



Estrasburgo, febrero de 2005

T-PD (2005) BIOM F

**COMITÉ CONSULTIVO DE LA CONVENCIÓN PARA LA PROTECCIÓN DE LAS PERSONAS RESPECTO AL PROCESO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL
(T-PD)**

INFORME DE SITUACIÓN RELATIVO A LA APLICACIÓN DE LOS PRINCIPIOS DE LA CONVENCIÓN 108 A LA RECOGIDA Y AL PROCESO DE LOS DATOS BIOMÉTRICOS

(Traducción al español NO OFICIAL realizada por la Agencia Española de Protección de Datos del documento original en inglés)

Elaborado por el T-PD en su 21ª reunión (2-4 de febrero de 2005)

Documento de la Secretaría
preparado por la
Dirección General de Asuntos Jurídicos

PRÓLOGO

1. El informe de situación relativo a la aplicación de los principios de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (STE No 108, en adelante la Convención 108) a la recogida y al proceso de datos biométricos es el resultado de los trabajos iniciados en el año 2003 por el Grupo de Proyecto sobre la Protección de Datos (CJ-PD) bajo la égida del Comité europeo de Cooperación Jurídica (CDCJ) y, tras la reestructuración de los comités de protección de datos, proseguidos en 2004 y 2005 por el Comité Consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (T-PD).

2. El CJ-PD fue comisionado por el Comité de Ministros para «elaborar en prioridad, a la atención del CDCJ o su Mesa, un informe relativo a la incidencia de los principios de protección de datos sobre el uso de los datos biométricos (huellas dactilares, identificación por el iris, identificación de la cara, geometría de la mano, etc.) en distintos campos.» Inspirado por ese objetivo, el CJ-PD comisionó a un experto científico, D. Marcel YON, Director General de la sociedad alemana de biometría Visage Technologies AG, para que realizase un estudio sobre la biometría que pusiese de manifiesto sus aspectos técnicos, con objeto de facilitar al CJ-PD los elementos necesarios para el cumplimiento de su labor. El estudio técnico debería leerse en relación con el presente informe, dado que explica algunos de los conceptos que se utilizan en el mismo.

3. Tras la fusión del CJ-PD y del T-PD a finales del año 2003, el T-PD renovado aceptó reanudar la actividad relativa a la biometría. Era perfectamente consciente tanto del carácter complejo de la biometría como de la necesidad de adoptar una posición respecto a la aplicación de los principios de protección de datos a ese campo, con el fin de contribuir a los debates y a los proyectos biométricos en curso a escala nacional e internacional. Por tales motivos, el T-PD acordó elaborar un informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos.

4. Un borrador de informe de situación fue elaborado por un experto científico, D. Alexander PATIJN, Asesor jurídico principal ante el Ministerio holandés de Justicia. El T-PD y su Mesa trabajaron a continuación en colaboración con el experto científico con el fin de revisar y finalizar el informe de situación. El T-PD acordó, durante su 21ª reunión del 2 al 4 de febrero de 2005 celebrada bajo la presidencia de Doña Charlotte Marie Pitrat, hacer público ese informe de situación con el fin de contribuir a los debates y proyectos en curso en materia de biometría en varios Estados miembros del Consejo de Europa e instancias internacionales, tales como la OCDE (Organización para la Cooperación y el Desarrollo Económico) y la OACI (Organización de Aviación Civil Internacional). A su vez, el T-PD se alegraría de recibir contribuciones y reacciones respecto al contenido de ese informe por parte de los Estados miembros u otras organizaciones o entidades internacionales interesadas. En efecto, en el campo de la biometría resulta de especial importancia adoptar un enfoque concertado dada la complejidad del tema y sus implicaciones para el ser humano.

5. El T-PD desea así mismo llamar la atención sobre los instrumentos e informes siguientes del Consejo de Europa, dado que ciertos elementos de los mismos son pertinentes en lo que a la biometría se refiere:

- Recomendación N° R (87) 15 del Comité de Ministros a los Estados miembros, tendente a regular el uso de datos de carácter personal en el campo de la policía, y sus tres informes de evaluación (17 de septiembre de 1987)

- Recomendación N° R (89) 2 relativa a la protección de datos de carácter personal utilizados con fines de empleo (18 de enero de 1989) y exposición de motivos
- Recomendación N° R (91) 10 relativa a la comunicación a terceros de datos de carácter personal por parte de los organismos públicos (9 de septiembre de 1991) y exposición de motivos
- Recomendación N° R (97) 5 relativa a la protección de datos médicos (13 de febrero de 1997) y exposición de motivos
- Informe con principios rectores para la protección de las personas respecto a la recogida y al proceso de datos por medio de la videovigilancia (2003)
- Principios rectores relativos a la protección de los datos de carácter personal respecto a las tarjetas con chip (2004)
- Estudio relativo a los números personales de identificación : su implantación, su uso y la protección de datos (1991)

6. El informe de situación se elaboró sobre la base del estado de los conocimientos relativos a la biometría en el momento de su redacción. Si le T-PD lo considera necesario teniendo en cuenta desarrollos posteriores en el campo de la biometría, podrá ser completado o se podrán redactar nuevos informes de etapa en el futuro.

7. El informe de situación consta de cuatro partes:

- Una parte introductoria
- Una segunda parte dedicada a identificar las especificidades de la biometría
- Una tercera parte que ofrece criterios para la elección de la estructura de los sistemas biométricos
- Una cuarta parte que se apoya en las partes II y III con el fin de ilustrar la aplicación de la Convención 108 a los datos biométricos. Por tal motivo, se hace referencia a ciertas nociones a la vez en las partes II ó III y en la parte IV.

ÍNDICE

I.	Introducción	6
II.	¿En qué es específica la biometría?	8
	<i>Descripción de los tecnicismos</i>	8
	<i>Verificación e identificación</i>	8
	<i>La dignidad humana</i>	10
	<i>Un carácter único y permanente</i>	10
	<i>Probabilidad</i>	10
	<i>Interoperabilidad</i>	12
	<i>El uso de la biometría como instrumento de protección de la vida privada (PET)</i>	13
III.	Criterios de selección de la estructura del sistema	13
IV.	¿Cómo se aplican los principios de la Convención 108 a los datos biométricos?	15
	<i>¿En qué momento se aplica la Convención 108 a los datos biométricos?</i>	15
	<i>¿Quién es el responsable del proceso?</i>	16
	<i>Proceso leal y lícito</i>	16
	<i>Definición de la finalidad y elección de una técnica particular</i>	17
	<i>Carácter no excesivo</i>	18
	<i>Exactitud y probabilidad</i>	18
	<i>Conservación de los datos</i>	19
	<i>Datos sensibles</i>	20
	<i>Seguridad de los datos</i>	20
	<i>Transparencia</i>	20
	<i>Derecho de acceso</i>	21
	<i>Derecho de rectificación y de cancelación</i>	22
	<i>Recurso efectivo</i>	23
	<i>Pertinencia del artículo 9º de la Convención respecto a los sistemas biométricos</i>	24
V.	Conclusiones del informe de situación	25

I. Introducción

8. La biometría es un método tradicional de identificación de las personas: las huellas dactilares, por ejemplo, se usan desde hace décadas. No obstante, dos recientes desarrollos convergentes favorecen notablemente el recurso a la biometría. En primer lugar, existe una necesidad creciente de identificación inequívoca de personas tanto en el ámbito privado como en el ámbito público. Las amenazas terroristas actuales a escala mundial inducen a la identificación de las personas, partiendo del hecho de que los terroristas recurren a identidades múltiples. En el sector privado, la usurpación de identidad es un problema creciente que permite por ejemplo a los infractores malversar importantes sumas de dinero de las víctimas cuya identidad han adoptado de forma fraudulenta. En segundo lugar, la nueva tecnología y su rápido desarrollo parecen responder a esa necesidad al permitir utilizar la biometría de forma automatizada para verificaciones masivas de identidad en escasos segundos, en un lugar dado y con un grado suficiente de fiabilidad.

9. En numerosos países, los poderes públicos están considerando incluir o están incluyendo ya los datos biométricos en los documentos de identidad, por ejemplo en los pasaportes¹. El uso de las huellas dactilares o las técnicas de identificación por el iris y por el reconocimiento facial son hoy en día los métodos más verosímiles. Sociedades privadas, como por ejemplo los bancos, están considerando la emisión de tarjetas con chip que lleven datos biométricos de sus clientes con el fin de realizar transacciones. De forma simultánea, las propias escuelas empiezan a identificar a sus alumnos para impedir que los niños no autorizados puedan entrar en sus comedores. En un futuro próximo, aplicaciones domésticas llegarán al mercado. Será conveniente observar y analizar entonces esas aplicaciones a medida que vayan haciendo su aparición.

10. La aplicación de la biometría plantea importantes cuestiones en materia de derechos humanos. La integridad del cuerpo humano y la manera en la que éste es utilizado por la biometría constituyen un aspecto de la dignidad humana. En consecuencia, al optar por recurrir o no a la biometría para resolver un problema particular, los responsables de proceso deberían dar muestras de un sentido ético particular. La biometría está aún en su etapa inicial y poco se sabe de sus posibles inconvenientes. Una vez que esa técnica se haya adoptado a gran escala, un desarrollo irreversible, portador de efectos imprevisibles, podría iniciarse. Por tal motivo, conviene aplicar el principio de precaución que, según las circunstancias, impone cierta prudencia. El artículo 8 de la Convención europea de Derechos Humanos (en adelante CEDH) es especialmente pertinente para el campo de la biometría. Por una parte, el derecho al respeto de la vida privada implica el respeto del cuerpo humano. La dignidad humana debe ser plenamente respetada durante el proceso de recogida y utilización de las características del cuerpo humano. Las cuestiones planteadas por las personas discapacitadas y por aquellas cuyas características físicas no se corresponden con las normas técnicas deben encontrar una respuesta. Deberían preverse unos procedimientos de emergencia en caso de avería del sistema si las características físicas no se corresponden con las normas técnicas. Por otra parte, la recogida de datos de carácter personal con vistas al proceso automatizado de los mismos plantea el problema de la protección de los datos, en particular si esos datos biométricos revelan inútilmente, pero de forma inevitable, datos sensibles como por ejemplo alguna información sobre un tipo de enfermedad o una discapacidad física.

¹ El reglamento del Consejo de la Unión europea 15152/04, aprobado en diciembre de 2004, prescribe la introducción de datos biométricos en los pasaportes.

11. Recientemente se han publicado numerosos informes relativos a la protección de los datos y la biometría². *La Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal del Consejo de Europa* (Convención 108, en adelante «la Convención») creó un Comité consultivo, en adelante «el Comité», que tiene entre otras la función de emitir dictámenes sobre la pertinencia de la Convención en campos particulares. La Convención da efecto al artículo 8 de la CEDH respecto al proceso automatizado de los datos de carácter personal. Establece los principios generales tendentes a evitar cualquier interferencia con la vida privada o, cuando tal interferencia resulte inevitable, a rodearla de garantías. Esos principios no indican de forma precisa qué tipos de proceso de datos están autorizados o no, de ahí que tengan que ser interpretados en caso de aplicaciones concretas. La biometría no escapa a esa regla general. El Comité opina que los principios de la Convención han sido formulados de forma acertada, de manera independiente de la tecnología. Podrán ser aplicados aun cuando las técnicas de proceso de los datos biométricos de carácter personal no fuesen aún conocidas en el momento de la redacción de la Convención.

12. Es evidente que vivimos en una época en la que las personas dejarán pronto de ser reconocidas e identificadas dentro de los límites de comunidades relativamente restringidas que expidan los documentos que acrediten su identidad. La reciente internacionalización de la sociedad y el carácter cada vez más anónimo de la misma, así como el incremento de las amenazas para la seguridad y el desarrollo rápido y constante de la tecnología de la información, han dado lugar a enormes esperanzas en el uso de la biometría en materia de verificación (la autenticación) e identificación de las personas. Por otra parte, muchos temen que, sin una normativa apropiada, se produzcan atentados contra los derechos relativos a la protección de la vida privada sin justificación suficiente.

13. El Comité considera necesario llamar la atención sobre ciertas cuestiones relativas a las relaciones entre la Convención y el uso de la biometría. La Convención permite la extensión de sus normas al proceso manual de datos personales. Se podría tomar el ejemplo de la tradicional comparación manual de la fotografía que figura en un pasaporte con la persona que lo presenta en el control de identidad, o el no tan lejano de la fastidiosa comparación de huellas dactilares descubiertas en el lugar de un crimen con las de criminales conocidos. El Comité no ha estudiado específicamente ese proceso manual. Se centra en el nuevo desarrollo que consiste en la verificación de una supuesta identidad, o en la identificación in situ y en escasos segundos, de grupos importantes de personas mediante el proceso automatizado de datos biométricos. En efecto, contamos con escasas experiencias de semejantes aplicaciones y las mismas implican riesgos de abusos. Aunque los propios datos no revelan en general ninguna información relativa a las personas sometidas al control, esos datos biométricos, puestos en relación con las circunstancias respecto a las cuales se recogen, suministran un conocimiento respecto a esas personas que podría, por una parte no ser necesario para el fin de la recogida y, por otra parte, no contar con una base legal adecuada.

14. El Comité no ha querido ahondar en las cuestiones ligadas a las autoridades de control y a la transmisión de los datos a países que no ofrecen un nivel de protección adecuado. Esos aspectos están tratados en el protocolo adicional de la Convención 108 relativo a las autoridades de control y los flujos transfronterizos de datos (STE No 181), que entró en vigor recientemente. Las normas generales expuestas en ese instrumento son así mismo válidas para los datos biométricos. No se han presentado aún problemas específicos de los datos biométricos en el ámbito de los flujos transfronterizos de datos pero podría resultar preciso proceder en el futuro a un nuevo examen de esta cuestión.

15. Este informe está concebido como una guía para todos aquellos que tienen que decidir si es preciso hacer uso de la biometría y, en ese caso, qué condiciones y garantías se podrían considerar. Es

² El Grupo de protección de datos, creado por el artículo 29º de la Directiva de la Unión Europea relativa a la protección de datos, publicó el 1 de agosto de 2003 un documento de trabajo sobre la biometría referente a los aspectos relativos a la Directiva (www.europa.eu.int/comm/privacy).

aún demasiado pronto para emitir un juicio definitivo. Las incertidumbres son aún numerosas. En efecto, las ventajas aparentes pueden ser una fuente de inconvenientes cuyas consecuencias no se pueden medir aún plenamente. Algunos de esos temores pueden resultar infundados. Por tal motivo, el Comité ha optado por limitarse a un informe de situación. Dicho informe no saca conclusiones definitivas sino que pretende contribuir al debate sobre el proceso de los datos biométricos y la protección de los datos. Recomienda la adopción de precauciones para evitar posibles desarrollos irreversibles no deseados pero que supongan inconvenientes considerables e inútiles para la protección de los datos de carácter personal. El Comité se propone actualizar el presente informe o publicar otros informes si nuevos hechos así lo exigiesen, o incluso redactar nuevos instrumentos jurídicos.

II. ¿En qué es específica la biometría?

Descripción de los tecnicismos

16. El término « biometría » se refiere a sistemas que utilizan características físicas, fisiológicas o elementos de conducta personal mensurables con el fin de determinar la identidad o de verificar la identidad supuesta de una persona. El sistema se basa en las etapas siguientes: Se obtiene una muestra biométrica de una persona, por ejemplo la marca de una huella dactilar o un barrido del iris. Esa característica física puede ser representada mediante una imagen. No obstante, sucede con frecuencia que de esa muestra se extraigan datos. Esos datos extraídos constituyen el patrón biométrico. Los datos biométricos, ya se trate de la imagen o del patrón, se conservan entonces en un soporte de almacenaje. Esas fases preparatorias se conocen con el nombre de proceso de registro. A la persona cuyos datos quedan así almacenados se le da el nombre de registrado.

17. La finalidad misma del sistema biométrico sólo interviene en una fase posterior. Cuando una persona se presenta al sistema, éste le va a solicitar que presente sus características biométricas. El sistema procederá entonces a una comparación entre la imagen de los datos presentados (o el patrón extraído de sus datos) y los datos biométricos del registrado. Si la comparación es positiva, la persona será reconocida y « aceptada » por el sistema. Si no lo es, la persona no será reconocida y será « rechazada ».

18. Sólo en contadas ocasiones la imagen o el patrón de los datos registrados resultará idéntico a la imagen o al patrón de los datos biométricos que serán posteriormente presentados al sistema. La característica cambia a menudo ligeramente o es presentada de forme distinta a como lo fue durante el registro. La comparación supone inevitablemente un cierto elemento de probabilidad. La falta de correspondencia total no impide establecer con un grado suficiente de certeza para numerosos fines que la persona que presenta sus características biométricas al sistema es la misma persona que la persona registrada.

Verificación e identificación

19. Para cumplir un fin dado, es preciso llevar a cabo una elección entre las dos funciones de la biometría, a saber la verificación y la identificación.

20. La verificación consiste en comparar una muestra biométrica presentada con los datos biométricos registrados pertenecientes a una única persona. Con el fin de reforzar la seguridad, se prevé verificar más de una característica biométrica de una persona, por ejemplo sus huellas dactilares y su iris. En ese caso, el sistema sólo reconocería a la persona en el caso de un resultado positivo de una verificación acumulada de ambos datos. El resultado es positivo o negativo, la comparación es aceptada o rechazada. El hecho de que los datos registrados se conserven en un

soporte de almacenamiento individual (la tarjeta con chip, por ejemplo), en una base de datos o en ambos, es neutro. El elemento decisivo es que, en el caso de un control de identidad, los datos relativos a una única persona sean objeto de un proceso automatizado.

21. En el momento de la identificación, los datos presentados no sólo se comparan con los datos registrados pertenecientes supuestamente a la misma persona sino también con los datos biométricos de otras personas afectadas contenidos en la misma base de datos o en bases de datos conectadas con la misma, lo que excluye la posibilidad de conservar los datos registrados únicamente en un soporte de almacenamiento individual. Es preciso llevar a cabo una búsqueda para establecer una concordancia posible entre la muestra presentada por una persona y los datos registrados de (varias) otras personas. Cabe pues la posibilidad de que el mismo dato biométrico parezca ligado a otras personas o que la misma persona parezca ligada a distintas características registradas en la base de datos. Eso podría significar que una persona utiliza varias identidades o que alguien está tratando de ocultar su verdadera identidad bajo el nombre de otra persona. En ese caso, se trataría de un caso de usurpación de identidad.

22. La elección de una función de verificación o de identificación depende en sumo grado de la finalidad prevista del sistema biométrico y de las circunstancias en las que se utilizará dicho sistema. El instrumento debe favorecer la finalidad para la que se han recogido los datos y no resultar inútilmente sobredimensionado. Dicho de otro modo, y en términos jurídicos: el instrumento no debe resultar desproporcionado con relación a la finalidad primera que tiene que cumplir. La elección de un sistema de identificación, siendo así que un sistema de verificación parece así mismo posible, exige una justificación particular. El informe técnico hace hincapié en este punto esencial: los problemas de verificación no deben ser resueltos mediante soluciones de identificación.

23. La expedición de un pasaporte, un documento de identidad o un visado tiene por objeto establecer que la persona afectada no ha presentado ya otra solicitud bajo otro nombre. La característica que se introduce durante el procedimiento de registro debe ser comparada con la lista de las características ya registradas en el sistema, lo que permite evitar las entradas duplicadas. Esa finalidad no se puede cumplir sin la ayuda de un sistema de identificación. No obstante, tras el registro, para determinar el poseedor legítimo, basta comprobar que la característica biométrica incorporada en el documento concuerda con la característica presentada con posterioridad por el titular del documento.

24. El Comité acepta que la verificación de los pasaportes puede tener otros fines legítimos. Si la finalidad no consiste únicamente en verificar que el usuario del pasaporte es el titular legítimo sino así mismo, por ejemplo, controlar que la persona afectada no figura en ninguna lista de personas buscadas, la simple verificación no es suficiente. Comprobar sobre la base de datos biométricos que alguien figura en una lista supone el recurso a la identificación. Esa finalidad adicional debe ser explicitada para que resulte posible juzgar si el sistema de identificación elegido es necesario para ese fin adicional.

25. Otro ejemplo es el de la emisión de una tarjeta bancaria. En circunstancias normales, resulta posible identificar a una persona verificando su pasaporte o cualquier otro documento de identidad. Suponiendo que los documentos presentados sean fiables, no es preciso establecer la identidad de esa persona de otra forma. La tarjeta bancaria podría contener las características biométricas de una persona para que fuese posible comprobar si la tarjeta es efectivamente utilizada por el titular legítimo. La verificación consistiría, en ese caso, en controlar que la característica biométrica del usuario concuerda con la característica biométrica almacenada en la tarjeta. Para esa finalidad, no es necesario que el banco almacene datos biométricos adicionales en la tarjeta bancaria. No es necesario a tal fin almacenar otros datos biométricos en una base de datos además de los ya incluidos en la tarjeta bancaria.

La dignidad humana

26. Los datos biométricos se recogen a partir de o proceden del cuerpo humano. No hay nada más personal, sostienen algunos, que el propio cuerpo. En efecto, la recogida de esos datos podría ser sentida como un atentado contra la dignidad humana. Ciertas personas se muestran indiferentes pero otras experimentarán una resistencia psicológica ante la idea de que el cuerpo humano sea utilizado como fuente de información. Otras incluso no aceptarán que una parte de su cuerpo, aunque sólo fuese un dedo, sea « analizada » por una máquina. Otras pueden expresar su preocupación ante la trivialización sin consideración del cuerpo humano. La resistencia puede depender de factores socioculturales, religiosos o propios de cada persona. La actitud frente a la utilización del cuerpo humano por la biometría podría así mismo evolucionar con el tiempo.

27. Esos argumentos no significan que el uso de la biometría sea inútil o esté injustificado, pero establecen los límites a los campos a los que se aplica. Un responsable de proceso debe valorar las ventajas y los inconvenientes del uso de los datos biométricos con una finalidad precisa antes de tomar la decisión de recurrir a la biometría o a soluciones sustitutivas. Esa valoración debería producirse antes de proceder a la elección. La biometría no debería ser elegida únicamente porque su uso resulte práctico. Es la finalidad de ese instrumento la que debería justificar el uso del mismo y el recurso a los datos biométricos no debería apartarse en demasía de esa finalidad teniendo en cuenta todos los intereses correspondientes y los valores en juego. El fin de este informe consiste en poner en evidencia algunos de esos intereses.

Un carácter único y permanente

28. La característica que identifica a una persona de forma única no la da el hombre sino la naturaleza y, en principio, dicha característica permanece inalterable a lo largo de toda la vida. Sean cuales sean los medios utilizados por una persona para ocultar su identidad, legítimos (por ejemplo los arrepentidos que buscan protegerse de los malhechores) o ilegítimos (por ejemplo los criminales que buscan huir de las fuerzas del orden), la biometría permitirá en muchos casos una identificación permanente. En el futuro, no hay que descartar la posibilidad de que se pueda recurrir a la biometría de forma generalizada para identificar a las personas a lo largo de toda su vida. No obstante, existen excepciones que pueden plantear un problema en cuanto a la identificación permanente. Las características biométricas de una persona pueden variar en el transcurso de su existencia, por ejemplo debido al envejecimiento, a una intervención quirúrgica o a un accidente. En ese caso, un sistema biométrico podría dejar de reconocerla.

Probabilidad

29. En lo que se refiere a la biometría, habría que distinguir dos momentos. El primero es el momento del registro, durante el cual se introduce el dato biométrico de una persona en el sistema; el segundo está constituido por cualquier recogida subsiguiente de datos biométricos a efectos de comparación con los datos iniciales. La correspondencia absolutamente perfecta entre los datos registrados y los presentados posteriormente al sistema es técnicamente imposible. El uso de un sistema basado en datos biométricos descansa inevitablemente en probabilidades de orden estadístico. No existe ningún sistema infalible. Si las dos características concuerdan con un grado suficiente de probabilidad, la persona en cuestión será « reconocida » por el sistema. Así pues, los sistemas biométricos son intrínsecamente falibles.

30. El riesgo de un falso reconocimiento o de un falso no reconocimiento puede tener consecuencias nefastas para la persona afectada. Si por ejemplo es « reconocida » de forma incorrecta como incluida en una lista de criminales o delincuentes buscados, la consecuencia práctica podría ser

que tuviese que probar su inocencia. La tasa de falso reconocimiento y de falsos rechazos depende de varias propiedades del sistema, tales como su calidad y su fiabilidad, el proceso de registro, etc. Las tasas pueden ser ajustadas con objeto de obtener el nivel de seguridad exigido para la finalidad del sistema. Los esfuerzos tendentes a prevenir resultados erróneos deberían ser proporcionales a la finalidad del sistema.

31. El principio de un proceso leal de los datos de carácter personal supone que la persona afectada sea informada de los aspectos del proceso que resultan pertinentes para ella. Las propiedades del sistema que descansan de forma inherente en probabilidades y son pues falibles constituyen un aspecto pertinente. Así pues, le corresponde al responsable del proceso poner este hecho en conocimiento de la persona afectada e informarla de lo que puede hacer si resulta víctima de ese sistema. Cualquier presunción de infalibilidad es errónea.

32. El carácter probabilista de los sistemas biométricos puede tener efectos contrarios para la persona afectada o el responsable de proceso, según la forma en la que esté establecido el sistema. Cabe distinguir cuatro situaciones:

- (a) Un sistema filtro de las personas indeseables, por ejemplo un estadio de fútbol desea impedir la entrada de hooligans que figuren en una lista con sus datos biométricos. Un error del sistema redundará en beneficio de la persona afectada. No será reconocida y, por lo tanto, no será filtrada. El hooligan entrará en el estadio.
- (b) El mismo sistema « reconoce » de forma incorrecta a la persona afectada. Ésta última tendrá dificultades para probar que ha sido falsamente catalogada como hooligan.
- (c) Un sistema admite únicamente a personas reconocidas que usen una tarjeta con chip que sirve de llave para entrar en instalaciones con sistema de seguridad. La falta de reconocimiento incorrecta de la persona autorizada se volverá en su contra si no existe ningún procedimiento alternativo que permita a la persona acceder por otro medio.
- (d) El mismo sistema « reconoce » de forma incorrecta a una persona que, en realidad, no está autorizada. El responsable de proceso se enfrenta a una amenaza en materia de seguridad. En la práctica, esa amenaza puede ser reducida a un mínimo aceptable, pero no puede ser eliminada.

33. Le corresponde al responsable de proceso asumir el carácter falible inherente al sistema biométrico por el que ha optado. A él le corresponde establecer el grado adecuado de probabilidad respecto a la finalidad del sistema. ¿Es adecuado, por ejemplo, aceptar una tasa de error de uno de cada diez mil o de uno de cada diez millones? Esto es especialmente importante para aplicaciones a gran escala. A él le corresponde probar de forma regular que el sistema sigue estando en concordancia con el grado de fiabilidad exigido para la finalidad que tiene que cumplir.

34. Se pueden plantear cuestiones relativas a la precisión respecto a una posible finalidad secundaria incompatible con la finalidad del sistema. En efecto, sería contrario al principio de proporcionalidad exigir que un sistema que use datos biométricos sea más preciso de lo que exige la finalidad inicial de ese sistema por el único motivo de que en casos excepcionales los datos podrían ser requeridos para un fin secundario, por ejemplo la represión de infracciones penales de conformidad con el artículo 9 de la Convención. Si, en casos excepcionales, los datos se utilizan para semejantes fines secundarios, su fiabilidad deberá ser valorada respecto a la finalidad para la que hayan sido inicialmente obtenidos. Tomemos el ejemplo de un caso de sistema biométrico diseñado para un fin específico en el que fuese suficiente registrar un patrón que incluyese doce elementos extraídas de la muestra biométrica original. Para un fin secundario incompatible, parece necesario un patrón que incluya como mínimo cincuenta elementos. Ahora bien, ese uso incompatible excepcional no puede justificar el almacenamiento de esos cincuenta elementos. Si, en

casos excepcionales, los datos deben ser utilizados para semejantes fines secundarios, habría entonces que tener en cuenta el carácter limitado de su fiabilidad.

35. Los datos biométricos tienen la reputación de ser sumamente fiables porque están ligados a la presencia física y real de una persona y, como tales, serían pues inalienables. Existe realmente una alta probabilidad de que el uso de los datos biométricos permita tener la seguridad de que se está ante la persona correcta. No obstante, siempre cabe la posibilidad de falsificaciones. Las huellas dactilares recogidas en un vaso pueden por ejemplo servir para crear con cera una huella idéntica en un soporte de almacenamiento. Resulta más difícil programar un ordenador para que genere artificialmente tantas imágenes necesarias para la reproducción del patrón registrado en un soporte de almacenamiento de datos robado. Esa imagen (impresa en la cera, por ejemplo) puede servir para hacerse pasar por el propietario legítimo del soporte robado. Ese procedimiento de falsificación no resulta afectado por una encriptación del patrón previa a su registro en el soporte de almacenamiento.

36. Aun cuando los sistemas biométricos parezcan fiables, resulta no obstante peligroso confiar excesivamente en los mismos. Las aplicaciones que afectan a un grupo amplio de personas son aún escasas. El carácter falible inherente a esos sistemas supone que se producirán forzosamente errores, aunque el sistema funcione perfectamente. La perspectiva es aún escasa en lo que se refiere a su eficacia, su fiabilidad y sus efectos sobre la vida privada. Los efectos sobre la sociedad de una introducción más general de cualquier tipo de sistemas biométricos tanto en los ámbitos privados como en los públicos se conocen aun menos, lo que nos lleva a abogar por una implantación gradual y prudente de esos sistemas. Una introducción excesivamente rápida y demasiado entusiasta podría tener unos efectos imprevistos cuya vuelta atrás resultaría harto difícil.

37. En función de las circunstancias, cabría la posibilidad de considerar el uso simultáneo de una o dos características biométricas. En teoría, el incremento o la reducción del riesgo de error parece depender de la estructura del sistema. Si existe un doble control de la identidad de una persona (por ejemplo una combinación de las huellas dactilares y del iris), a priori el sistema sería más fiable. No obstante, dado que los errores son inevitables, el procedimiento tendría un doble riesgo de errores. El Comité desea poner de relieve esas cuestiones sin darles respuesta alguna. Cabe pensar que las respuestas definitivas a esas cuestiones sólo serán posibles a través de experiencias concretas.

Interoperabilidad

38. Existe la tendencia, comprensible por lo demás, a recoger las características biométricas de conformidad con unos procedimientos normalizados, con objeto de permitir que distintos sistemas funcionen entre sí. Los sistemas que permiten la compatibilidad pueden reconocer a las personas en función de sus datos biométricos, independientemente del responsable de proceso que haya puesto a punto el sistema y de la finalidad para la que hayan sido recogidos los datos. Esa evolución tiene no obstante por resultado ampliar la divergencia entre intereses antagonistas: la utilidad de los sistemas que usan datos biométricos aumenta, pero también aumentan los riesgos de uso para fines incompatibles.

39. No se puede descartar que la interoperabilidad tecnológica en curso pueda tener como consecuencia práctica, a largo plazo, la asimilación del uso de ciertos datos biométricos a un identificador único de aplicación general³. Un ejemplo de semejante identificador es el número de identificación personal (PIN)⁴. Un factor agravante podría derivar del hecho que, contrariamente al

³ Véase al respecto el artículo 8º, apartado 7º, de la Directiva 95/46/CE

⁴ Véase así mismo el informe del Consejo de Europa relativo a *Los números personales de identificación: su implantación, su uso y la protección de datos* (1991).

número PIN que se puede cambiar a lo largo de una vida (por ejemplo tras una emigración), semejante cambio no es necesariamente factible en el caso de los datos biométricos.

40. Las recomendaciones de la OACI que tienen por objeto garantizar la compatibilidad de los sistemas a escala mundial con el fin de reforzar la seguridad de los transportes en la aviación civil suponen una dimensión adicional. Sin unas normas precisas, podrían fácilmente tener por resultado una diseminación general de los datos biométricos dado que ciertos países no cuentan con legislación alguna en el campo de la protección de datos o aplican dicha legislación únicamente a sus propios ciudadanos. El Comité es consciente de la estrecha cooperación existente entre el Consejo de Europa, la OACI, la OCDE y la Unión Europea con el fin de abordar algunos de esos problemas y espera muchísimo del resultado de esos trabajos.

El uso de la biometría como instrumento de protección de la vida privada (PET)

41. La biometría puede ser utilizada como instrumento de protección de la vida privada (PET). Una característica biométrica en una tarjeta bancaria impide que ésta pueda ser utilizada por otra persona que no sea el titular legítimo de la misma. La biometría puede así mismo servir para proteger las bases de datos que contengan datos de carácter personal frente a un acceso abusivo. Si la persona que accede a los datos almacenados en una base de datos es identificada mediante una característica biométrica, es probable que no sea una persona no autorizada la que solicita acceder a los mismos.

III. Criterios de selección de la estructura del sistema

42. El uso de la biometría es posible en distintas estructuras del sistema. Los sistemas se pueden diferenciar con vistas a su pertinencia para la protección de datos de carácter personal. Desde el punto de la protección de los datos, varios criterios parecen ser pertinentes. En este contexto, se puede citar el enfoque que consiste en privilegiar la imagen o el patrón y la forma en la que los datos son almacenados y pueden ser consultados. No obstante, la evolución de la tecnología en un futuro próximo podría llevar a sistemas o criterios en los que aún no se piensa.

43. La elección entre el registro de la imagen completa de una característica biométrica o de un extracto bajo la forma de un patrón se refiere al principio según el cual no hay que recoger más datos de los necesarios para el fin para el que se recogen dichos datos. Tradicionalmente, las huellas dactilares y la fotografía de los delincuentes detenidos se almacenan con el fin de recuperarlas más fácilmente en caso de reincidencia tras su condena. Más tarde, pueden dejar huellas dactilares en el lugar del crimen o ser reconocidos por testigos en las fotografías de la policía. El registro de la imagen completa es necesaria, ya que no se sabe de antemano qué parte de la huella digital se podrá recoger en el lugar del crimen. Esa imagen puede revelar datos sensibles, por ejemplo ciertas formas de enfermedades o discapacidades físicas. Esos datos pueden no ser necesarios para el fin, pero su conservación no deja por eso de ser indispensable.

44. Es menos evidente que sea necesario conservar en un sistema una imagen completa en el caso de que el reconocimiento mediante datos biométricos se lleve a cabo solicitando la cooperación de la persona afectada para que someta la muestra biométrica pertinente en el momento de la recogida secundaria. Un grado suficiente de probabilidad para numerosos fines se alcanzará extrayendo un patrón de las características sometidas y comparándolas con las que se han registrado.

45. Otro punto pertinente es la forma en la que los datos registrados, ya se trate de imágenes o de patrones, se conservan ya que esto tiene consecuencias en cuanto a la accesibilidad y la posible diseminación de los mismos. La estructura de un sistema biométrico puede ser diseñada de distintas

formas. La primera posibilidad es que el dato se almacene únicamente en un soporte de almacenamiento individual dotado de seguridad, por ejemplo una tarjeta con chip⁵. Este sistema podría ser suficiente a efectos de verificación. Los datos necesarios sólo están disponibles en la tarjeta. Si la persona afectada pierde su tarjeta, todos los datos se pierden. La tarjeta se puede comparar con una llave. Hasta hace poco, se entendía que de esa forma la persona afectada mantenía el control del uso de los datos que la concernían. Se pensaba que nadie podía tener acceso a los datos mientras la persona afectada no utilizaba su tarjeta. El responsable de proceso que determina la finalidad del sistema, sus medios y la clase de datos que se han de tratar no tendría acceso alguno a los datos mientras la propia persona no los sometiese voluntariamente y con pleno conocimiento de causa. Una nueva tecnología permite disponer de una tarjeta con chip con la que se puede proceder a la lectura sin contacto directo del dato registrado y almacenado en esa tarjeta (*RFID*). La persona afectada pierde así el control exclusivo de uso de sus datos. Este hecho podría ser compensado mediante medidas de seguridad adicionales. Cabría la posibilidad, por ejemplo, de dar efecto al principio del proceso legal avisando al titular cada vez que se produzca la lectura de los datos en su tarjeta. La lectura secreta de datos, si es necesaria, debería estar específicamente prevista por la ley incluyendo garantías adecuadas contra los abusos. No obstante, si la persona afectada no está en el campo de un lector, el responsable de proceso no tiene acceso a los datos.

46. Otra estructura posible del sistema consiste en almacenar los datos registrados en una base de datos local o regional, por ejemplo, bajo el control exclusivo de las autoridades municipales responsables de la expedición de un pasaporte. No importa pues saber si los datos están o no almacenados además en un soporte individual de almacenamiento para la persona afectada. Gracias a su base de datos, el responsable de proceso puede comprobar si los datos biométricos de un solicitante constan ya en el sistema. En el caso de un pasaporte, las autoridades municipales pueden verificar si un residente local ha solicitado ya un pasaporte bajo otro nombre. Unida a otras garantías, esa estructura podría ser considerada como adecuada para impedir cualquier adquisición de una doble identidad. Así, la legislación alemana sobre pasaportes no permite la creación de una base de datos federal que incluya datos biométricos, procedentes de las autoridades locales de expedición de los pasaportes. Así mismo, sus autoridades federales no tienen acceso automático a los datos⁶. Para ciertos fines, será preciso almacenar los datos registrados en una base de datos central o permitir que se pueda acceder a los mismos a través de la interconexión de un grupo de responsables de proceso⁷.

47. El Comité señala que se están llevando a cabo experimentos en distintos países con el fin de probar la estructura que concilie de la mejor forma posible las necesidades de la determinación de la identidad de una persona mediante la verificación o la identificación con las exigencias legales de protección de los datos biométricos de acuerdo con los principios de protección de datos. El Comité no cree poder descartar que otras características de la estructura del sistema sean o puedan llegar a ser legalmente pertinentes desde el punto de vista de la protección de los datos.

48. La distinción entre un soporte de almacenamiento individual y una base de datos no está ligada a la distinción entre las funciones de verificación y de identificación. Un sistema que use la función de verificación puede fundamentarse en el simple soporte de almacenamiento individual o

⁵ Véanse los « principios rectores del Consejo de Europa para la protección de los datos de carácter personal respecto a las tarjetas con chip. » (2004)

⁶ El Parlamento Europeo ha abogado por una solución similar en su opinión sobre la propuesta de la Comisión Europea de introducir datos biométricos en los pasaportes de los ciudadanos de la UE. En octubre de 2004, la Comisión de las Libertades, la Justicia y los Asuntos Internos publicó un proyecto de programa contrario a los proyectos de elaboración de una base de datos centralizados de los pasaportes emitidos a escala de la UE en la medida en que con ello se incrementase el riesgo de usos incompatibles.

⁷ Un ejemplo es Eurodac, sistema que tiene por objeto identificar por medio de sus huellas dactilares a las personas refugiadas o supuestamente refugiadas que hayan pedido asilo en alguno de los países de la UE.

en una base de datos. En caso de soporte de almacenamiento individual, sólo es posible una comparación *con* la persona que está en posesión del soporte. Aunque se pueda organizar una base de datos para proceder únicamente a esta clase de comparación, existe la posibilidad de comparar la muestra presentada en el momento de la recogida secundaria con los datos biométricos registrados de otras personas afectadas. Las funciones de la base de datos pueden cambiar de la noche a la mañana con el fin de permitir la comparación de un dato presentado con los datos biométricos de más de una persona. No obstante, la elección de una base de datos para la función de verificación exige una justificación particular.

49. En ciertos casos excepcionales, el cambio ad hoc de función o la interconexión ad hoc de distintas bases de datos biométricos puede resultar necesario y derogar a la finalidad para la que se concibió inicialmente el sistema. En ese supuesto, el artículo 9 de la Convención 108 exige que la ley describa esos casos de forma previa y con precisión. Un procedimiento debe posteriormente describir quién decide la aplicación de esos casos particulares. Podría así mismo prever condiciones adicionales, por ejemplo definir la finalidad precisa de la interconexión y prever una revisión periódica. Ciertas circunstancias especiales pueden justificar la exigencia de una estructura específica que incluyese funciones técnicas que permitiesen cumplir con semejantes exigencias jurídicas excepcionales. De nuevo, la ley debería prever de forma explícita semejante caso. El Comité ha debatido la cuestión de saber si pueden darse casos en los que podría estar justificado exigir que la estructura del sistema incorpore la facilidad técnica que permite recoger más datos biométricos o datos asociados o incluso un patrón más detallado de lo que exige la finalidad del sistema. El Comité ha considerado que no estaba en condiciones de responder a esa pregunta. No obstante, hace hincapié en que si semejante recogida de datos adicionales, incompatible con la finalidad del sistema, es considerada necesaria, debe fundamentarse en una ley específica que cumpla todos los requisitos del artículo 8, apartado 2º, de la Convención europea de Derechos Humanos y de la jurisprudencia del Tribunal europeo de derechos humanos correspondiente, en particular en lo que se refiere a la exigencia de proporcionalidad.

50. Toda base de datos corre el peligro de ser pirateada o que los datos que contiene sean puestos en peligro, sean cuales sean las medidas técnicas, organizativas o reglamentarias que se adopten. Puede suceder que un pirata informático logre engañar la seguridad de un sistema. En el pasado, muchas medidas de seguridad consideradas adecuadas han sido no obstante rodeadas. La encriptación de los datos procesados ayuda a incrementar la seguridad, pero no puede garantizar una seguridad absoluta. El personal que tenga acceso a los datos puede hacer un uso incorrecto de los mismos, sean cuales sean los reglamentos y el control existentes. Por último, la historia ha enseñado que a regímenes que respetan el Estado de derecho pueden suceder otros que no lo respetan.

IV. ¿Cómo se aplican los principios de la Convención 108 a los datos biométricos?

¿En qué momento se aplica la Convención 108 a los datos biométricos?

51. La Convención 108 se aplica al proceso automatizado de los datos de carácter personal (artículo 1º). En la definición del artículo 2º, letra a, de la Convención 108, los datos de carácter personal designan cualquier información relativa a una persona física identificada o identificable. Existen distintos puntos de vista respecto a la cuestión de saber si los datos biométricos constituyen siempre datos de carácter personal. Algunos alegan el hecho de que podría resultar imposible identificar a alguien sobre la base, por ejemplo, de una huella dactilar incompleta. Además, se podría sostener que los datos biométricos en sí mismos no facilitan información alguna sobre la

persona. Otros, en cambio, defienden la idea de que los datos biométricos permiten por su propia naturaleza la identificación de una persona, ya que esos datos pueden ser relacionados de forma única y permanente con una persona. Futuras tecnologías podrían permitir llevar a cabo fácilmente una identificación que podría parecer imposible en la actualidad. El argumento según el cual los datos biométricos no facilitarían ninguna información sobre la persona puede ser rebatido, ya que se trata sólo de un argumento puramente teórico. En efecto, la recogida de datos biométricos sólo puede producirse en ciertas circunstancias relativas, por ejemplo, al lugar y al momento de la recogida. Ahora bien, esas circunstancias suministran siempre ciertos datos sobre la persona afectada que es la fuente de los datos biométricos.

52. El Comité considera que no es preciso decidir si los datos biométricos son datos personales o si sólo lo son en determinadas circunstancias. Opina que tan pronto como se recogen los datos con vistas a un proceso automatizado cabe la posibilidad de que esos datos sean relacionados con una persona identificable. En ese caso, la Convención se aplica.

¿Quién es el responsable de proceso?

53. El responsable de proceso es la persona que decide cuál será la finalidad de los datos, qué categorías de datos se recogerán y qué operaciones se les aplicarán (artículo 2º, letra d). Cuando se aplica la Convención, debe existir una persona responsable de la conformidad con las normas de protección de los datos. Esa persona es considerada como responsable de proceso, incluso en los casos en los que su responsabilidad sólo consiste en evitar cualquier identificación real. En el caso de sistemas biométricos, el responsable de proceso no resulta siempre fácilmente identificable en el primer momento. Tomemos el ejemplo de bases de datos que contengan los datos biométricos de los titulares de pasaportes: cabe la posibilidad de que sólo las autoridades locales que expiden pasaportes tengan acceso a los datos, aun cuando la finalidad, las categorías de datos que se deben almacenar y su uso sean todas determinadas por el legislador. En ese caso, la legislación debería estipular quién tiene que asumir las responsabilidades en cuestión.

54. Múltiples responsables de proceso pueden, como por ejemplo para las bases de datos descentralizadas, asumir las responsabilidades que les confiere la Convención. Puede darse una situación aun más compleja en la que, aunque un responsable de proceso defina el sistema, su finalidad, etc., los datos sólo sean accesibles para la persona afectada ya que están almacenados exclusivamente en una tarjeta con chip en posesión de la misma.

55. A veces, son subcontratistas quienes procesan los datos por cuenta del responsable de proceso, sin que la plena responsabilidad de éste último disminuya por ese motivo. En la Directiva 95/46 de la UE, dichos subcontratistas se definen en el artículo 2º, letra e), como « *subcontratistas* ».

56. En todas esas situaciones complejas, es preciso determinar con claridad quién es el responsable de proceso y lograr que esa información sea transparente para la persona afectada. En efecto, ésta última tiene el derecho de saber sin indagaciones complicadas a quién dirigirse en caso de supuesto incumplimiento de las normas de protección de los datos. No le corresponde a ella indagar, en situaciones complejas, quién acepta o quién – al término de actuaciones judiciales – está obligado a asumir la responsabilidad de ese incumplimiento.

Proceso leal y lícito

57. Los datos de carácter personal deben ser obtenidos y procesados de forma leal y lícita (artículo 5º, letra a). La lealtad es un concepto amplio. Aplicado a los datos biométricos, implica en particular el hecho de comunicar a la persona afectada que es objeto de una recogida de datos, salvo

que esté ya en posesión de esa información. La persona afectada debe conocer con precisión la finalidad de la recogida y la identidad del responsable de proceso.

58. En teoría, la primera recogida de datos biométricos será obligatoria de conformidad con una ley, o voluntaria. La expedición por una autoridad pública de un documento de identidad es un ejemplo de recogida obligatoria. Si existe en un país la obligación de presentar un documento de identidad a un agente del Estado que lo solicita (por ejemplo un pasaporte) y si está previsto que ese documento contenga características biométricas, la persona afectada no tiene la opción de negarse. En el ámbito del derecho privado, se considera a menudo que los datos biométricos se recogen sobre la base del voluntariado. Se supone que la persona afectada puede optar libremente, por ejemplo, por una tarjeta bancaria para realizar reintegros de fondos. El Comité señala que sistemas similares se crearon en el pasado sobre la base de la libre elección para el cliente, si bien a través de una aplicación a importantes grupos de personas y de la aceptación de contratos de adhesión⁸ o de cláusulas estándar negociables han evolucionado hacia una situación en la que *de hecho* las personas afectadas que desean llevar una vida normal no gozan ya de la libertad de elección.

59. La segunda fase del proceso de los datos biométricos se produce cuando el sistema se utiliza, mediante la presentación de una característica biométrica que se compara con los datos registrados con anterioridad. Si ambos concuerdan, la persona es aceptada por el sistema. Muchos sistemas biométricos están concebidos para conservar datos relativos a la utilización del sistema. Se hace referencia a esos datos con los términos « datos virtuales », « datos de tráfico » o « datos asociados ». Por lo general, indican cuándo y en qué lugar una persona ha estado en contacto con el sistema. A efectos del presente informe, el término utilizado será « datos asociados ».

60. Una finalidad legítima del proceso de datos asociados es, por ejemplo, asegurarse del correcto funcionamiento del sistema biométrico. No obstante, tienen por resultado secundario revelar información concreta sobre el comportamiento de una persona. Cada vez que la persona afectada presenta sus características biométricas, deja indicios más o menos precisos de su comportamiento: dónde estaba, cuándo, durante cuánto tiempo, con quién, etc. Según el principio de proceso leal, la persona afectada debe ser informada de cada recogida posterior de datos biométricos, ya sea porque ésta se le presenta de forma evidente y que introduce deliberadamente sus datos biométricos o porque es informada de la recogida por iniciativa del responsable de proceso. En ciertos contextos, podría resultar suficiente facilitar información de carácter general. En otros casos en los que no es obvio que se recojan datos asociados, la « lealtad » impone facilitar información cada vez que se recogen los datos. Los datos asociados no deberían ser utilizados con fines incompatibles con aquellos para los que se hayan recogido.

Definición de la finalidad y elección de una técnica particular

61. Los datos de carácter personal deben ser procesados para unas finalidades determinadas y legítimas (artículo 5º, letra b). Optar por utilizar los datos biométricos implica determinar y explicitar la finalidad de su proceso. El uso de datos biométricos con el fin de controlar el acceso a un país, una zona o locales protegidos puede ser considerado como un uso legítimo de datos biométricos. Otro uso legítimo de datos biométricos podría ser su utilización en pasaportes o visados para impedir el uso de identidades fraudulentas, la obtención de un segundo pasaporte o la emisión de un pasaporte a una persona no autorizada. No existe ninguna lista exhaustiva de las finalidades legítimas.

62. En cuanto se determinan los fines, el sistema técnico no debería permitir la recogida y el proceso de más datos personales de los que exigen los fines, ya sean datos biométricos o datos asociados. Así

⁸ En inglés, « standard contracts ».

pues, es preciso proceder a una distinción clara entre las distintas funciones de verificación y de identificación⁹. Éstas son los instrumentos al servicio de esa finalidad. Son las finalidades del sistema las que determinan la elección de instalación de un sistema de identificación o de verificación. El Comité no puede pronunciarse de forma general en favor de un sistema u otro. Debe limitarse a recordar que si un proceso de verificación es suficiente para los fines de la finalidad elegida, la instalación de un sistema de identificación exige una justificación especial.

Carácter no excesivo

63. Los datos biométricos tienen una característica singular, a saber que contienen con frecuencia más información de la que resulta necesaria para la verificación o la identificación de las personas (artículo 5º, letra c). Cabe la posibilidad de evitar el proceso de los datos sobrantes limitando el almacenamiento y uso de los datos biométricos, durante la fase de registro y la recogida secundaria, a una extracción que cumpla asimismo con la finalidad del sistema. El término técnico utilizado para esa extracción es « patrón ». El patrón debe estar concebido de tal modo que los datos obtenidos sólo revelen la información necesaria para la finalidad del sistema. En particular, debe evitar cualquier vínculo posible con datos de carácter sensible. Se puede citar útilmente un ejemplo: la imagen del iris puede revelar ciertas enfermedades, información que no resulta necesaria para el reconocimiento de una persona. El patrón debe estar concebido de manera que no contenga esa información superflua.

64. Un patrón puede ser comparado con una lista de palabras clave extraídas de un texto que no se conserva. Basta que las palabras clave concuerden con las presentadas tras el proceso posterior del mismo texto. Así, el patrón extraído de la imagen biométrica en el transcurso de la recogida adicional puede ser comparado con el patrón registrado cada vez que se utiliza el sistema. La noción de « datos biométricos » abarca la imagen biométrica y el patrón que se extrae de la misma.

65. Desde el punto de vista de la protección de los datos, la otra ventaja de ese patrón es que la imagen original de la característica biométrica no puede ser reconstruida, de la misma forma que un texto no se puede reconstruir a partir de palabras clave. Si sólo se toma una parte de huella digital y si esa parte no contiene todas las características extraídas, la persona no puede ser identificada por medio del patrón previamente registrado. Será preciso, con el fin de identificar a posibles malhechores, poseer una imagen biométrica completa. Para otros muchos fines, un patrón resulta suficiente.

66. La noción de carácter no excesivo interviene así mismo para la recogida y el almacenamiento de los datos asociados. Sólo se deben almacenar – y no más tiempo del necesario – los datos asociados necesarios para la finalidad de la recogida. Por ese motivo, la finalidad del proceso de los datos asociados debe quedar precisada desde el principio ya que forma parte de la estructura del sistema.

Exactitud y probabilidad

67. Los datos de carácter personal deben ser exactos (artículo 5º, letra d). Una de las características del proceso de los datos biométricos es que encierra un elemento de probabilidad inevitable. En efecto, el resultado del proceso puede ser falso aun cuando todos los datos almacenados sean exactos. Esta paradoja merece una explicación.

⁹ Para una descripción de la distinción entre verificación e identificación, véase el apartado 2º, descripción de los tecnicismos.

68. De vez en cuando y aunque el sistema funcione perfectamente, es inevitable que las dos características de una misma persona no concuerden. Así pues, alguien será rechazado sin motivo alguno. De la misma manera, el sistema podría aceptar el grado de probabilidad entre dos características, aunque pertenezcan a distintas personas. En ese caso, alguien será aceptado sin razón.

69. Se ha dicho que los datos biométricos tienen un carácter único y permanente (véase párrafo 28). No obstante, caben excepciones. Las personas, al envejecer, pueden cambiar de características biométricas. Las enfermedades, los accidentes o la cirugía pueden afectar a las características biométricas en cuestión y causar una disfunción del sistema biométrico respecto a una persona dada. No se puede ya considerar que los datos registrados son exactos a la vista de la finalidad que deben cumplir.

70. Si los datos no alcanzan un grado adecuado de exactitud o de similitud, se debería otorgar un derecho de rectificación a la persona afectada, a petición suya.

Conservación de los datos

71. Los datos de carácter personal no se deben conservar durante un plazo superior al necesario para el fin para el que se han registrado (artículo 5º, letra e). En lo que se refiere a los datos biométricos, esa exigencia parece poco problemática. Mientras el sistema cumple su función, los datos biométricos registrados se conservarán en un soporte de almacenamiento, sea cual sea. El artículo 5º, letra e) menciona en general la posibilidad de conservación de los datos en una forma que permita la identificación de las personas afectadas durante un plazo que no exceda del necesario para los fines para los que se han registrado. Con respecto a los datos biométricos, la opción que consiste en anonimizar los datos no es válida dado que los datos biométricos, por su propia naturaleza, son un instrumento de identificación de las personas, especialmente cuando se procesan automáticamente.

72. Los datos obtenidos en el momento de la recogida secundaria no serán de ninguna utilidad una vez que hayan sido comparados con los datos registrados. En principio, no serán almacenados sino borrados de inmediato. El almacenamiento de los datos presentados para una recogida secundaria sólo se podrá justificar en casos excepcionales, cuando existan motivos válidos para sospechar un fraude de identidad.

73. Más problemático podría resultar el tema de la conservación de los datos asociados (véase párrafo 59), que tienen distintas funciones. Para proteger zonas con nivel de seguridad elevado, por ejemplo una central nuclear, podría parecer legítimo que el sistema pudiese detectar con precisión quién ha penetrado en ciertas zonas, cuándo y durante cuánto tiempo. Esos datos tienen una función primera. Otros sistemas pueden tener otra finalidad, por ejemplo determinar que el poseedor de un documento de identidad es efectivamente el titular legítimo del mismo. Esos datos pueden ser útiles para verificar que el sistema, en su conjunto, funciona correctamente. Se podría imaginar un sistema capaz de detectar si se utilizan datos biométricos idénticos durante un plazo en zonas geográficamente distantes. Si ese fuese el caso, podría tratarse de una duplicación de datos, incluso de un fraude. Semejante finalidad secundaria podría ser considerada compatible con la finalidad primera. El artículo 5º, letra b, de la Convención 108 permite conservar los datos asociados para semejantes finalidades secundarias. En el caso de una utilización primaria y secundaria, el sistema debe poder especificar y explicitar la duración de la conservación de los datos asociados respecto a la finalidad para la que se han registrado. La conservación de datos asociados con fines incompatibles con la finalidad de la recogida queda prohibida. Una derogación sólo es posible si se cumplen los requisitos del artículo 9º de la Convención.

Datos sensibles

74. Los datos biométricos pueden revelar enfermedades o un origen racial. El artículo 6º los clasifica dentro de las « categorías particulares de datos » que exigen garantías adecuadas. En la doctrina de la protección de los datos, se designan con el nombre de datos sensibles. El progreso técnico podría así mismo brindar la posibilidad de extraer de los datos biométricos mucha más información de la que se hubiese podido imaginar. En general, esa nueva información no concuerda con la finalidad para la que se han recogido los datos. El Comité reconoce que en semejantes circunstancias el proceso de datos biométricos implica el proceso inevitable de datos que no son necesarios, situación comparable con la que se presenta cuando un nombre revela el origen étnico. Muchos sistemas biométricos extraen datos de la imagen biométrica de origen, durante el registro y en el momento de la entrada posterior de los datos. Sólo esos datos extraídos son objeto de comparación. La elección de los datos que se han de extraer debe ser realizada de tal modo que se evite la recogida de semejantes datos sensibles porque en general esos datos no permitirán verificar la identidad de la persona afectada o identificarla.

Seguridad de los datos

75. El artículo 7º trata del deber de prever medidas de seguridad adecuadas que protejan los datos de carácter personal. Las normas de calidad del software y del material podrían ser definidas por el sector industrial, en particular las aplicaciones a gran escala y los sistemas que exigen un nivel de seguridad elevado. Las autoridades de protección de los datos deberían velar por que los estándares técnicos abarquen los aspectos necesarios relativos a la aplicación de la Convención. La formación del personal que use el sistema y los equipos es otro factor importante que tener en cuenta. Debería incluir una sensibilización del personal al funcionamiento del sistema.

76. Más tarde, esos estándares y los sistemas que los aplican deberían ser periódicamente objeto de una auditoría y de una evaluación llegado el caso por un organismo independiente, teniendo en cuenta todas las partes del sistema, como el registro, los datos conservados, el proceso de comparación de los datos registrados y de los datos presentados, la encriptación de las distintas fases, el personal destinado a su funcionamiento, etc.

77. Una medida de protección general, aplicable también a los datos biométricos, consiste en utilizar algoritmos fiables para extraer un patrón de una imagen biométrica y comparar los datos registrados con los presentados más tarde. La transparencia de esos algoritmos es actualmente objeto de un debate entre otras cosas con vistas a su interoperabilidad. La utilización de la encriptación se recomienda durante el proceso de registro para evitar que personas no autorizadas puedan acceder a los datos brutos y usarlos para usurpar la identidad del usuario legítimo. La encriptación sofisticada de los datos biométricos durante el proceso de registro, para el almacenamiento y la transmisión por líneas de telecomunicación incrementa la seguridad y hace más difícil el uso no autorizado de los datos biométricos. Quienquiera que interceptase la señal encriptada y no dispusiese de la clave de encriptación no podría reconstruir la señal de respuesta del sistema biométrico.

Transparencia

78. La existencia de un sistema que utiliza los datos biométricos, la finalidad del sistema y la identidad y la residencia del responsable de proceso deben ser comunicadas, previa petición, no sólo a la persona afectada sino también al público en general (artículo 8º, letra a). Pueden plantearse problemas particulares en lo que se refiere a la noción de finalidad. En ciertos casos, un sistema cumplirá otras finalidades, algunas evidentes, otras no. En semejantes circunstancias, sería recomendable que el responsable de proceso tomase la iniciativa de informar a las personas afectadas

y al público del sistema, de las finalidades para las que se usan los datos personales, de la manera en la que se usan y de los riesgos posibles. En otros casos, el principio de transparencia puede respetarse facilitando la información previa petición.

79. Cualquier derogación a la transparencia relativa a las finalidades, sean cuales sean, deberá, de conformidad con el artículo 9º de la Convención 108, ser prevista por la ley y hecha necesaria en una sociedad democrática, en interés por ejemplo de la seguridad pública.

Derecho de acceso

80. Toda persona puede acceder a los datos biométricos que la conciernen (artículo 8º, letra b, Convención 108). Ese derecho se aplica tanto a los datos biométricos como a los datos asociados que revelan, intencionalmente o no, información relativa a la persona afectada. Podría ser beneficioso para una persona afectada verificar los datos biométricos que el sistema asocia a su identidad, porque no está descartado que puedan haber sido deteriorados o falsificados, causando por este motivo falsos rechazos. En ese caso, a petición de la persona afectada, una investigación debe ser llevada a cabo sobre los datos biométricos relacionados con su nombre.

81. La persona afectada puede alegar que los datos biométricos o los patrones no concuerdan o ya no concuerdan con los datos biométricos que introduce cada vez que utiliza el sistema, y que ello causa una tasa de falsos rechazos superior a la media. Puede ser la consecuencia de alteraciones de las características biométricas debidas al envejecimiento, a una intervención quirúrgica o a un accidente de la persona afectada, que han producido un cambio duradero de sus características biométricas. El Comité opina que el derecho de acceso implica la verificación de semejante denuncia. La persona afectada no necesita justificar su petición.

82. La persona afectada tiene el derecho de acceder a sus datos de una « forma inteligible ». Otorgar el derecho de acceso a los datos biométricos supondrá a menudo que esté a disposición una máquina capaz de leer los datos biométricos. Podría así mismo exigir la intervención de un experto para interpretar y verificar los datos. El Comité considera que el responsable de proceso no debería poder rechazar semejantes peticiones con el único motivo de que no se dispone de máquina o de experto.

83. El Comité ha examinado la posibilidad de que se recurra de forma abusiva al derecho de acceso. En cierta medida, el artículo 8º, letra b, de la Convención 108 trata de ese tema. Las peticiones de acceso excesivamente frecuentes pueden ser rechazadas, porque sólo se deben aceptar las peticiones realizadas « a intervalos razonables ». Se pueden imaginar así mismo otras formas de peticiones abusivas. El Comité considera que los principios generales del derecho, que no se limitan al campo de la protección de los datos, se aplican a la doctrina del abuso de derechos y de solicitud de indemnizaciones.

84. En ciertos casos, si tiene razones válidas para sospechar una usurpación de identidad, el responsable de proceso debería hacer cuanto esté a su alcance para llevar a cabo indagaciones sobre el caso específico.

85. En la práctica, esa investigación sólo puede naturalmente llegar a un resultado si el responsable de proceso tiene él mismo acceso a esos datos. Cabe la posibilidad de que ése no sea el caso (véase el capítulo III relativo al almacenamiento de los datos en un soporte de almacenamiento individual). No obstante, la persona afectada puede sin embargo presentar una solicitud de verificación, si tiene motivos para creer que alguien usurpa sus datos biométricos en el sistema. El Comité considera entonces que el responsable de proceso tiene la obligación de tomar las medidas

necesarias para garantizar la exactitud de los datos. Una pista posible al efecto podría ser el uso de los datos asociados para detectar un posible fraude.

Derecho de rectificación y de cancelación

86. Los datos biométricos o los datos asociados pueden resultar inexactos. En ese caso, la persona afectada puede solicitar su rectificación o su cancelación (artículo 8º, letra c).

87. La exactitud de los datos debe ser juzgada en relación con las finalidades para las que se han recogido. Cuando los datos se utilizan exclusivamente para permitir el acceso a un edificio, sin almacenamiento posterior de los datos asociados ligados a las personas, el responsable de proceso podría legítimamente aceptar un grado más alto de probabilidad de falsa aceptación o de falso rechazo, por ejemplo para evitar que el sistema se vuelva excesivamente costoso.

88. El grado de probabilidad desempeña un papel tanto en la fase de registro como en la de la utilización subsiguiente del sistema. Durante la fase de registro, el algoritmo que sirve para extraer el patrón de la característica biométrica puede ser más o menos extenso según la finalidad del sistema. Un algoritmo menos extenso va a incrementar la probabilidad de falsas aceptaciones o de falsos rechazos, ya que el patrón será menos específico. En el transcurso de usos posteriores, el sistema puede ser ajustado mediante una comparación más o menos ampliada entre la imagen o el patrón registrado y el dato biométrico presentado. El Comité opina que es en primer término el responsable de proceso quien decide el grado de probabilidad que debe aceptar el sistema, teniendo en cuenta las finalidades del mismo. La persona afectada no puede exigir una certeza absoluta – dado que lo absoluto es irrealizable – sino acercar esa certeza tanto como lo haga posible la técnica.

89. El carácter por esencia probabilista de la utilización y de la correspondencia de los datos biométricos tiene a veces como consecuencia inevitable que se relacionen los datos asociados con una persona que no sea la afectada. Si ése es el caso, la interpretación de esos datos para las necesidades de una persona debe tener en cuenta ese hecho. Dado que la correspondencia (la aceptación) o la no correspondencia (el rechazo) no están nunca garantizadas al cien por cien, lo mismo sucede con los datos asociados relacionados con una persona específica. El grado de probabilidad sigue siendo el mismo.

90. Esto plantea problemas particulares en un sistema en el que los datos se usen para controlar sistemáticamente el comportamiento de una persona, lo que podría estar justificado por ejemplo en una zona muy protegida en la que fuese preciso saber quién estaba allí, cuándo y durante cuánto tiempo. El sistema debe pues ofrecer un grado de precisión más alto. En lo que se refiere a los datos biométricos, resulta de lo que antecede que la probabilidad de una falsa aceptación o de un falso rechazo es bastante escasa.

91. La exactitud del « reconocimiento » de la persona afectada tampoco es algo que deba darse por sentado. La persona afectada no debe esperar que el reconocimiento sea rigurosamente exacto. Se podría añadir en corolario que el hecho de detectar datos asociados inexactos no significa que el responsable de proceso haya actuado de forma ilegal, lo que implicaría un derecho de indemnización.

92. Ligado al derecho de rectificación está el derecho de cancelación, que se produce si los datos biométricos se almacenan contrariamente a la ley.

93. En lo que se refiere a los datos biométricos, es posible que se dé un conflicto entre el responsable de proceso y la persona afectada respecto al grado aceptable de probabilidad de falsos

rechazos. Si la persona afectada pide un nuevo registro cuando el responsable de proceso no admite que los datos sean inexactos, el derecho de rectificación podría ser interpretado en el sentido de dar derecho en principio a un nuevo registro por la persona afectada sin costes excesivos. Lo mismo sucede si los datos registrados son correctos pero la característica biométrica ha sido modificada con la edad, un accidente o la cirugía. Con el correr de los años, los datos se han vuelto gradualmente incorrectos.

Recurso efectivo

94. Todo el mundo tiene derecho a un recurso efectivo cuando el derecho de transparencia, de acceso, de rectificación o de cancelación no se respeta (artículo 8º, letra d, de la Convención 108). En lo que se refiere a los datos biométricos, se podría imaginar una definición más completa de ese derecho. Se ha dicho varias veces que la naturaleza probabilista del uso de los datos biométricos es la causa de problemas específicos ligados a la protección de los datos. La elección de utilizar un sistema biométrico es un riesgo asumido por el responsable de proceso. No le corresponde a la persona afectada sufrir los posibles inconvenientes de semejantes sistemas. En función de las circunstancias, la persona afectada debería tener la posibilidad de ver su situación rectificada de inmediato o tener acceso a un recurso lo antes posible.

95. Una persona puede no ser « reconocida » por un sistema biométrico. Las causas pueden ser diversas, por ejemplo:

- (a) La persona no es la misma que aquella cuyos datos biométricos están registrados. El resultado es exacto. Los datos no concuerdan y el sistema rechaza a la persona afectada.
- (b) El sistema contiene datos biométricos falsos. Los datos deben ser rectificadas.
- (c) Los datos son exactos pero la recogida secundaria no funciona correctamente y la puesta en concordancia de los datos biométricos no llega a resultado alguno. La máquina debe ser ajustada.
- (d) El sistema funciona perfectamente y los datos son exactos. No obstante, el sistema no detecta correspondencia alguna a causa de la naturaleza probabilista de la operación de puesta en concordancia.

96. Se podría pensar en otros muchos casos. La comparación de los datos presentados con los datos registrados puede resultar correcta sin motivo alguno. La correspondencia hace que la persona afectada aparezca incluida en una lista de personas no autorizadas, cuando ése no es el caso.

97. En todas esas situaciones, una persona debe poder solicitar un nuevo examen. En el caso (a), el rechazo será confirmado. En todos los demás casos, el resultado automatizado debe ser corregido. En última instancia, la persona afectada debería poder dirigirse a un ser humano quien, en nombre del responsable de proceso, decide si la persona afectada debe ser rechazada o aceptada¹⁰. El procedimiento de ese recurso no debe ser excesivamente apremiante para la persona afectada. El derecho de recurso debe así mismo aplicarse a las personas que no pueden utilizar el sistema a causa de una discapacidad física. Una persona que no tenga manos no puede ser aceptada por un sistema que funcione con un lector de huellas dactilares. El responsable de proceso debe velar por que esas personas dispongan de otra solución sin poner en peligro el nivel de seguridad previsto.

98. En el supuesto de que la persona afectada y el responsable de proceso tengan una discrepancia duradera, podrán dirigirse a la autoridad de control de conformidad con el Protocolo adicional de la Convención 108.

¹⁰ Véase el artículo 15º de la directiva 95/46 de la UE relativa a la protección de los datos personales.

Pertinencia del artículo 9º de la Convención respecto a los sistemas biométricos

99. El artículo 9º, apartado 2º de la Convención prevé derogaciones a los principios mencionados más arriba, dentro de ciertos límites. Ese apartado se inspira en el artículo 8º, apartado 2º de la Convención Europea de Derechos Humanos (CEDH).

100. La recogida de datos de carácter personal, ya sean biométricos o asociados, y su proceso posterior pueden atentar contra la vida privada. Semejante interferencia queda prohibida por el artículo 8º, apartado 1º, de la CEDH, salvo que esté justificada de conformidad con el artículo 8º, apartado 2º. Si se procesan datos biométricos, los principios de la Convención 108 se aplicarán, esté o no en juego la vida privada. Esas operaciones sólo son posibles si los criterios y los procedimientos conformes con el apartado 2º se aplican. Una derogación a los principios de la Convención 108 sólo es posible si se aplican los criterios del artículo 9º, letra 2. Esos criterios son similares a los del artículo 8º, letra 2, de la CEDH.

101. En el fallo *Rotaru c. Rumania* de mayo de 2000, el Tribunal europeo de Derechos Humanos considera que la recogida secreta de datos de carácter personal por motivos de seguridad de Estado podían interferir con la vida privada. El Tribunal aplicó así los criterios del artículo 8º, letra 2 de la CEDH. En su fallo, el Tribunal considera que las categorías de personas a las que se aplican esos atentados contra la vida privada y la naturaleza de los datos que se pueden consignar deben ser previamente definidas de manera precisa y previsible de acuerdo con los criterios jurídicos. La derogación al derecho general a la protección de la vida privada se hace pues visible. Se ha admitido a veces que no se había producido ninguna interferencia con la vida privada de la persona afectada en la medida en que ésta última no lo advertía. El fallo *Rotaru c. Rumania* pone claramente de manifiesto el carácter no válido de ese argumento.

102. El fallo *Rotaru c. Rumania* con respecto al artículo 8º, letra 2 de la CEDH podría tener implicaciones en la interpretación del artículo 9º, letra 2 de la Convención 108. El proceso de los datos biométricos y las distintas categorías de datos de carácter personal asociados, la finalidad de su recogida y la identidad del responsable de proceso deberían en principio ser informaciones transparentes para la persona afectada. Nuevas tecnologías tales como el reconocimiento facial que permiten la búsqueda inmediata de malhechores buscados constituirían una forma de proceso sin almacenamiento de los datos de todas las personas identificadas que sólo duraría los escasos segundos necesarios para llevar a cabo la verificación. No obstante, esa forma de proceso estaría cubierta por la Convención 108. En efecto, el proceso secreto de esos datos sería contrario al principio de proceso leal de los datos y sólo debería pues ser autorizado si se respetasen los criterios del artículo 9º.

103. Tomemos un ejemplo para ilustrar este punto de vista. A pesar de los intentos hasta ahora infructuosos, no cabe descartar que en un futuro próximo la técnica permita identificar a las personas que van por la calle comparando su cara con una lista de personas buscadas. En efecto, dentro de poco será posible extraer informaciones digitalizadas a partir de imágenes, con el fin de compararlas con bases de datos. El registro podría consistir en sacar fotos de un criminal tras su detención. Éstas podrían ser comparadas con las imágenes producidas por la vídeovigilancia de los ciudadanos que van por la calle. En la práctica, esa vídeovigilancia se podría llevar a cabo de forma secreta. Ahora bien, dado que eso constituye un proceso desleal, sólo debería estar permitido si se respetasen los criterios del artículo 9º de la Convención, lo que haría necesaria la adopción de una ley que describiese con precisión las excepciones admitidas a la norma general del proceso leal.

104. Algunos hacen hincapié en un uso secundario de datos asociados procedentes de sistemas que utilizan datos biométricos cuya compatibilidad con la finalidad para la que se han recogido sería

discutible. Por ejemplo, podría resultar interesante para los servicios de información conservar esos datos con el fin de vigilar a personas a las que creen capaces de cometer actos terroristas. En muchas ocasiones, esa conservación será incompatible con la finalidad de origen de recogida de esos datos. El artículo 9º de la Convención 108 ofrece la posibilidad de semejante conservación en una sociedad democrática por motivos de seguridad pública. Si es preciso, se pueden prever derogaciones al criterio de compatibilidad en una ley que defina la manera en la que esos datos se pueden utilizar para esa nueva finalidad.

105. El artículo 8º, letra 2 de la CEDH y el artículo 9º de la Convención 108 son excepciones que justifican una interferencia con los principios enunciados en esas dos convenciones. Una interferencia limitada en la vida privada o una derogación limitada a las normas de la Convención 108 no constituiría excepción alguna a esos principios. Una vigilancia secreta general del público, incluso prevista por la ley, no sería ni conforme con las disposiciones de la Convención europea de derechos humanos ni con las de la Convención 108.

V. Conclusiones del informe de situación

106. El Comité ha mantenido intercambios preliminares sobre ciertas cuestiones planteadas por la biometría en su relación con los principios de la protección de los datos, tal como se enuncian en la Convención 108. Muchas cuestiones siguen estando abiertas. A pesar de los avances tecnológicos considerables que se han producido desde la redacción de la Convención, el Comité ha considerado que sus principios siguen siendo pertinentes y se pueden aplicar a los sistemas que utilizan la biometría. El presente informe traduce la pertinencia de los principios jurídicos con respecto a esas nuevas técnicas. Pretende contribuir al debate sobre la relación que existe entre los derechos humanos y la biometría a escala nacional e internacional. El Comité tiene intención de actualizar el presente informe o publicar otros informes si así lo exigen hechos nuevos, o incluso redactar nuevos instrumentos jurídicos.

107. A estas alturas, el Comité destaca sobre todo los puntos siguientes:

1. Los datos biométricos deben ser considerados como una categoría específica de datos en la medida en que proceden del cuerpo humano, siguen siendo los mismos en distintos sistemas y son inalterables de por vida. No obstante, pueden alterarse por ejemplo debido al envejecimiento o a una intervención quirúrgica.
2. Antes de recurrir a la biometría, el responsable de proceso debería evaluar por una parte las ventajas e inconvenientes posibles para la vida privada de la persona afectada y, por otra parte, las finalidades previstas, así como tener en cuenta posibles soluciones alternativas que supongan un menor atentado contra la vida privada.
3. No se debería optar por la biometría únicamente por el hecho de que su uso resulte práctico. En efecto, la utilización de la biometría puede atentar contra la dignidad humana. Es preciso tener en cuenta los aspectos socioculturales y las posibles reticencias con respecto al uso instrumental de cuerpo humano.
4. Los datos biométricos y todos los datos asociados generados por el sistema deben ser utilizados con fines determinados, explícitos y legítimos, y no deber ser procesados posteriormente de manera incompatible con esas finalidades.
5. Los datos deberían ser adecuados, pertinentes y no excesivos en comparación con la finalidad del proceso. Un sistema de proceso de datos debería estar configurado de

forma que excluyese la recogida y el proceso de más datos biométricos o asociados de los que exija su finalidad. Si basta con patrones, se debería evitar la recogida o el almacenamiento de la imagen biométrica.

6. A la hora de elegir la estructura del sistema, el responsable de proceso debería sopesar por una parte las ventajas y los inconvenientes para la vida privada de la persona afectada y, por otra parte, las finalidades previstas. Se debería proceder a una elección motivada entre el almacenamiento únicamente en un soporte de almacenamiento individual, en una base de datos descentralizada o en una base de datos centralizada, teniendo a la vez en mente los aspectos de seguridad.
7. La estructura de un sistema biométrico no debería ser desproporcionada respecto a la finalidad del proceso. Así pues, si basta con la verificación, el responsable de proceso no debería desarrollar una solución de identificación. Los datos biométricos que se utilizan únicamente con fines de verificación deberían ser almacenados preferentemente en un soporte de almacenamiento individual con medidas de seguridad, por ejemplo una tarjeta con chip, que sólo poseería la persona afectada.
8. La persona afectada debería ser informada de la finalidad del sistema y de la identidad del responsable de proceso, así como de los datos procesados y de las categorías de personas a las que se comunicarán esos datos, en la medida en que esa información es necesaria para garantizar la lealtad del proceso.
9. La persona afectada tiene un derecho de acceso, de rectificación, de bloqueo y de cancelación de sus datos. Esos derechos se extienden a los datos biométricos que son objeto de un proceso automatizado y nominativo, a los posibles datos asociados (tales como la fecha y localización de la utilización del sistema), y a las personas a las que hayan sido comunicados.
10. El responsable de proceso debe prever medidas técnicas y organizativas adecuadas con el fin de proteger los datos biométricos y los demás datos de carácter personal asociados a los mismos contra la destrucción – accidental o ilícita – y la pérdida accidental, así como contra el acceso, la modificación, la comunicación no autorizado o cualquier otra forma de proceso ilícita.
11. Se debería desarrollar un procedimiento de certificación y de control, en particular en el caso de las aplicaciones de masa, con el fin de establecer normas de calidad para el software y el material, así como para la formación del personal responsable del registro y de la verificación. Se recomienda una auditoría periódica que pruebe las cualidades técnicas del sistema.
12. Si una persona afectada registrada en un sistema biométrico es rechazada, el responsable de proceso debería, a petición de ésta, volver a examinar el caso y si fuese preciso ofrecerle soluciones de sustitución adecuadas. Se deberían establecer procedimientos para informar a la persona afectada en el momento de un supuesto no reconocimiento por el sistema.