GRUPO DE TRABAJO DEL ARTÍCULO 29

00720/12/ES

WP193

Dictamen 3/2012 sobre la evolución de las tecnologías biométricas

adoptado el 27 de abril de 2012

Resumen

Los sistemas biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación. Mientras que los datos biométricos de una persona pueden suprimirse o alterarse, la fuente de la que se han extraído en general no puede ser modificada ni suprimida.

Los datos biométricos se utilizan con éxito y eficacia en la investigación científica, son un elemento clave de la ciencia forense y un valioso elemento de los sistemas de control de acceso. Pueden contribuir a aumentar el nivel de seguridad y a facilitar, acelerar y simplificar los procedimientos de identificación y autenticación. Anteriormente, el uso de esta tecnología era caro y como consecuencia de esta presión económica la repercusión en los derechos de protección de datos de los particulares era limitada. En los últimos años, la situación ha cambiado radicalmente. El análisis de ADN es rápido y asequible para casi todos. El progreso tecnológico ha abaratado el espacio de almacenamiento y la potencia de cálculo, lo que ha posibilitado el surgimiento de álbumes de fotos en línea y de redes sociales con miles de millones de fotografías. Los lectores de huellas dactilares y los dispositivos de vigilancia por vídeo se han convertido en artículos baratos. El desarrollo de estas tecnologías ha contribuido a la facilidad de muchas operaciones, a resolver muchos delitos y a hacer más fiables los sistemas de control del acceso, pero también ha introducido nuevas amenazas para los derechos fundamentales: la discriminación genética se ha convertido en un problema real y la usurpación de identidad ha dejado de ser una amenaza teórica.

Mientras que otras tecnologías nuevas centradas en grandes poblaciones y que han planteado recientemente problemas de protección de datos no se centran necesariamente en establecer un vínculo directo a una persona determinada -o bien la creación de este vínculo exige considerables esfuerzos-, los datos biométricos, por su naturaleza, están directamente vinculados a un individuo. Esto no es siempre positivo, sino que tiene varios inconvenientes. Por ejemplo, el dotar a los sistemas de vigilancia por vídeo y teléfonos inteligentes (*smartphones*) de sistemas de reconocimiento facial basados en las bases de datos de las redes sociales podría poner fin al anonimato y a la circulación no registrada de personas. Por otra parte, los lectores de huellas dactilares, lectores de venas o, simplemente, una sonrisa a una cámara, podrían sustituir a las tarjetas, códigos, contraseñas y firmas.

Estas y otras evoluciones recientes se abordan en el presente dictamen a fin de aumentar la sensibilización tanto entre los interesados como entre los órganos legislativos. Estas innovaciones técnicas que a menudo se presentan como tecnologías únicamente dirigidas a mejorar la experiencia del usuario y la comodidad de las aplicaciones podrían conducir a una disminución gradual de la intimidad en caso de que no se apliquen las garantías adecuadas. Por tanto, el presente dictamen establece medidas técnicas y organizativas destinadas a mitigar los riesgos para la protección de datos y la protección de la intimidad y que pueden contribuir a evitar los efectos negativos en la intimidad de los ciudadanos europeos y en su derecho fundamental a la protección de datos.

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Vistos el artículo 29 y el artículo 30, apartado 1, letra a), y apartado 3, de dicha Directiva,

Visto su Reglamento interno,

HA ADOPTADO EL PRESENTE DICTAMEN

1. Ámbito del dictamen

En el documento de trabajo sobre biometría (WP80) de 2003, el Grupo de Trabajo del Artículo 29 (Grupo de Trabajo) estudió las cuestiones de protección de datos relacionadas con el uso de tecnologías futuras capaces de leer y tratar electrónicamente los datos biométricos. En los últimos años, el uso de esta tecnología se ha generalizado tanto en el sector público como en el privado, y se han desarrollado una serie de nuevos servicios emergentes. Las tecnologías biométricas que anteriormente necesitaban considerables recursos financieros o informáticos han pasado a ser considerablemente más baratas y rápidas. El uso de lectores de huellas dactilares se ha generalizado. Por ejemplo, algunos ordenadores portátiles incluyen un lector de huellas dactilares para el control de acceso biométrico. Los avances en el análisis del ADN suponen que los resultados están disponibles en cuestión de minutos. Algunas tecnologías desarrolladas recientemente como el reconocimiento del patrón de venas o el reconocimiento facial ya han madurado. Su utilización en diferentes ámbitos de nuestra vida diaria está próxima. Las tecnologías biométricas están estrechamente vinculadas a determinadas características de una persona y algunas de ellas pueden utilizarse para revelar datos sensibles. Además, muchas permiten el seguimiento, rastreo o elaboración del perfil de las personas y, como tal, su potencial impacto en la intimidad y el derecho a la protección de los datos de las personas es elevado. Este impacto aumenta con el creciente despliegue de estas tecnologías. Cada individuo puede figurar en uno o varios sistemas biométricos.

El propósito del presente dictamen es proporcionar un marco revisado y actualizado de recomendaciones y directrices generales unificadas sobre la aplicación de los principios de protección de datos y de la intimidad en las aplicaciones biométricas. El dictamen se dirige a las autoridades legislativas nacionales y europeas, a la industria de sistemas biométricos y a los usuarios de estas tecnologías.

2. Definiciones

Las tecnologías biométricas no son nuevas y ya han sido abordadas en distintos dictámenes del Grupo de Trabajo. Esta sección tiene por objeto recopilar las definiciones pertinentes y proporcionar una actualización siempre que sea necesario.

Datos biométricos: como ya señaló el Grupo de Trabajo en el Dictamen 4/2007 (WP136), los datos biométricos pueden definirse como:

> «propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad.»

Los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior.

Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica.

Fuente de datos biométricos: la fuente de datos biométricos puede variar considerablemente e incluye elementos físicos, fisiológicos, de comportamiento o psicológicos de un individuo. Según el dictamen 4/2007 (WP136):

> «Las muestras de tejido humano (al igual que las muestras de sangre) son fuentes a partir de las cuales se extraen datos biométricos, pero no son en sí mismas datos biométricos (mediante la extracción de información de las muestras).»

Tal como se precisaba en el WP80, se puede distinguir entre dos categorías principales de técnicas biométricas:

- En primer lugar, existen técnicas basadas en aspectos físicos y **fisiológicos** que miden las características fisiológicas de una persona e incluyen: comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN y análisis de los poros de la piel, etc.

- En segundo lugar, existen técnicas basadas en aspectos **comportamentales**, que miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, la forma de moverse, pautas que indiquen pensamiento subconsciente como mentir, etc.

También debe tenerse en cuenta el reciente ámbito de las técnicas basadas en elementos **psicológicos**, que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico.

Plantilla biométrica: pueden extraerse características clave de los datos biométricos brutos (p. ej., mediciones faciales de una imagen) y almacenarse para su posterior tratamiento, en lugar de almacenar los datos brutos. Esto conforma la plantilla biométrica de los datos. La definición del tamaño (cantidad de información) de la plantilla es una cuestión crucial. Por una parte, el tamaño de la plantilla debe ser lo bastante grande para gestionar la seguridad (evitando solapamientos entre los diferentes datos biométricos, o sustituciones de identidad), y por otra, no deberá ser demasiado grande a fin de evitar los riesgos de reconstrucción de los

datos biométricos. La generación de la plantilla debe ser una vía de sentido único, en que no sea posible regenerar los datos biométricos brutos a partir de la plantilla.

Sistemas biométricos: según el dictamen WP80, los sistemas biométricos son:

> «aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona. Se suelen utilizar aplicaciones de autenticación/comprobación para diversas tareas en campos muy distintos y bajo la responsabilidad de una amplia gama de entidades diferentes.»

Debido a la evolución tecnológica reciente ahora es posible utilizar los sistemas biométricos para fines de categorización o segregación.

Los riesgos que presentan los sistemas biométricos se derivan de la propia naturaleza de los datos biométricos utilizados en el tratamiento. Por tanto, una definición más general sería un sistema que extrae y trata los datos biométricos.

El tratamiento de los datos biométricos en un sistema biométrico suele constar de diferentes procesos tales como el registro, almacenamiento y correspondencia:

- Registro de datos biométricos: abarca todos los procesos que se llevan a cabo en un sistema biométrico con el fin de extraer datos biométricos de una fuente biométrica y vincular estos datos a un individuo. La cantidad y calidad de los datos que se requiere durante el registro deberá ser suficiente para permitir una identificación, autenticación, clasificación o verificación exactas del individuo, sin registrar datos excesivos. La cantidad de datos extraídos de una fuente biométrica durante la fase de registro ha de ser adecuada para los fines del tratamiento y el nivel de rendimiento del sistema biométrico.

La fase de registro es normalmente el primer contacto de un individuo con un sistema biométrico. En la mayoría de los casos el registro requiere la implicación personal del individuo (por ejemplo, en el caso de toma de huellas dactilares) y, por tanto, puede ofrecer una oportunidad para proporcionar información adecuada y notificar un tratamiento justo. No obstante, también es posible registrar individuos sin su conocimiento o consentimiento (por ejemplo, mediante sistemas de circuito cerrado de televisión -CCTV- con funcionalidad de reconocimiento facial). La exactitud y seguridad del proceso de registro es esencial para el funcionamiento de todo el sistema. Un individuo puede tener la posibilidad de volver a registrarse en un sistema biométrico para actualizar los datos biométricos registrados.

- Almacenamiento biométrico: los datos obtenidos durante el registro pueden almacenarse localmente en el centro de operaciones en el que haya tenido lugar el registro (por ejemplo, en un lector) para su uso posterior, o en un dispositivo transportado por el individuo (por ejemplo, una tarjeta inteligente) o podrían ser enviados y almacenados en una base de datos centralizada accesible por uno o más sistemas biométricos.

- Correspondencia biométrica: es el proceso de comparación de los datos o plantillas biométricas (capturados durante el registro) con los datos o plantillas biométricas recogidos en una nueva muestra a efectos de identificación, verificación y autenticación o categorización.

Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Categorización/separación biométrica: la categorización/separación de un individuo por un sistema biométrico es típicamente el proceso de establecer si sus datos biométricos pertenecen a un grupo con características predefinidas, a fin de adoptar una medida específica. En este caso no es importante identificar o verificar al individuo, sino asignarle automáticamente a una categoría determinada. Por ejemplo, una pantalla de publicidad podrá mostrar diferentes anuncios dependiendo del individuo que la mira, basándose en su edad o sexo.

Biometría multimodal: puede definirse como la combinación de diversas tecnologías biométricas con el fin de aumentar la exactitud o rendimiento del sistema (también se denomina biometría a varios niveles). Los sistemas biométricos utilizan dos o más rasgos o modalidades biométricas del mismo individuo en el proceso de búsqueda de correspondencias. Estos sistemas pueden funcionar de distintas maneras, bien recogiendo datos biométricos diferentes con distintos sensores o recogiendo múltiples unidades del mismo elemento biométrico. Algunos estudios incluyen también en esta categoría los sistemas que funcionan realizando múltiples lecturas del mismo elemento biométrico o aquellos que utilizan algoritmos múltiples para la extracción de características de la misma muestra biométrica. Ejemplos de sistemas biométricos multimodales son el pasaporte electrónico a escala de la UE, así como los servicios de identificación biométrica US-VISIT en los Estados Unidos.

Precisión: cuando se utilizan sistemas biométricos es difícil obtener resultados con un 0 % de errores. Ello puede deberse a diferencias en el medio en la obtención de datos (iluminación, temperatura, etc.) y a diferencias entre los equipos utilizados (cámaras, dispositivos de escaneado, etc.). Los medidores de evaluación del rendimiento convencionales más utilizados son la Tasa de Falsa Aceptación y la Tasa de Falso Rechazo, y pueden adaptarse al sistema que se utilice.

- La Tasa de Falsa Aceptación (*False Acceptance Rate* o FAR) es la probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o no rechace a un impostor. Mide el porcentaje de entradas inválidas aceptadas incorrectamente. También se conoce como tasa de falso positivo.

- La Tasa de Falso Rechazo (*False Rejection Rate* o FRR) es la probabilidad de que el sistema arroje un falso rechazo; esto se produce cuando no se establece la correspondencia entre una persona y su propia plantilla biométrica. También es se conoce como tasa de falso negativo.

Con una configuración y ajuste adecuados, los errores críticos de los sistemas biométricos pueden minimizarse al nivel permitido para su uso operativo reduciendo los riesgos de evaluaciones incorrectas. Un sistema perfecto tendrá un FAR y FRR igual a cero, pero más

comúnmente, guarda una correlación negativa: el aumento de FAR suele reducir el nivel del FRR.

Al evaluar si es aceptable la precisión de un determinado sistema biométrico, es importante evaluar la finalidad del tratamiento, la FAR y la FRR, así como el tamaño de la población. Además, para evaluar la precisión de un sistema biométrico también podrá tenerse en cuenta la capacidad para detectar una muestra viva. Por ejemplo, las impresiones dactilares latentes pueden copiarse y utilizarse para crear dedos falsos. Un lector de huellas dactilares no deberá caer en la trampa de realizar una identificación positiva en tal situación.

3. Análisis jurídico

El marco jurídico pertinente es la Directiva sobre protección de datos (95/46/CE). El Grupo de Trabajo ya declaró en su documento WP80 que los datos biométricos son, en la mayoría de los casos, datos personales. Por tanto, solo pueden tratarse si existe una base jurídica y si el tratamiento es adecuado, pertinente y no excesivo en relación con los fines para los que dichos datos se recaben o traten.

Propósito

Un requisito previo para la utilización de datos biométricos es una definición clara de los fines para los que se recaben y traten los datos biométricos, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas.

Los datos biométricos pueden recabarse, por ejemplo, para garantizar o aumentar la seguridad de los sistemas de tratamiento mediante la aplicación de medidas adecuadas para proteger los datos personales contra el acceso no autorizado. En principio, no hay obstáculos para la aplicación de medidas de seguridad apropiadas basadas en elementos biométricos de los responsables del tratamiento de los datos a fin de garantizar un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. Sin embargo, debe tenerse en cuenta que el uso de la biometría en sí no garantiza una mayor seguridad, ya que muchos de los datos biométricos pueden tomarse sin el conocimiento del interesado. Cuanto mayor sea el nivel de seguridad previsto, menos podrán los datos biométricos por sí solos alcanzar dicho objetivo.

El principio de limitación de la finalidad debe respetarse junto con los demás principios de protección de datos; especialmente, los principios de necesidad, proporcionalidad y minimización de datos han de tenerse en cuenta al definir los diferentes fines de una aplicación. Siempre que sea posible, el interesado deberá tener la posibilidad de elegir entre los diversos fines de una aplicación con múltiples funcionalidades, en especial si uno o varios de ellos exigen el tratamiento de datos biométricos.

Ejemplo:
La utilización de dispositivos electrónicos que prevean procedimientos de autenticación específicos basados en datos biométricos se ha recomendado en relación con las medidas de seguridad que deben adoptarse en caso de:

- tratamiento de los datos personales recogidos por los operadores telefónicos en el marco de actividades de escuchas telefónicas autorizadas por un tribunal;
- acceso a los datos de tráfico (y datos de localización) conservados con fines judiciales por parte de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red de comunicaciones pública, y acceso a los locales donde se traten esos datos;

- recogida y conservación de datos genéticos y muestras biológicas.

Las fotografías en internet, en las redes sociales, en aplicaciones de puesta en común o de gestión de fotos en línea no podrán tratarse con el fin de extraer plantillas biométricas ni registrarse en un sistema biométrico a fin de reconocer a las personas de las imágenes automáticamente (reconocimiento facial) sin una base jurídica específica (por ejemplo, consentimiento) para esta nueva finalidad. Si existe una base jurídica para dicha finalidad secundaria, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Si un interesado ha consentido en que las fotografías en las que aparece puedan tratarse para etiquetarle automáticamente en un álbum de fotografías en línea con un algoritmo de reconocimiento facial, este tratamiento deberá efectuarse de forma favorable a la protección de datos: los datos biométricos que no sean necesarios tras el etiquetado de las imágenes con el nombre, alias o cualquier otro texto especificado por el interesado deberán suprimirse. La creación de una base de datos biométricos permanente no es a priori necesaria para este fin.

Proporcionalidad

El uso de la biometría plantea la cuestión de la proporcionalidad de cada categoría de datos tratados a la luz de los fines para los que se traten los datos. Puesto que los datos biométricos solo pueden utilizarse si son adecuados, pertinentes y no excesivos, ello implica una evaluación estricta de la necesidad y la proporcionalidad de los datos tratados y de si la finalidad prevista podría alcanzarse de manera menos intrusiva.

Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar[1]. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado[2].

Ejemplo:
En un gimnasio se instala un sistema biométrico centralizado basado en la recogida de impresiones dactilares a fin de permitir el acceso a las instalaciones y servicios conexos únicamente a los clientes que han pagado su cuota.

---

[1] La biometría se utilizará para la identificación o verificación: un identificador biométrico puede considerarse técnicamente idóneo para la una y no para la otra (por ejemplo, las tecnologías caracterizadas por unas bajas tasas de rechazo deberán tener prioridad en los sistemas destinados a utilizarse con fines de identificación a efectos de la aplicación de la ley).

[2] Por ejemplo, tarjetas inteligentes u otros métodos que no recojan o centralicen datos biométricos para fines de autentificación.

Para que funcione dicho sistema, es preciso almacenar las huellas dactilares de todos los clientes y miembros del personal. Esta aplicación biométrica parece desproporcionada en relación con la necesidad de controlar el acceso al club y facilitar la gestión de las inscripciones. Es fácil imaginar que otras medidas, como una mera lista de control, el uso de etiquetas RFID o tarjetas de banda magnética, que no requieren el tratamiento de datos biométricos, serían igualmente factibles y eficaces.

El Grupo de Trabajo advierte de los riesgos que conlleva la utilización de datos biométricos para fines de identificación en grandes bases de datos centralizadas, dadas las consecuencias potencialmente perjudiciales parar las personas afectadas.

Debe tenerse en cuenta el importante impacto en la dignidad humana de los interesados y las implicaciones en cuestión de derechos fundamentales de tales sistemas. A la luz del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales y de la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el artículo 8 del Convenio, el Grupo de Trabajo subraya que cualquier interferencia con el derecho a la protección de datos solo podrá autorizarse si es conforme a la ley y si es necesaria, en una sociedad democrática, para proteger un interés público importante[3].

Para garantizar el cumplimiento de estas condiciones, es preciso especificar el objetivo perseguido por el sistema y evaluar la proporcionalidad de los datos que deben introducirse en el sistema en relación con dicho objetivo.

Para ello, el responsable del tratamiento ha de determinar si el mismo y sus mecanismos, las categorías de datos que deben recogerse y tratarse, así como la transferencia de la información contenida en la base de datos, son necesarios e indispensables. Las medidas de seguridad adoptadas deben ser adecuadas y eficaces. El responsable del tratamiento ha de considerar los derechos que deben concederse a las personas a que se refieren los datos personales, y garantizar que a la aplicación se incorpore un mecanismo apropiado para ejercer tales derechos.

Ejemplo:
Utilización de datos biométricos para fines de identificación. Los sistemas que analizan la cara de una persona, así como los sistemas que analizan el ADN, pueden contribuir muy eficazmente a la lucha contra la delincuencia y revelar eficazmente la identidad de una persona desconocida sospechosa de haber cometido un delito grave. No obstante, estos sistemas utilizados a gran escala pueden producir efectos secundarios graves. En el caso del reconocimiento facial, donde los datos biométricos pueden capturarse fácilmente sin conocimiento del interesado, un uso amplio podría terminar con el anonimato en los espacios públicos y permitir un seguimiento continuo de las personas. En el caso de los datos de ADN, la utilización de la tecnología conlleva el riesgo de que puedan revelarse datos sensibles relativos a la salud de una persona.

[3] Véase Tribunal de Justicia de las Comunidades Europeas, sentencia de 20 de mayo de 2003 en los asuntos acumulados C-465/00, C-138/01 y C-139/01 (Rechnungshof contra Österreichischer Rundfunk y otros), Tribunal Europeo de Derechos Humanos, sentencia de 4 de diciembre de 2008, nº 30562/04 y 30566/04 (S. y Marper contra Reino Unido) y sentencia de 19 de julio de 2011, nº 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 y 64027/09 (Goggins y otros contra Reino Unido).

Precisión

Los datos biométricos tratados deberán ser exactos y pertinentes en proporción a la finalidad para la que fueron recogidos. Estos datos deberán ser exactos en la recogida y al establecer el vínculo entre la persona y los datos biométricos. La exactitud en el registro es también importante para prevenir la usurpación de identidad.

Los datos biométricos son únicos y la mayoría de ellos generan una plantilla o imagen únicas. Si se utilizan ampliamente, para una proporción considerable de una población, los datos biométricos podrán considerarse como un identificador de aplicación general en el sentido de la Directiva 95/46/CE. El artículo 8, apartado 7, de la Directiva 95/46/CE sería entonces aplicable y los Estados miembros tendrían que determinar las condiciones de su tratamiento.

Minimización de datos

Puede surgir una dificultad específica por cuanto los datos biométricos a menudo contienen más información de la necesaria para las funciones de búsqueda de correspondencias. El responsable del tratamiento deberá aplicar el principio de minimización de datos. En primer lugar, esto significa que solo deberá tratarse, transmitirse o almacenarse la información necesaria, no toda la información disponible. En segundo lugar, el responsable del tratamiento deberá garantizar que la configuración por defecto promueva la protección de datos, sin tener que tomar medidas al efecto.

Periodo de conservación

El responsable del tratamiento deberá determinar un periodo de conservación de los datos biométricos que no podrá ser superior al necesario para los fines para los que dichos datos fueron recabados o para los que se traten ulteriormente. El responsable del tratamiento deberá garantizar que los datos, o los perfiles derivados de esos datos, se supriman una vez transcurrido este periodo de tiempo justificado.

Deberá estar clara la diferencia entre los datos personales generales que puedan ser necesarios durante un periodo de tiempo más largo y los datos biométricos que ya no vayan a utilizarse, por ejemplo cuando ya no se conceda al interesado acceso a una zona determinada.

Ejemplo:
Un empleador gestiona un sistema biométrico para controlar el acceso a una zona restringida. El cometido de un empleado ya no le exige acceder a la zona restringida (por ejemplo, por un cambio de funciones o de puesto). En este caso, sus datos biométricos deberán suprimirse puesto que los fines para los que se recabaron ya no están vigentes.

3.1. Motivo legítimo

El tratamiento de los datos biométricos deberá basarse en uno de los motivos legítimos previstos en el artículo 7 de la Directiva 95/46/CE.

3.1.1. Consentimiento, artículo 7, letra a)

El primero de estos motivos legítimos que figura en la letra a) del artículo 7 es si el interesado ha dado su consentimiento al tratamiento. Con arreglo al artículo 2, letra h), de la Directiva de protección de datos, el consentimiento debe ser una manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan. Debe quedar claro que este consentimiento no puede obtenerse libremente haciendo si se hace obligatoria la aceptación de los términos y condiciones

generales, ni mediante posibilidades de exclusión voluntaria. Además, el consentimiento debe ser revocable. A este respecto, en su dictamen sobre la definición de consentimiento, el Grupo de Trabajo subraya diversos aspectos importantes del concepto: validez del consentimiento; el derecho de los individuos a retirar su consentimiento; consentimiento dado antes del inicio del tratamiento; y requisitos relativos a la calidad y la accesibilidad de la información[4].

En muchos casos en los que se tratan datos biométricos, sin una alternativa válida como una contraseña o una tarjeta de banda magnética, el consentimiento no puede considerarse otorgado libremente. Por ejemplo, un sistema que disuada a los interesados de su utilización (que requiera demasiado tiempo del usuario o que sea demasiado complicado) no puede considerarse como una alternativa válida y por ende no daría lugar a un consentimiento válido.

Ejemplos:
En ausencia de otros motivos legítimos alternativos, podría utilizarse un sistema de autentificación biométrica para controlar el acceso a un videoclub solo si los clientes son libres de decidir si hacer uso de dicho sistema. Esto significa que el propietario del videoclub debe prever mecanismos alternativos menos invasores de la intimidad. Tal sistema permitirá la no participación de los clientes que no quieran o no puedan someterse a la toma de huellas dactilares por sus circunstancias personales. La posibilidad de elegir entre no utilizar un servicio y dar los datos biométricos es un importante indicador de que el consentimiento no era libre y no puede considerarse un motivo legítimo.

En una guardería se instala un lector de venas para comprobar si toda persona adulta que entre (padres y personal) tiene derecho o no a entrar. Para que funcione dicho sistema será preciso almacenar las huellas dactilares de todos los padres y miembros del personal. El consentimiento será una base jurídica cuestionable especialmente para los empleados, ya que podrían no tener una verdadera posibilidad de elegir si negarse a utilizar tal sistema. También sería cuestionable para los padres, mientras no existiera ningún método alternativo para entrar en la guardería.

Aunque hay motivos de peso para suponer que el consentimiento es débil debido al habitual desequilibrio entre empleador y empleado, el Grupo de Trabajo no excluye completamente su utilización «en los casos en que existan garantías suficientes de que es realmente libre»[5].

Por tanto, el consentimiento en el contexto del empleo debe cuestionarse y justificarse debidamente. En lugar de solicitar el consentimiento, los empleadores podrían investigar si es demostrable la necesidad de utilizar datos biométricos de los empleados para un fin legítimo, y ponderar esa necesidad frente a los derechos y libertades fundamentales de los trabajadores. En los casos en que la necesidad pueda justificarse adecuadamente, la base jurídica de tal tratamiento podría basarse en el interés legítimo del responsable del tratamiento según lo definido en el artículo 7, letra f), de la Directiva 95/46/CE. El empleador debe buscar siempre el medio menos invasivo optando por un tratamiento no biométrico, si es posible.

Sin embargo, como se describe en el apartado 3.1.3, puede haber casos en que un sistema biométrico redunde en interés legítimo del responsable del tratamiento de los datos. En estos casos, el consentimiento no sería necesario.

---

4 WP 187, dictamen 15/2011 sobre la definición de consentimiento.

5 WP 187, dictamen 15/2011 sobre la definición de consentimiento.

El consentimiento solo es válido cuando se proporciona información suficiente sobre la utilización de los datos biométricos. Dado que los datos biométricos pueden utilizarse como un identificador único y universal, el suministro de información clara y fácilmente accesible sobre cómo se utilizan los datos específicos debe considerarse absolutamente necesario para garantizar un tratamiento equitativo. Por tanto, este es un requisito esencial para un consentimiento válido en el uso de los datos biométricos.

Ejemplos:
Un consentimiento válido para un sistema de control de acceso que utilice huellas dactilares requiere información sobre si el sistema biométrico crea una plantilla única para ese sistema o no. Si se utiliza un algoritmo que genere la misma plantilla biométrica en diferentes sistemas biométricos, el interesado debe saber que puede ser reconocido en varios sistemas biométricos diferentes.

Una persona guarda su imagen en un álbum de fotos en internet. El registrar esta imagen en un sistema biométrico requiere un consentimiento explícito basado en información exhaustiva sobre lo que se hace con los datos biométricos, para qué fines se tratan y durante cuánto tiempo.

Puesto que el consentimiento puede ser revocado en cualquier momento, los responsables del tratamiento de datos deben aplicar medios técnicos que puedan invertir el uso de datos biométricos en sus sistemas. Por tanto, un sistema biométrico que funcione sobre la base del consentimiento debe poder suprimir eficientemente todos los enlaces de identidad que haya creado.

3.1.2. Contrato, artículo 7, letra b)

El tratamiento de datos personales puede ser necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado. Sin embargo, cabe señalar que esto se aplica, en general, solo cuando se prestan servicios biométricos puros. Esta base jurídica no se puede utilizar para legitimar un servicio secundario consistente en registrar a una persona en un sistema biométrico. Si tal servicio puede separarse del servicio principal, el contrato por el servicio principal no puede legitimar el tratamiento de datos biométricos. Los datos personales no son bienes que puedan intercambiarse por un servicio, por lo que los contratos que prevean o que ofrezcan un servicio solo bajo la condición de que una persona consienta el tratamiento de sus datos biométricos para otro servicio no puede servir de base jurídica para dicho tratamiento.

Ejemplos:
a) Dos hermanos proporcionan a un laboratorio muestras para realizar una prueba de ADN a fin de averiguar si son verdaderamente hermanos. El contrato con el laboratorio para realizar la prueba es una base jurídica suficiente para el registro y el tratamiento de los datos biométricos.

b) Una persona aporta una foto para mostrarla a sus amigos en su álbum en una red social. Si el contrato (condiciones de uso) establece que el uso del servicio está vinculado al registro de este usuario en un sistema biométrico, esta disposición no constituye una base jurídica suficiente para dicho registro.

3.1.3. Obligación jurídica, artículo 7, letra c)

Otra base jurídica para el tratamiento de datos personales es que este sea necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del mismo. Es el caso, por ejemplo, en algunos países al expedir o utilizar los pasaportes[6] y los visados[7].

3.1.4. Interés legítimo perseguido por el responsable del tratamiento, artículo 7, letra f)

Según el artículo 7 de la Directiva 95/46/CE, el tratamiento de datos biométricos también puede justificarse cuando sea «necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.»

Esto significa que hay casos en que la utilización de los sistemas biométricos es del interés legítimo del responsable del tratamiento de los datos. Este interés, no obstante, solo es legítimo cuando el responsable del tratamiento puede demostrar que su interés prevalece objetivamente sobre el derecho de los interesados a no estar registrados en un sistema biométrico. Por ejemplo, cuando la seguridad de zonas de riesgo elevado debe garantizarse específicamente mediante un mecanismo que pueda verificar con precisión si las personas tienen derecho de acceso a estas zonas, la utilización de un sistema biométrico puede ser del interés legítimo del responsable del tratamiento de datos. En el ejemplo que figura a continuación, de un sistema de control de acceso biométrico a un laboratorio, el responsable del tratamiento no puede ofrecer al trabajador un mecanismo alternativo sin que ello repercuta directamente en la seguridad de la zona restringida, ya que no existen medidas alternativas menos invasivas adecuadas para alcanzar un nivel de seguridad apropiado de esta zona. Por tanto, redunda en su interés legítimo aplicar el sistema y registrar a un número limitado de personas. No precisa obtener su consentimiento. Sin embargo, en el caso en que un interés legítimo del responsable del tratamiento constituya una base jurídica válida para el tratamiento, todos los demás principios de protección de datos seguirán siendo aplicables, especialmente los principios de proporcionalidad y minimización de datos, como siempre.

---

[6] Las impresiones dactilares se han integrado en los pasaportes, en cumplimiento de lo dispuesto en el Reglamento UE nº 2252/2004 del Consejo, de 13 de diciembre de 2004, y en los permisos de residencia, de conformidad con lo dispuesto en el Reglamento UE nº 1030/2002 del Consejo, de 13 de junio de 2002.

[7] El registro de identificadores biométricos en el Sistema de Información de Visados (VIS) fue creado por el Reglamento (CE) nº 767/2008, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS). Véase también el Dictamen n° 3/2007 sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica la Instrucción consular común dirigida a las misiones diplomáticas y oficinas consulares de carrera en relación con la introducción de datos biométricos y se incluyen disposiciones sobre la organización de la recepción y la tramitación de las solicitudes de visado [COM (2006) 269 final]. WP134, Dictamen 2/2005 sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros [COM (2004) 835 final] WP 110; Dictamen 7/2004 sobre la inclusión de elementos biométricos en los permisos de residencia y visados teniendo en cuenta la creación del Sistema de Información de Visados (VIS) WP 96.

Ejemplo:
El laboratorio de una empresa que investiga sobre virus peligrosos está protegido por puertas que se abren únicamente tras una verificación satisfactoria de las huellas dactilares y reconocimiento del iris. La finalidad de este sistema es garantizar que solo las personas familiarizadas con los riesgos específicos, formadas sobre los procedimientos y consideradas fiables por la empresa experimentan con estos materiales peligrosos. El interés legítimo de la empresa para asegurarse de que solo las personas autorizadas entran en una zona restringida, a fin de garantizar que los riesgos para la seguridad que conlleva el acceso a dicha zona específica se reduzcan significativamente, prevalece sobre el deseo de las personas de que no se traten sus datos biométricos.

Como norma general, el uso de la biometría para las exigencias generales de seguridad de los bienes y las personas no puede considerarse un interés legítimo que prevalezca sobre los intereses o los derechos y libertades fundamentales del interesado. Por el contrario, el tratamiento de datos biométricos solo puede justificarse como un instrumento necesario para asegurar los bienes o las personas cuando se disponga de pruebas, sobre la base de las circunstancias objetivas y documentadas, de la existencia de un riesgo considerable. Para ello, el responsable del tratamiento deberá probar que determinadas circunstancias plantean un riesgo considerable específico, que deberá evaluar con especial cuidado. Con el fin de cumplir con el principio de proporcionalidad, el responsable del tratamiento, ante estas situaciones de alto riesgo, deberá verificar si posibles medidas alternativas podrían ser igualmente eficaces pero menos intrusivas en relación con los objetivos perseguidos, y optar por tales alternativas.
La existencia de las circunstancias en cuestión también deberá revisarse periódicamente. Sobre la base de esta revisión, las operaciones de tratamiento de datos que no se justifiquen deberán concluirse o suspenderse.

3.2. Responsable del tratamiento y encargado del mismo

La Directiva 95/46/CE impone obligaciones a los responsables del tratamiento de datos en relación con dicho tratamiento. En el contexto de la biometría, distintos tipos de entidades pueden ser responsables del tratamiento de datos, por ejemplo, empleadores, autoridades con funciones coercitivas o autoridades de migración.

El Grupo de Trabajo recuerda las orientaciones facilitadas en su Dictamen sobre los conceptos de responsable y encargado del tratamiento[8], que contiene aclaraciones sobre cómo interpretar estas definiciones esenciales de la Directiva.

3.3. Tratamiento automatizado (artículo 15 de la Directiva)

Cuando se utilicen sistemas basados en el tratamiento de datos biométricos, deberá prestarse especial atención a las posibles consecuencias discriminatorias para las personas rechazadas por el sistema. Además, con el fin de proteger el derecho del individuo a no estar sujeto a una medida que le afecte sobre la base exclusivamente de un tratamiento automatizado de los datos, deberán introducirse garantías adecuadas, tales como intervenciones humanas, soluciones o mecanismos que otorguen al interesado la posibilidad de defender su punto de vista.

---

[8] WP169, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento».

De conformidad con el artículo 15 de la Directiva 95/46/CE, «Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.»

3.4. Transparencia e información del interesado

Según el principio de tratamiento leal, los interesados deberán ser conscientes de la recogida o utilización de sus datos biométricos (artículo 6 de la Directiva 95/46/CE). Deberá evitarse cualquier sistema que pueda recoger dichos datos sin el conocimiento de los interesados.

El responsable del tratamiento deberá asegurarse de que, de conformidad con el artículo 10 de la Directiva sobre protección de datos, los interesados estén adecuadamente informados de los elementos clave del tratamiento, tales como la identidad del responsable, la finalidad del mismo, el tipo de datos, la duración, los derechos de los interesados a acceder, rectificar o suprimir sus datos y el derecho a retirar el consentimiento, así como la información acerca de los destinatarios o categorías de destinatarios a quienes se comuniquen los datos. Puesto que el responsable de un sistema biométrico está obligado a informar al interesado, los datos biométricos no deberán tomarse a una persona sin su conocimiento.

3.5. Derecho de acceso a los datos biométricos

Los interesados tienen derecho a obtener de los responsables del tratamiento el acceso a sus datos en general, incluidos sus datos biométricos. Los interesados también tienen derecho a acceder a posibles perfiles basados en estos datos biométricos. Si el responsable del tratamiento tiene que verificar la identidad de los interesados para conceder dicho acceso, es esencial que este se ofrezca sin que medie tratamiento de datos personales adicionales.

3.6. Seguridad de los datos

El responsable del tratamiento debe aplicar las medidas técnicas y organizativas adecuadas para proteger los datos personales contra una destrucción accidental o ilícita o la pérdida accidental, la alteración, la difusión o el acceso no autorizados y contra cualquier otro tratamiento ilícito[9].

Los datos recogidos y almacenados deberán estar debidamente asegurados. Los diseñadores de los sistemas deberán colaborar con expertos en seguridad a fin de garantizar que las vulnerabilidades en materia de seguridad se aborden adecuadamente, especialmente si los sistemas existentes se migran a internet.

3.7. Garantías para personas con necesidades especiales

El uso de la biometría podría suponer un impacto significativo sobre la dignidad, la protección de la intimidad y el derecho a la protección de datos de personas vulnerables como los niños de corta edad, las personas de edad avanzada y las personas físicamente incapaces de completar el proceso de registro con éxito. Dadas las consecuencias potencialmente perjudiciales para las personas afectadas, deberán cumplirse requisitos más rigurosos en el proceso de evaluación de impacto de cualquier medida que interfiera con la dignidad de una persona, en términos de cuestionamiento de la necesidad y proporcionalidad, así como de las posibilidades de los individuos para ejercer su derecho a la protección de datos, a fin de que la

---

[9] Artículo 17, apartado 1, de la Directiva 95/46/CE.

medida en cuestión se considere admisible. Deberán establecerse garantías contra los riesgos de discriminación o estigmatización de las personas por razón de su edad o su incapacidad para registrarse.

Por lo que respecta a la introducción de una obligación jurídica generalizada de recoger identificadores biométricos para estos grupos, en particular niños y personas de edad avanzada, en los controles fronterizos a efectos de identificación, el Grupo de Trabajo opina que «en razón de la dignidad de la persona y para garantizar la fiabilidad del procedimiento, la recogida y el tratamiento de impresiones dactilares debería limitarse en el caso de los niños y las personas mayores, y que el límite de edad debería coincidir con los límites de edad que se aplican en otras bases de datos biométricos de la UE (Eurodac, especialmente).»[10]

En cualquier caso, deberían aplicarse garantías específicas (tales como procedimientos alternativos adecuados), a fin de garantizar el respeto de la dignidad humana y las libertades fundamentales de las personas que no puedan completar con éxito el proceso de registro y, de ese modo, evitar cargar a estas personas con las imperfecciones del sistema técnico[11].

3.8. Datos sensibles

Algunos datos biométricos pueden considerarse sensibles en el sentido del artículo 8 de la Directiva 95/46/CE y, en particular, los datos que revelen el origen racial o étnico o los datos relativos a la salud. Por ejemplo, los datos de ADN de una persona a menudo incluyen datos sobre la salud o pueden revelar el origen racial o étnico. En este caso, los datos de ADN son datos sensibles y deben aplicarse las garantías especiales previstas en el artículo 8, además de los principios generales de protección de datos de la Directiva. Con objeto de evaluar la sensibilidad de los datos tratados por un sistema biométrico, también deberá tenerse en cuenta el contexto del tratamiento[12].

3.9. Función de las autoridades nacionales de protección de datos

Teniendo en cuenta la creciente normalización de las tecnologías biométricas a efectos de la interoperabilidad, en general se admite que el almacenamiento centralizado de datos biométricos aumenta tanto el riesgo de utilización de datos biométricos como clave para interconectar bases de datos múltiples (lo que puede conducir a crear perfiles detallados de un individuo) como los peligros específicos de la reutilización de tales datos para fines incompatibles, especialmente en caso de acceso no autorizado.

El Grupo de Trabajo recomienda que los sistemas que utilizan datos biométricos como clave para interconectar bases de datos múltiples requieran garantías adicionales, dado que este tipo de tratamiento puede suponer riesgos específicos para los derechos y libertades de los interesados (artículo 20 de la Directiva 95/46/CE). Para establecer las garantías adecuadas y, en particular, atenuar los riesgos para los interesados, los responsables del tratamiento deberán consultar a las autoridades nacionales competentes de protección de datos antes de introducir tales medidas.

---

[10] WP134 - Dictamen nº 3/2007 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica la Instrucción consular común dirigida a las misiones diplomáticas y oficinas consulares de carrera en relación con la introducción de datos biométricos, y se incluyen disposiciones sobre la organización de la recepción y la tramitación de las solicitudes de visado [COM(2006)269 final].

[11] Véase WP134 - Dictamen n° 3/2007, p. 8.

[12] Véase WP 29 Dictamen sobre categorías especiales de datos («datos sensibles») ref. Ares (2011)444105 – 20.4.2011.

4. Nuevos avances y tendencias tecnológicas, nuevos escenarios

4.1. Introducción

Las tecnologías biométricas se han utilizado durante un largo periodo de tiempo principalmente por las autoridades públicas, pero recientemente la situación ha evolucionado gradualmente a que las organizaciones comerciales desempeñen una función principal utilizando estas tecnologías y desarrollando nuevos productos.

Uno de los principales motores de esa situación es que la tecnología ha madurado de forma que los sistemas biométricos que solo funcionaban bien en condiciones controladas se han perfeccionado y ahora son adecuados para un uso extenso en diferentes entornos. En ese sentido, los datos biométricos, en algunos casos, sustituyen o mejoran los métodos de identificación convencionales, especialmente los basados en factores de identificación múltiples necesarios para los sistemas de autenticación fuertes. Las tecnologías biométricas también se están utilizando cada vez más en aplicaciones que pueden identificar rápidamente y convenientemente a alguien a cambio de un menor nivel de precisión.

El uso de las tecnologías biométricas también está ampliando gradualmente su ámbito de aplicación: de la identificación y autenticación al análisis del comportamiento, vigilancia y prevención del fraude.

Los avances en tecnologías y redes informáticas están propiciando asimismo la subida de lo que se considera la segunda generación de datos biométricos basada en la utilización de los rasgos de comportamiento y psicológicos solos o combinados con otros sistemas clásicos que conforman sistemas multimodales. Para completar el cuadro, hay una evolución gradual hacia la utilización de datos biométricos en los entornos inteligentes y en la evolución informática ubicua.

4.2. Nuevas tendencias sobre biometría

Existen una serie de tecnologías biométricas que pueden considerarse tecnologías maduras, con diversas aplicaciones en la aplicación de la ley, la administración electrónica y los sistemas comerciales. De forma no exhaustiva, cabe mencionar las impresiones dactilares, la geometría de la mano, el reconocimiento del iris y algunos tipos de reconocimiento facial. También están apareciendo tecnologías biométricas que analizan rasgos del organismo. Mientras que algunas son nuevas, otras tecnologías biométricas tradicionales están tomando un nuevo impulso a partir de nuevas capacidades de procesamiento.

Elementos típicos de estos nuevos sistemas son el uso de rasgos del organismo que permiten la categorización o identificación de individuos y la recogida a distancia de dichos rasgos. Los datos recogidos se utilizan para la elaboración de perfiles, la vigilancia a distancia o incluso tareas más complejas como los entornos inteligentes.

Esto se ha hecho posible debido al continuo desarrollo de sensores que permiten la recogida de nuevas características fisiológicas, así como de nuevas formas de tratamiento de datos biométricos tradicionales.

También cabe mencionar la utilización de las denominadas tecnologías biométricas ligeras, definida por el uso de rasgos muy comunes no aptos para distinguir claramente o identificar a un individuo, pero que permiten mejorar los resultados de otros sistemas de identificación.

Otro elemento esencial de los nuevos sistemas biométricos es el potencial para recoger información a distancia o en movimiento sin necesidad de colaboración o acción del

individuo. Aunque todavía no es una tecnología plenamente desarrollada, se está haciendo un gran esfuerzo, especialmente para fines policiales.

Lo que está avanzando rápidamente es el uso de sistemas multimodales que utilizan diferentes datos biométricos de manera simultánea o múltiples lecturas o unidades de los mismos datos biométricos que pueden ajustarse con objeto de optimizar la relación entre seguridad y adecuación de los sistemas biométricos. Esto puede reducir la tasa de falsa aceptación, mejorar los resultados de un sistema de reconocimiento o facilitar la recogida de datos de una población mayor equilibrando la no universalidad de una fuente de datos biométricos al combinarla con otra.

Los sistemas biométricos son cada vez más utilizados por las entidades públicas y privadas; tradicionalmente, en el sector público, las autoridades con funciones coercitivas utilizan los datos biométricos regularmente; en los sectores financiero, bancario y de salud en línea el uso de la biometría está creciendo, así como en otros sectores como la educación, la venta al por menor y las telecomunicaciones. Esta evolución estará alimentada por las nuevas funciones derivadas de la convergencia o fusión de las tecnologías existentes. Un ejemplo es la utilización de los sistemas de TVCC que permiten la recogida y el análisis de datos biométricos y de comportamientos humanos.

Lo anterior puede considerarse también un cambio en la óptica del desarrollo de los sistemas biométricos, de herramientas de identificación a fines de reconocimiento ligero, en otras palabras, de la identificación a la detección de comportamientos o necesidades específicas de las personas. Esto también abre puertas a usos muy diferentes de las aplicaciones de seguridad a gran escala: la seguridad personal, el juego y la venta al por menor se beneficiarán de una mayor interacción entre hombre y máquina que permita algo más que la identificación o categorización de un individuo.

4.3. Impacto en la protección de datos y la intimidad

Desde el principio de su aplicación, se ha reconocido que los sistemas biométricos son susceptibles de generar fuertes inquietudes en varios ámbitos, incluidos los de la intimidad y la protección de datos, que sin duda han influido en su aceptación social y han impulsado el debate sobre la legalidad y los límites de su uso, así como sobre las salvaguardias y garantías necesarias para atenuar los riesgos detectados.

La clásica reticencia a los sistemas biométricos ha estado vinculada a la protección de los derechos individuales, y lo sigue estando. Sin embargo, los nuevos sistemas y la evolución de los sistemas existentes suscitan una serie de preocupaciones. Ello incluye la posibilidad de recoger, almacenar y tratar datos de forma encubierta, así como la recogida de material con información muy sensible que pueda invadir el espacio más íntimo de las personas.

La desvirtuación de funciones ha sido un serio motivo de preocupación desde que comenzaron a utilizarse las tecnologías y sistemas biométricos: pese a ser un riesgo conocido y previsto en la biometría tradicional, es evidente que el mayor potencial técnico de los nuevos sistemas informáticos plantea el riesgo de que los datos se utilicen de forma distinta a la inicialmente prevista.

Las técnicas encubiertas permiten la identificación de los individuos sin su conocimiento, dando lugar a una grave amenaza para la intimidad y a la filtración del control sobre los datos personales. Esto tiene graves consecuencias sobre la capacidad de las personas para ejercer el libre consentimiento o simplemente obtener información sobre el tratamiento. Además, algunos sistemas pueden recabar secretamente información sobre los estados emocionales o

características del organismo y revelar información sobre la salud que resulte en un tratamiento de datos no proporcionado, así como en el tratamiento de datos sensibles en el sentido del artículo 8 de la Directiva 95/46/CE.

Teniendo en cuenta que las tecnologías biométricas no pueden garantizar una total precisión, siempre existe un riesgo implícito de identificaciones incorrectas. Estos falsos positivos dan lugar a decisiones que afectan a los derechos individuales. La usurpación de identidad basada en el uso de fuentes biométricas suplantadas o robadas puede causar graves daños. A diferencia de lo que sucede con otros sistemas de identificación, no puede darse a una persona una nueva identificación solo porque la primera se encuentre en peligro.

Debe hacerse referencia a la elaboración de perfiles en el contexto de la toma de decisiones automatizadas o de la predicción del comportamiento o las preferencias en una situación específica. Algunos datos biométricos pueden revelar información física sobre una persona. Esto puede utilizarse para la selección de objetivos y la elaboración de perfiles, pero también puede dar lugar a discriminación, estigmatización y confrontación no deseada con información inesperada o no querida.

4.4. Referencia a tecnologías y sistemas biométricos específicos

4.4.1. Patrón de venas y usos combinados

Dos de las principales tecnologías utilizadas se basan en el reconocimiento del patrón de venas: el reconocimiento de venas de la palma y el reconocimiento de venas del dedo. Ambas técnicas se utilizan actualmente de forma amplia, especialmente en Japón.

Técnicamente, el reconocimiento del patrón de venas se basa en la plantilla de venas captada por una cámara de infrarrojos cuando el dedo o la mano se someten a una luz infrarroja. La imagen obtenida se trata para esbozar las características del patrón de venas, dando lugar a una imagen postprocesada de la red vascular. La principal ventaja de esta tecnología es el hecho de que los individuos no dejan rastro de su rasgo biométrico[13], dado que no existe la necesidad de «tener contacto» con el lector. A día de hoy también es difícil recoger los datos biométricos sin el consentimiento del interesado. Por último, esta técnica también puede utilizarse para detectar si el interesado expuesto al sistema está vivo o no, analizando si fluye la sangre.

El reconocimiento de los patrones de venas puede utilizarse para aplicaciones de acceso lógico y para el acceso físico a locales. Los fabricantes también ofrecen la posibilidad de incluir el sensor en otros productos, especialmente en el sector bancario.

Los riesgos de protección de datos asociados al uso de los sistemas de reconocimiento del patrón de venas pueden describirse de la manera siguiente:

- Precisión: el nivel de exactitud del patrón de venas es elevado, y esta tecnología se considera una alternativa viable a las impresiones dactilares. El reconocimiento de venas también ofrece un bajo porcentaje de no registro, ya que no está sujeto a deterioros del dedo o de la mano. Estas tecnologías aún no

[13] Algunos autores afirman que las tecnologías asociadas al reconocimiento de venas pueden revelar enfermedades como hipertensión o anomalías vasculares.

se han experimentado ni utilizado con una población muy amplia (en Japón, la plantilla se compara con la plantilla almacenada en la tarjeta inteligente). En algunos casos, esta tecnología también puede verse afectada por las condiciones climáticas que influyen en el sistema vascular (calor, presión, etc.).

- Impacto: el impacto de los sistemas del patrón de venas en la protección de datos es limitado, dado que los datos biométricos no se recogen fácilmente y el uso del patrón de venas se limita en la actualidad a aplicaciones del sector privado.

- Consentimiento y transparencia: puesto que los datos del patrón de venas solo pueden recogerse utilizando luz infrarroja y cámaras, puede considerarse que la persona es consciente del tratamiento y que otorga su consentimiento al presentar su mano o su dedo al lector. Sin embargo, al igual que con cualquier sistema biométrico, esta presunción debe mitigarse en algunos contextos específicos, por ejemplo, cuando la persona es un empleado del responsable del tratamiento de los datos.

- Fin o fines ulteriores del tratamiento: actualmente, los datos del patrón de venas presentan riesgos limitados en relación con su utilización para otros fines. Este riesgo podría aumentar si esta clase de tratamiento se generaliza y se facilita la suplantación.

- Vinculación: los datos del patrón de venas no aportan información que pueda vincularse con otros datos, excepto con los datos del patrón de venas de otro tratamiento.

- Seguimiento y elaboración de perfiles: el riesgo de seguimiento y de elaboración de perfiles de los datos del patrón de venas es limitado, en tanto en cuanto este tipo de datos biométricos no se utilice de forma amplia, por ejemplo, en una base de datos central para las tarjetas de pago.

- Tratamiento de datos sensibles: los únicos datos sensibles que podrían derivarse de los datos del patrón de venas se refieren al estado de salud, pero hasta ahora no se ha realizado ninguna evaluación formal sobre este tema.

- Revocabilidad: los datos del patrón de venas parecen muy estables con el tiempo, pero esta afirmación debe confirmarse experimentalmente (los sistemas del patrón de venas son demasiado recientes para proporcionar resultados confirmados). Los datos del patrón de venas deben considerarse, por tanto, irrevocables.

- Protección anti-suplantación: aún no se ha explorado ampliamente la suplantación de los datos del patrón de venas, aunque una investigación reciente puso de manifiesto que es posible suplantar un lector de venas de la palma de la mano[14]. La principal dificultad para suplantar los datos del patrón de venas es la recogida de una muestra de los datos biométricos.

---

[14] Véase: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

4.4.2. Impresiones dactilares y usos combinados

El reconocimiento de las impresiones dactilares es uno de los sistemas biométricos más antiguos y más ampliamente estudiados y utilizados. La identificación por medio de las impresiones dactilares lleva utilizándose más de 100 años con fines policiales, con fines de identificación y verificación. Se basa en el hecho de que cada individuo tiene impresiones dactilares únicas que muestran características específicas que pueden medirse para decidir si una impresión dactilar corresponde con una muestra registrada.

El registro exige que la persona esté físicamente presente, así como, en función del uso previsto, contar con personal bien formado a fin de garantizar una buena calidad de los datos. La captación de las huellas dactilares no es una tarea menor. En este sentido, la precisión de la correspondencia dependerá de la calidad de la imagen en relación con la técnica de imagen. Las técnicas pueden variar entre uno o dos dedos a los diez dedos, tomados de forma plana o girando los dedos. En función del sistema, las impresiones dactilares puede utilizarse solo para la verificación (1:1) o, para la identificación y la correspondencia con huellas (1:n). No obstante, como han mostrado algunos estudios, una parte de la población no es capaz de registrarse por distintos motivos, lo que supone un problema que exige contar con procedimientos alternativos adecuados, en particular para los grandes sistemas, a fin de evitar privar a los individuos de algo a lo que tienen derecho.

Incluso sin tratarse de un método extremadamente invasivo en principio, puede dar la impresión de serlo, pues lleva aparejado la sensación negativa de ser tratado como sospechoso debido a su uso común con fines policiales.

Las impresiones dactilares muestran rasgos distintos que pueden utilizarse para fines de verificación o identificación, si bien el análisis de los detalles sigue siendo la técnica más empleada. El desarrollo de nuevas técnicas (escáneres de alta resolución) permitirá el uso de otras características. Las técnicas también se han desarrollado respecto a las capacidades de identificación, permitiendo el uso de grandes bases de datos con fines identificativos.

En ese sentido, los sistemas más avanzados son los denominados sistemas automáticos de identificación dactilar (SAID), utilizados con fines policiales y que pueden usarse para el intercambio de datos, buscando en diferentes depósitos en emplazamientos transfronterizos. El intercambio de datos se enfrenta a problemas relacionados con los diferentes emplazamientos, los formatos y los niveles de calidad.

Ejemplos de SAID a nivel de la UE son Eurodac y el Sistema de Información de Visados que, según las expectativas, estarán entre las bases de datos más importantes del mundo, habida cuenta que en estos sistemas se almacenarán cerca de 70 millones de impresiones dactilares. En sus anteriores dictámenes, el Grupo de Trabajo planteó varias cuestiones sobre la utilización de las bases de datos a gran escala, teniendo en cuenta la necesidad de garantizar la proporcionalidad. Es preciso abordar los problemas de fiabilidad en términos de falsos positivos y falsos negativos, el control de acceso efectivo a estas bases de datos y los problemas relacionados con el uso de las impresiones dactilares de los niños y las personas de edad avanzada.

Las plantillas se utilizan de forma general en los sistemas biométricos de huellas dactilares, y suelen considerarse por los proveedores de los sistemas como una forma de proteger a los individuos. Sin embargo, dependiendo del sistema o del algoritmo utilizado para generar la plantilla, existen riesgos potenciales relacionados con la posibilidad de vincular las plantillas con otras bases de datos de huellas dactilares con el fin de identificar a las personas.

El uso de sistemas para burlar los sistemas de reconocimiento de impresiones dactilares utilizando dedos artificiales o impresiones dactilares hechas de material artificial, que permiten la usurpación de identidad, es también un problema importante. Existen diversos enfoques para reducir la vulnerabilidad de estos sistemas, tales como los sistemas de detección de vida, los sistemas basados en el reconocimiento de múltiples dedos y también la intervención de una supervisión humana adecuada para las tareas de registro, identificación y verificación.

Existen problemas de protección de datos relacionados con el uso de las impresiones dactilares que pueden describirse brevemente de la manera siguiente:

- Precisión: aunque las impresiones dactilares presentan un alto índice de precisión, esto puede fallar debido a limitaciones relacionadas con la información (baja calidad de los datos o proceso de adquisición no consistente) o la representación (rasgos seleccionados o calidad de los algoritmos de extracción). Esto puede dar lugar a falsos rechazos o a falsas correspondencias.

- Impacto: la irreversibilidad del proceso puede reducir la posibilidad de un individuo para ejercer sus derechos o invalidar las decisiones adoptadas basándose en una identificación falsa. El confiar en la precisión de la toma de huellas dactilares puede hacer más difícil rectificar los posibles errores, dando lugar a consecuencias de gran envergadura para los individuos. Esto debe tenerse en cuenta al evaluar la proporcionalidad del tratamiento en relación con la decisión específica que deba adoptarse sobre la base de las impresiones dactilares. Debe también mencionarse que la falta de medidas de seguridad puede dar lugar a la usurpación de identidad, que puede tener un fuerte impacto para el individuo.

- Vinculación: las impresiones dactilares proporcionan posibilidades de uso indebido, ya que los datos pueden estar vinculados con otras bases de datos. Esta posibilidad de vincularse con otras bases de datos puede dar lugar a usos no compatibles con los fines originales. Existen algunas técnicas, como la biometría convertible o la codificación biométrica, que pueden utilizarse para reducir el riesgo.

- Tratamiento de datos sensibles: según algunos estudios, las imágenes de huellas dactilares pueden revelar información étnica de la persona[15].

- Fin o fines ulteriores del tratamiento: el almacenamiento central de datos, especialmente en las grandes bases de datos, implica riesgos asociados a la seguridad de los datos, la vinculación y la desvirtuación de funciones. Esto permite, en ausencia de garantías, el uso de las impresiones dactilares para fines diferentes de los que justificaron originalmente el tratamiento.

- Consentimiento y transparencia: el consentimiento es una cuestión esencial en el uso de las impresiones dactilares para usos distintos de los policiales. Las impresiones dactilares pueden ser copiadas fácilmente de las impresiones dactilares latentes e incluso fotografías, sin conocimiento del individuo. Otras cuestiones relativas al consentimiento son las relacionadas con la obtención del consentimiento de los

---

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm y http://www.crime-scene-investigator.net/fingerprintpatterns.html.

menores y el papel de los padres a este respecto (por ejemplo, para tomar las huellas dactilares en las escuelas), así como la validez del consentimiento para proporcionar las impresiones dactilares en un contexto laboral.

- Revocabilidad: los datos de impresiones dactilares son muy estables con el tiempo y deben considerarse irrevocables. Una plantilla de impresión dactilar podrá ser revocada con determinadas condiciones.

- Protección anti-suplantación: las impresiones dactilares pueden ser fácilmente recogidas debido a las múltiples huellas que deja una persona. Además, las impresiones dactilares falsas pueden utilizarse con muchos sistemas y sensores, especialmente cuando tales sistemas no incluyen medidas específicas anti-suplantación. El éxito de un ataque depende en gran medida del tipo de sensor (óptico, capacitivo, etc.) y del material utilizado por el atacante.

Ejemplo:
Un hospital utiliza huellas dactilares en una base de datos central para autenticar a los pacientes en un servicio de radioterapia a fin de asegurarse de que se da el tratamiento correcto al paciente correcto. Las huellas dactilares son preferibles a los patrones de venas porque el tratamiento deteriora el sistema vascular. Además, se utiliza una base de datos central porque la situación de los pacientes (edad, patología) implica un riesgo elevado de pérdida de tarjetas de identificación que bloquearía el acceso a los tratamientos. En este caso, el uso de las impresiones dactilares parece ser una solución adecuada.

4.4.3. Reconocimiento facial y usos combinados

La cara, al igual que las huellas dactilares, ha sido ampliamente utilizada como fuente de datos biométricos durante años. Más recientemente, no solo la identidad puede determinarse a partir de una cara, sino también características fisiológicas y psicológicas tales como el origen étnico, emociones y bienestar. La capacidad para extraer este volumen de datos de una imagen y el hecho de que una fotografía puede tomarse a distancia sin conocimiento del interesado demuestra la cantidad de problemas de protección de datos que pueden derivarse de estas tecnologías.

El reconocimiento facial como medio para la identificación y la verificación no ha pasado inadvertido para las autoridades con funciones coercitivas, otras autoridades públicas u organizaciones privadas. Durante muchos años las fotografías han aparecido en pasaportes, carnets de conducir, documentos de identidad y fotos de archivos policiales. No es raro que se tome una fotografía en un control de acceso o en cualquier otro documento de identidad de una organización. Estas imágenes se toman normalmente con iluminación controlada y se limitan a una vista frontal o de perfil del individuo. La utilización de este conjunto de imágenes controlado es un punto de partida natural para el tratamiento y reconocimiento automático de los individuos. Esta capacidad ya se ha superado y la tecnología se encuentra en un punto en que es posible realizar una identificación a partir de imágenes utilizando una gama de cámaras, ángulos y condiciones de iluminación. También existe un gran volumen de imágenes disponibles públicamente en internet, como las existentes en las redes sociales y galerías puestas a disposición del público. Estos riesgos no se limitan a las imágenes tradicionales, ya que el reconocimiento facial se ha integrado con éxito en los vídeos en tiempo real. Al añadir nuevas capacidades de tratamiento a un sistema existente (por ejemplo, el reconocimiento facial a la TVCC) los responsables del tratamiento de datos deben

reconocer que esto puede cambiar el fin o los fines del sistema original y deben reevaluar el impacto del cambio en la intimidad.

Los riesgos para la protección de datos asociados al uso de los sistemas de reconocimiento facial pueden describirse de la manera siguiente:

- Precisión: si la calidad de las imágenes no puede garantizarse, existe el riesgo de que la exactitud se vea comprometida. Si no se capta una cara (oscurecida por el pelo o por un sombrero) está claro que la correspondencia o categorización no podrá darse sin un alto índice de error. Las variaciones en la pose y la iluminación siguen siendo un enorme reto para el reconocimiento facial, que afecta en gran medida a la precisión.

- Impacto: el impacto específico en la protección de datos de un determinado sistema de reconocimiento facial dependerá de su finalidad y circunstancias particulares. Un sistema de categorización para el recuento de visitantes a una atracción, sin capacidad de registro, tendrá un impacto diferente en la protección de datos que el de un sistema utilizado para la vigilancia discreta por las autoridades con funciones coercitivas a fin de identificar a posibles alborotadores.

- Consentimiento y transparencia: un riesgo de protección de datos que no está presente en muchos otros tipos de tratamiento de datos biométricos es el hecho de que las imágenes pueden capturarse y tratarse desde una serie de puntos de vista, condiciones ambientales y sin el conocimiento del interesado. En el Dictamen 15/2011 sobre la definición del consentimiento, el Grupo de Trabajo destaca el hecho de que para que el consentimiento constituya una base jurídica para el tratamiento, debe ser «informado». Si el interesado no tiene conocimiento del tratamiento de imágenes a efectos del reconocimiento facial, no puede dar un consentimiento informado. Incluso si el interesado es consciente de que hay una cámara funcionando, puede no distinguirse si se trata de un sistema de TVCC que funcione en directo o que grabe las imágenes, o de una lente que capture imágenes para un sistema de reconocimiento facial.

- Fin o fines ulteriores del tratamiento: una vez capturadas, de forma legítima o ilegítima, las imágenes digitales pueden fácilmente compartirse o copiarse para su tratamiento en sistemas diferentes de aquellos para los que estaban destinadas originalmente. Esto resulta evidente en el ámbito de los medios de comunicación social, donde los usuarios cargar sus fotografías personales para compartirlas con su familia, amigos y compañeros. Una vez en la plataforma de medios sociales, las imágenes están disponibles para su reutilización por la propia plataforma para una amplia gama de fines, algunos de los cuales pueden introducirse en la plataforma incluso después de que la imagen haya sido tomada o cargada.

- Vinculación: un gran número de servicios en línea permiten a los usuarios cargar una imagen para vincularla con el perfil del usuario. El reconocimiento facial puede utilizarse para vincular los perfiles de diferentes servicios en línea (a través de la imagen del perfil), pero también entre el mundo en línea y fuera de línea. No está fuera de lo posible tomar una fotografía de una persona en la calle y determinar su identidad en tiempo real buscando en estas imágenes de perfil público. Servicios de terceros también pueden rastrear fotografías de perfil y otras fotografías públicamente disponibles para crear grandes colecciones de imágenes a fin de asociar una identidad del mundo real con tales imágenes.

- Seguimiento/elaboración de perfiles: también podría utilizarse un sistema de identificación si no se conoce la identidad real de una persona. Podría utilizarse un sistema de reconocimiento facial en un centro comercial o espacio público similar para seguir las rutas y costumbres de los consumidores individuales. La finalidad podría ser una gestión eficaz de las colas o la colocación de productos con el fin de mejorar la experiencia del cliente. No obstante, junto con la capacidad para seguir o localizar a un individuo concreto está la capacidad para elaborar perfiles y enviar publicidad u otros servicios específicos.

- Tratamiento de datos sensibles: como ya se ha mencionado, el tratamiento de datos biométricos podría utilizarse para determinar datos sensibles, en especial aquellos con señales visuales tales como la raza, grupo étnico o quizá una enfermedad.

- Revocabilidad: un individuo puede cambiar fácilmente su apariencia (barba, gafas, sombrero, etc.) y burlar fácilmente los sistemas de reconocimiento facial, especialmente cuando operan en un entorno no controlado. No obstante, las principales características faciales de una persona son estables en el tiempo y los sistemas también pueden mejorar el reconocimiento recogiendo y asociando diferentes «caras» conocidas de una persona.

- Protección anti-suplantación: muchos sistemas de reconocimiento facial son fáciles de suplantar, pero los fabricantes intentan mejorar esta deficiencia con técnicas tales como la imagen en 3D o la grabación en vídeo. Sin embargo, la mayoría de los sistemas básicos utilizados en aplicaciones públicas no incluyen este tipo de protección.

Ejemplo:
Un ejemplo imaginario extremo sería el de un sistema de vigilancia por vídeo de un centro comercial de próxima generación que permita reconocer a las personas, registrar automáticamente los movimientos y diferenciar características faciales como sonrisa o enfado. Podría reconocer a los clientes habituales que entren en el aparcamiento y dirigirlos a las mejores plazas de aparcamiento. Cuando los clientes entren en el centro comercial, el sistema podría identificar su ropa para sugerir qué tiendas visitar en función de las ofertas, el historial de compras anteriores o a partir de una serie de indicadores previstos. También puede organizarse la publicidad personalizada en los escaparates o la denegación automática de acceso a tiendas, restaurantes y otros lugares. Los ladrones potenciales de coches podrían ser identificados y seguidos antes incluso de que toquen un automóvil. En caso necesario, vehículos aéreos teledirigidos (no pilotados) con cámaras y otros sensores podrían seguir la pista de sospechosos hasta que la sospecha se descarte o se confirme. Podrían detectarse objetos ocultos en la ropa (cuchillos o artículos hurtados). Esta tecnología no solo se basa en los nuevos sistemas biométricos, sino que combina y procesa información ya disponible con otros datos de una gama de diferentes sistemas.

Una aplicación similar se ha diseñado en el proyecto INDECT (sistema de información inteligente para el apoyo de la observación, búsqueda y detección para la seguridad de los ciudadanos en el medio urbano) en el que las tecnologías se combinan para luchar contra posibles actos de terrorismo y delincuencia antes de que se produzcan. El Grupo de Trabajo

destaca enérgicamente que este uso de la biometría requeriría una base jurídica adecuada y consideraciones estrictas por lo que respecta a la necesidad y la proporcionalidad de tales medidas.

4.4.4. Reconocimiento de voz y usos combinados

Además de utilizar el reconocimiento de voz como un elemento biométrico de identificación, un uso relativamente común implica la identificación de características específicas en el patrón de voz para clasificar a la persona que habla. Un ejemplo sería analizar las respuestas de una persona durante una conversación telefónica para identificar las pautas de estrés y las irregularidades del discurso a fin de señalar posibles casos de fraude.

Los testimonios publicados por los fabricantes señalan que, al aplicar dicha tecnología, las empresas de servicios financieros han incrementado los índices de detección del fraude y han permitido un servicio más rápido para resolver reclamaciones fundadas.

Cuando se utilizan en un sistema de categorización, los riesgos para la protección de datos son ligeramente diferentes a los de un sistema de identificación biométrica por cuanto no debería existir ninguna fase de registro ni necesidad de almacenamiento de larga duración de un modelo biométrico. No obstante, si se graba una conversación telefónica, como suele ser el caso de las entidades financieras, deberán existir controles adecuados a fin de garantizar la seguridad de estos datos.

- Precisión: un riesgo para la protección de datos de dicho sistema radica en las tasas de detección, específicamente los falsos positivos y falsos negativos, es decir, ¿cuántas personas han sido identificadas erróneamente como fraudulentas o cuántas alegaciones fraudulentas no se han identificado? Si bien un sistema de categorización puede soportar tasas de error más elevadas que la verificación o la identificación, deberán existir procesos adecuados para tratar a su debido tiempo los casos que puedan no estar correctamente categorizados.

- Consentimiento y transparencia: a estas tecnologías podrá aplicarse un enfoque respetuoso de la intimidad tal como garantizar que las llamadas sean analizadas para examinar su idoneidad y los interesados sean informados del proceso realizado. En un estudio de casos, se consideró que las personas no eran aptas para la prueba si no tenían el inglés como primera lengua o si tenían una discapacidad auditiva o cogitativa, o si no tenían acceso a un teléfono. Los reclamantes podían negarse a participar en la llamada y proporcionar información de forma tradicional; asimismo, los interesados que no deseaban o no podían participar en este sistema no se veían desfavorecidos.

- Fin o fines ulteriores del tratamiento: mientras que en la mayoría de los casos esta tecnología requeriría cambios específicos en la infraestructura, a medida que los sectores público y privado consolidan sus infraestructuras informáticas para incluir tecnologías tales como voz sobre IP, las tecnologías de reconocimiento vocal pueden integrarse más fácilmente sin el debido respeto de las obligaciones de protección de datos del responsable del tratamiento.

- Revocabilidad: si bien un individuo puede modificar su voz de forma deliberada, los patrones de voz son bastante estables y pueden ser eficaces para identificar de manera inequívoca a una persona, en particular cuando el individuo no está informado (y, por tanto, no modifica su voz).

- Protección anti-suplantación: las voces grabadas pueden utilizarse para burlar los sistemas de reconocimiento vocal. Las técnicas anti-suplantación incluyen preguntas y respuestas sobre cuestiones contextuales (preguntar la fecha del día o solicitar que se repitan palabras raras).

4.4.5. ADN

Las mejoras de los dispositivos utilizados para la correspondencia y secuenciación del ADN y la disponibilidad de equipos para el análisis del ADN a precios asequibles hace necesario reconsiderar algunos de los supuestos del anterior documento de trabajo sobre biometría (WP80).

Uno de los principales cambios en las tecnologías de la elaboración de perfiles de ADN es la reducción del tiempo necesario para las operaciones de correspondencia y secuenciación del ADN. Los continuos avances realizados a lo largo de los años por los investigadores académicos y los desarrolladores de biotecnología han reducido el tiempo necesario para la generación de un perfil de ADN de días a horas e incluso a fracciones de hora.

La fase inicial de un mercado de servicios en línea basado en el ADN es una amenaza para los derechos a la protección de datos de los particulares, especialmente cuando el servicio requiera transferencias de muestras biométricas y datos biométricos entre diferentes países (incluidos países terceros), múltiples procesadores de datos y falta de garantías adecuadas para el tratamiento de datos relativos a la salud o a la genética.

Es muy probable que en un futuro próximo sea posible elaborar perfiles de ADN y realizar correspondencias de muestras en tiempo real (o casi), utilizando dispositivos portátiles, lo que será el punto de partida para el desarrollo de sistemas de autentificación o identificación biométrica del ADN con mayores niveles de precisión en relación a la autenticación mediante impresiones dactilares, voz y reconocimiento facial.

Las mejoras en la elaboración de perfiles de ADN se deben también al creciente interés de los gobiernos, jueces y autoridades con funciones coercitivas en las biotecnologías para la investigación penal. Debido a la fiabilidad de la correspondencia del ADN y al hecho de que las muestras de ADN pueden recogerse sin el conocimiento del interesado, con el tiempo varios Estados miembros han creado o emprendido iniciativas para crear bancos de datos centralizados de perfiles de ADN relacionados con personas condenadas y muestras recogidas en la escena del crimen.

En mayo de 2005, siete Estados miembros de la UE firmaron el acuerdo conocido como «Tratado de Prüm» para mejorar la cooperación judicial y las investigaciones penales transfronterizas mediante el intercambio de información. El acuerdo establece nuevas bases para la cooperación, ya que proporciona a los signatarios determinados derechos de acceso a las bases de datos nacionales de ADN solo en el contexto policial (persecución de la delincuencia), datos sobre impresiones dactilares, datos personales y no personales, así como datos de matriculación de vehículos. Desde entonces, varios Estados miembros se han adherido al Tratado y los elementos esenciales del acuerdo se han incluido en la Decisión 2008/615/JAI del Consejo.

Con arreglo a este marco jurídico, varios Estados miembros de la UE tienen o tendrán en breve un banco de datos funcional nacional con los perfiles de ADN de personas condenadas y pruebas de la escena del crimen, que plantea algunas preocupaciones sobre este tratamiento de datos específico.

Una de las principales cuestiones relacionadas con la creación de bancos de datos de ADN es el hecho de que los datos genéticos procedentes de muestras de ADN (*loci*) pueden revelar (no inmediatamente durante la fase de recogida de información) información asociada con la salud, la predisposición a enfermedades o los orígenes étnicos. Por esta razón, la creación de bases de datos de ADN supone un riesgo significativo para la dignidad humana y los derechos fundamentales. Este riesgo se ha tenido en cuenta en la Resolución 2009/C 296/01 del Consejo. Existen disposiciones específicas para limitar el análisis del ADN a las zonas cromosómicas sin expresión genética recurriendo a un conjunto específico de marcadores de ADN que no contienen, que se sepa, información sobre características hereditarias específicas (esto también se conoce como Conjunto de Normas Europeas - *European Standard Set* «ESS»).

Sin embargo, la posibilidad de que uno de los marcadores de ADN extraído incluido en una base de datos nacional de ADN pueda revelar en el futuro algunas características hereditarias u otra información sensible requiere una atención constante a la evolución en la biología con la consecuencia de que, lamentablemente, en este caso, una parte de la información de la base de datos deberá suprimirse inmediatamente. Además, como estas bases de datos de ADN recogen perfiles de personas condenadas, el análisis estadístico de los datos debería limitarse en gran medida para evitar la elaboración de perfiles basados en el sexo o la raza.

Por lo que respecta a las bases de datos de ADN para fines policiales y de justicia penal, el Tribunal Europeo de Derechos Humanos ha declarado que debe establecerse una clara distinción entre el tratamiento de los datos personales y los perfiles genéticos de los sospechosos y de las personas condenadas por un delito[16].

Existe también un riesgo potencial de que el análisis del ADN pueda utilizarse para identificar a miembros de la familia o parientes relacionados con delitos no resueltos o personas condenadas, porque los perfiles de ADN pueden buscarse en la base de datos utilizando conjuntos parciales de marcadores o comodines («wild-cards»). Esta funcionalidad plantea la cuestión sobre las implicaciones del seguimiento de la información procedente de una búsqueda familiar.

También cabe señalar que existen riesgos específicos relacionados con el uso de los conjuntos de datos sobre el genoma en contextos de investigación. El Grupo de Trabajo considera que el acceso a las muestras y los datos debería estar limitado estrictamente a la comunidad investigadora y permitido exclusivamente con fines de investigación; además, es necesario aclarar en qué circunstancias se comunicarán a las personas los resultados de la investigación (teniendo también en cuenta su derecho a no saber) o se integrarán en expedientes médicos.

Los riesgos de protección de datos asociados con el uso del ADN como elemento biométrico pueden describirse de la manera siguiente:

- Precisión: si bien el ADN presenta un elevado nivel de precisión, debe tenerse en cuenta que ello dependerá del número de marcadores (loci) analizados. Los sistemas de prueba deben garantizar el más alto grado de precisión.

---

[16] TEDH, sentencia de 4.12.2008, S. y Marper contra Reino Unido (solicitud nº 30562/04 y 30566/04) en particular, apartado 125.

- Impacto: el uso de ADN puede considerarse extremadamente invasivo para el individuo. Los datos genéticos pueden revelar información sensible. El análisis estadístico de los datos puede utilizarse también para la elaboración de perfiles y puede tener efectos discriminatorios para las personas afectadas.

- Fin o fines ulteriores del tratamiento: las nuevas tecnologías permiten ahora un mayor intercambio de datos. Por esta razón, debe estar claro quién puede tener acceso a la información de una base de datos de ADN. La búsqueda de familiares y la orientación racial puede considerarse una nueva tecnología que desafía el propósito original del tratamiento en las bases de datos de ADN actualmente disponibles.

- Consentimiento y transparencia: actualmente se ofrecen servicios para efectuar análisis del ADN en muestras biológicas enviadas por correo postal (por ejemplo, saliva) cuyos resultados se envían por internet. Unos controles de identidad insuficientes podrían permitir que las personas o entidades presentasen muestras de otros individuos y a resultas de ello obtuvieran datos personales sensibles sobre otras personas.

- Vinculación: habida cuenta de la cantidad y variedad de información que puede obtenerse de la secuenciación del ADN, es muy susceptible de utilizarse indebidamente, ya que los datos extraídos pueden fácilmente vincularse con otras bases de datos que permitan la elaboración de perfiles de las personas. Una búsqueda familiar permite también la creación de vínculos con familiares.

- Tratamiento de datos sensibles: el ADN puede revelar información asociada a la salud, la predisposición a enfermedades o el origen étnico de las personas. Es por tanto muy importante aplicar el principio de minimización de datos al elegir los loci pertinentes. La información de ADN puede extraerse de muchas muestras durante un periodo de tiempo más largo, por lo que es aconsejable garantizar que el acceso a las muestras se limite estrictamente a los usuarios autorizados y únicamente para los usos autorizados.

- Revocabilidad: el ADN es irrevocable.

- Protección anti-suplantación: el ADN es, a priori, muy difícil de suplantar; sin embargo en muchos casos no es difícil recoger muestras de ADN de alguien (por ejemplo, pelo) sin su conocimiento.

4.4.6. Firma biométrica

La firma biométrica puede considerarse un ejemplo de nuevo uso de las tecnologías biométricas tradicionales. La firma biométrica es una técnica biométrica basada en el comportamiento, que mide la conducta de una persona según lo expresado por la dinámica de su firma manuscrita. Mientras que el reconocimiento de firma tradicional se basa en el análisis de características fijas o geométricas de la imagen visual de la firma (aspecto de la firma), la firma biométrica, en cambio, hace referencia al análisis de las características dinámicas de la firma (cómo se hizo la firma) y esto hace que estas técnicas se denominen «firma dinámica».

Las características dinámicas típicas medidas por un sistema de firma biométrica (como un tablero digitalizador) son la presión, el ángulo de escritura, la velocidad y aceleración del bolígrafo, la formación de las letras, la dirección de los rasgos de la firma y otras características dinámicas únicas. Estas características varían en uso e importancia entre los distintos proveedores y normalmente se recogen utilizando dispositivos de contacto sensibles.

Algunos dispositivos de reconocimiento de firma pueden realizar verificaciones mediante la combinación del análisis tanto estático (imagen) como dinámico (presión, ángulo, velocidad, etc.) de las características de una firma.

Los riesgos de protección de datos asociados a la utilización de firmas biométricas pueden describirse de la manera siguiente:

- Precisión: las personas no siempre firman de la misma manera, por lo que podrían tener problemas durante el proceso de registro y al verificar su identidad.

- Impacto: los elementos biométricos basados en características de comportamiento tales como la firma pueden no ser únicos con el tiempo y pueden ser modificados por el interesado. Los cambios en la firma también pueden tener un origen fisiológico y pueden impedir una buena verificación, lo que se traduce en la necesidad de procedimientos alternativos para verificar la identidad de los individuos.

- Anti-suplantación: mientras que la imagen gráfica de una firma tradicional puede reproducirse fácilmente y ser falsificada por una persona entrenada, por una fotocopia o por un programa informático de gráficos, una firma dinámica es más segura porque el proceso de verificación comprueba también las características dinámicas, que son complejas y únicas y corresponden al estilo de escribir de una persona.

5. Directrices generales, recomendaciones sectoriales y medidas técnicas y organizativas

El despliegue de un sistema biométrico se basa en la cooperación de varios actores:

- fabricantes: diseño y prueba de los sensores biométricos, y definición del funcionamiento de las tecnologías biométricas;
- integradores: diseño del producto final que se venderá al cliente: elección de la tecnología biométrica y definición parcial de los fines del sistema (eligiendo los clientes a que se dirige);
- revendedores: comercialización del producto final al cliente; suelen informar al cliente sobre la ejecución, los riesgos y potencialmente el marco jurídico;
- instaladores: instalación del producto en los locales del cliente;
- clientes: elección de compra de un sistema biométrico: determinan los fines y medios del tratamiento y son, por tanto, los responsables del tratamiento de datos;
- interesados: proporcionan los datos biométricos utilizados por el sistema.

Algunos agentes cumplen una o varias de las funciones anteriormente descritas. Cada papel tiene la responsabilidad de garantizar una utilización de los sistemas biométricos respetuosa de la intimidad: por ejemplo, el instalador no podrá aplicar un elemento de seguridad definido por el integrador.

5.1. Principios generales

En lo que respecta a los datos biométricos, la seguridad debería ser una preocupación fundamental, ya que los datos biométricos son irrevocables. Por consiguiente, una violación por lo que respecta a los datos biométricos constituye una amenaza para el uso seguro de la biometría como identificador y para el derecho a la protección de datos de los interesados, para los que no existe ninguna posibilidad de mitigar los efectos de la violación.

Los riesgos aumentan con el número de aplicaciones que utilizan estos datos (especialmente los riesgos de violación y de desvirtuación de funciones). Cuantos más datos biométricos se utilicen, más probable es que se produzca una sustracción de datos biométricos.

El Grupo de Trabajo reconoce la tendencia actual a permitir el acceso a distancia a los sistemas biométricos, por ejemplo interfaces enviadas por internet. Esta tendencia introduce una nueva serie de problemas de seguridad, muchos de los cuales son bien conocidos por la industria informática. En el despliegue de tal sistema deberían participar, ya en la fase de diseño, técnicos en materia de seguridad del sector informático.

El Grupo de Trabajo recomienda un alto nivel de protección técnica para el tratamiento de los datos biométricos, utilizando las últimas posibilidades técnicas. A este respecto, el Grupo de Trabajo recomienda seguir las normas del sector relativas a la protección de los sistemas en los que se trata la información biométrica.

5.2. Protección de la intimidad desde el diseño

La intimidad desde el diseño es el concepto de integrar la intimidad de forma proactiva en la propia tecnología.

Por lo que respecta a los sistemas biométricos, la intimidad desde el diseño se refiere a toda la cadena de valor de los sistemas biométricos:

- los fabricantes deben aplicar los principios de la intimidad desde el diseño al diseñar nuevas tecnologías y sensores: esto puede incluir la supresión automática de los datos brutos una vez calculada la plantilla, o la utilización del cifrado para el almacenamiento de los datos biométricos (ya sea en una base de datos central o en una tarjeta inteligente). Los fabricantes deben centrarse también en el desarrollo de las tecnologías biométricas respetuosas de la intimidad;
- los integradores y revendedores también deben aplicar los principios de protección de la intimidad desde el diseño al definir el producto final que va a ser vendido, optando por tecnologías respetuosas de la intimidad y añadiendo medidas de seguridad al producto final, tales como la descentralización de la base de datos;
- los clientes (futuros responsables del tratamiento de datos) deben aplicar los principios de intimidad desde el diseño siempre que soliciten un determinado sistema biométrico o definan las características técnicas del sistema. En este caso, los fabricantes e integradores deberán ofrecer un cierto grado de flexibilidad en su producto con el fin de responder a los principios de proporcionalidad, limitación de la finalidad, seguridad y minimización de datos.

Estos principios ya han sido aplicados con éxito en algunos dispositivos biométricos: algunos fabricantes han incluido en un lector biométrico determinado características de cifrado y conmutadores anti-extracción y anti-manipulación para prevenir el acceso no autorizado a los datos biométricos.

El Grupo de Trabajo recomienda que los sistemas biométricos se diseñen de conformidad con «ciclos de desarrollo» formales que incluyan las siguientes etapas:

1. especificación de requisitos sobre la base de un análisis de riesgo o una evaluación específica del impacto en la intimidad,
2. descripción y justificación sobre cómo el diseño cumple los requisitos,
3. validación con pruebas funcionales y de seguridad,
4. verificación de la conformidad del diseño final con el marco normativo.

El Grupo de Trabajo fomenta la definición de sistemas de certificación que garanticen la aplicación de la intimidad desde el diseño y refuercen la información de los responsables del tratamiento de datos sobre los riesgos para la protección de datos asociados a los sistemas biométricos.

5.3. Marco de la evaluación del impacto en la intimidad

5.3.1. Principios generales

La evaluación del impacto en la intimidad es un proceso en el que una entidad realiza una evaluación de los riesgos asociados con el tratamiento de datos personales y una definición de las medidas adicionales destinadas a mitigar esos riesgos. Por ejemplo, con la tecnología RFID, el Grupo de Trabajo ha establecido que la entidad que define la aplicación es responsable de realizar la evaluación del impacto en la intimidad. Esta entidad puede ser la responsable del tratamiento de los datos o el prestador que diseñe la aplicación RFID.

Debido a los riesgos específicos aparejados a la utilización de datos biométricos, el Grupo de Trabajo recomienda que quien defina la finalidad y los medios del dispositivo realice evaluaciones del impacto en la intimidad como parte integrante de la fase de diseño de los sistemas que tratan este tipo de datos. Puede ser el fabricante, el integrador o el cliente final.

Las evaluaciones del impacto en la intimidad deberán tener en cuenta lo siguiente:

- la naturaleza de la información recogida,
- la finalidad de la información recogida,
- la exactitud del sistema, partiendo de la base de que de la correspondencia o no de una plantilla biométrica podrían derivar decisiones importantes para un individuo,
- la base jurídica y el cumplimiento de las normas; ¿se requiere el consentimiento?,
- el acceso al dispositivo y la transmisión interna y externa de información en el seno del responsable del tratamiento de datos, que implicará técnicas y procedimientos de seguridad para la protección de los datos personales contra el acceso no autorizado,
- las medidas menos invasivas de la intimidad ya adoptadas, ¿existe un procedimiento alternativo al dispositivo biométrico (como solicitar la tarjeta de identidad)?,
- las decisiones tomadas en cuanto al tiempo de conservación y la supresión de datos. ¿de qué periodo de tiempo se trata? ¿se recogen todos los datos durante el mismo periodo de tiempo? ¿existe un mecanismo automático de decisión y un proceso alternativo apropiado?,
- los derechos de los interesados.

Las evaluaciones del impacto en la intimidad no solo deben orientarse a la identificación de los riesgos, sino que también deberían proporcionar medidas adecuadas de protección de datos y abordar la forma en que el responsable del tratamiento aporta soluciones adecuadas para atenuar los riesgos para la protección de los datos identificados en la sección anterior.

Cuando el fabricante o el integrador realizan la evaluación del impacto en la intimidad, el despliegue del sistema biométrico puede también requerir una evaluación adicional para tener en cuenta las especificidades del responsable del tratamiento. Por ejemplo, cuando un sistema biométrico se integra en el sistema informático del cliente, este deberá realizar una evaluación

adicional del impacto en la intimidad que tenga en cuenta sus propios procedimientos y medidas de seguridad informática.

5.3.2. Especificidad de los datos biométricos

Los datos biométricos requieren una atención específica porque identifican inequívocamente a los individuos utilizando sus características fisiológicas o de comportamiento únicas.

Por esta razón, las evaluaciones del impacto en la intimidad deben evaluar la manera en que el sistema analizado puede evitar o limitar sustancialmente los tres riesgos siguientes.

El primer riesgo es la usurpación de la identidad, especialmente en el caso de la identificación y la autenticación. El dispositivo biométrico no debe ser burlado por una suplantación y debe garantizar que la persona que realiza la correspondencia es realmente la persona registrada en el sistema. Esa amenaza parece menos importante para los datos biométricos que no pueden recogerse sin el conocimiento del interesado, tales como el patrón de venas[17]. Sin embargo, es una cuestión importante para los dispositivos que tratan huellas o reconocimiento facial. Las impresiones dactilares se dejan en cualquier lugar por el mero contacto con un objeto, y la cara también puede ser captada por una foto sin que la persona sea consciente de ello.

El segundo riesgo es el desvío de la finalidad, bien por el responsable del tratamiento de datos o por un tercero, incluidas las autoridades con funciones coercitivas. Esta amenaza común en lo que respecta a los datos personales se convierte en crucial cuando se utilizan datos biométricos. Los fabricantes deben adoptar todas las medidas de seguridad a fin de evitar toda utilización indebida de los datos y asegurarse de que los que dejen de ser necesarios para la finalidad del tratamiento se supriman inmediatamente.

Al igual que cualquier otro dato, los datos biométricos tratados o almacenados legítimamente o las fuentes de datos biométricos no podrán ser tratados ni registrados por el responsable del tratamiento para ningún fin nuevo ni distinto, a menos que exista un nuevo motivo legítimo para este nuevo tratamiento de esos datos.

El tercer riesgo es la violación de los datos, que requiere acciones especiales en el contexto de los datos biométricos dependiendo del tipo de datos en peligro. Si se utiliza un sistema que crea datos biométricos basándose en un algoritmo que convierte una plantilla biométrica en un determinado código, y los datos biométricos o el algoritmo son robados o están en peligro, deberán ser sustituidos. Cuando una violación de datos implique la pérdida de datos biométricos directamente identificados que estén muy cerca de la fuente de datos biométricos, tales como fotos de caras o huellas dactilares, deberá notificarse detalladamente al interesado para que pueda defenderse en un posible incidente futuro en el que esos datos biométricos puedan utilizarse contra él como prueba.

5.4. Medidas técnicas y organizativas

Debido a la naturaleza de los datos biométricos, su tratamiento exige medidas organizativas y técnicas especiales y precauciones para evitar efectos adversos al interesado en caso de violación de los datos, en particular debido a los riesgos de conducta ilícita que resulte en una «reconstrucción» no autorizada de un rasgo biométrico a partir de la plantilla de referencia, su vinculación con otras bases de datos, su «uso» ulterior sin conocimiento de los interesados para fines no compatibles con los originales, o la posibilidad de que algunos datos

[17] Si bien es difícil predecir qué ataques a la tecnología del patrón de venas serán posibles en los próximos años si esta tecnología se generaliza.

biométricos puedan utilizarse para revelar información sobre la raza o la salud de las personas.

5.4.1. Medidas técnicas

- *Uso de plantillas biométricas*

Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible.

La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

- *Almacenamiento en un dispositivo personal frente a almacenamiento centralizado*

Cuando se permita tratar datos biométricos, es preferible evitar el almacenamiento centralizado de la información biométrica personal.

Especialmente para la verificación, el Grupo de Trabajo considera aconsejable que los sistemas biométricos se basen en la lectura de los datos biométricos almacenados como plantillas cifradas en soportes que puedan ser conservados exclusivamente por los interesados (por ejemplo, tarjetas inteligentes o dispositivos similares). Sus rasgos biométricos pueden compararse con las plantillas almacenadas en la tarjeta o dispositivo mediante procedimientos de comparación estándar que se aplican directamente en la tarjeta o dispositivo en cuestión, por lo que la creación de una base de datos que incluya información biométrica deberá evitarse, en general y en la medida de lo posible. De hecho, si la tarjeta o dispositivo se pierde, los riesgos de que la información biométrica que contiene se utilice abusivamente son limitados. Para reducir el riesgo de usurpación de identidad, en dichos dispositivos deberán almacenarse datos de identificación limitados relacionados con el interesado.

Sin embargo, para fines específicos y ante necesidades objetivas, puede considerarse admisible una base de datos centralizada que contenga datos o plantillas biométricos. El sistema biométrico utilizado y las medidas de seguridad elegidas deberán limitar los riesgos mencionados y asegurarse de que la reutilización de los datos biométricos en cuestión para otros fines es imposible o al menos rastreable. Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

Cuando los datos biométricos se almacenan en un dispositivo controlado físicamente por el interesado, deberá utilizarse una clave de encriptado específica para los dispositivos de lectura a fin de proteger efectivamente estos datos contra todo acceso no autorizado. Además, tales sistemas descentralizados prevén una mejor protección de los datos biométricos mediante el diseño, puesto que el interesado controla físicamente sus datos biométricos y no existe un punto que pueda ser contemplado o explotado.

El Grupo de Trabajo también subraya que la idea de una base de datos centralizada cubre una amplia gama de aplicaciones técnicas, desde el almacenamiento en el lector hasta una base de datos alojada en una red.

- *Renovabilidad y revocabilidad*

Como la fuente de datos biométricos no puede cambiarse, los sistemas biométricos cuya finalidad sea establecer un vínculo de identidad deberán estar diseñados de manera que el proceso de registro y el tratamiento de los datos biométricos permita que de la misma fuente

puedan extraerse múltiples e independiente plantillas biométricas, a fin de poder sustituirlas en caso de violación de los datos o de evolución tecnológica.

Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad, bien para renovarlo o para suprimirlo de forma permanente, por ejemplo, cuando se revoque el consentimiento[18].

- *Forma cifrada*

Por lo que respecta a la seguridad, deberán adoptarse medidas adecuadas para proteger los datos almacenados y tratados por el sistema biométrico: la información biométrica deberá almacenarse siempre de forma cifrada. Deberá definirse un marco de gestión de las claves para garantizar que las claves de descifrado solo sean accesibles por razón de la necesidad de conocer.

Habida cuenta del uso generalizado de las bases de datos públicas y privadas que contienen información biométrica y del aumento de la interoperabilidad de los diferentes sistemas que utilizan la biometría, deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

- *Anti-suplantación*

A fin de mantener la fiabilidad de un sistema biométrico y prevenir la usurpación de identidad, el fabricante tiene que aplicar sistemas dirigidos a determinar si los datos biométricos son auténticos y siguen estando relacionados con una persona física. Por lo que respecta al reconocimiento facial, puede resultar vital garantizar que la cara es real y no, por ejemplo, una foto unida a la cabeza del impostor.

- *Cifrado y descifrado biométrico*

El cifrado biométrico es una técnica que utiliza las características biométricas como parte del algoritmo de cifrado y descifrado. En este caso, generalmente se utiliza un extracto de los datos biométricos como clave para encriptar un identificador necesario para el servicio.

Este sistema tiene muchas ventajas[19]. Con el mismo, no existe almacenamiento del identificador ni de los datos biométricos: solo se almacena el resultado del identificador cifrado con los datos biométricos. Además, los datos personales son revocables ya que es posible crear otro identificador que pueda protegerse asimismo con cifrado biométrico. Por último, este sistema es más seguro y fácil de usar para la persona: resuelve el problema de recordar contraseñas largas y complejas.

---

[18] Por ejemplo, la tecnología TURBINE destinada a proteger la plantilla biométrica mediante la transformación criptográfica de la información de huellas dactilares en una clave no-invertible que permite establecer correspondencias mediante una comparación bit a bit. Los datos biométricos transformados se consideran irreversibles a las muestras biométricas y las plantillas originales. Además, a fin de reforzar la confianza de los usuarios, esta clave también será revocable, es decir, podrá generarse una nueva clave independiente para volver a expedir identidades biométricas. Véase también: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf.

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

Sin embargo, el problema criptográfico que hay que superar no es fácil, porque el cifrado y el descifrado no admiten cambios en la clave, mientras que la biometría proporciona un patrón diferente que puede dar lugar a cambios en la clave extraída. Por consiguiente, el sistema debe ser capaz de calcular la misma clave a partir de datos biométricos ligeramente diferentes, sin aumentar la tasa de falsa aceptación.

El Grupo de Trabajo está de acuerdo en que la tecnología de cifrado biométrico es un ámbito provechoso para la investigación y que está suficientemente maduro para una mayor consideración por las políticas públicas, el desarrollo de prototipos y el estudio de solicitudes.

- *Mecanismos automatizados de supresión de datos*

A fin de impedir que los datos biométricos se conserven más tiempo del necesario para los fines para los que fueron recogidos o tratados, es preciso establecer mecanismos automatizados de supresión de datos también en caso de que el periodo de conservación se amplíe legalmente, garantizando así la oportuna supresión de los datos personales que sean innecesarios para el funcionamiento del sistema biométrico.

Al utilizar el almacenamiento integrado en el lector, los fabricantes pueden introducir también el almacenamiento de plantillas biométricas en memorias volátiles que garanticen que estos datos serán borrados cuando el lector esté desconectado. Por tanto, la base de datos biométricos no se mantiene cuando el lector se vende o se desinstala. También podrán utilizarse conmutadores anti-extracción para borrar los datos automáticamente en caso de que alguien trate de robar el lector.

- *Grandes bases de datos biométricos y bases de datos de conexiones indirectas*

Algunos países utilizan grandes bases de datos biométricos, principalmente con dos fines: ayudar a las investigaciones penales y garantizar la entrega de documentos de identidad (pasaportes, tarjetas de identidad, permisos de conducir). Las bases de datos utilizadas para la investigación penal generalmente recogen información sobre delincuentes y sospechosos y deberán diseñarse para identificar a una persona con los datos biométricos. Por el contrario, las bases de datos utilizadas para luchar contra la usurpación de identidad incluyen datos biométricos del conjunto de la población y deben utilizarse únicamente para autenticar a la persona (por ejemplo, si la persona ha perdido sus documentos o destruido el chip de seguridad del pasaporte en el que se almacenan los datos biométricos).

Cuando se utiliza una base de datos central a efectos de lucha contra la usurpación de identidad, el Grupo de Trabajo considera que deben aplicarse medidas técnicas para evitar cualquier desvío de la finalidad. En primer lugar, el principio de minimización de datos exige que solo deberán recogerse los datos necesarios para autenticar a la persona. Por ejemplo, se considera que la comparación de las impresiones dactilares de dos dedos es suficientemente precisa para autenticar a una persona.

Además, los responsables del tratamiento de datos pueden utilizar bases de datos de conexiones indirectas en las que la identidad de una persona no está vinculada a un único conjunto de datos biométricos, sino a un conjunto de datos biométricos. El diseño de la base de datos debe garantizar la autenticación de la persona con muy alta probabilidad (por ejemplo, 99,9 %, lo que es suficiente para disuadir a los infractores) y garantizar que la base de datos no pueda utilizarse para la identificación (porque un conjunto de datos biométricos corresponde a un gran número de personas).

El Grupo de Trabajo apoya el uso de esos sistemas cuando se utilizan grandes bases de datos biométricos a efectos de la lucha contra la usurpación de identidad.

Ejemplo: medidas técnicas para los sistemas de autenticación
La fuente de datos biométricos es única y está potencialmente asociada al interesado de forma permanente. Si se utiliza como base para los sistemas de autentificación, debe tenerse en cuenta que no puede cambiarse, mientras que en las tecnologías de autenticación comunes que por lo general exigen conocer o poseer un credencial (por ejemplo, un usuario o contraseña) siempre es posible el cambio de credencial. Por tanto, los sistemas que utilizan la autentificación biométrica deberán aplicar garantías especiales para proteger el vínculo entre los elementos biométricos y otros datos de identidad:
- Los datos de la plantilla no deben almacenarse de forma centralizada, dado que la seguridad del almacenamiento de datos biométricos es esencial por lo que respecta a la seguridad general del sistema biométrico. Es preferible un almacenamiento distribuido (por ejemplo, en una tarjeta inteligente). En ese caso, tanto la fuente de los datos como la plantilla son transportadas por el interesado.
- El almacenamiento y la transmisión de datos biométricos deben estar protegidos contra la interceptación, la revelación no autorizada y la modificación, mediante el uso de tecnologías adecuadas de cifrado.
- Algunos tipos de datos biométricos no son secretos (por ejemplo, la cara) y no pueden guardarse, bloquearse ni cambiarse en caso de violación, revelación o uso indebido de los datos. Como consecuencia de ello, la autenticación deberá combinarse con otras credenciales que puedan cerrarse con llave o modificarse.

5.4.2. Medidas organizativas

Para garantizar la protección de los datos, deben preverse y aplicarse medidas organizativas. Por ejemplo, el responsable del tratamiento debe establecer un procedimiento claro sobre quién puede acceder a la información del sistema, si el acceso es parcial o no, y por qué motivos. Todas las acciones deberán ser objeto de seguimiento.

El Grupo de Trabajo observa que la externalización a proveedores de servicios es posible incluso para las solicitudes de visado [artículos 13 y 43 del Reglamento (CE) n° 810/2009, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados] y que es cada vez más frecuente debido al mayor uso del almacenamiento en la nube.

En ese caso, el responsable del tratamiento deberá establecer una política detallada sobre cómo controlar a sus contratistas, por ejemplo mediante inspecciones no programadas, y exigir garantías relativas a los empleados, procedimientos en relación con los derechos individuales, etc.

Hecho en Bruselas, el 27 de abril de 2012

Por el Grupo de Trabajo
El Presidente
Jacob KOHNSTAMM