12168/02/ES
WP 80

Documento de trabajo sobre biometría

Adoptado el 1 de agosto de 2003

El Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE y es el órgano asesor comunitario independiente sobre protección de datos y vida privada; sus tareas están fijadas en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE. Gestión administrativa:

Dirección E (Servicios, Propiedad Intelectual e Industrial, Medios de Comunicación y Protection de Datos) de la Comisión Europea, Dirección General de Mercado Interior, B-1049 Bruselas, Bélgica, Despacho nº C100-6/136.

Website: www.europa.eu.int/comm/privacy

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

creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Visto el artículo 29, así como la letra a) del apartado 1 y el apartado 3 del artículo 30 de dicha Directiva,

Visto su reglamento interno, y en particular sus artículos 12 y 14,

ha adoptado el presente documento de trabajo.

1. INTRODUCCIÓN

El rápido progreso de las tecnologías biométricas y su aplicación generalizada estos últimos años precisan de un estudio pormenorizado desde el punto de vista de la protección de datos[2]. Una utilización amplia y sin control de la biometría es preocupante desde el punto de vista de la protección de los derechos y libertades fundamentales de las personas. Este tipo de datos es de una naturaleza especial, ya que tienen que ver con las características comportamentales y fisiológicas de una persona y pueden permitir su identificación inequívoca[3].

En la actualidad, el tratamiento de datos biométricos se suele utilizar en procedimientos automatizados de autenticación/comprobación e identificación, principalmente para el control de entrada a las zonas físicas y virtuales (acceso a sistemas o servicios electrónicos particulares).

Anteriormente, el uso de la biometría estaba limitado sobre todo a los ámbitos del ADN y la comprobación de las huellas digitales. La recopilación de las huellas digitales se utilizaba especialmente para fines legales (por ejemplo investigación criminal). Si la sociedad fomenta el desarrollo de bases de datos de huellas digitales u otras bases de datos biométricos para otras aplicaciones corrientes, se puede incrementar la reutilización potencial de esos datos por parte de otros como elemento de comparación e investigación en el marco de sus propios fines, sin haber pretendido inicialmente ese objetivo; las autoridades encargadas de hacer cumplir la ley podrían figurar entre esos "otros".

---

[1] Diario Oficial nº L 281 de 23.11.1995, p. 31; se puede consultar en: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[2] A partir del 11 de septiembre de 2001, la biometría se ha presentado a menudo como un medio adecuado para mejorar la seguridad pública. En la Unión Europea, se debate sobre la introducción de la biometría en carnés de identidad, pasaportes, documentos de viaje y visados. Próximamente, los EEUU van a exigir identificadores biométricos para extranjeros al entrar y salir del país. El Convenio OIT n° 108 se modificó en 2003 con objeto de introducir datos biométricos obligatorios para la gente de mar. También se está debatiendo en otros foros internacionales como el G8, la OCDE, etc.

[3] No obstante, la identificación única depende de diversos factores como las dimensiones de la base de datos y el tipo de biometría utilizada.

Una preocupación específica relacionada con los datos biométricos es que el público se insensibilice, mediante la ampliación del uso de esos datos, ante los efectos que pueda tener el tratamiento para la vida cotidiana. Por ejemplo, el uso de la biometría en las bibliotecas escolares puede hacer que los niños sean menos conscientes de los riesgos relativos a la protección de datos que pueden tener consecuencias para ellos en una etapa posterior de su vida.

El presente documento se propone contribuir a la aplicación eficaz y armoniosa de las disposiciones nacionales sobre protección de datos adoptadas de acuerdo con la Directiva 95/46/CE a los sistemas biométricos. El presente documento se va a centrar principalmente en las aplicaciones biométricas para fines de autenticación y comprobación. El Grupo pretende proporcionar unas orientaciones europeas uniformes, especialmente para el sector de los sistemas biométricos y para los usuarios de estas tecnologías.

2. DESCRIPCIÓN DE LOS SISTEMAS BIOMÉTRICOS

Los sistemas biométricos son aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona[4]. 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.

Cada biometría, ya se utilice para autenticación/comprobación o para identificación, depende, más o menos, del elemento biométrico en cuestión, que puede ser:
- **universal:** el elemento biométrico existe en todas las personas[5];
- **único**: el elemento biométrico debe ser distintivo para cada persona;
- y **permanente:** la propiedad del elemento biométrico es permanente a lo largo del tiempo para cada persona.

Se puede distinguir entre dos categorías principales de técnicas biométricas, en función de que se utilicen datos estables o datos dinámicos sobre el comportamiento[6].

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,

---

[4] La diferencia entre autenticación (comprobación) e identificación es importante. La autenticación responde a la pregunta: ¿soy quien pretendo ser? El sistema certifica la identidad de la persona mediante el tratamiento de datos biométricos referidos a la persona que pregunta y toma una decisión sí/no (comparacion1:1). La identificación responde a la pregunta: ¿quién soy? El sistema reconoce a la persona que pregunta distinguiéndola de otras personas, cuyos datos biométricos también están almacenados. En ese caso, el sistema toma una decisión 1 entre n, y responde que la persona que pregunta es X.

[5] A este respecto, no todos los elementos biométricos son equivalentes y el índice de diferenciación de una persona frente a otra es muy diferente, en función del tipo de biometría utilizada. Los elementos biométricos más distintivos parecen ser el ADN, la retina y las huellas digitales.

[6] Algunas técnicas pueden ser fisiológicas y comportamentales a la vez.

detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN[7] 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, etc.

Teniendo en cuenta la rápida evolución técnica y la creciente preocupación por la seguridad, numerosos sistemas biométricos funcionan combinando diferentes características biométricas del usuario con otras tecnologías de identificación o autenticación. Algunos sistemas, por ejemplo, asocian el reconocimiento facial y el registro de la voz. Para realizar la autenticación, se pueden utilizar conjuntamente tres métodos diferentes – basándose en algo que conozca una persona (contraseña, número de identificación personal, etc.), algo que posea una persona (ficha, clave CAD, tarjeta inteligente, etc.) y algo que sea una persona (un rasgo biométrico). Por ejemplo, se podría introducir en un ordenador una tarjeta inteligente, teclear una contraseña y presentar sus huellas digitales.

La recopilación de muestras biométricas, los denominados datos biométricos (imagen de las huellas digitales, del iris o de la retina, grabación de la voz), se lleva a cabo durante una fase llamada de “inscripción” utilizando un sensor específico para cada tipo de biometría. El sistema biométrico extrae rasgos específicos del usuario a partir de los datos biométricos para elaborar una “plantilla" biométrica. La plantilla es una reducción estructurada de una imagen biométrica: la medida biométrica registrada de una persona. Lo que debe almacenarse es la plantilla, presentada en forma digitalizada, y no el propio elemento biométrico. Además, se pueden tratar datos biométricos como datos brutos (una imagen) dependiendo del funcionamiento del sistema biométrico utilizado[8].

La fase de inscripción juega un papel fundamental ya que es la única en que aparecen al mismo tiempo los datos brutos, los algoritmos de extracción y protección (criptografía, comprobación aleatoria, etc.) junto con las plantillas. Debería destacarse a este respecto, que si los datos brutos revelan información que puede considerarse sensible en el sentido del artículo 8 de la Directiva 95/46/CE, el proceso de inscripción de esos datos deberá realizarse de acuerdo con dicha disposición (véase más adelante el punto 3.7).

Otras cuestión igualmente importante desde el punto de vista de la protección de datos es la forma del almacenamiento de las plantillas personales, que depende del tipo de aplicación para el que se vaya a usar el dispositivo biométrico y del tamaño de las propias plantillas. Las plantillas se pueden almacenar de una de las siguientes maneras:

a) - en la memoria de un dispositivo biométrico;
b) - en una base de datos central;

---

[7] Aunque el uso del ADN para la identificación biométrica plantea cuestiones específicas, el presente documento no va a ocuparse de ellas. Se puede señalar que la generación de un perfil de ADN en tiempo real como instrumento de autenticación no parece posible actualmente.

[8] El presente documento hace referencia básicamente a sistemas biométricos basados en plantillas y podría aplicarse asimismo a datos brutos. Sin embargo, la especificidad de los datos brutos puede dar lugar a una adaptación de los requisitos en materia de protección de datos.

c) - en tarjetas de plástico, tarjetas ópticas o tarjetas inteligentes. Este método de almacenamiento permite a los usuarios llevar consigo sus plantillas como dispositivos de identificación.

En principio, no es necesario almacenar los datos de referencia en una base de datos a efectos de autenticación/comprobación; es suficiente almacenar los datos personales de manera descentralizada. A la inversa, la identificación sólo puede realizarse almacenando los datos de referencia en una base de datos centralizada, porque, con objeto de averiguar la identidad del interesado, el sistema debe comparar sus plantillas o datos brutos (imagen) con las plantillas o datos brutos de todas las personas cuyos datos ya están almacenados de forma centralizada.

Otro extremo de gran importancia desde el punto de vista de la protección de datos es el hecho de que algunos sistemas biométricos se basan en datos como huellas digitales o muestras de ADN, que se pueden recopilar sin que el interesado sea consciente ya que puede dejar rastros sin darse cuenta de ello. Al aplicar un algoritmo biométrico a las huellas digitales encontradas en un vaso, se puede[9] averiguar si la persona está registrada en una base de datos que contenga datos biométricos, y en ese caso, determinar su identidad, mediante la comparación de las dos plantillas. Todo esto ocurre también con otros sistemas biométricos, como los basados en el análisis de la pulsación sobre las teclas o el reconocimiento facial a distancia, gracias a las características de la tecnología utilizada[10]. El aspecto problemático es, por una parte, que esta recogida y este tratamiento de datos puede hacerse sin el conocimiento del interesado y, por la otra, que independientemente de su fiabilidad actual, esas tecnologías biométricas se prestan a una utilización generalizada a causa de su "bajo nivel de intrusión". Por consiguiente, parece necesario establecer garantías específicas a este respecto.

3. APLICACIÓN DE LOS PRINCIPIOS DE LA DIRECTIVA 95/46/CE

3.1. Aplicación de la Directiva 95/46/CE

El apartado a) del artículo 2 de la Directiva 95/46/CE define los “datos personales” como “toda información sobre una persona física identificada o identificable (…); se considerará identificable toda persona cuya identidad pueda determinarse, directamente o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica (…)”. El considerando 26 añade la siguiente explicación “para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento *o por cualquier otra persona*, para identificar a dicha persona”.

---

[9] No obstante, esto implica al menos ciertos medios como la capacidad de recopilar las huellas digitales del vaso sin deteriorarlas, el material técnico para el tratamiento de los datos procedentes de las huellas digitales, el acceso al algoritmo del constructor y/o a la base de datos de huellas digitales.

[10] Véase el punto 3 sobre la aplicación de la Directiva 95/46/CE y más concretamente el punto 3.3. sobre la obligación de informar al interesado.

De acuerdo con esta definición, las medidas de identificación biométrica o su versión digital en forma de plantilla son casi siempre datos personales[11]. Resulta que los datos biométricos siempre pueden considerarse como "información sobre una persona física" ya que afectan a datos que proporcionan, por su propia naturaleza, información sobre una persona determinada. En el contexto de la identificación biométrica, la persona es generalmente identificable, porque los datos biométricos se usan para identificar o autenticar/comprobar al menos en la medida en que el interesado se distingue de cualquier otro[12].

De conformidad con el apartado 1 del artículo 3 de la Directiva 95/46/CE, los principios de la protección de datos se aplican al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. La directiva no se aplica si los datos los trata una persona física durante una actividad puramente personal o doméstica. Numerosas aplicaciones biométricas en el ámbito domestico entrarán en esta categoría.

Aparte de estas excepciones específicas, el tratamiento de datos biométricos sólo se puede considerar lícito si se realizan todos los procedimientos en cuestión (empezando por la inscripción) respetando las disposiciones de la Directiva 95/46/CE.

El presente documento no examina todas las cuestiones que plantea la aplicación de la Directiva 95/46/CE a los datos biométricos, sino que se tratan sólo los más relevantes y, por tanto, no facilita una visión exhaustiva de las consecuencias de la aplicación de la Directiva 95/46/CE.

3.2. Principio de fines y proporcionalidad

Con arreglo al artículo 6 de la Directiva 95/46/CE, los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Además, los datos personales serán adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de fines).

El cumplimiento de este principio implica en primer lugar una determinación clara de los fines para los que se recogen y tratan los datos biométricos. Por otra parte, hace falta evaluar el cumplimiento de la proporcionalidad y de la legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas y especialmente si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva. La proporcionalidad ha sido el criterio principal en casi todas las decisiones adoptadas hasta ahora por las autoridades encargadas de la protección de datos sobre el tratamiento de datos biométricos[13].

---

[11] Cuando los datos biométricos, como una plantilla, se almacenan de manera que el responsable del tratamiento o cualquier otra persona no pueden utilizar ningún medio razonablemente para identificar al interesado, dichos datos no se clasificarán como datos personales.

[12] La identificabilidad de la persona depende también de la disponibilidad de otros datos que (conjunta o separadamente) permiten la identificación de la persona en cuestión. La posibilidad de "identificación directa" por medio de "uno o varios elementos específicos, característicos de su identidad física" se menciona explícitamente en la definición de los datos personales del apartado a) del artículo 2 de la Directiva 95/46/CE.

[13] Por ejemplo, las decisiones de las autoridades neerlandesas, francesas, alemanas, italianas y griegas.

Para fines de control de acceso (autenticación/comprobación), el Grupo opina que los sistemas biométricos relativos a características físicas que no dejan rastro (por ejemplo la forma de la mano, pero no las huellas digitales) o los sistemas biométricos relativos a características físicas que dejan rastro pero no dependen de la memorización de los datos poseídos por una persona distinta del interesado (en otras palabras, los datos no se memorizan en el dispositivo de control de acceso ni en una base de datos central) crean menos riesgos para la protección de los derechos y libertades fundamentales de las personas[14]. Diversas Autoridades encargadas de la protección de datos han respaldado esta opinión y han declarado que sería preferible no almacenar la biometría en una base de datos sino más bien sólo en un objeto disponible exclusivamente para el usuario, como una tarjeta con microchip, un teléfono móvil o una tarjeta bancaria[15]. Dicho de otro modo, las aplicaciones de autenticación/comprobación que se pueden llevar a cabo sin un almacenamiento centralizado de datos biométricos no debería suponer la utilización de excesivas técnicas de identificación.

Por consiguiente, el Grupo considera que debería examinarse cuidadosamente el uso de tipos distintos de aplicación (basados en plantillas de huellas digitales en una terminal o en una base de datos central) antes de su puesta en marcha. No obstante, si se va a aplicar ese tipo de sistema, por ejemplo en el caso de instalaciones de alta seguridad[16], se puede considerar como un tratamiento de datos que presenta riesgos en el sentido del artículo 20 de la Directiva 95/46/CE y debe presentarse al control previo de las autoridades de protección de datos de acuerdo con la legislación nacional (véase el punto 3.5).

La Directiva 95/46/CE prohíbe el tratamiento ulterior que fuera incompatible con los fines para los que se recogieron los datos. Por ejemplo cuando los datos biométricos se tratan con fines de control de acceso, el uso de esos datos para evaluar el estado emocional del interesado o para vigilarlo en el lugar de trabajo no sería compatible con los fines originales de la recogida. Deben tomarse todas las medidas posibles para evitar esta reutilización incompatible[17]. La Directiva 95/46/CE establece excepciones a la prohibición de someter los datos a un tratamiento ulterior con fines incompatibles, pero bajo una serie de condiciones específicas.

Se acepta generalmente que el riesgo de reutilización de datos biométricos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta (por ejemplo: huellas digitales) para fines incompatibles es relativamente bajo si los datos no están almacenados en bases de datos centralizadas, sino en poder de la persona y son inaccesibles para terceros. El almacenamiento centralizado de datos biométricos incrementa asimismo el riesgo del uso de datos biométricos como llave para

---

[14] Se pueden distinguir los datos biométricos que se tratan de manera centralizada de los datos de referencia biométricos que se almacenan en un dispositivo móvil y el proceso de conformidad se realiza en la tarjeta y no en el sensor o cuando éste forma parte del dispositivo móvil.

[15] Deben tenerse en cuenta los mecanismos empleados para resolver los problemas derivados de la pérdida, robo o deterioro de tarjetas y hay que fomentar los que no implican almacenamiento de datos biométricos. Cuando sea viable, deberán recogerse de nuevo los datos directamente a partir del interesado.

[16] En la situación actual de la tecnología biométrica no existen aún soluciones fiables, de identificación pura en tiempo real par una población de cualquier dimensión, y no es probable que esté disponible en un futuro previsible.

[17] Como se afirma más arriba, estos fines deben definirse claramente.

interconectar distintas bases de datos, lo cual podría permitir obtener perfiles detallados de los hábitos de una persona tanto a nivel público como privado. Además, la cuestión de la compatibilidad de los fines nos lleva a la interoperabilidad de diferentes sistemas que utilizan la biometría. La normalización que requiere la interoperabilidad puede dar lugar a una mayor interconexión entre bases de datos.

El uso de la biometría plantea también el tema de la proporcionalidad de cada categoría de datos a la luz de los fines para los que se tratan dichos datos. Los datos biométricos sólo pueden usarse de manera adecuada, pertinente y no excesiva, lo cual supone una estricta valoración de la necesidad y proporcionalidad de los datos tratados[18]. Por ejemplo, la CNIL francesa ha rechazado el uso de huellas digitales en el caso del acceso de los niños a un comedor escolar[19], pero ha aceptado con el mismo fin el uso de los resultados de muestras de las manos. La autoridad portuguesa de protección de datos ha tomado recientemente una decisión desfavorable sobre la utilización de un sistema biométrico (huellas digitales) por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente[20]. La autoridad alemana de protección de datos adoptó una decisión favorable sobre la introducción de características biométricas en los documentos de identidad con objeto de evitar su falsificación, siempre que los datos se almacenen en el microchip de la tarjeta y no en una base de datos para compararlos con las huellas digitales del propietario.

Puede surgir una dificultad específica porque los datos biométricos contienen con frecuencia más información de la necesaria para las funciones de identificación o autenticación/comprobación. Esto ocurre con más probabilidad en el caso de la imagen original (datos brutos) ya que la plantilla puede y debe construirse técnicamente de manera que no se traten los datos que no son necesarios. Los datos innecesarios deberían destruirse cuanto antes[21]. Por otra parte, ciertos datos biométricos pueden revelar el origen racial o hacer referencia a la salud (véase más adelante el punto 3.7.).

Por último, debe mencionarse que el uso de sistemas biométricos puede realizarse de manera que se considere como una tecnología que mejora la protección de la vida privada entre otras cosas porque es capaz de reducir el tratamiento de otros datos personales como el nombre, la dirección, la residencia, etc.

---

[18] Por otra parte, el anonimato o el uso de pseudónimos debe ser posible en determinadas circunstancias. Deben tenerse en cuenta los mecanismos empleados para resolver los problemas derivados de la pérdida, robo o deterioro de tarjetas en este contexto y hay que fomentar los que no implican almacenamiento de datos biométricos. Cuando sea viable, deberán recogerse de nuevo los datos directamente a partir del interesado.

[19] Sin embargo, parece que la autoridad británica de protección de datos ha aceptado el uso de huellas digitales en circunstancias similares cuando se han adoptado las garantías apropiadas.

[20] La autoridad portuguesa de protección de datos considera que la aplicación de ese tipo de sistemas es desproporcionada y excesiva, teniendo en cuenta los fines del tratamiento de datos. El sistema debería almacenar esos datos en un dispositivo biométrico y el corpus de personas a controlar era aproximadamente de 140.

[21] Esta supresión puede apoyarse también en la letra e) del apartado 1 del artículo 6 de la Directiva 95/46/CE que estipula que los datos personales se conserven durante un periodo *no superior* al necesario para los fines para los que se traten.

3.3. Obtención leal e información sobre el interesado

El tratamiento de datos biométricos y en particular su recogida se realizará de manera leal[22]. El responsable del tratamiento informará al interesado de conformidad con los artículos 10 y 11 de la Directiva 95/46/CE[23], lo cual incluye concretamente la definición exacta de los fines y la identidad del responsable del tratamiento del registro (que será frecuentemente la persona encargada del sistema biométrico o de la técnica biométrica).

Deben evitarse los sistemas que recogen datos biométricos sin el conocimiento de los interesados. Algunos sistemas biométricos como el reconocimiento facial a distancia, la recogida de huellas digitales o la grabación de la voz presentan más riesgos desde este punto de vista.

3.4. Criterios de legitimación del tratamiento de datos

El tratamiento de los datos biométricos debe basarse en uno de los motivos de legitimidad contemplados en el artículo 7 de la Directiva 95/46/CE. Si el responsable del tratamiento del registro utiliza el consentimiento como motivo de legitimidad, el Grupo subraya que deberá cumplir las condiciones fijadas en el artículo 2 de la Directiva 95/46/CE (toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen).

3.5. Control previo – notificación

Como se ha indicado anteriormente, el Grupo apoya el uso de sistemas biométricos que no memoricen rastros en un dispositivo de control de acceso ni los almacene en una base de datos central (véase el punto 3.2.). Pero si está prevista la utilización de esos sistemas y, teniendo en cuenta el riesgo de la (re)utilización con distintos fines y los peligros específicos en caso de acceso no autorizado, el Grupo recomienda que los Estados miembros contemplen la posibilidad de presentarlos al control previo por parte de las autoridades encargadas de la protección de datos de conformidad con el artículo 20 de la Directiva 95/46/CE, ya que es probable que ese tipo de tratamiento comporte riesgos específicos para los derechos y libertades de los interesados. Si los Estados miembros desean introducir controles previos relativos al tratamiento de los datos biométricos, deberá consultarse oportunamente a las autoridades nacionales encargadas de la protección de datos antes de la introducción de las mencionadas medidas.

3.6. Medidas de seguridad

En virtud del artículo 17 de la Directiva 95/46/CE, el responsable del tratamiento deberá tomar todas las medidas de seguridad técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular

---

[22] Apartado a) del artículo 6 de la Directiva 95/46/CE.

[23] Las excepciones a la obligación de informar a los interesados contempladas en los artículos 10 y 11 de la Directiva 95/46/CE deberán basarse en medidas legislativas y constituir una medida necesaria para restringir el ámbito de actuación de la obligación de información para proteger los intereses enumerados en el artículo 13 de la Directiva 95/46/CE (la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales, etc.).

cuando el tratamiento incluya la transmisión de datos biométricos dentro de una red. Deben adoptarse medidas de seguridad con motivo del tratamiento de datos biométricos (almacenamiento, transmisión, extracción de características y comparación, etc.) y sobre todo si el responsable del tratamiento transmite esos datos a través de Internet. Las medidas de seguridad podrían incluir, por ejemplo, la codificación de las plantillas y la protección de las claves de codificación aparte del control del acceso y una protección que convierta en virtualmente imposible la reconstrucción de los datos originales a partir de las plantillas.

En este contexto, deberían tomarse en consideración determinadas nuevas tecnologías. La posibilidad de utilizar datos biométricos como claves de codificación constituye un desarrollo interesante; con ello habría a priori menos riesgos para el interesado ya que la descodificación sólo podría hacerse en base a una nueva recogida de los datos biométricos a partir del propio interesado y así se evita la creación de bases de datos con plantillas de datos biométricos que puedan reutilizarse para fines ajenos.

Las medidas de seguridad necesarias deberán aplicarse desde el primer momento del tratamiento, y especialmente durante la fase de “inscripción”, en la que los datos biométricos se transforman en plantillas o imágenes. No hace falta decir que toda pérdida de las cualidades de integridad, confidencialidad y disponibilidad con respecto a las bases de datos sería claramente perjudicial para cualquier aplicación futura basada en la información contenida en dichas bases de datos, y causaría asimismo un daño irreparable a los interesados. Por ejemplo, si las huellas digitales de una persona autorizada se asociaran con la identidad de una persona no autorizada, esta última podría acceder a los servicios de que dispone el propietario de las huellas digitales, sin tener derecho a ello. El resultado sería un robo de identidad, que (independientemente de su detección) quitaría fiabilidad a las huellas digitales de la persona para futuras aplicaciones y, en consecuencia, limitaría su libertad.

Los errores que se producen dentro de los sistemas biométricos pueden tener graves consecuencias para la persona y, en particular, la denegación errónea a personas autorizadas y la aceptación errónea de personas no autorizadas pueden provocar serios problemas a muy diferentes niveles. A priori, el uso de datos biométricos debería reducir el riesgo de ese tipo de errores. Sin embargo, también puede crear la ilusión de que la identificación o autenticación/comprobación del interesado siempre es correcta. Para el interesado puede ser difícil o incluso imposible demostrar lo contrario. Por ejemplo, un sistema puede identificar erróneamente a una persona como alguien al que se hubiera prohibido tomar un avión o entrar en un país específico y que no dispusiera de muchos medios para resolver el problema cuando se presenta esa prueba "indiscutible" contra él. En tales casos, debería destacarse una vez más que toda decisión que afecte jurídicamente a una persona sólo debería adoptarse una vez se haya confirmado el resultado del tratamiento automatizado de conformidad con el artículo 15 de la Directiva 95/46/CE.

Por último, hay que señalar que el uso de la biometría podría mejorar los procedimientos de control, por ejemplo en el caso de acceso a datos personales relativos a terceros, como en caso de robo y utilización indebida (procedimientos de autorización).

3.7. Datos sensibles

Determinados datos biométricos podrán 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, en sistemas biométricos basados en el reconocimiento facial, se pueden tratar los datos que revelan el origen racial o étnico. En esos casos, se aplicarán las garantías especiales contempladas en el artículo 8 además de los principios generales de protección de la Directiva.

Esto no significa que todo tratamiento de datos biométricos vaya a incluir necesariamente datos sensibles. Si un tratamiento contiene datos sensibles es una cuestión de apreciación vinculada con la característica biométrica específica utilizada y la aplicación biométrica en sí. Es más probable que eso ocurra en caso de tratamiento de datos biométricos en forma de imágenes, porque en principio los datos brutos no se pueden reconstruir a partir de la plantilla.

3.8. Identificador único

Los datos biométricos son únicos y la mayoría generan una plantilla (o imagen) única. Si se utilizan ampliamente, en particular para una parte sustancial de una población, los datos biométricos pueden considerarse como un identificador de aplicación general en el sentido de la Directiva 95/46/CE. El apartado 7 del artículo 8 de la Directiva 95/46/CE sería entonces aplicable y los Estados miembros deberían determinar las condiciones de su tratamiento.

Cuando se desea que los datos biométricos sirvan como clave para la conexión de bases de datos que contienen datos personales[24], pueden plantearse problemas especialmente difíciles si el interesado no tiene posibilidad de oponerse al tratamiento de datos biométricos; esto puede producirse en las relaciones entre ciudadanos y autoridades públicas.

En esta perspectiva, sería deseable que las plantillas y sus representaciones digitales se traten mediante manipulaciones matemáticas (codificación, algoritmos o funciones de comprobación aleatoria), que utilicen parámetros diferentes para cada producto biométrico, para evitar la combinación de datos personales procedentes de diversas bases de datos a través de la comparación de plantillas o representaciones digitales.

3.9. Código de conducta y utilización de tecnologías que mejoran la protección de la vida privada

El Grupo anima a la industria a producir sistemas biométricos que faciliten la aplicación de las recomendaciones que aparecen en el presente documento de trabajo y, si deben desarrollarse normas europeas o internacionales en este campo, deberían elaborarse en coordinación con las autoridades de protección de datos a fin de fomentar sistemas biométricos que tengan en cuenta la protección de datos a la hora de su elaboración, minimicen los riesgos sociales y evitan la utilización indebida de datos biométricos. El

[24] Véase también el punto 3.2 sobre la reutilización compatible.

Grupo desea destacar la importancia de las tecnologías que mejoran la protección de la vida privada en este contexto con objeto de reducir al mínimo la recogida de datos y evitar el tratamiento ilícito.

Además, el Grupo subraya la importancia de los códigos de conducta destinados a contribuir a la correcta aplicación de los principios de la protección de datos teniendo en cuenta las características específicas de los diversos sectores, de conformidad con el artículo 27 de la Directiva 95/46/CE. Pueden presentarse códigos comunitarios al Grupo para que éste determine, entre otras cosas, si los proyectos presentados son conformes con las disposiciones nacionales sobre protección de datos, adoptadas en virtud de la Directiva 95/46/CE.

CONCLUSIONES

El Grupo opina que la mayor parte de los datos biométricos implican el tratamiento de datos personales. Por consiguiente, es necesario respetar plenamente los principios de la protección de datos que aparecen en la Directiva 95/46/CE teniendo en consideración, al desarrollar los sistemas biométricos, la especial naturaleza de la biometría, y entre otras cosas su capacidad de recopilar datos biométricos sin el conocimiento del interesado y la casi seguridad del vínculo con la persona.

El cumplimiento del principio de proporcionalidad, que constituye el núcleo de la protección garantizada por la Directiva 95/46/CE impone, especialmente en el contexto de la autenticación/comprobación, una clara preferencia por las aplicaciones biométricas que no tratan datos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta o que no se almacenan en un sistema centralizado. Ello permite al interesado ejercer un mejor control sobre los datos personales tratados que le afectan.

El Grupo desea revisar el presente documento de trabajo a la luz de la experiencia de las autoridades de protección de datos y del progreso tecnológico relacionado con las aplicaciones biométricas. Como los datos biométricos ya se están introduciendo con objeto de una amplia gama de usos en numerosos y distintos foros, deberá empezarse ya a trabajar especialmente en el contexto del empleo, los visados y la inmigración, y la seguridad en los transportes.

En caso de que la responsabilidad de desarrollar sistemas biométricos que respeten la protección de datos deba recaer sobre el sector, sería muy beneficioso desde todos los puntos de vista un diálogo fructífero, en particular en base a un proyecto de código de conducta, entre todas las partes interesadas incluidas las autoridades de protección de datos.

Hecho en Bruselas, el 13 de junio de 2003
Por el Grupo
El Presidente
Stefano RODOTÀ