DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de información de visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (COM (2004)835 final)

(2005/C 181/06)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado constitutivo de la Comunidad Europea, y en particular su artículo 286,

Vista la Carta de los Derechos Fundamentales de la Unión Europea, y en particular su artículo 8,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,

Visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, y en particular su artículo 41,

Vista la solicitud de dictamen de conformidad con lo dispuesto en el artículo 28, apartado 2 del Reglamento (CE) nº 45/2001, presentada por la Comisión y recibida el 25 de enero de 2005,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1. **INTRODUCCIÓN**

1.1. **Observaciones introductorias**

La creación del Sistema de Información de Visados (VIS) constituye una parte importante de la política común de visados de la UE y ha sido objeto de diversos instrumentos interrelacionados.

— En abril de 2003, se presentó un estudio de viabilidad ([1]) del VIS encargado por la Comisión.

— En septiembre de 2003, la Comisión propuso una modificación ([2]) del anterior Reglamento por el que se establece un modelo uniforme de visado. El principal objetivo era introducir en el nuevo modelo de visado una serie de datos biométricos (imagen facial y dos impresiones dactilares) que irían almacenados en un microchip.

([1]) Sistema de Información de Visados, informe final, encargado por la CE a Trasys, abril de 2003.
([2]) COM(2003)558 final que contiene 2003/0217 (CNS) y 2003/0218 (CNS).

— En junio de 2004, una Decisión del Consejo ([1]) dio inicio a la creación del Sistema de Información de Visados con la constitución del fundamento jurídico que permite su inclusión en el presupuesto de la UE. Esta Decisión propone una base de datos central con información sobre las solicitudes de visado y prevé un procedimiento de comitología para gestionar el desarrollo técnico del VIS.

En diciembre de 2004, la Comisión adoptó la propuesta de Reglamento sobre el VIS y el intercambio de datos sobre visados de corta duración entre los Estados miembros ([2]) (en adelante, «la propuesta») que constituye el objeto de este dictamen. Acompaña a la propuesta un estudio relativo a la evaluación de impacto ampliada ([3]) (en adelante, «EIA»).

No obstante, tal y como se explica en la exposición de motivos, para completar este Reglamento serán necesarios otros instrumentos jurídicos, especialmente para:

— modificar la Instrucción Consular Común dirigida a las Misiones Diplomáticas y Oficinas Consulares de carrera de las Partes Contratantes del Convenio de Schengen (en adelante, «Instrucción Consular Común») en lo que respecta a la inclusión de datos biométricos en el procedimiento;

— desarrollar un nuevo mecanismo de intercambio de datos con Irlanda y el Reino Unido;

— intercambiar datos sobre visados de larga duración.

Según se decidió en el Consejo de Justicia y Asuntos de Interior de los días 5 y 6 de junio de 2003 y como se explica en el artículo 1, apartado 2 de la Decisión del Consejo de junio de 2004 antes mencionada, el VIS se basará en una arquitectura centralizada y consistirá en una base de datos central donde se almacenarán los archivos de las solicitudes de visado, esto es, el Sistema Central de Información de Visados (CS-VIS), y en una Interfaz Nacional (NI-VIS) en cada Estado miembro. Los Estados miembros designarán ([4]) una autoridad nacional central que estará conectada a la Interfaz Nacional, a través de la cual podrán acceder al CS-VIS las respectivas autoridades competentes.

1.2. **Principales elementos de la propuesta desde el punto de vista de la protección de datos**

El objetivo de la propuesta es mejorar la gestión de la política común de visados al facilitar el intercambio de datos entre los Estados miembros gracias a la creación de una base de datos central. El Reglamento prevé la introducción de datos biométricos (fotografía e impresiones dactilares) durante el procedimiento de solicitud y su almacenamiento en la base de datos central.

También podrían utilizarse datos biométricos en la etiqueta adhesiva del visado, como ya se ha previsto en un reglamento de modificación propuesto por la Comisión sobre el modelo uniforme de visado, mediante la incorporación de la fotografía y las impresiones dactilares almacenadas en un microchip (se está a la espera de una decisión del Consejo basada en los resultados de los estudios que se están llevando a cabo).

La propuesta describe detalladamente las distintas operaciones a que serán sometidos los datos (introducción, modificación, supresión y consulta) y los diversos datos que se añadirán al VIS en función de la situación del expediente de solicitud (aceptación, denegación, etc.).

La propuesta prevé que los datos correspondientes a cada solicitud se conserven durante cinco años.

En la propuesta se enumeran de forma restrictiva las autoridades competentes distintas de las autoridades responsables de los visados que tendrán acceso al VIS, especificando el tipo de datos que tendrán derecho a consultar:

— las autoridades responsables de los controles de los visados en las fronteras exteriores y en el territorio de los Estados miembros

— las autoridades responsables de inmigración

([1]) 2004/512/CE, DO L 213 de 15.6.2004, p. 5.
([2]) COM(2004)835 que contiene 2004/0287 (COD)
([3]) Estudio para la evaluación de impacto ampliada del Sistema de Información de Visados; informe final del EPEC (Consorcio para la Evaluación de Políticas Europeas), diciembre de 2004.
([4]) Artículo 24, apartado 2 de la propuesta.

— las autoridades competentes en materia de asilo.

En las disposiciones sobre el funcionamiento del VIS y las responsabilidades inherentes, la propuesta destaca que la Comisión trata los datos del VIS en nombre de los Estados miembros. Se expone la necesidad de llevar unos registros del tratamiento de datos para garantizar la seguridad de los mismos y se especifican las respectivas responsabilidades a la hora de garantizar el nivel de seguridad.

La propuesta incluye un capítulo sobre la protección de datos en el que se exponen en detalle las funciones de las autoridades nacionales y del Supervisor Europeo de Protección de Datos (en adelante, «SEPD»).

La aplicación técnica del VIS y la selección de las tecnologías necesarias se encomienda al comité creado en virtud del artículo 5, apartado 1 del Reglamento (CE) nº 2424/2001 sobre el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II).

La propuesta va acompañada de una evaluación de impacto ampliada del VIS elaborada por el EPEC a instancias de la Comisión. La evaluación llega a la conclusión de que la opción de un VIS basado en la utilización de indicadores biométricos constituye la mejor solución posible para mejorar la política común de visados.

2. **CONTEXTO**

La propuesta tendrá importantes repercusiones sobre el derecho a la intimidad y otros derechos fundamentales de las personas, por lo que procederemos a cotejarla con los principios en materia de protección de datos. Los principales puntos de referencia de nuestro examen son los siguientes:

— El respeto de la intimidad está garantizado en Europa desde que en 1950 se adoptara el Convenio para la protección de los derechos humanos y de las libertades fundamentales (en adelante, «CEDH»). El artículo 8 del CEDH establece el «derecho al respeto de la vida privada y familiar».

  De conformidad con el apartado 2 de dicho artículo, toda injerencia de la autoridad pública en el ejercicio de este derecho sólo se permitirá cuando «esté prevista por la ley» y sea necesaria «en una sociedad democrática» para proteger intereses importantes. En la jurisprudencia del Tribunal Europeo de Derechos Humanos, estas condiciones han llevado a la adopción de otros requisitos relacionados con la índole del fundamento jurídico que permite la injerencia, la proporcionalidad de las medidas y la necesidad de garantías adecuadas frente a los abusos.

  Los principios básicos para la protección de las personas con respecto al tratamiento de datos de carácter personal se establecen en el Convenio sobre la protección de datos del Consejo de Europa que se adoptó en 1981.

— Más recientemente, el derecho al respeto de la vida privada y el derecho a la protección de los datos de carácter personal han quedado establecidos por la Carta de los Derechos Fundamentales de la Unión Europea, que ha sido incorporada a la Parte II de la nueva Constitución para Europa.

  En el artículo 52 de la Carta se prevé que estos derechos pueden ser objeto de limitaciones, siempre y cuando se den unas condiciones similares a las establecidas en el artículo 8 del CEDH. Estas condiciones se han de tener presentes en el momento de evaluar cualquier propuesta con vistas a una posible injerencia.

En lo que se refiere a la UE, las normas básicas en materia de protección de datos están recogidas actualmente en los siguientes actos:

— La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31). Esta Directiva, a la que nos referiremos como «Directiva 95/46/CE», contiene los principios detallados que sirven de referencia a la hora de analizar la propuesta en la medida en que ésta vaya a aplicarse a los Estados miembros. Este aspecto es tanto más importante cuanto que la propuesta se aplicará junto con la legislación nacional que da cumplimiento a la Directiva. Por consiguiente, la eficacia de esta combinación será la que determine la eficacia de las disposiciones y garantías previstas en la propuesta en cada caso concreto.

— El Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8, p. 1). Este Reglamento, al que nos referiremos como «Reglamento (CE) nº 45/2001», contiene principios similares a los de la Directiva 95/46/CE y es pertinente en este contexto en la medida en que la propuesta se aplicará, junto con las disposiciones del Reglamento, a las actividades de la Comisión. Esta combinación también merece pues cierta atención.

La Directiva 95/46/CE y el Reglamento (CE) nº 45/2001 han de leerse conjuntamente con otros instrumentos. Dicho de otro modo, en la medida en que sus disposiciones regulan el tratamiento de datos de carácter personal, que podría conculcar libertades fundamentales, en particular el derecho a la intimidad, la Directiva y el Reglamento han de interpretarse a la luz de los derechos fundamentales. Así también se desprende de la jurisprudencia del Tribunal de Justicia Europeo ([1])

— Por último, el SEPD también desea remitirse en su análisis al Dictamen nº 7/2004, de 11 de agosto de 2004, del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales ([2]), «sobre la inclusión de elementos biométricos en los permisos de residencia y visados teniendo en cuenta la creación del Sistema de Información de Visados (VIS)». En dicho dictamen, el Grupo manifestaba su inquietud ante algunos elementos de la propuesta. El SEPD se propone comprobar si en la propuesta se ha tenido en cuenta esta inquietud y de qué modo.

3. **ANÁLISIS DE LA PROPUESTA**

3.1. **Generalidades**

El SEPD reconoce que para profundizar en una política común de visados es necesario un intercambio eficaz de los datos pertinentes, y el VIS es uno de los mecanismos que puede garantizar la fluidez de la circulación de la información. No obstante, este nuevo instrumento debería limitarse a la recogida e intercambio de datos, en la medida en que estas operaciones sean necesarias para el desarrollo de un política común de visados y sean proporcionados al objetivo perseguido.

La creación del VIS puede repercutir positivamente en otros intereses públicos legítimos, pero esto no afecta al hecho de que la finalidad del VIS es otra. El objetivo limitado del sistema cobra suma importancia a la hora de determinar el contenido y la utilización legítimos del mismo y, por tanto, también a la hora de permitir el acceso al VIS (o a parte de sus datos) a las autoridades de los Estados miembros, por razones legítimas de interés público.

La propuesta incluye además el uso de datos biométricos en el VIS. El SEPD reconoce las ventajas de utilizar datos biométricos, pero desea destacar la importantísima repercusión del uso de este tipo de datos, por lo que sugiere que se incluyan garantías estrictas sobre su utilización.

El presente dictamen ha de leerse teniendo presentes estos importantes factores. Señalemos también la conveniencia de incluir en el preámbulo del Reglamento, antes de los considerandos, una referencia al presente dictamen («Visto el dictamen…»).

([1]) En este contexto, conviene referirse a la sentencia del Tribunal de Justicia en el caso Österreichischer Rundfunk y otros (asuntos acumulados C-465/00, C-138/01 y C-139/01, Sentencia de 20 de mayo de 2003, en Pleno (2003) ECR I-489). El Tribunal se ocupó del caso de una ley austriaca que establece la obligación de comunicar las retribuciones de empleados del sector público al Tribunal de Cuentas austriaco y su posterior publicación. En su sentencia, el Tribunal determina una serie de criterios, extraídos del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos, que deberían utilizarse al aplicar la Directiva 95/46/CE, por cuanto dicha Directiva prevé ciertas limitaciones al derecho al respeto de la intimidad.

([2]) Se trata de un grupo independiente de carácter consultivo, que está formado por representantes de las autoridades de protección de datos de los Estados miembros, el SEPD y la Comisión y fue creado por la Directiva 95/46/CE.

3.2. **Finalidad**

La finalidad del VIS reviste una importancia crucial, tanto a la luz del artículo 8 del CEDH como del marco general relativo a la protección de los datos. En el artículo 6 de la Directiva 95/46/CE se dispone que es preciso que los datos personales sean «recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines». Únicamente una definición clara de estos fines permitirá evaluar correctamente la proporcionalidad y adecuación del tratamiento de los datos personales, evaluación cuya importancia es fundamental debido a la naturaleza misma de los datos (incluidos los biométricos) y la magnitud de la operación de tratamiento prevista.

La finalidad del VIS se hace constar claramente en el apartado 2 del artículo 1 del de la propuesta:

> «El VIS mejorará la gestión de la política común de visados, la cooperación consular y las consultas entre las autoridades consulares centrales al facilitar el intercambio de datos entre los Estados miembros sobre las solicitudes y las decisiones relativas a las mismas».

Por consiguiente, todos los elementos del VIS han de ser instrumentos necesarios y proporcionados para alcanzar este objetivo en interés de la política común de visados.

En el artículo 1, apartado 2 de la propuesta se enumeran asimismo otros beneficios que se obtendrán con la mejora de la política de visados, como son:

a) prevenir las amenazas a la seguridad interior;

b) contribuir a la lucha contra el fraude;

c) facilitar los controles en los puntos de control de las fronteras exteriores.

El SEPD considera estos elementos como ejemplos de las consecuencias positivas de establecer el VIS y de mejorar la política común de visados, pero no como objetivos autónomos *per se*.

Esto, en esta fase, acarrea dos consecuencias:

— El SEPD es consciente de que los servicios policiales están interesados en que se les dé acceso al VIS; el 7 de marzo de 2005 se adoptaron conclusiones del Consejo al respecto. Debe observarse que, dado que el objetivo del VIS es mejorar la política común de visados, el acceso sistemático de los servicios policiales no es conforme con este objetivo. Aun cuando, a tenor del artículo 13 de la Directiva 95/46/CE, podría concederse ese acceso *ad hoc*, en determinadas circunstancias y con las garantías que procedan, no podrá otorgarse un acceso sistemático.

  Más en general, es capital una valoración de la proporcionalidad y la necesidad en caso de que en el futuro se tomen decisiones sobre la posibilidad de permitir a otras autoridades el acceso al VIS. Las actividades para las que se conceda dicho acceso deberán ser coherentes con los objetivos del VIS.

— Es poco feliz la referencia expresa a «prevenir las amenazas a la seguridad interior de los Estados miembros» en la letra a). El beneficio principal del VIS será la prevención del fraude y de la «prospección» de visados (la lucha contra el fraude es además la principal razón de la inclusión de la biometría en el sistema) ([1]). La prevención de amenazas contra la seguridad deberá considerarse, pues, como un beneficio «secundario», aunque muy deseable.

  El SEPD recomienda que esta distinción entre «objetivo» y «beneficios» quede más explícita en el artículo 1, apartado 2, por ejemplo, como sigue:

  «EL VIS tiene el objetivo de mejorar la gestión de la política común de visados, la cooperación consular y las consultas entre las autoridades consulares centrales al facilitar el intercambio de datos entre los Estados miembros sobre las solicitudes y las decisiones relativas a las mismas. Al hacerlo así contribuirá también …»

([1]) La evaluación de impacto ampliada lo expone muy claramente (p. 6, punto 2.7).: «*la falta de eficacia de la lucha contra la búsqueda del servicio de visados menos exigente y de la realización de los controles es causa también de falta de eficacia en lo que respecta a la seguridad interna de los Estados miembros*». Esto supone que las amenazas a la seguridad se deben en parte a una política de visados ineficaz. Lo primero que hay que hacer en este sentido es mejorar la política de visados, sobre todo combatiendo el fraude y mejorando los controles. De la mejora de la política de visados resultará una mejora de la seguridad.

Merece señalarse a este respecto que las «Líneas directrices para la instauración de un sistema común de intercambio de datos de visados» adoptadas por el Consejo JAI de 13 de junio de 2002 [1] ponían la prevención de las amenazas a la seguridad interior al final de la lista de objetivos. Sería posible hacerlo también así en el presente texto, lo que resultaría mucho más coherente con el objetivo del VIS.

3.3. **Calidad de los datos**

De acuerdo con el artículo 6 de la Directiva 95/46/EC, los datos personales deberán ser también «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente». Esto se refiere no sólo a la proporcionalidad del propio VIS, sino también a la de los datos recopilados y almacenados en la VIS y a su uso posterior, así como a las garantías adicionales que se apliquen en ese contexto. Estos elementos son también esenciales para la evaluación de la propuesta a la luz del artículo 8 del CEDH.

La creación del VIS representa sin duda una importante injerencia en el ejercicio del derecho a la intimidad, aunque sólo fuera por su magnitud y por las categorías de datos personales procesados. Por eso el Grupo del Artículo 29, en su Dictamen nº 7/2004, preguntó «qué estudios de la magnitud e importancia de esos fenómenos sustanciaban razones apremiantes de seguridad pública o de orden público que justificasen ese enfoque.»

EL SEPD ha tomado cuidadosa nota de los elementos de prueba presentados en la evaluación de impacto ampliada. Aunque estos elementos no son del todo concluyentes, hay al parecer suficientes razones para justificar la creación del VIS a efectos de mejorar la política común de visados.

En ese contexto, parece caer dentro del ámbito de apreciación del legislador decidir sobre la creación del VIS como instrumento de mejora de las condiciones de expedición de visados por los Estados miembros. En sí mismo, este sistema podría integrarse y apuntalar el establecimiento gradual de un espacio de libertad, seguridad y justicia, tal y como prevé el Tratado CE.

Con todo, la creación y la utilización del VIS nunca podrán dar lugar a que no pueda garantizarse en este sector un alto nivel de protección de los datos personales. Incumbe a la función asesora del SEPD estudiar hasta qué punto el VIS afectará al nivel actual de protección de las personas cuyos datos se someten a tratamiento.

Así las cosas, el SEPD centrará su dictamen en los puntos siguientes:

— proporcionalidad y adecuación de los datos y de su uso (por ejemplo, categorías de datos, acceso a los datos por parte de cada una de las autoridades interesadas y plazo de conservación)

— funcionamiento del sistema (por ejemplo, responsabilidades y seguridad)

— derechos de las personas a que se refieren los datos (por ejemplo, información, posibilidad de corregir o eliminar datos inexactos o irrelevantes)

— control y supervisión del sistema.

Aparte de los apartados que siguen, la propuesta no da lugar a observaciones importantes respecto a las categorías de los datos que se habrán de incluir en el VIS y su uso. Las disposiciones al respecto se han redactado con la debida atención y el conjunto parece coherente y adecuado.

---

[1] «Decisión marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo (2002/475/JAI)», (DO L 164 de 22.6.2002, p. 3.

3.4. **Biometría**

3.4.1. *Repercusión del empleo de la biometría*

Nunca carece de importancia la elección del uso de la biometría en sistemas de información, especialmente cuando el sistema en cuestión afecta a un número tan grande de personas. La biometría no es una tecnología de información más. Cambia de manera irrevocable la relación entre cuerpo e identidad, en el sentido de que hace que «una máquina pueda leer» las características del cuerpo humano y éstas quedan sometidas a su uso posterior. Aunque el ojo humano no pueda leer las características biométricas, sí pueden hacerlo, y hacer uso de ellas, los instrumentos adecuados, sin límite de tiempo y dondequiera que la persona se encuentre.

Por muy útil que la biometría pueda ser para ciertos fines, su uso generalizado tendrá una repercusión importante en la sociedad, por lo que deberá someterse a un debate amplio y abierto. El SEPD se ve en la obligación de declarar que este debate no ha tenido lugar antes de que la propuesta se desarrollase. Esto recalca aún más la necesidad de establecer garantías estrictas en cuanto al uso de datos biométricos y de llevar a cabo una cuidadosa reflexión y un debate durante el proceso legislativo.

3.4.2. *Naturaleza específica de la biometría*

Como ya se ha subrayado en varios dictámenes del Grupo del artículo 29 ([1]), la introducción y tratamiento de datos biométricos en los documentos de identidad debe ir acompañada de garantías especialmente sólidas y rigurosas. En efecto, los datos biométricos son muy sensibles debido a algunas de sus características específicas.

Cierto es que es casi imposible que la persona en cuestión pierda los datos biométricos, a diferencia de lo que puede ocurrir con una contraseña o clave. Ofrecen un *carácter distintivo casi absoluto*, es decir, que cada persona posee una biometría única. Casi nunca cambian a lo largo de la vida de una persona, y ello proporciona *permanencia* a esas características. Todos tenemos además los mismos «elementos» físicos, lo que da asimismo a la biometría una dimensión de *universalidad*.

Con todo, es casi imposible la revocación de los datos biométricos: un dedo o un rostro es difícil de cambiar. Estas características -positivas desde diversas perspectivas- tienen su lado negativo en caso de *robo de identidad*: el almacenamiento en una base de datos de impresiones dactilares y fotografías vinculadas con un documento de identidad robado podría acarrear problemas importantes y permanentes para el auténtico propietario de esa identidad. Asimismo, por su propia naturaleza, los datos biométricos *no son secretos* y pueden además *dejar huellas* (impresiones dactilares, ADN) que posibiliten recopilar esos datos *sin que su propietario sea consciente* de ello.

Debido a estos riesgos, inherentes a la biometría, deberán aplicarse importantes garantías (especialmente en lo que se refiere al respeto del principio de limitación de objetivos, la restricción de acceso y medidas de seguridad).

3.4.3. *Imperfección técnica de las impresiones dactilares*

Las principales ventajas de la biometría según lo dicho (universalidad de los datos, carácter distintivo, permanencia, funcionalidad, etc.) nunca son absolutas. Esto tiene una repercusión directa en la eficacia del registro de datos biométricos y de los procedimientos de verificación previstos en el Reglamento.

Se considera que hasta un 5 % de personas ([2]) no podrán registrarse (debido a que no tienen impresiones dactilares legibles o carecen totalmente de ellas). La evaluación de impacto ampliada aneja a la propuesta ha previsto que habrá alrededor de 20 millones de solicitantes de visado en 2007, lo que supone que hasta un millón de personas no podrán someterse al proceso «normal» de registro, con las consecuencias evidentes para la solicitud de visado y el control fronterizo.

([1]) Dictamen nº 7/2004 sobre la inclusión de elementos biométricos en los permisos de residencia y visados teniendo en cuenta la creación del Sistema de Información de Visados (VIS) (Markt/11487/04/EN — WP 96) y documento de trabajo sobre biometría (MARKT/10595/03/EN — WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention:Usability and Trust in Information Systems*, en «Foresight cybertrust and crime prevention project». 04/1151, 10 de junio de 2004, p. 7, y Technology Assessment, «Using Biometrics for Border Security», United States General Accounting Office, GAO-03-174, noviembre de 2002.

La identificación biométrica es también, por definición un proceso estadístico. Es normal un margen de error del 0,5 al 1 % ([1]), lo que quiere decir que el sistema de control en las fronteras exteriores tendrá una tasa de rechazo por error de entre el 0,5 y el 1 %. Esta tasa se modulará con un umbral basado en la política de riesgos de las autoridades competentes (que corresponde a un equilibrio establecido entre el número de personas rechazadas por error y el de las aceptadas por error). Por eso es exagerado decir que estas tecnologías ofrecerán una «identificación exacta» de las personas registradas, tal y como se dice en el considerando 9 del Reglamento propuesto.

Según un estudio prospectivo ([2]) encargado por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo, debería disponerse de unos *procedimientos accesorios* que serían una garantía esencial para la introducción de la biometría, dado que los datos biométricos no son ni accesibles a todos ni del todo exactos. Deberían implantarse y usarse estos procedimientos para respetar la dignidad de las personas que no puedan seguir con éxito el proceso de registro y para evitar que sean ellas quienes deban soportar la carga de las imperfecciones del sistema ([3]).

Por ello, el SEPD recomienda que los procedimientos accesorios se desarrollen e incluyan en la propuesta. Estos procedimientos no deberían ni disminuir el nivel de seguridad de la política de visados ni estigmatizar a las personas con impresiones dactilares ilegibles.

3.5. **Categorías especiales de datos**

Algunas categorías de datos (aparte de los datos biométricos) merecen una consideración especial: se trata de los datos relativos a los motivos de denegación del visado (3.5.1) y los datos relativos a otros miembros de un grupo (3.5.2).

3.5.1. *Motivos de denegación del visado*

En el artículo 10, apartado 2, de la propuesta se prevé el tratamiento de datos relativos a los motivos de denegación, una vez adoptada la decisión de denegación del visado. Estos motivos de denegación están plenamente normalizados.

— Los dos primeros motivos, recogidos en las letras a) y b), son más bien de carácter administrativo: no haber presentado un documento de viaje válido o documentos válidos que justifiquen el motivo y las condiciones de la estancia prevista.

— En la letra c) se menciona «el solicitante está incluido en la lista de no admisibles», lo que implica la consulta de la base de datos SIS.

— Por último, en la letra d), como motivo de denegación del visado se menciona que el solicitante «constituye una amenaza para el orden público, la seguridad interior, la salud pública o las relaciones internacionales de un Estado miembro».

([1])

Identificador biométrico	Rostro	Dedo	Iris
FTE % Imposibilidad de registro	no disponible	4	7
FNMR % Rechazo por error	4	2,5	6
FMR1 % Error de cotejo en verificación	10	< 0,01	< 0,001
FMR2 % Error de identificación en bases de datos con más de 1 millón de identidades	40	0.1	no disponible
FMR3 % Error de cotejo con datos de personas buscadas (con lista de 500 identidades)	12	< 1	no disponible

A. K. Jain et al., *Biometrics: A grand Challenge*, Proceedings of International Conference on Pattern Recognition, Cambridge, UK., agosto de 2004

([2]) *Biometrics at the frontiers: assessing the impact on Society*, febrero de 2005, Institute for Prospective Technological Studies, DG Centro Común de Investigación, Comisión Europea.

([3]) *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*, Consejo de Europa, 2005, página 11

Todos los motivos de denegación deben aplicarse con mucha cautela, debido a las consecuencias que pueden derivarse para las personas. Además, algunos de ellos, como los que señalan en las letras c) y d), darían lugar al tratamiento de «datos sensibles», en el sentido indicado en el artículo 8 de la Directiva 95/46/CE.

El SEPD desea llamar la atención más concretamente sobre la condición relativa a la salud pública, que parece imprecisa y conlleva el tratamiento de datos muy sensibles. Según el comentario sobre los artículos anejo a la propuesta, la referencia a la amenaza para la salud pública se basa en la «Propuesta de Reglamento del Consejo por el que se establece un "Código comunitario sobre el régimen de cruce de fronteras por las personas"» (COM (2004)391 final).

El SEPD es consciente de que el criterio de la «salud pública», ampliamente utilizado en la legislación comunitaria sobre la libre circulación de personas, se aplica de manera muy estricta, tal como lo muestra la Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros. En el artículo 29 de esta Directiva se fijan las condiciones para tomar en consideración un amenaza para la salud pública: «Las únicas enfermedades que podrán justificar una medida que limite la libertad de circulación serán las enfermedades con potencial epidémico como se definen en los instrumentos correspondientes de la Organización Mundial de la Salud, así como otras enfermedades infecciosas o parasitarias contagiosas siempre que sean, en el país de acogida, objeto de disposiciones de protección para los nacionales.»

— No obstante, debe señalarse que la propuesta antes mencionada constituye, hasta la fecha, sólo una propuesta, y que la inclusión en el Reglamento VIS de la condición de no representar una amenaza para la salud pública está sujeta a la adopción del Código comunitario.

— Además, en caso de adopción, este motivo de denegación de la entrada debería entenderse de manera restrictiva. En efecto, la propuesta de Código comunitario se basa a su vez en la Directiva 2004/38/CE que se acaba de mencionar.

Por ello, el SEPD recomienda que en el texto de la propuesta se incluya una referencia al artículo 29 de la Directiva 2004/38/CE para asegurar que la «amenaza a la salud pública» es entendida a la luz de dicha disposición. En cualquier caso, si se considera la sensibilidad de los datos, éstos sólo deberían tratarse si la amenaza para la salud pública es auténtica, actual y suficientemente grave.

3.5.2. *Datos relativos a otros miembros de un grupo*

En el artículo 2, apartado 7, se define a los «miembros del grupo» como «otros solicitantes que viajen con el solicitante, incluidos el cónyuge y los niños que acompañen al solicitante». En el comentario sobre los artículos se señala que las definiciones que figuran en el artículo 2 de la propuesta se refieren al Tratado o al acervo de Schengen sobre la política de visados, exceptuando algunos términos, incluido el de «miembros del grupo», que son objeto de una definición específica a efectos del presente Reglamento. Por consiguiente, puede suponerse que esta definición no se refiere a la definición de «visado colectivo» que figura en el artículo 2.1.4 de la Instrucción consular común. En el comentario sobre los artículos se hace referencia a los solicitantes que viajan en grupo con otros solicitantes, por ejemplo en el marco de un acuerdo ADS, o con miembros de la familia.

El SEPD insiste en que en el Reglamento debe darse una definición precisa y completa de «miembros del grupo». El SEPD debe señalar que en la actual propuesta, debido a que falta una referencia precisa al Tratado o al acervo de Schengen, la definición es demasiado imprecisa. A tenor del texto, entre los «miembros del grupo» podrían figurar colegas, otros clientes de la misma agencia de viajes que participen en un viaje

organizado, etc. Las consecuencias son de hecho muy importantes: según el artículo 5 del Reglamento, el expediente de solicitud de un solicitante se pondrá en relación con los expedientes de solicitud de los demás miembros del grupo.

3.6. **Conservación de datos**

El artículo 20 del proyecto de Reglamento contempla un período de conservación de cinco años para cada expediente de solicitud, quedando a la discreción del legislador comunitario la determinación de un plazo razonable.

No existen pruebas -al menos a tenor de los argumentos avanzados en los comentarios por artículos- que hagan suponer que la opción seguida en esta propuesta no sea razonable o pudiera tener consecuencias inaceptables, siempre que se establezcan los mecanismos correctores apropiados, lo que significa que debe garantizarse la corrección o supresión de aquellos datos que hayan dejado de ser exactos, en particular cuando una persona haya adquirido la nacionalidad de un Estado miembro o adquirido un estatuto que no requiera su inclusión en el sistema.

Además, mientras los datos figuren en el sistema, no podrán en modo alguno prejuzgar cualquier nueva decisión. La vigencia de algunos de los motivos de denegación (inclusión del solicitante en una lista de no admisibles o amenaza para la salud pública en particular) es temporalmente limitada y el hecho de que hayan sido considerados válidos para denegar la entrada en un momento dado no debería influir en una nueva decisión. Es preciso reconsiderar completamente la situación en cada nuevo expediente de solicitud, lo que debería explicitarse convenientemente en el Reglamento.

3.7. **Acceso al VIS y utilización de sus datos**

3.7.1. *Observaciones preliminares*

A modo de observación preliminar, el Supervisor Europeo de Protección de Datos reconoce la especial atención que se ha prestado a la regulación del acceso al VIS y a la utilización de sus datos. El hecho de que cada autoridad tenga acceso a datos diferentes con fines diferentes es, a juicio del Supervisor Europeo de Protección de Datos, un planteamiento apropiado que no puede sino alentar. Las observaciones siguientes tienen por objeto que se aplique este planteamiento de la manera más generalizada posible.

3.7.2. *Controles de visados en los puntos de control de las fronteras exteriores y en el territorio de los Estados miembros*

En el caso del control de visados en las fronteras exteriores, el artículo 16 de la propuesta explicita claramente sus dos objetivos exactos:

— «verificar la identidad de la persona», lo que significa de acuerdo con la definición dada, una comparación «individual»;

— «verificar la autenticidad del visado». Tal como proponen las normas de la OACI, el microchip del visado podría utilizar un sistema de clave pública/privada (PKI) para llevar a cabo este proceso de autentificación.

Pueden conseguirse convenientemente estos dos objetivos gracias al acceso por parte de las autoridades responsables de los controles en las fronteras exclusivamente al microchip protegido. En este caso concreto, el acceso a la base de datos central del VIS sería, por tanto, desproporcionado. Esta última opción supondría la conexión de más autoridades al VIS, con lo que aumenta el riesgo de utilización abusiva, y podría también resultar más onerosa al aumentar considerablemente el número de accesos seguros y controlados al VIS así como las necesidades de formación específica derivadas de los mismos.

Existen, además, dudas acerca de la adecuación del acceso a los datos contemplado en el apartado 2 del artículo 16. En la letra a) del apartado 2 se indica efectivamente que si de una búsqueda inicial se deduce que los datos sobre el solicitante están registrados en el VIS (lo que debería ocurrir en principio), se permitirá a la autoridad competente consultar otros datos, siempre con el único objetivo de comprobar su identidad. Estos datos cubren toda la información relacionada con la solicitud, fotografías, impresiones dactilares, así como con visados expedidos, anulados, retirados o ampliados con anterioridad.

Si se consigue verificar la identidad, no está nada claro el motivo por el que aún se necesita el resto de los datos, a los que sólo debería permitirse el acceso, con condiciones restrictivas, en caso de que los procedimientos de verificación no dieran resultados, en cuyo caso los datos contemplados en el apartado 2 del artículo 16 servirían para poner en marcha un procedimiento accesorio que ayude a comprobar la identidad de la persona. No debería, por tanto, tener acceso a estos datos el personal de todos los puntos de control sino únicamente los funcionarios responsables de los casos difíciles.

Por último, debería precisarse mejor la definición de las autoridades a las que se permite el acceso. Concretamente, no queda claro cuáles son «las autoridades responsables de los controles en las fronteras exteriores y en el territorio de los Estados miembros». El Supervisor Europeo de Protección de Datos supone que se trata de las autoridades responsables de los controles *de visados*, y debería modificarse el artículo 16 en este sentido.

3.7.3. *Utilización de los datos para la identificación y repatriación de inmigrantes ilegales y para procedimientos de asilo*

En los casos contemplados en los artículos 17, 18 y 19 (repatriación de inmigrantes ilegales y procedimientos de asilo), el VIS se utiliza a efectos de identificación. Entre los datos que pueden utilizarse para este fin están las fotografías. Sin embargo, habida cuenta de la situación actual de la tecnología de reconocimiento facial automático para sistemas de tecnología de la información de esta magnitud, no pueden utilizarse fotografías para la identificación (comparación de una persona con los datos de otras muchas) al no poder ofrecer resultados fiables. No deben, por tanto, considerarse datos apropiados para la identificación.

Por consiguiente, el Supervisor Europeo de Protección de Datos sugiere encarecidamente que se retiren las fotografías de la listas del apartado 1 de estos artículos y que se mantengan en el apartado 2 (las fotografías pueden servir como medio para comprobar la identidad de una persona pero no para identificar en una base de datos a gran escala).

Otra posibilidad consistiría en modificar el artículo 36 diciendo que sólo podrán utilizarse las funciones de tratamiento de fotografías a efectos de identificación cuando se considere fiable esta tecnología (eventualmente previo dictamen del comité técnico).

3.7.4. *Publicación de las autoridades que tienen acceso*

El artículo 4 del proyecto de Reglamento establece la publicación en el Diario Oficial de las Comunidades Europeas de las autoridades competentes designadas en cada Estado miembro cuyo personal tendrá acceso al VIS. Dicha publicación debería hacerse de forma periódica (anual), al objeto de informar de todo cambio que se produzca en el plano nacional. El Supervisor Europeo de Protección de Datos destaca la importancia de esta publicación como instrumento indispensable de control tanto a nivel europeo como nacional o local.

3.8. **Responsabilidades**

Se recuerda que el VIS se fundamentará en una arquitectura centralizada con una base de datos central en la que se almacenará toda la información sobre visados y en interfaces nacionales ubicadas en los Estados miembros, pudiendo sus autoridades competentes acceder al sistema central. Con arreglo a los considerandos (14) y (15) del proyecto de Reglamento, se aplicará la Directiva 95/46/CE al tratamiento de datos personales por los Estados miembros en aplicación del Reglamento y se aplicará el Reglamento (CE) nº 45/2001 a las actividades de la Comisión relacionadas con la protección de los datos personales. Como se indica en los citados considerandos en este contexto, la propuesta aspira a aclarar algunos puntos relativos, entre otras cosas, a la responsabilidad derivada de la utilización de los datos y al control de la protección de los datos.

De hecho, estos aspectos estarían, al parecer, relacionados con algunos detalles de crucial importancia sin los que el sistema de salvaguardias previsto en la Directiva 95/46/CE y el Reglamento (CE) nº 45/2001 no sería aplicable o no se adecuaría plenamente a la propuesta. La aplicabilidad de la normativa nacional en virtud de la Directiva presupone normalmente la existencia de un responsable del tratamiento establecido en un Estado miembro dado (artículo 4), mientras que la aplicabilidad del Reglamento depende del tratamiento de datos personales por una institución u órgano comunitario en el ejercicio de actividades pertenecientes total o parcialmente al ámbito de actuación del Derecho comunitario (artículo 3).

De conformidad con el apartado 2 del artículo 23 del proyecto de Reglamento, «los datos serán tratados por el VIS en nombre de los Estados miembros». De conformidad con el apartado 3 del artículo 23 cada Estado miembro designará a la autoridad que será considerada responsable del tratamiento con arreglo a la letra d) del artículo 2 de la Directiva 95/46/CE, lo que parece sugerir que, de acuerdo con el sistema previsto en la Directiva, debería considerarse a la Comisión encargada del tratamiento, extremo éste que se confirma en la explicación del articulado ([1]).

Este lenguaje tiende a subestimar el importantísimo y, de hecho, vital papel de la Comisión tanto en la fase de desarrollo del sistema como en el transcurso de su funcionamiento normal. Resulta difícil establecer una relación exacta entre el papel de la Comisión y el concepto de responsable del tratamiento o encargado del tratamiento; se trata bien de un encargado del tratamiento con poderes extraordinarios (por ejemplo, la concepción del sistema) o bien de un responsable del tratamiento con limitaciones (puesto que son los Estados miembros los que introducen y utilizan los datos). No cabe duda de que el papel de la Comisión en el VIS es un papel *sui generis* ([2]).

Debería reconocerse este destacado papel con una descripción exhaustiva de los cometidos de la Comisión en lugar de con un texto que, sin cambiar nada en el funcionamiento del VIS, no se corresponde con la realidad por ser demasiado restrictivo y sólo crea confusión. Habida cuenta también de la importancia de este extremo en aras de una supervisión coherente y eficaz del VIS (véase asimismo el punto 3.11), el Supervisor Europeo de Protección de Datos recomienda que se suprima el apartado 2 del artículo 23.

El Supervisor Europeo de Protección de Datos querría insistir en la enorme importancia de describir exhaustivamente los cometidos de la Comisión en relación con el VIS, si la Comisión prevé confiar las tareas de control a otro órgano. La «ficha de financiación» que acompaña la propuesta apunta la posibilidad de asignar estos cometidos a la Agencia de fronteras exteriores. En este contexto, es fundamental que la Comisión despeje cualquier duda sobre el alcance de sus competencias para que su sucesor conozca perfectamente su margen de actuación.

3.9. **Seguridad**

La gestión y el mantenimiento de un nivel óptimo de seguridad para el VIS constituye una condición indispensable para garantizar la protección necesaria de los datos personales almacenados en su base de datos. Para conseguir este nivel satisfactorio de protección, deben utilizarse las salvaguardias apropiadas para hacer frente a los riesgos potenciales derivados de la infraestructura del sistema y de las personas implicadas. Este aspecto, sobre el que se trata ahora en varias partes de la propuesta, es susceptible de mejora.

Los artículos 25 y 26 de la propuesta incluyen diferentes medidas de seguridad de los datos y especifican los tipos de utilización incorrecta que deben evitarse. No obstante, sería conveniente completar estas disposiciones con medidas destinadas a controlar e informar sistemáticamente acerca de la eficacia de las medidas de seguridad antes mencionadas. El Supervisor Europeo de Protección de Datos recomienda, más concretamente, que se añadan a estos artículos disposiciones relativas al (auto)control de las medidas de seguridad.

Se relaciona esto con el artículo 40 de la propuesta, en el que se establecen medidas en materia de seguimiento y evaluación, que no deberían referirse únicamente a aspectos tales como resultados, rentabilidad y calidad del servicio sino también al cumplimiento de las disposiciones legales, fundamentalmente en materia de protección de datos. El Supervisor Europeo de Protección de Datos recomienda por tanto que se añadan al ámbito de aplicación del artículo 40 el control de la legalidad del tratamiento de los datos y la elaboración de informes al respecto.

Por otro lado, como complemento a lo dispuesto en la letra c) del apartado 4 del artículo 24 o en la letra e) del apartado 2 del artículo 26 sobre el personal debidamente autorizado con acceso a los datos, debería añadirse que los Estados miembros deberían garantizar que se disponga de perfiles precisos de usuario (que deberían mantenerse a disposición de las autoridades nacionales de control). Además de estos perfiles, debe elaborarse una lista exhaustiva de identidades de usuarios que los Estados miembros mantendrán permanentemente actualizada. Análogas medidas serán aplicables a la Comisión, por lo que la letra b) del apartado 2 del artículo 25 debería completarse en este mismo sentido.

([1]) Véase la página 37 de la propuesta.

([2]) Aunque la definición de responsable del tratamiento que se hace en la Directiva 95/46/CE y en el Reglamento (CE) nº 45/2001 contempla asimismo la posibilidad de que existan más responsables con diferentes competencias.

Estas medidas de seguridad se completan con salvaguardias de control y organización. El artículo 28 de la propuesta estipula las condiciones en las que han de mantenerse los registros de todas las operaciones de tratamiento de datos, así como sus fines. No se almacenarán estos registros con el único objetivo de controlar la protección de los datos y garantizar la seguridad de los mismos sino también para llevar a cabo auto-controles periódicos del VIS. Los informes de autocontrol ayudarán a las autoridades de control a ejecutar eficazmente sus cometidos ya que podrán encontrar los puntos débiles y concentrarse en ellos durante su propio procedimiento de control.

3.10 **Derechos del interesado**

3.10.1. *Información del interesado*

Facilitar información al interesado con vistas a garantizar un tratamiento leal es de suma importancia y constituye una garantía indispensable para proteger los derechos de la persona. A tal efecto, el artículo 30 de la propuesta sigue básicamente el artículo 10 de la Directiva 95/46/CE.

No obstante, esta disposición podría beneficiarse de algunas modificaciones con vistas a adaptarla mejor al marco del VIS. La Directiva, es cierto, dispone que se facilite determinada información, pero permite que, si procede, se facilite más información ([1]). En consecuencia, el artículo 30 debería modificarse para incluir los siguientes aspectos:

— El interesado debería ser informado también acerca del plazo de retención que se aplique a sus datos.

— El artículo 30, apartado 1, letra e), afecta al «derecho de acceso y de rectificación de los datos». Sería más preciso mencionar el «derecho de acceso y el de *solicitar* la rectificación *o supresión* de los datos». En este sentido, los interesados deberían ser informados de la posibilidad de solicitar asesoramiento o asistencia a las autoridades de control competentes.

— Por último, en el artículo 30, apartado 1, letra a), se menciona la información relativa a la identidad de la autoridad responsable del tratamiento y, en su caso, de su representante. Dado que la autoridad responsable del tratamiento está instalada siempre en el territorio de la Unión Europea, no es necesario prever esta última posibilidad.

3.10.2. *Derecho de acceso, rectificación y supresión*

En la última frase del artículo 31, apartado 1, se declara que «el acceso a estos datos sólo podrá ser autorizado por un Estado miembro». Cabe suponer que este medio de acceso a los datos (o a que éstos sean comunicados) no puede ser concedido por la unidad central, sino por cualquier Estado miembro. El SEPD recomienda que se explicite que dicha comunicación puede solicitarse en cualquier Estado miembro.

Por otra parte, la redacción de esta disposición parece implicar que no puede denegarse el acceso, y que éste se facilitará sin autorización previa del Estado miembro responsable. Ello explicaría por qué las autoridades nacionales deben cooperar para hacer que se respeten los derechos que se establecen en el artículo 31, apartados 2, 3 y 4, pero no en el apartado 1 del mismo artículo ([2]).

3.10.3 *Asistencia por parte de las autoridades de control*

En el artículo 33, apartado 2, se dispone que las obligaciones de las autoridades nacionales de control de prestar asistencia y asesorar a la persona interesada se mantendrán durante todo el procedimiento (ante un órgano jurisdiccional). El significado de este apartado no es claro. Las autoridades nacionales de control adoptan actitudes diferentes en lo que se refiere a su cometido durante los procedimientos ante un órgano jurisdiccional. Parece como si dichas autoridades tuvieran que desempeñar el papel de consejero de la parte reclamante en esos órganos, cosa que no es posible en numerosos países.

([1]) Se hace mención de«*cualquier otra información (…) en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado*».

([2]) En consecuencia, el artículo 31, apartado 3, que se refiere a la cooperación entre las autoridades nacionales en el ejercicio de los derechos de rectificación y supresión, podría modificarse, para mayor claridad, en este sentido: «si la solicitud *mencionada en el apartado 2 del artículo 31*...». La solicitud mencionada en el apartado 1 del mismo artículo (acceso) no implica la cooperación entre las autoridades correspondientes.

3.11. **Supervisión**

La propuesta distribuye la labor supervisora entre las autoridades nacionales de control y el SEPD. Ello es coherente con el enfoque de la propuesta sobre la legislación aplicable y las responsabilidades en lo que se refiere al funcionamiento y la utilización del VIS, y con la necesidad de una supervisión eficaz. Por ello, el SEPD se felicita de este enfoque, recogido en los artículos 34 y 35.

Las autoridades nacionales de control supervisarán la legalidad del tratamiento de datos personales por los Estados miembros, *así como su transmisión al VIS y desde el VIS*. El SEPD controlará las actividades de la Comisión. *(…) También controlará la legalidad de la transmisión de datos personales entre las Interfaces Nacionales y el Sistema Central de Información de Visados*. Ello podría dar como resultado una duplicidad de cometidos, ya que las autoridades nacionales de control y el SEPD son ambos responsables al mismo tiempo del control de la legalidad de la transmisión de datos entre las Interfaces Nacionales y el Sistema Central de Información de Visados.

Por ello, el SEPD sugiere que se modifique el artículo 34 con objeto de dejar claro que las autoridades nacionales de control controlarán la legalidad del tratamiento de los datos personales por el Estado miembro de que se trate, así como su transmisión a la Interfaz Nacional del VIS.

Por lo que se refiere a la supervisión del VIS, es importante destacar que las actividades de supervisión de las autoridades nacionales de control y del SEPD deberían coordinarse en cierta medida para garantizar un nivel suficiente de coherencia y eficacia global. Efectivamente, es necesario que la aplicación del Reglamento se haga de forma armonizada y que se intente alcanzar un enfoque común frente a problemas igualmente comunes. Además, por lo que se refiere a la seguridad, cabe añadir que el nivel de seguridad del VIS quedará definido en última instancia por el nivel de seguridad que ofrezca su punto más débil. A este respecto, debe estructurarse y reforzarse la cooperación entre el SEPD y las autoridades nacionales de control. Así, el artículo 35 debería incluir una disposición en ese sentido, en la que se establezca que el SEPD convocará una reunión, al menos una vez al año, con todas las autoridades nacionales de control.

3.12 **Aplicación**

En el artículo 36, apartado 2, de la propuesta se estipula lo siguiente: *«Las medidas necesarias para la aplicación técnica de las funcionalidades a que se refiere el apartado 1 se adoptarán de conformidad con el procedimiento previsto en el apartado 2 del artículo 39.»* El artículo 39 hace referencia a un comité que asiste a la Comisión, que se creó en diciembre 2001 ([1]) y se ha utilizado en varios instrumentos jurídicos.

La aplicación técnica de las funcionalidades del VIS (interacciones con las autoridades competentes y modelo uniforme de visado) presenta varias repercusiones potenciales de gran importancia para la protección de datos. Por ejemplo, la opción de incorporar un microchip o no en el visado tendrá repercusiones en la manera en que se utilice la base de datos central, así como las normas del modelo utilizado para intercambiar datos biométricos generará o dará forma a la política de protección de datos correspondiente. ([2])

La selección de tecnologías tendrá unas repercusiones determinantes en la aplicación adecuada de los principios de finalidad y proporcionalidad, y en consecuencia es preciso supervisarla. Por tanto, las opciones tecnológicas con una repercusión muy importante en la protección de datos deben plasmarse preferiblemente mediante un reglamento, con arreglo al procedimiento de codecisión. Sólo en este caso puede asegurarse el control político necesario. En todos los demás casos con repercusiones en la protección de datos, debería darse al SEPD la posibilidad de asesorar sobre las opciones del comité.

3.13. **Interoperabilidad**

La interoperabilidad es una condición previa crítica y vital para la eficacia de los sistemas de TI de gran envergadura como el VIS. Ofrece la posibilidad de reducir los gastos generales de manera constante y evitar la redundancia natural de elementos heterogéneos. La interoperabilidad puede también contribuir al objetivo de una política común de visados mediante la aplicación de las mismas normas de procedimiento a todos los elementos constitutivos de dicha política. No obstante, es fundamental distinguir entre dos niveles de interoperabilidad:

— La interoperabilidad entre los Estados miembros de la UE es muy deseable; es evidente que las solicitudes de visado enviadas por las autoridades de un Estado miembro tienen que ser interoperables con las enviadas por cualesquiera autoridades de otro Estado miembro.

([1]) Reglamento (CE) nº 2424/2001 del Consejo, de 6 de diciembre de 2001, sobre el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II).

([2]) La propuesta de Reglamento del Consejo por el que se modifica el Reglamento (CE) nº 1683/95 (modelo uniforme de visado) de septiembre de 2003 incluía un artículo parecido.

— La interoperabilidad entre sistemas diseñados para propósitos distintos o con sistemas de terceros países es mucho más cuestionable.

Entre las salvaguardias disponibles que se usan para limitar los objetivos del sistema y evitar la desviación de uso («function creep»), el uso de normas tecnológicas distintas puede contribuir a esta limitación. Además, cualquier forma de interacción entre dos sistemas distintos debe documentarse exhaustivamente. La interoperabilidad nunca debe conducir a una situación en que una autoridad que no tenga derecho a acceder o utilizar determinados datos pueda obtener este acceso a través de otro sistema de información.

En este contexto, el SEPD quisiera hacer referencia a la Declaración del Consejo de 25 de marzo de 2004 sobre la lucha contra el terrorismo, en la que se pide a la Comisión que presente propuestas para mejorar la interoperabilidad y las sinergias entre sistemas de información (SIS, VIS y Eurodac).

También quisiera hacer referencia a los debates en curso sobre a qué organismo podría asignársele la gestión de los distintos sistemas de gran envergadura en el futuro (véase también el punto 3. 8 del presente dictamen).

El SEPD desea volver a insistir en que la interoperabilidad de los sistemas no puede aplicarse en violación del principio de limitación del objetivo, y en que es preciso someterle cualquier propuesta en esta materia.

4. **CONCLUSIONES**

4.1 **Aspectos de carácter general**

1. El SEPD reconoce que la continuación del desarrollo de una política común de visados requiere un intercambio eficaz de los datos correspondientes. Uno de los mecanismos que puede garantizar una circulación sin contratiempos de información es el VIS. El SEPD ha tomado cuidadosa nota de los elementos presentados en la Evaluación de Impacto Ampliada (EIA). Aunque estas pruebas no sean completamente concluyentes, parece que hay suficientes razones que justifican el establecimiento del VIS con el objetivo de mejorar la política común de visados.

   No obstante, este nuevo instrumento debe limitarse a la recogida e intercambio de datos, en la medida en que dicha recogida o intercambio sean necesarios para el desarrollo de una política común de visados y estén en proporción con dicho objetivo.

2. El establecimiento del VIS puede tener consecuencias positivas para otros intereses públicos legítimos, pero esto no altera el objetivo del VIS. Por tanto, todos los elementos del VIS deben ser instrumentos necesarios y proporcionados para lograr el objetivo político mencionado anteriormente. Por lo demás:

   — El acceso sistemático por parte de las autoridades policiales no estaría en consonancia con este propósito.

   — El SEPD recomienda que se explicite mejor la distinción entre el «objetivo» y las «ventajas» en el texto del artículo 1, apartado 2.

   — La interoperabilidad con otros sistemas no puede aplicarse en violación del principio de limitación de objetivo.

3. El SEPD reconoce las ventajas del uso de la biometría, pero insiste en las importantes repercusiones del uso de este tipo de datos y sugiere la inclusión de garantías estrictas para el uso de los datos biométricos. Por otra parte, las imperfecciones técnicas de las impresiones dactilares requieren el desarrollo e inclusión en la propuesta de procedimientos «de emergencia».

4. El presente dictamen debe mencionarse en el preámbulo del Reglamento con anterioridad a los considerandos («Visto el dictamen …»).

4.2. **Otros aspectos**

5. En relación con los motivos de denegación de visado: es preciso incluir una referencia al artículo 29 de la Directiva 2004/58/CE en el texto de la propuesta para asegurarse de que se entiende «amenaza para la salud pública» a la vista de dicha disposición.

6. Los datos sobre los miembros de un grupo tienen un significado especial en la propuesta: por tanto hay que incluir una definición precisa y exhaustiva de «miembros del grupo».

7. No hay pruebas de que la opción de política aplicada en esta propuesta sobre el plazo de retención de datos sea poco razonable o tenga consecuencias inaceptables, siempre que se apliquen todos los mecanismos de corrección adecuados.

   Además, debería explicitarse en la propuesta que los datos personales deben reevaluarse completamente para cada nueva solicitud de visado.

8. En relación con los controles de visados en las fronteras exteriores: el artículo 16 de la propuesta debe modificarse, puesto que en estos casos el acceso a la base de datos central del VIS sería desproporcionado. Es suficiente el acceso por parte de las autoridades competentes para el control de visados exclusivamente al microchip protegido.

   Por otra parte, si se ha conseguido la verificación de identidad, no está claro en absoluto por qué razón siguen siendo necesarios el resto de los datos.

9. En relación con el uso de los datos para identificación y repatriación de inmigrantes ilegales y para procedimientos de asilo: el término «fotografías» debe suprimirse del apartado 1 de los artículos 17, 18 y 19 y debe mantenerse en el apartado 2.

10. En relación con las responsabilidades de la Comisión y los Estados miembros: hay que suprimir el artículo 23, apartado 2.

11. Deben añadirse a la propuesta disposiciones sobre un (auto)control de las medidas de seguridad. Es preciso ampliar el ámbito de aplicación del artículo 40 al control y notificación sobre la legalidad del tratamiento. Además:

   — Los Estados miembros deben elaborar una lista completa de identificaciones de usuarios y mantenerla actualizada permanentemente. Lo mismo se aplica a la Comisión: así pues el artículo 25, apartado 2, letra b), debe completarse en el mismo sentido.

   — El artículo 28 de la propuesta describe las condiciones y los fines para los que debe llevarse registro de todas las operaciones de tratamiento de datos. Estos registros no sólo deben almacenarse para la vigilancia de la protección de datos y para garantizar la seguridad de los datos, sino también para proceder a un autocontrol periódico del VIS.

12. En relación con los derechos del afectado por el tratamiento de los datos:

   — Es preciso modificar el artículo 30 para garantizar que los interesados también reciben información sobre el plazo de retención que se aplica a sus datos.

   — En el artículo 30, apartado 1, letra e), se debe mencionar «el derecho de acceso y el derecho de solicitar la rectificación o supresión de los datos».

   — El artículo 31, apartado 1, debe explicitar que la comunicación de ciertos datos podrá solicitarse en cualquier Estado miembro.

13. En relación con la supervisión:

— Es preciso modificar el artículo 34 para clarificar que las autoridades nacionales de control vigilan la legalidad del tratamiento de datos personales por parte del Estado miembro, incluida su transmisión en ambos sentidos a la interfaz nacional del VIS.

— El artículo 35 debería incluir, pues, una disposición que estableciera que el SEPD convocará una reunión con todas las autoridades nacionales de control al menos una vez al año.

14. En relación con la aplicación:

— Sería preferible realizar las elecciones tecnológicas que tengan una repercusión sustancial en la protección de datos mediante reglamento, con arreglo al procedimiento de codecisión.

— En los demás casos es preciso ofrecer al SEPD la posibilidad de asesorar sobre las elecciones realizadas por el comité previsto en la propuesta.

Bruselas, 23 de marzo de 2005.

Peter HUSTINX

El Supervisor Europeo de Protección de Datos