A propósito del escaneo de iris a cambio de criptomonedas y sobre la regulación de los sistemas biométricos.

En Madrid, han llamado la atención estos días las largas colas de jóvenes en el intercambiador de Avenida de América (además de algún centro comercial) que se han reunido para cambiar su iris por criptomonedas.

Según puede leerse en la web de la empresa "*Las imágenes recopiladas por el Orb se utilizan para crear un código del iris que es una representación numérica de las características más importantes de un patrón de iris. Luego se eliminan de inmediato a menos que la persona que se registra solicite específicamente lo contrario. Si bien la copia de seguridad de las imágenes es completamente opcional, ayuda a nuestro equipo a mejorar el sistema con futuras actualizaciones. Y si alguna vez cambia de opinión, las imágenes siempre se pueden eliminar más tarde en la configuración de Privacidad en su cuenta de World App*".

La empresa dice que la imagen del iris se aloja en la memoria RAM de cada orbe, y finalmente es descartada en cuanto se convierte a un hash, mediante algoritmo criptográfico, para crear un identificador único para cada persona a partir de la imagen del iris.

Asumiendo como cierto que la imagen del iris se llegase a eliminar definitivamente, habrá que determinar si al final se produce una anonimización del dato, lo que dependerá de si es posible o no revertir la información y convertir el hash en el iris original, o de si es posible relacionar el hash con la imagen. Por otra parte, se establece que el hash no podrá ser eliminado una vez haya sido generado. Habrá que ver si lo que la compañía está construyendo es una base de datos de hashes parciales protegidos criptográficamente que únicamente pretenden demostrar que una persona es única, es decir, pero de tal manera que resulta imposible pasar de los datos almacenados a la identificación de la persona.

La Agencia Española de Protección de Datos (AEPD) ya está analizando varias denuncias relacionadas con el tratamiento de datos por parte de la empresa de criptomonedas. Las denuncias proceden de la Comunidad de Madrid y de Cataluña, donde se han implantado centros de operaciones, y en estos momentos están "en fase de análisis".

Por su parte, ante las informaciones recogidas estos días por los medios, que aseguran que cientos de personas, entre ellas menores de edad (cosa que la empresa niega, ya que al menos en los términos y condiciones se establece la oferta para mayores de 18), aceptan el escaneo de su iris a cambio de criptomonedas en varios establecimientos comerciales de Cataluña, la Autoridad Catalana de Protección de Datos (APDCAT) ha puesto de manifiesto resumidamente que;

El tratamiento de datos personales requiere una base jurídica para su realización, y, en caso de datos biométricos, puede ser el consentimiento explícito. Debe ser libre, informado, específico e inequívoco. Esto exige que la persona que le otorga debe ser plenamente consciente de las consecuencias que se pueden derivar del tratamiento de su información.

Para tratar los datos biométricos no es suficiente con el consentimiento, sino que la organización que lleva a cabo el tratamiento debe **informar previamente a las personas** sobre aspectos como:

• **Quien** trata los datos (identidad y datos de contacto) y para qué **finalidad**

• Datos de contacto del **Delegado** de Protección de Datos.

• Cuál es la **base jurídica** que le permite tratarlas.

• El tiempo que las **conservar**á

• Si las **cederá** a terceros

• Si se realizarán **transferencias internacionales** de datos fuera de la Unión Europea

• Ante quién y cómo pueden ejercerse los **derechos** de acceso, rectificación, supresión u oposición y limitación del tratamiento

• El derecho a presentar una **reclamación** ante la autoridad de control de protección de datos.

Esta información a la persona afectada por el tratamiento de sus datos debe ser clara, concisa y adaptada a cada colectivo, especialmente en el caso de menores de edad. Por tanto, este consentimiento informado exige que la persona también entienda y sea consciente de qué supone realmente el tratamiento de sus datos personales.

Y podríamos añadir que la consecuencia es que, si no se cumplen los requisitos relativos al consentimiento informado, el consentimiento no será válido y el responsable podría estar incumpliendo el artículo 6 de RGPD.

El uso de datos biométricos se limita (por regulación) a supuestos muy concretos de la normativa de protección de datos, dado el alto impacto en los derechos y libertades de las personas que puede suponer. Es necesario justificar muy bien la proporcionalidad de este tipo de sistemas, y garantizar el principio de minimización de datos (utilizar los datos mínimos para la finalidad perseguida).

Esta acción comporta la comunicación de un dato personal considerado como una categoría especialmente sensible. Es un dato biométrico que permite la identificación inequívoca de la persona a través de una característica física que no puede variarse a lo largo de la vida.

Pues bien, como veremos a continuación, como siempre, lo primero que tiene que concurrir es alguna de las bases de legitimación del artículo 6 RGPD (por ejemplo, un consentimiento inequívoco y previamente informado) junto a las condiciones que establece el 9.2 del RGPD al estar afectadas en este caso categorías especiales de datos.

En cuanto a regulación, el punto de partida es que el Reglamento General de Protección de Datos (RGPD), que es la norma que aplica, establece de entrada que el tratamiento de los datos biométricos, como categoría especial de datos personales, está en principio prohibido por regla general.

Por su parte, el artículo 6.1 del RGPD supedita la licitud de un tratamiento al cumplimiento de al menos una de las condiciones enumeradas en dicho artículo, y entre ellas se encuentra efectivamente el consentimiento, pero debe tenerse en cuenta que el artículo 9, apartado 1, del RGPD establece una **regla general consistente en prohibir el tratamiento de determinadas categorías especiales de datos personales**, entre los que se encuentran los "**datos biométricos** dirigidos a identificar de manera unívoca a una persona física".

Únicamente **cabe excepcionar la prohibición** de tratamiento de los datos de categoría especial, cuando concurra alguna de las circunstancias que se especifican en el apartado 2 del artículo 9 del RGPD.

En relación con la excepción del consentimiento explícito (**manifestación de voluntad libre, informada, específica e inequívoca**), en este caso para levantar la prohibición, además de analizar el consentimiento hay que valorar el concepto "necesidad" con una interpretación restrictiva de su acepción.

Además, deberá de haber superado favorablemente una **evaluación de impacto (EIPD)** que incluya el tradicional triple juicio de idoneidad, necesidad y proporcionalidad.

Así, por un lado, el artículo 9 del RGPD, apartado 2, letra a) levanta la prohibición del tratamiento de categorías especiales cuando "*el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado*".

El artículo 4.11 del RGPD se refiere al consentimiento del interesado como "*toda manifestación de voluntad libre, especifica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*".

Y además cabe traer a colación el Artículo 7, apartado 4, del RGPD: «*Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.*»

Véase también el considerando 43 RGPD, que afirma que: «[…] *Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento*».

La expresión «se presume» que aparece en el considerando 43, indica claramente que dichos casos tendrán un carácter sumamente excepcional.

Superado este levantamiento de prohibición que, (ya veremos lo que ocurre en este caso), aún debería acudirse, además de a una base de legitimación válida, a un conjunto de requisitos que son de obligado cumplimiento para determinar que el tratamiento es conforme a la normativa de protección de datos y, por lo tanto, que se puede llevar a cabo.

Este conjunto de requisitos comprende los siguientes pasos a seguir con carácter *previo*:

Que se realice una gestión del riesgo desde el diseño y por defecto.

Que se apliquen las medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento es conforme con el RGPD.

Que se supere favorablemente, en caso de alto riesgo, una **Evaluación de Impacto** para la Protección de los Datos del artículo 35 del RGPD que incluya y supere el **juicio de idoneidad, necesidad y proporcionalidad**. En este sentido, los sistemas

biométricos implementados con técnicas de inteligencia artificial tienen la consideración de sistemas de alto riesgo según el Anexo III de la propuesta de Regulación de Inteligencia Artificial y para poder incluirlos en un tratamiento se deberán tener en cuenta las prohibiciones, limitaciones y exigencias establecidas en la normativa sobre Inteligencia Artificial.

Como otras referencias para estudiar este caso, podemos tener presente diversas guías de la AEPD, incluso salvando las distancias, la guía sobre tratamientos de control de presencia mediante sistemas biométricos de la AEPD (que enlazamos abajo) que entiende que, aunque la tecnología permita y sea accesible para realizar tratamientos de datos biométricos, se trata de sistemas que recogen mucha más información de la que es realmente necesaria para la finalidad del tratamiento o, al menos, con mucho más detalle del requerido.

Por último; en el marco del tratamiento donde se encuentra la operación biométrica hay que plantear escenarios de brechas, y determinar el impacto que una brecha de datos personales derivados del uso de técnicas biométricas puede ocasionar en los derechos y libertades de los interesados. Estas **brechas de seguridad** pueden provocar el filtrado o pérdidas de patrones biométricos, suplantación de patrones almacenados, intrusión en el sistema de análisis biométrico y sus resultados, by-pass de la comunicación entre subsistemas, ataques de denegación de servicio, discontinuidad de servicios de terceros, etc. Todos los escenarios hay que analizarlos independientemente de la probabilidad estimada de su materialización y midiendo el grado de intrusión que puede ocasionar en los derechos y libertades.

Asimismo, hay que conocer la realidad de qué brechas ya se están produciendo y que podrían determinar la falta de adecuación de una técnica biométrica o biometría en general. Esto supone el realizar una evaluación continua del tratamiento en función de los eventos que se estén produciendo.

En resumen, si bien la práctica de escanear el iris a cambio de criptomonedas plantea beneficios potenciales en términos de verificación de identidad, también plantea importantes preocupaciones en cuanto a privacidad, seguridad y potencial uso indebido de los datos biométricos. Tenemos intención de volver actualizar el comentario sobre este caso, aparentemente tan disruptivo, y que puede considerarse paradigmático, una vez que se hayan clarificado las consecuencias jurídicas por parte de la AEPD, CEPD, o tribunales en su caso.

Salvo mejor opinión

RGPD

Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos.

Guía sobre tratamientos de control de presencia mediante sistemas biométricos