechos de las personas**, entonces es importante que se establezcan escenarios de protección jurídica acorde a estas nuevas realidades tecnológicas", agregó la abogada.

Consejos para protegerse de la vulneración de datos

En medio de este escenario, David Ruete, académico de la UNAB, entregó una serie de consejos para la protección de los datos personales.

- **Sea consciente de la información que comparte en línea:** No comparta información personal que no sea necesaria.
- **Utilice contraseñas seguras y únicas:** No utilice la misma contraseña para diferentes cuentas.
- **Lea los términos y condiciones antes de utilizar cualquier servicio en línea:** Asegúrese de entender cómo se utilizarán sus datos.
- **Utilice herramientas de privacidad:** Hay muchas herramientas disponibles para ayudarle a proteger su privacidad en línea.
- **Manténgase actualizado sobre las últimas amenazas a la privacidad:** Es importante estar al tanto de las últimas formas en que los piratas informáticos y otros actores malintencionados pueden intentar robar sus datos.