SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos

— sobre la propuesta de Decisión del Consejo relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (COM(2005)230 final);

— la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (COM(2005)236 final), y

— la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso al Sistema de Información de Schengen de segunda generación (SIS II) por los servicios de los Estados miembros responsables de la expedición de los certificados de matriculación de vehículos (COM(2005)237 final)

(2006/C 91/11)

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 el Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas respecto al tratamiento de los datos personales por las instituciones y órganos comunitarios y a la libre circulación de estos datos, y en particular su artículo 41,

Vista la solicitud de dictamen formulada por la Comisión de conformidad con lo dispuesto en el apartado 2 del artículo 28 del Reglamento (CE) nº 45/2001, recibida el 17 de junio de 2005,

HA ADOPTADO EL PRESENTE DICTAMEN:

1. INTRODUCCIÓN

1.1. Antecedentes

El Sistema de Información de Schengen (SIS) es un sistema informático europeo a gran escala creado para compensar la supresión de los controles en las fronteras interiores del espacio Schengen. El SIS permite que las autoridades competentes de los Estados miembros intercambien información a efectos del control de las personas y los objetos en las fronteras exteriores o dentro del territorio, así como para la expedición de visados y permisos de residencia.

El Convenio de Schengen, que es un acuerdo intergubernamental, entró en vigor en 1995. Posteriormente, mediante el Tratado de Amsterdam, se integró en el marco de la UE el SIS previsto por el Convenio de Schengen.

Un nuevo Sistema de Información de Schengen «de segunda generación» (el SIS II) sustituirá al sistema actual y permitirá ampliar el espacio Schengen a los nuevos Estados miembros de la UE. Por otra parte, este sistema incorporará nuevas funcionalidades. Las disposiciones Schengen, elaboradas en forma de marco intergubernamental, se transformarán íntegramente en instrumentos jurídicos europeos clásicos.

El 1 de junio de 2005, la Comisión Europea presentó tres propuestas para el establecimiento del SIS II, a saber:

— una propuesta de Reglamento basado en el título IV del Tratado CE (visados, asilo, inmigración y otras políticas relacionadas con la libre circulación de personas) que regulará los aspectos de SIS II relativos al primer pilar (inmigración), denominada en lo sucesivo «la propuesta de Reglamento»;

— una propuesta de Decisión basada en el título VI del Tratado UE (cooperación policial y judicial en materia penal) que regulará la utilización del SIS con fines relativos al tercer pilar, denominada en lo sucesivo «la propuesta de Decisión»;

— una propuesta de Reglamento basado en el título V (transportes) relativo específicamente al acceso de los servicios responsables de la matriculación de vehículos a los datos del SIS, que se examinará por separado (véase el apartado 4.6 *infra*).

En este contexto, es necesario tener en cuenta que, en los próximos meses, la Comisión presentará una comunicación relativa a la interoperatividad y el aumento de las sinergias entre los sistemas de información de la UE (SIS, VIS, Eurodac).

El SIS II consiste en una base de datos central denominada «Sistema Central de Información de Schengen» (CS-SIS), de cuya gestión operativa se encargará la Comisión, conectada a los puntos de acceso nacionales definidos por cada Estado miembro (NI-SIS). Las autoridades SIRENE realizarán el intercambio de toda la información complementaria (información relacionada con inscripciones del SIS II pero no almacenada en éste).

Los Estados miembros abastecerán al SIS II de datos relativos a las personas buscadas para su detención, entrega o extradición, buscadas en el marco de procedimientos judiciales, personas que deban ser objeto de una vigilancia discreta o de un control específico, o cuya entrada deba denegarse en la frontera exterior, así como a objetos perdidos o robados. El objetivo de las «inscripciones» , es decir, de los conjuntos de datos introducidos en el SIS, es permitir que las autoridades competentes identifiquen a una persona o un objeto.

El SIS II presenta nuevas características, como un acceso ampliado (Europol, Eurojust, fiscales nacionales, servicios responsables de la matriculación de vehículos), la interconexión de las inscripciones, la adición de nuevas categorías de datos, incluidos los datos biométricos (huellas dactilares y fotografías), así como una plataforma técnica común al Sistema de Información de Visados. Estas nuevas características han alimentado durante años los debates sobre el cambio de finalidad del SIS, que pasa de ser una herramienta de control a convertirse en un sistema de información e investigación.

1.2 **Evaluación general de las propuestas**

1. El SEPD toma nota con satisfacción de que se le consulta sobre la base del artículo 28 (2) del Reglamento (CE) nº 45/2001. Sin embargo, teniendo en cuenta el carácter vinculante de esta disposición, el presente dictamen debería mencionarse en el preámbulo de los textos.

2. El SEPD se congratula por estas propuestas por varios motivos. La transformación de una estructura intergubernamental en instrumentos del Derecho europeo implica varias consecuencias positivas: se precisará la fuerza jurídica de las disposiciones que regularán el SIS II, el Tribunal de Justicia será competente para interpretar el instrumento relativo al primer pilar y el Parlamento Europeo participará al menos parcialmente (aunque de forma algo tardía) en el proceso.

3. Además, por lo que se refiere al fondo, las propuestas contienen una parte importante relativa a la protección de datos, que aportan algunas mejoras con respecto a la situación actual y que se acogen con satisfacción. En particular, merecen mencionarse las medidas en favor de las víctimas de usurpación de identidad, la ampliación del Reglamento 45/2001 a las operaciones de tratamiento de datos realizadas por la Comisión en el marco de actividades relativas al título VI y una mejor definición de los motivos para la introducción de inscripciones a efectos de no admisión.

4. Por otra parte, es evidente que se ha prestado gran atención a la redacción de las propuestas, cuya complejidad refleja la complejidad inherente al sistema que regulan. La mayoría de las observaciones formuladas en el presente dictamen tiene por objeto clarificar o completar disposiciones, sin que ello requiera una reorganización del conjunto.

Sin embargo, a pesar de esta valoración globalmente positiva, procede formular las siguientes reservas:

1. A menudo resulta difícil comprender la intención que justifica el texto, y es de lamentar la falta de una exposición de motivos. Teniendo en cuenta la gran complejidad de estos documentos, una exposición de motivos habría sido fundamental. En ocasiones, su ausencia no deja al lector más elección que aventurar suposiciones.

2. Además, la falta de un análisis de impacto no puede sino lamentarse. El hecho de que la primera versión del sistema ya esté en funcionamiento no justifica esta omisión, teniendo en cuenta las diferencias considerables entre ambas versiones. En particular, habría sido necesaria una mayor reflexión sobre las consecuencias de la introducción de datos biométricos.

3. El marco jurídico para la protección de datos es un ámbito muy complejo que se basa en la aplicación combinada de la *lex generalis* y la *lex specialis*. Sería necesario garantizar que, aunque se elabore una legislación específica, el marco jurídico para la protección de datos ya previsto en la Directiva 95/46/CE y el Reglamento 45/2001 siga siendo plenamente aplicable. La aplicación combinada de distintos instrumentos jurídicos no debe generar divergencias sobre aspectos fundamentales entre los regímenes nacionales, ni tampoco una merma del nivel actual de protección de los datos.

4. La ampliación del acceso a numerosas autoridades nuevas que no persiguen el objetivo inicial de «controles sobre personas y objetos» debería combinarse con garantías más estrictas.

5. Las propuestas están fundamentadas, en gran medida, en otros instrumentos jurídicos aún en curso de elaboración (o incluso todavía no propuestos). El SEPD, si bien comprende las dificultades que plantea la elaboración de legislación en un entorno complejo y en constante evolución como es éste, considera inaceptable esta situación, habida cuenta de sus consecuencias para los interesados y de la inseguridad jurídica que genera.

6. El reparto de competencias entre los Estados miembros y la Comisión es un tanto confuso. La claridad a este respecto es indispensable, no sólo para el buen funcionamiento del sistema, sino también para el control del conjunto del mismo.

1.3. **Estructura del dictamen**

El presente dictamen se estructura como se expone a continuación. En primer lugar, se precisa el marco jurídico aplicable al SIS II. Seguidamente, se define la finalidad del SIS II y se examinan los elementos que presentan diferencias considerables con respecto al sistema actual. El apartado 5 recoge observaciones sobre los papeles respectivos de la Comisión y de los Estados miembros por lo que se refiere al funcionamiento del SIS II. El apartado 6 trata de los derechos de las personas a quienes conciernen los datos. El apartado 7 se refiere al control efectuado a nivel nacional y por el SEPD, así como a la cooperación entre los supervisores. El apartado 8 contiene algunas observaciones y propone posibles modificaciones relativas a la seguridad. Los apartados 9 y 10 tratan de la comitología y la interoperatividad, respectivamente. Por último, un resumen de las conclusiones refleja las principales conclusiones sobre cada punto.

2. MARCO JURÍDICO APLICABLE

2.1. **Marco jurídico aplicable en materia de protección de los datos del SIS II**

Las propuestas hacen referencia a la Directiva 95/46/CE, al Convenio 108 del Consejo de Europa y al Reglamento (CE) nº 45/2001, como marco jurídico para la protección de datos. También procede tener en cuenta otros instrumentos.

Para clarificar este marco y los principales elementos en los que se basa el presente dictamen, conviene recordar lo siguiente:

— En Europa se garantiza el respeto de la intimidad desde la aprobación por el Consejo de Europa, en 1950, del Convenio para la protección de los derechos humanos y de las libertades fundamentales (en lo sucesivo «CEDH»), cuyo artículo 8 consagra el «derecho al respeto de la vida privada y familiar».

  Según el apartado 2 del artículo 8, del CEDH, no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino «en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria» para la protección de intereses importantes. Según la jurisprudencia del Tribunal Europeo de Derechos Humanos, el cumplimiento de estas condiciones implica exigencias adicionales relativas a la calidad del fundamento jurídico de la injerencia, la proporcionalidad de las medidas y la necesidad de garantías adecuadas contra los abusos.

— Más recientemente, en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea se consagraron el derecho al respeto de la vida privada y la protección de los datos de carácter personal. El artículo 52 de dicha Carta reconoce que estos derechos podrán ser objeto de limitaciones, a condición de que se cumplan condiciones similares a las previstas en el artículo 8 del CEDH.

— Según el apartado 2 del artículo 6 del Tratado de la UE, la Unión respetará los derechos fundamentales tal y como se garantizan en el CEDH.

Los tres textos explícitamente aplicables a las propuestas relativas al SIS II son los siguientes:

— El Convenio nº 108 del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en lo sucesivo «Convenio 108») enuncia principios fundamentales en materia de protección de las personas con respecto al tratamiento de datos personales. Todos los Estados miembros han ratificado este Convenio, que se aplica también a las actividades realizadas en los ámbitos policial y judicial. El Convenio 108 es el régimen de protección de datos que se aplica actualmente al Convenio de Schengen, junto con la recomendación R (87) 15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa, destinada a regular la utilización de datos personales en el sector de la policía.

— La Directiva 95/46/CE del Parlamento Europeo y el 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), en lo sucesivo «*Directiva 95/46/CE*». Conviene señalar que, en la mayoría de los Estados miembros, la legislación nacional por la que se aplica la Directiva también cubre las operaciones de tratamiento de datos realizadas en los ámbitos policial y judicial.

— El Reglamento (CE) nº 45/2001 del Parlamento Europeo y el 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), denominado en lo sucesivo «*Reglamento nº 45/2001*».

La interpretación de la Directiva 95/46/CE y del Reglamento (CE) nº 45/2001 depende en parte de la jurisprudencia pertinente del Tribunal Europeo de Derechos Humanos, de acuerdo con el Convenio para la protección de los derechos humanos y de las libertades fundamentales de 1950 (CEDH). En otros términos, la Directiva y el Reglamento, en la medida en que se refieren a un tratamiento de datos personales que puede menoscabar las libertades fundamentales y, en particular, el derecho a la vida privada, deben interpretarse a la luz de los derechos fundamentales. Es también lo que se desprende de la jurisprudencia del Tribunal de Justicia ([1]).

([1]) A este respecto, procede citar la sentencia del Pleno del Tribunal de Justicia *Österreichischer Rundfunk* y otros (asuntos acumulados C-465/00, C-138/01 y C-139/01 de 20 de mayo de 2003, Rec. (2003), p. I-4989). El Tribunal examina aquí una ley austriaca que prevé la transmisión al Tribunal de Cuentas austriaco de información relativa a los ingresos de los empleados del sector público así como su posterior publicación. El Tribunal fija en su sentencia una serie de criterios, extraídos del artículo 8 del Convenio Europeo de Derechos Humanos, que procede tener en cuenta para aplicar la Directiva 95/46/CE, en la medida en que ésta autoriza algunas limitaciones al derecho a la intimidad.

El 4 de octubre de 2005, la Comisión presentó una «propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal» ([1]) (denominada en lo sucesivo *«proyecto de Decisión marco»*). El objetivo de esta Decisión marco es sustituir al Convenio 108 como texto jurídico de referencia del proyecto de Decisión relativa al SIS II, cosa que en este contexto puede tener una incidencia sobre el régimen de protección de datos (véase el apartado 2.2.5 *infra*).

2.2. **Régimen jurídico de protección de datos del SIS II**

2.2.1. *Observaciones generales*

La base legislativa necesaria para regular el SIS II consiste en instrumentos distintos; no obstante, tal como se recuerda en los considerandos, esto «no afecta al principio de que el SIS II constituye un único sistema de información que deberá funcionar como tal. En consecuencia, algunas disposiciones de dichos instrumentos serán idénticas.»

Los dos documentos se estructuran básicamente de la misma manera, siendo los capítulos I a III prácticamente idénticos en ambos textos. El hecho de que el SIS II deba considerarse como un único sistema de información dotado de dos bases jurídicas diferentes se traduce también en el régimen, más bien complejo, de protección de los datos.

El régimen de protección de datos se determina parcialmente en las propias propuestas: se trata de la «*lex specialis*», completada por una legislación de referencia («*lex generalis*») diferente para cada sector (Comisión, Estados miembros en el marco del primer pilar y Estados miembros en el marco del tercer pilar).

Teniendo en cuenta esta estructura, es necesario interrogarse sobre el modo de abordar las normas particulares con respecto a la norma general. En el caso presente, el SEPD considera la norma particular como una aplicación de la norma general. De esto se desprende que la *lex specialis* debe siempre ajustarse a la *lex generalis;* si bien desarrolla la *lex generalis* (precisándola o completándola), no se concibe como una excepción a ésta.

En cuanto a la cuestión de qué norma conviene aplicar en cada caso preciso, el principio quiere que se aplique prioritariamente *la lex specialis* pero que, cuando ésta guarda silencio o es confusa, sea necesario referirse *a la lex generalis*.

Esta estructura da lugar a tres combinaciones diferentes entre *lex generalis* y *lex specialis*, que podrían resumirse como se expone a continuación.

2.2.2. *Régimen aplicable para la Comisión*

Cuando esté implicada la Comisión, se aplicará el Reglamento (CE) nº 45/2001, incluso por lo que se refiere a la intervención del SEPD, tanto si se trata de actividades realizadas en el marco del primer pilar (propuesta de Reglamento) como del tercer pilar (propuesta de Decisión). El considerando 21 de la propuesta de Decisión establece que «el Reglamento (CE) nº 45/2001 (…) se aplica al tratamiento de datos personales por la Comisión cuando dicho tratamiento tiene lugar en el ejercicio de actividades que entran total o parcialmente en el ámbito de aplicación del Derecho comunitario. Una parte del tratamiento de datos personales en el SIS II entra en el ámbito de aplicación del Derecho comunitario.»

Esto se explica por razones prácticas: sería extremadamente difícil, por lo que se refiere a la Comisión, determinar si los datos se tratan en el marco de actividades pertenecientes al primer o al tercer pilar.

Además, no sólo es más lógico, desde el punto de vista práctico, aplicar un único instrumento jurídico a todas las actividades realizadas por la Comisión en el marco del SIS II, sino que así también se mejora la coherencia (garantizando, según el considerando 21 de la propuesta de Decisión: «una aplicación coherente y homogénea de las normas sobre protección de los derechos y libertades fundamentales de la persona con respecto al tratamiento de datos personales»). Por lo tanto, el SEPD se felicita de que la Comisión considere que el Reglamento (CE) nº 45/2001 se aplica a todas las actividades de tratamiento de datos que ésta realiza en el SIS II.

2.2.3. *Régimen aplicable para los Estados miembros*

La situación es más compleja en lo que respecta a los Estados miembros. El tratamiento de datos personales en aplicación de la propuesta de Reglamento es regulado por el propio Reglamento propuesto, así como por la Directiva 95/46/CE. El texto del considerando 14 de la propuesta de Reglamento estipula claramente que la Directiva debe considerarse como la *lex generalis*, mientras que el Reglamento «SIS II» será la *lex specialis*. Esto implica una serie de consecuencias que se enumeran a continuación.

Por lo que se refiere a la propuesta de Decisión, el instrumento jurídico de referencia (*lex generalis*) en materia de protección de datos es el Convenio 108, lo que puede significar una diferencia importante sobre algunos puntos entre los regímenes de protección de datos aplicables en el primer y tercer pilar.

2.2.4. *Consecuencias para el nivel de protección de los datos*

El SEPD formula las siguientes observaciones generales sobre esta arquitectura de la protección de datos:

— La aplicación de la propuesta de Reglamento como *lex specialis* de la Directiva 95/46/CE (así como la de la propuesta de Decisión como *lex specialis* del Convenio 108) no debería originar en ningún caso una merma del nivel de protección de los datos garantizado con arreglo a la Directiva o al Convenio. El SEPD hará recomendaciones a tal efecto (véase, por ejemplo, el derecho de recurso).

([1]) Doc. COM(2005) 475 final.

— Del mismo modo, la aplicación combinada de instrumentos jurídicos no puede tener como resultado la reducción del nivel de protección de datos garantizado en el marco del actual Convenio de Schengen (véanse, por ejemplo, las observaciones formuladas más adelante con respecto al artículo 13 de la Directiva 95/46/CE).

— La aplicación de dos instrumentos diferentes, si bien es necesaria debido al marco del Derecho comunitario, no debería llevar a disparidades injustificadas en la protección de los datos de los interesados según el tipo de datos tratados. Esto debe evitarse en la medida de lo posible. Las recomendaciones formuladas a continuación pretenden también mejorar la coherencia en la mayor medida posible (véanse, por ejemplo, las competencias de las autoridades nacionales de control).

— El marco jurídico es tan complejo que con toda probabilidad generará cierta confusión en la aplicación práctica. En algunos casos, resulta difícil ver cómo interactúan la *lex generalis* y la *lex specialis*, y sería conveniente aclararlo en las propuestas. Además, en esta situación jurídica compleja, el SEPD considera muy interesante la sugerencia formulada por la ACC de Schengen en su dictamen sobre la base jurídica propuesta para el SIS II (27 de septiembre de 2005), consistente en elaborar un «vademécum» donde se enumeren todos los derechos existentes en relación con el SIS II y se establezca una jerarquía clara de la legislación aplicable.

Como conclusión, el presente dictamen tratará de garantizar un alto nivel de protección de datos, de coherencia y claridad, con el fin de ofrecer a los interesados la seguridad jurídica necesaria.

2.2.5. *Consecuencias del proyecto de Decisión marco en la protección de datos en el tercer pilar*

La Decisión marco relativa a la protección de datos en el tercer pilar sustituirá al Convenio 108 como instrumento de referencia para la protección de datos en el proyecto de Decisión SIS II [1]. Esto no se menciona en la propuesta, pero se desprende de la propuesta de Decisión marco, que establece, en su artículo 34 (2), que «las referencias al Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de los datos personales se entenderán como referencias a la presente Decisión marco». Dado que en las próximas semanas el SEPD emitirá un dictamen sobre el proyecto de Decisión marco, en el presente dictamen no analizará su contenido con detalle. Sin embargo, siempre que la aplicación de la Decisión marco pueda tener una incidencia notable en el régimen de protección de datos del SIS II, sí se mencionará.

2.2.6. *Aplicación del artículo 13 de la Directiva 95/46/CE y del artículo 9 del Convenio 108*

El artículo 13 de la Directiva 95/46/CE y el artículo 9 del Convenio 108 establecen que los Estados miembros podrán adoptar medidas legislativas destinadas a limitar el alcance de las obligaciones y derechos previstos por estos instrumentos cuando esta limitación constituya una medida necesaria para salvaguardar intereses superiores (como la seguridad del Estado, la defensa, la seguridad pública, etc.) [2].

Tanto los considerandos de la propuesta de Reglamento como los de la propuesta de Decisión indican que los Estados miembros podrían utilizar esta posibilidad en la aplicación de estos textos a nivel nacional. En tal caso, sería necesario establecer una condición doble: la aplicación del artículo 13 de la Directiva 95/46/CE deberá ajustarse al artículo 8 del CEDH y además no deberá originar una merma del régimen actual de protección de datos.

Esto resulta tanto más importante en el caso del SIS II, puesto que el sistema debe ser previsible. Dado que los Estados miembros comparten sus datos, deben poder saber con suficiente certeza cómo se tratarán a nivel nacional.

A este respecto, es un motivo particular de inquietud que las propuestas puedan suponer una reducción del nivel actual de protección de datos. El artículo 102 del Convenio de Schengen establece un sistema que regula de forma estricta y limita, incluso en el Derecho nacional, la utilización de los datos («Toda utilización de datos que no sea conforme con los apartados 1 a 4 se considerará como una desviación de la finalidad respecto al Derecho nacional de cada Parte contratante»). Ahora bien, tanto la Directiva 95/46/CE como el Convenio 108 prevén la posibilidad de incluir excepciones en el Derecho nacional, entre otras, al principio de limitación de la finalidad. De hacerse, esto supondría una discrepancia con respecto al régimen actual del Convenio de Schengen, que establece que la legislación nacional no puede apartarse del principio esencial de limitación de la finalidad y la utilización.

La aprobación de la Decisión marco no variaría esta observación: se trata más de preservar el principio estricto de limitación de la finalidad del tratamiento de los datos del SIS II que de velar por que los datos se traten en cumplimiento de la Decisión marco.

[1] También sustituirá al régimen general de protección de datos del Convenio de Schengen (artículos 126 a 130 del Convenio de Schengen). Este régimen no se aplica al SIS.

[2] Un Estado miembro que recurra a esta posibilidad de restringir los derechos sólo podrá hacerlo en cumplimiento del artículo 8 del CEDH, como se indica anteriormente.

El SEPD sugiere introducir en las propuestas relativas al SIS II (es decir, en el artículo 21 de la propuesta de Reglamento y en el artículo 40 de la propuesta de Decisión) disposiciones que tengan el mismo efecto que el actual artículo 102 (4) del Convenio de Schengen, y que limiten la posibilidad de que los Estados miembros autoricen una utilización de los datos que no esté prevista en los textos sobre el SIS II. Otra solución consistiría en restringir explícitamente, en las propuestas de Decisión y Reglamento, el alcance de las excepciones autorizadas en virtud del artículo 13 de la Directiva o del artículo 9 del Convenio, disponiendo, por ejemplo, que los Estados miembros sólo podrán limitar los derechos de acceso y de información, y no los principios relativos a la calidad de los datos.

3. **OBJETIVO**

De acuerdo con el artículo 1 de ambos documentos («Establecimiento y objetivo general del SIS II»), el SIS II se establece con el fin de permitir «cooperar a las autoridades competentes de los Estados miembros, mediante el intercambio de información, en los controles sobre personas y objetos» y de contribuir «a mantener un alto nivel de seguridad en el espacio sin controles fronterizos interiores entre los Estados miembros».

El objetivo del SIS II se formula en términos bastante generales, y las disposiciones anteriormente mencionadas no precisan, por sí mismas, qué cubre (o comporta) este objetivo.

El objetivo del SIS II parece mucho más amplio que el del actual SIS tal como se enuncia en el artículo 92 del Convenio de Schengen, que menciona expresamente el acceso a «inscripciones de personas y objetos, al efectuar controles en la frontera y comprobaciones y otros controles de policía y de aduanas (…)», así como (para la categoría de descripciones contemplada en el artículo 96) «a efectos del procedimiento de expedición de visados, de expedición de permisos de residencia y de la administración de extranjeros (…)».

Este objetivo ampliado resulta también de la introducción en el SIS II de nuevas funcionalidades y nuevos accesos que no corresponden al objetivo inicial de control de personas y objetos, sino más bien al de una herramienta de investigación. En particular, se ha previsto el acceso de autoridades que utilizarán los datos del SIS II para sus propios objetivos, y no para los objetivos del SIS II (ver más adelante). Además, se generalizará la interconexión de las inscripciones, aunque esto constituye una característica típica de una herramienta de investigación policial.

También se plantean cuestiones con respecto al motor de búsqueda biométrico, que deberá ponerse a punto en los próximos años, y que permitirá realizar búsquedas en el sistema que van más allá de las necesidades de un sistema de control.

Como conclusión, las propuestas tienen un alcance mucho más amplio que el marco actual, lo que requiere garantías suplementarias. A este respecto, el SEPD centrará su análisis no tanto en la definición general que figura en el artículo 1, sino en las funcionalidades y los demás elementos constitutivos del SIS II.

4. **MODIFICACIONES SIGNIFICATIVAS EN EL SIS II**

El presente capítulo se referirá en primer lugar a los nuevos elementos que aporta el SIS II, es decir la introducción de la biometría, el nuevo concepto de acceso, con especial atención al acceso de Europol, Eurojust y los servicios responsables de la matriculación de vehículos, la interconexión de las inscripciones y el acceso de las distintas autoridades a los datos de inmigración.

4.1. **Biometría**

Las propuestas relativas al SIS II introducen la posibilidad de tratar una nueva categoría de datos que merecen una atención especial, los datos biométricos. Como ya destacó el SEPD en su dictamen sobre el sistema de información de visados [1], el carácter sensible inherente a los datos biométricos requiere garantías específicas que no se han introducido en las propuestas relativas al SIS II.

Por lo general, va en aumento la tendencia a recurrir a los datos biométricos en los sistemas de información de la UE (VIS, EURODAC, Sistema de información sobre permisos de conducción, etc.), sin que lleve aparejado un examen atento de los riesgos en que se incurre y las garantías necesarias.

La Resolución sobre el uso de la biometría, difundida recientemente por la Conferencia internacional de Comisarios de Protección de Datos celebrada en Montreux [2], también hace hincapié en la necesidad de profundizar en esta reflexión. Hasta ahora, solamente se han subrayado las ventajas de la elaboración de normas a efectos de aumentar la interoperatividad entre los sistemas, y no que tales normas elevarían también la calidad de los tratamientos biométricos.

---

[1] Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento del Parlamento Europeo y el Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros, 23 de marzo de 2005, apartado 3.4.2.

[2] 27ª Conferencia internacional de Comisarios de Protección de Datos y Privacidad, Montreux, 16 de septiembre de 2005, Resolución sobre el uso de la biometría en los pasaportes, tarjetas de identidad y documentos de viaje.

Sería conveniente establecer un conjunto de obligaciones o requisitos comunes vinculadas a la especificidad de estos datos, así como una metodología común para su aplicación. En particular, estos requisitos comunes podrían constar de los elementos siguientes (cuya necesidad reflejan las propuestas relativas al SIS II):

— **Evaluación de impacto específica:** Conviene destacar que las propuestas no han sido objeto de una evaluación de impacto por lo que se refiere a la utilización de la biometría ([1]).

— **Énfasis en el procedimiento de registro de los datos:** El origen de los datos biométricos y la manera en que se recogerán no se describen con detalle. El registro de los datos es una etapa fundamental en el procedimiento de identificación biométrica y no basta con limitarse a definirlo por medio de anexos o de debates en subgrupos, ya que ello condiciona directamente el resultado final del proceso, por ejemplo en relación con la tasa de error.

— **Énfasis en el nivel de precisión**: El uso de la biometría con fines de identificación (comparación entre un elemento y muchos otros), que se presenta en la propuesta como la futura aplicación de un «motor de búsqueda de datos biométricos», es más delicada, ya que los resultados de este método son menos precisos que los que resultan de la utilización de los datos con fines de autenticación o control (comparación entre dos elementos). Por lo tanto, la identificación biométrica no debería constituir el único método de identificación ni la única clave de acceso a otra información.

— **Procedimiento de emergencia**: Deberán existir procedimientos de emergencia de acceso rápido con el fin de respetar la dignidad de las personas que hayan podido ser identificadas de forma errónea y de evitar que padezcan las imperfecciones del sistema.

La utilización de datos biométricos sin una evaluación previa correcta indica también que se sobrestima la fiabilidad de la biométrica. Los datos biométricos son datos «vivos» que evolucionan con el tiempo, y las muestras que se almacenan en la base de datos sólo son una fotografía instantánea de un elemento dinámico, cuya permanencia no es absoluta y debe comprobarse. La precisión de la biometría siempre debe ponerse en perspectiva con otros elementos, ya que nunca será absoluta.

([1]) El análisis podría fundarse en los denominados «siete pilares de la sabiduría en materia de biometría» en «Biometrics at the frontiers: Assessing the impact on Society» Institute for Prospective Technological Studies, DG Centro Común de Investigación, Comisión Europea, apartado 1.2, página 32.

La posible utilización de los datos del SIS II con fines de investigación presenta graves riesgos para los interesados si se da mayor importancia o una importancia exagerada a las pruebas biométricas, como ya sucedió en casos anteriores ([2]).

Por lo tanto, las propuestas deberían tener en cuenta y subrayar la capacidad real de la biometría a efectos de identificación.

4.2. **Acceso a los datos del SIS II**

4.2.1. *Un nuevo concepto de acceso*

Las autoridades que tienen acceso a los datos del SIS se determinan para cada inscripción. En principio, debe cumplirse una condición doble para conceder el acceso a los datos del SIS: se concederá el acceso a las autoridades en pleno cumplimiento del objetivo general del SIS y además del objetivo específico de cada inscripción.

Así se desprende de la definición de «descripción» que figura en la propuesta de Reglamento y en la propuesta de Decisión (artículo 3 (1) a) de ambos instrumentos: «*inscripción», un conjunto de datos introducidos en el SIS II que permite a las autoridades competentes identificar a una persona o un objeto con vistas a emprender una acción específica)*. El artículo 39 (2) de la propuesta de Decisión confirma este punto: «*Los datos mencionados en el apartado 1 sólo se utilizarán para fines de identificación de personas, con vistas a la acción específica que deberá emprenderse de conformidad con la presente Decisión*». A este respecto, el SIS II conserva las características de un sistema de respuestas positivas o negativas en el cual se introduce cada inscripción para un objetivo particular (entrega, no admisión, etc.).

Las autoridades que pueden acceder a los datos del SIS tienen una utilización de estos datos limitada *de facto*, ya que en principio sólo se accede para emprender una acción específica.

Sin embargo, algunos accesos previstos en las nuevas propuestas rompen con esta lógica, ya que tienen por objeto proporcionar información a las autoridades, y no que éstas puedan identificar a una persona para emprender la acción específica prevista en la inscripción.

([2]) En junio de 2004, un abogado de Portland (Estados Unidos) fue encarcelado durante dos semanas porque el FBI había establecido que sus huellas dactilares correspondían a impresiones encontradas en el marco de los atentados de Madrid (en la bolsa de plástico que contenía el detonador). Finalmente se comprobó que la técnica de comparación era defectuosa y había dado lugar a un error de interpretación.

Concretamente, se trata de los siguientes accesos:

— el acceso de las autoridades competentes en materia de asilo a los datos de inmigración

— el acceso de las autoridades habilitadas para conceder el estatuto de refugiado a los datos de inmigración

— el acceso de Europol a las inscripciones relativas a extradición, vigilancia discreta y documentos robados a efectos de su incautación

— el acceso de Eurojust a los datos relativos a extradición y localización.

Todas estas autoridades presentan las mismas características por lo que se refiere a los datos del SIS II:

no están facultadas para emprender la acción específica contemplada en la definición de la inscripción. Se les concede el acceso para que puedan obtener una información que sirva a sus propios objetivos.

Incluso entre estas autoridades conviene establecer una distinción entre las que tienen acceso con fines propios, pero con un objetivo particular, y aquellas para las cuales no se da ninguna precisión sobre el objetivo del acceso (es decir, Europol y Eurojust). Las autoridades competentes en materia de asilo, por ejemplo, tienen acceso para un objetivo particular, aunque no sea el que se menciona en la inscripción. Pueden tener acceso a los datos de inmigración «a fin de determinar si un solicitante de asilo ha permanecido ilegalmente en otro Estado miembro». En cambio, Europol y Eurojust tienen acceso a los datos contenidos en algunas categorías de inscripciones que sean «necesarios para el cumplimiento de sus cometidos».

En resumen, el acceso a los datos del SIS II se concede en tres casos:

— para dar curso a una descripción

— para un objetivo que no es el del SIS II, pero bien definido en las propuestas

— para un objetivo que no es el del SIS II, pero no definido con precisión.

El SEPD considera que cuanto más general sea el objetivo del acceso, más rigurosas deben ser las garantías que se apliquen. A continuación se detallan las garantías generales, antes de abordar la situación particular de Europol y Eurojust.

4.2.2. *Condiciones para la concesión de acceso*

1. En cualquier caso, sólo puede concederse el acceso si es compatible con el objetivo general del SIS II y conforme a su fundamento jurídico.

   En la práctica, esto significa que el acceso a los datos de inmigración, en el marco de la propuesta de Reglamento, debe apoyar la aplicación de las políticas en materia de libre circulación de personas que forman parte del acervo de Schengen.

   Del mismo modo, el acceso a las inscripciones previsto en la Decisión debe tener como objetivo apoyar la cooperación operativa en materia penal entre servicios de policía y autoridades judiciales.

   A este respecto, el SEPD llama la atención sobre el capítulo relativo al acceso al SIS II por los servicios responsables de la expedición de los certificados de matriculación (véase el apartado 4.6).

2. Es necesario probar la necesidad de acceder a los datos del SIS II, y demostrar que es imposible o muy difícil obtener los datos por otros medios menos lesivos para el derecho a la intimidad. Este punto debería haberse mencionado en una exposición de motivos, cuya ausencia es, como ya se ha subrayado, muy lamentable.

3. Debe definirse de manera explícita y restrictiva el uso que se dará a los datos.

   Por ejemplo, las autoridades competentes en materia de asilo tienen acceso a los datos de inmigración «a fin de determinar si un solicitante de asilo ha permanecido ilegalmente en otro Estado miembro». En cambio, Europol y Eurojust tienen acceso a los datos contenidos en algunas categorías de inscripciones que sean «necesarios para el cumplimiento de sus cometidos», formulación que no es suficientemente precisa (véase más adelante).

4. Las condiciones de acceso deben definirse y delimitarse correctamente. En particular, solamente deben obtener acceso al SIS II los servicios dependientes de dichas organizaciones que deban tratar los datos del SIS II. Esta obligación mencionada al artículo 40 de la Decisión y en el artículo 21 (2) de la propuesta de Reglamento debería completarse con la obligación para las autoridades nacionales de conservar una lista actualizada de las personas autorizadas a acceder al SIS II. La misma norma debería aplicarse a Europol y Eurojust.

5. El hecho de que estas autoridades dispongan de un acceso a los datos del SIS II no podría justificar en ningún caso que introduzcan o conserven en el sistema datos que no sean útiles para la descripción particular de la que forman parte. No pueden añadirse nuevas categorías de datos porque serían útiles a otros sistemas de información. Por ejemplo, el artículo 39 de la propuesta de Decisión prevé la introducción, en las inscripciones, de datos relativos a la autoridad informadora. Estos datos no son necesarios para emprender una acción específica (detención, vigilancia, etc.), y probablemente la única razón que explicaría su introducción es que interesan a Europol o Eurojust. Es necesario justificar con claridad el tratamiento de estos datos.

6. El periodo de conservación de los datos no puede prolongarse cuando no sea necesario para el objetivo para el cual se introdujeron. Esto significa que aunque Europol y Eurojust tengan acceso a los datos, esto no es motivo suficiente para conservarlos en el sistema (por ejemplo, cuando se haya efectuado la extradición de una persona buscada, los datos deberían suprimirse aunque puedan ser útiles a Europol). Una vez más, será necesario un control minucioso para garantizar el respeto de esta norma por las autoridades nacionales.

4.2.3. *Acceso de Europol y Eurojust*

a) *Motivos del acceso*

El acceso de Europol y Eurojust a algunos datos del SIS ya fue objeto de debate antes de quedar instaurado mediante la Decisión del Consejo de 24 de febrero de 2005 ([1]). Frente a las demás autoridades que disponen de acceso para sus propios objetivos, éste se les concede en términos muy generales. Aunque la utilización de los datos se define en el capítulo XII de la Decisión, no están suficientemente detallados los motivos que justifican el propio principio de la atribución de acceso, y esto es tanto más cierto cuanto que es probable que las misiones de Europol y Eurojust evolucionen con el tiempo.

El SEPD insiste en que la Comisión defina de forma restrictiva los cometidos para cuya realización se justificaría el acceso de Europol y Eurojust.

b) *Limitación de los datos*

Con el fin de evitar búsquedas de datos aleatorias (*fishing expeditions*) por parte de Europol y Eurojust, y para asegurarse de que sólo tengan acceso a los datos «necesarios para el cumplimiento de sus cometidos», la Autoridad de Control Común de Schengen sugirió, en su dictamen de 27 de septiembre de 2005 relativo a las propuestas relativas al SIS II, limitar el acceso de Europol y Eurojust a los datos relativos a aquellas personas cuyos nombres ya figuren en sus ficheros. Así se tendría la garantía de que Europol y Eurojust sólo consultan las inscripciones que les conciernen. El SEPD apoya esta recomendación.

c) *Aspectos relativos a la seguridad*

El SEPD acoge favorablemente la obligación de registrar todas las transacciones realizadas por Europol y Eurojust en una conexión, así como la prohibición de copiar o descargar partes del sistema.

El artículo 56 de la propuesta de Decisión establece que Europol y Eurojust definan «uno o dos» puntos de acceso al SIS II cada uno. Aunque es comprensible que un Estado miembro necesite varios puntos de acceso debido a la descentralización de sus autoridades competentes, el estatus y las actividades de Europol y Eurojust no justifican esta demanda. Por otra parte, conviene destacar que, desde el punto de vista de la seguridad, la multiplicación de los puntos de acceso aumenta el riesgo de abusos y debería por lo tanto justificarse mediante elementos más probatorios. Por lo tanto, en ausencia de argumentos convincentes, el SEPD sugiere conceder sólo un punto de acceso a Europol y a Eurojust.

4.3. **Interconexión de las descripciones**

El artículo 26 del Reglamento y el artículo 46 de la Decisión prevén que los Estados miembros puedan interconectar las inscripciones, de acuerdo con su legislación nacional, para establecer un vínculo entre dos o varias inscripciones.

Aunque seguramente puede resultar útil conectar inscripciones con fines de control (una orden de detención relativa a un ladrón de automóviles puede, por ejemplo, vincularse con la descripción de un vehículo robado), la introducción de vínculos entre inscripciones es una característica típica de un instrumento de investigación policial.

La interconexión de inscripciones puede tener repercusiones importantes en los derechos de los interesados, dado que ya no se «evalúa» a estas personas sobre la base de datos que se refieren solamente ellas, sino basándose en su posible asociación con otras personas. Aquellas personas cuyos datos se conectan con los de delincuentes o de personas buscadas pueden ser tratadas con más recelos que otras. Además, la interconexión de inscripciones constituye una ampliación de las competencias de investigación del SIS, ya que esto permitirá introducir presuntas bandas o redes (por ejemplo, si los datos relativos a inmigrantes clandestinos están vinculados a datos relativos a traficantes). Por último, puesto que el establecimiento de vínculos se deja a la legislación nacional, podría ocurrir que un Estado miembro establezca vínculos que son ilegales en otro Estado miembro, lo que alimentaría el sistema con datos «ilegales».

([1]) Decisión 2005/211/JAI del Consejo, de 24 de febrero de 2005, relativa a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo, DO L 68 de 15.3.2005, p. 44.

En las conclusiones del Consejo del 14 de junio de 2004 sobre las exigencias funcionales relativas al SIS II, se precisa que cada vínculo debe tener exigencias funcionales claras, ajustarse al principio de proporcionalidad y basarse en una relación definida con precisión. Además, un vínculo no puede afectar a los derechos de acceso. En cualquier caso, puesto que la interconexión de las inscripciones constituye una operación de tratamiento, debe ajustarse a las disposiciones de la legislación nacional por la que se aplican la Directiva 95/46/CE o el Convenio 108.

Las propuestas recuerdan que la existencia de vínculos no debe afectar en modo alguno a los derechos de acceso (pues, de lo contrario, se concedería el acceso a datos cuyo tratamiento no estaría autorizado por la legislación nacional, vulnerando así el artículo 6 de la Directiva).

El SEPD subraya que es importante interpretar de forma estricta el artículo 26 de la propuesta de Reglamento, así como el artículo 46 de la propuesta de Decisión, y esto puede hacerse, en particular, precisando que las autoridades que no tienen derecho de acceso a determinadas categorías de datos no sólo no podrán acceder a los vínculos hacia estas categorías, sino que ni siquiera deben tener conocimiento de la existencia de estos vínculos. La visualización de los vínculos debe ser imposible cuando no se tiene derecho de acceso a los datos asociados a los mismos.

Además el SEPD desearía ser consultado sobre las medidas técnicas que permiten garantizar este aspecto.

4.4. **Inscripción en la lista de no admisibles**

4.4.1. *Motivos para la inscripción*

La «inscripción de nacionales de terceros países en la lista de no admisibles» (artículo 15 del Reglamento) tiene repercusiones importantes en las libertades individuales. En efecto, a una persona respecto de quien se haya introducido una inscripción en virtud de esta disposición se le prohibirá el acceso al espacio Schengen durante varios años. Hasta ahora, estas descripciones han sido las más utilizadas, en términos de personas descritas. Teniendo en cuenta las consecuencias de estas inscripciones y el número de afectados, conviene ser muy prudente en su concepción y su aplicación. Aunque esto también es válido para otras inscripciones, el SEPD dedica un capítulo específico a estas inscripciones, ya que plantean problemas particulares vinculados a los motivos para su introducción.

La nueva inscripción a efectos de no admisión presenta algunas mejoras con respecto a la situación actual, pero no es enteramente satisfactoria ya que se basa en gran parte en instrumentos que aún no han sido adoptados, o ni siquiera propuestos.

Estas mejoras consisten en una descripción más precisa de los motivos para la introducción de los datos. La formulación actual del Convenio de Schengen ha originado que existan grandes diferencias entre los Estados miembros por lo que se refiere al número de personas descritas en virtud del artículo 96 del mismo. La Autoridad de Control Común de Schengen realizó un estudio completo [1] a este respecto y recomendó que los responsables políticos estudien la posibilidad de armonizar los motivos para la introducción de una inscripción en los distintos Estados Schengen.

El artículo 15 propuesto es más detallado en su formulación, y esto es motivo de satisfacción.

Además, el artículo 15, apartado 2, presenta una lista de los casos en los que no se puede efectuar una inscripción, porque el interesado reside legalmente en el territorio de un Estado miembro en aplicación de distintos estatutos. Aunque este mecanismo podría deducirse del actual Convenio de Schengen, la experiencia ha demostrado que su aplicación difiere según el Estado miembro. Por lo tanto, se acoge con satisfacción esta aclaración.

Sin embargo, esta disposición se presta también a críticas, ya que se basa en gran parte en un texto que aún no se ha adoptado, como es la Directiva sobre «repatriación».

Desde la aprobación de las propuestas relativas al SIS II, la Comisión propuso (el 1 de septiembre de 2005) una «Directiva relativa a procedimientos y normas comunes en los Estados miembros para el retorno de los nacionales de terceros países que se encuentren ilegalmente en su territorio». No obstante, al no ser definitivo, este texto no puede considerarse una base válida para la introducción de datos en el sistema. En particular, constituye una infracción al artículo 8 del Convenio Europeo de Derechos Humanos ya que la intrusión en la vida privada debe basarse, entre otras cosas, en una disposición jurídica clara y accesible.

Por lo tanto, el SEPD insta a la Comisión a que retire o reformule esta disposición, basándola en disposiciones existentes, de tal modo que los interesados puedan saber exactamente qué medidas pueden adoptar las autoridades en su caso.

4.4.2. *Acceso a las inscripciones introducidas con arreglo al artículo 15*

El artículo 18 establece las autoridades que tienen acceso a estas inscripciones, y con qué fin. En los apartados 1 y 2, el artículo 18 precisa las autoridades que tienen acceso a las inscripcionesintroducidas sobre la base de la Directiva relativa a la repatriación. Esta situación provoca el mismo comentario que la anterior.

---

[1] Informe de la Autoridad de Control Común de Schengen acerca de un estudio sobre el recurso a las descripciones del artículo 96 en el Sistema de información Schengen, Bruselas, 20 de junio de 2005

El artículo 18, apartado 3, de la propuesta de Reglamento otorga el acceso a las autoridades habilitadas para la concesión del estatuto de refugiado en virtud de una Directiva que ni siquiera se ha propuesto aún. Ante la falta de texto, el SEPD debe repetir el mismo comentario.

4.4.3. *Periodo de conservación de las inscripciones introducidas con arreglo al artículo 15*

Con arreglo al artículo 20, las inscripciones no se conservarán durante un período superior al período de no admisión establecido en la decisión (de expulsión o retorno). Esta disposición se ajusta a las normas aplicables en materia de protección de datos. Además, las inscripciones se borrarán automáticamente al término del plazo de cinco años, excepto decisión contraria del Estado miembro que introdujera los datos en el SIS II.

Sería necesario garantizar, mediante un control conveniente a nivel nacional, que no se prolongue de forma automática e injustificada el periodo de conservación y que los Estados miembros borren los datos antes del plazo de cinco años si el período de no admisión resulta ser más breve.

4.5. **Periodo de conservación**

Aunque el principio que rige la conservación de las inscripciones no sufre cambios (por regla general, una inscripción debe suprimirse del SIS II cuando se haya realizado la conducta solicitada en la inscripción), las propuestas tendrán como resultado la prolongación general del periodo de conservación de las descripciones.

El Convenio de Schengen establece que se revisará la necesidad de conservar los datos a más tardar tres años después de su introducción (o un año, para los datos introducidos a efectos de vigilancia discreta). Las nuevas propuestas prevén el borrado automático (al que puede oponerse el Estado miembro autor de la inscripción) al término de un periodo de cinco años para los datos de inmigración, de diez años para los datos relativos a las detenciones, a las personas desaparecidas y a las personas buscadas en el marco de procedimientos judiciales, y de tres años para las personas que deban ser objeto de vigilancia discreta.

Aunque, en principio, los Estados miembros deberán borrar los datos cuando se alcance el objetivo de la inscripción, se trata de una prolongación importante del periodo máximo de conservación (en la mayoría de los casos, este periodo se triplica) que la Comisión no justifica de ninguna manera. En el caso de los datos de inmigración, puede suponerse que el periodo de cinco años está vinculado al de la prohibición de readmisión que figura en la propuesta de Directiva relativa a la repatriación. En los demás casos, el SEPD no advierte ningún elemento que justifique esta prolongación.

Las posibles repercusiones para la vida de los interesados de una inscripción en el SIS pueden ser considerables, lo que resulta especialmente preocupante en el caso de las inscripciones de personas a efectos de vigilancia discreta o de control específico, ya que pueden introducirse sobre la base de meras sospechas.

El SEPD desearía que se justificara debidamente la prolongación de los periodos de conservación de los datos. A falta de una justificación convincente, sugiere que se limiten a su duración actual, y subraya en particular el caso de las inscripciones a efectos de vigilancia discreta o de control específico.

4.6. **Acceso de los servicios responsables de la matriculación de vehículos**

El problema principal reside en la elección de una base jurídica más que cuestionable. La Comisión no justifica de forma convincente el recurso a una base jurídica relativa a «transportes» y perteneciente al primer pilar para una medida que permitiría a las autoridades administrativas acceder al SIS con el objetivo de prevenir y luchar contra la delincuencia (tráfico de vehículos robados). La necesidad de una motivación y de una base jurídica sólidas para conceder el acceso al SIS II ya se ha expuesto con detalle en el apartado 4.2.2. del presente dictamen.

El SEPD se remite a las observaciones formuladas a este respecto por la Autoridad de Control Común de Schengen en su dictamen sobre la base jurídica propuesta para el SIS II. En particular, conviene seguir su sugerencia de modificar la propuesta de Decisión para incluir este acceso.

5. **PAPEL DE LA COMISIÓN Y LOS ESTADOS MIEMBROS**

Es absolutamente necesario ser preciso en la descripción y la distribución de las responsabilidades en el marco del SIS II, no sólo para garantizar el correcto funcionamiento del sistema, sino también para su control. El reparto de las competencias en materia de vigilancia se derivará de la descripción de las responsabilidades; por lo tanto, es necesario ser de una precisión absoluta.

5.1. **Papel de la Comisión**

El SEPD se felicita por la presencia en ambas propuestas del capítulo III, donde se describen el papel y las responsabilidades de la Comisión con respecto al SIS II (en su función de «gestión operativa»). Esta aclaración no figuraba en la propuesta sobre el VIS. No obstante, este capítulo no basta por sí solo para hacer una descripción exhaustiva del papel de la Comisión. En efecto, tal como se indica en el capítulo 9 del presente dictamen, la Comisión también participa en la aplicación y la gestión del sistema por medio de la comitología.

En materia de protección de datos, la Comisión desempeña un papel que ya se reconoce en los sistemas VIS y Eurodac, puesto que es responsable de la gestión operativa. Como esta responsabilidad de gestión viene a añadirse al importante papel que le corresponde en el desarrollo y el funcionamiento del sistema, conviene considerar que la Comisión desempeña un papel de supervisor *sui generis*. Como ya se indica en el dictamen del SEPD sobre el VIS, este papel va mucho más allá del tratamiento de los datos, y al mismo tiempo es más limitado que el de un supervisor normal, puesto que la Comisión no tiene acceso a los datos tratados en el SIS II.

Dado que el SIS II estará basado en sistemas complejos, algunos de los cuales se basan en tecnologías emergentes, el SEPD insiste en que se refuerce la responsabilidad de la Comisión en la mejora constante de los sistemas mediante la aplicación de las mejores tecnologías disponibles en materia de seguridad y protección de los datos.

Por lo tanto, en el artículo 12 de las propuestas conviene añadir que la Comisión debería proponer regularmente la aplicación de nuevas tecnologías que sean las más avanzadas en este ámbito y que permitan reforzar la protección de los datos y el nivel de seguridad, facilitando al mismo tiempo la tarea de las autoridades nacionales que tienen acceso a estos datos.

5.2. **Papel de los Estados miembros**

La situación no queda muy clara por lo que se refiere a los Estados miembros, ya que resulta difícil saber qué autoridad o autoridades asumirán la función de supervisor de los datos.

Las propuestas describen el papel de las Oficinas nacionales del SIS II (para garantizar el acceso de las autoridades competentes al SIS II) así como el de las autoridades SIRENE (encargadas de intercambiar toda la información suplementaria). Los Estados miembros también deben garantizar el funcionamiento y la seguridad de su sistema nacional (NS). No se dice claramente si esta última responsabilidad debe incumbir a una de las autoridades previamente mencionadas. En cualquier caso, es necesario aportar precisiones al respecto.

Por lo que se refiere a la protección de los datos, la Comisión y los Estados miembros deberían ser considerados como supervisor es conjunto, cada uno con sus propias responsabilidades. Constatar esta complementariedad en términos de responsabilidades es el único medio para evitar que uno u otro aspecto de las actividades del SIS II escape al control.

6. **DERECHOS DE LOS INTERESADOS**

6.1. **Información**

6.1.1. *Propuesta de Reglamento*

El artículo 28 de la propuesta de Reglamento prevé el derecho del interesado a la información, que se deriva principalmente del artículo 10 de la Directiva 95/46/CE. Se trata de un cambio bienvenido con relación a la situación actual, en la que no está previsto el derecho a la información explícitamente en el Convenio. No obstante, aún se podrían mejorar las cosas, tal como se indica a continuación.

Debería añadirse alguna información a la lista, lo que contribuiría a garantizar un tratamiento equitativo de los interesados ([1]). Esta información debería referirse al periodo de conservación de los datos, la existencia del derecho a solicitar una revisión o a recurrir la decisión de introducir la inscripción (en algunos casos, véase el artículo 15.3 de la propuesta de Reglamento), la posibilidad de obtener asistencia de la autoridad encargada de la protección de los datos, así como la existencia de vías de recurso.

La propuesta de Reglamento no menciona en ningún momento cuándo debe comunicarse la información. Esto podría impedir al interesado el ejercicio de sus derechos. Para que éstos sean efectivos, el Reglamento debería prever en qué momento preciso debe proporcionarse la información, según la autoridad que haya introducido la descripción.

Una solución práctica consistiría en primer lugar en añadir información sobre la inscripción en la decisión que la justifica: una decisión judicial o administrativa, fundada en una amenaza para orden público o la seguridad (…), una decisión de retorno o una orden de expulsión acompañada de una prohibición de regreso, y debería añadirse en el artículo 28 del Reglamento.

6.1.2. *Propuesta de Decisión*

El artículo 50 de la Decisión estipula que se dará información a petición del interesado y cita los motivos que pueden alegarse para negarse a comunicar esta información. Sin duda es perfectamente comprensible que este derecho se someta a algunos límites, teniendo en cuenta la naturaleza de los datos y el contexto en el que se tratan.

No obstante, el derecho a la información no debería supeditarse a una petición del interesado (se trataría en este caso de un derecho de acceso). Se puede suponer que la necesidad de una «solicitud» de información se explica por la posibilidad de que no pueda informarse a un interesado porque no se le localiza.

Esta cuestión podría solucionarse incluyendo una cláusula de excepción al derecho a la información en caso de que la comunicación de la información resulte imposible o implique un esfuerzo desproporcionado. Procede modificar el artículo 50 en este sentido.

([1]) En este mismo sentido, véase el dictamen del SEPD sobre la creación del Sistema de Información de Visados, apartado 3.10.1.

Esta solución se ajustaría también a la aplicación del proyecto de Decisión marco sobre la protección de los datos en el marco del tercer pilar.

6.2. **Acceso**

Las propuestas de Reglamento y Decisión establecen ambas plazos para responder a las solicitudes de acceso, lo que constituye una evolución positiva. Sin embargo, dado que el procedimiento para ejercer el derecho de acceso se fija a nivel nacional, cabe plantearse cómo pueden adaptarse los plazos impuestos en estas propuestas a los procedimientos existentes, en particular cuando los Estados miembros establezcan plazos de respuesta más breves. Sería necesario precisar claramente que procede aplicar los plazos más favorables al interesado.

6.2.1. *Propuesta de Reglamento*

Es interesante tener en cuenta que las restricciones al derecho de acceso que existen actualmente en el Convenio de Schengen (no se facilitará la información cuando «pueda ser perjudicial para la ejecución de una tarea legal relacionada con datos introducidos en el SIS II o para la protección de los derechos y libertades de la persona interesada o de terceros») no figuran en la propuesta de Reglamento.

Sin embargo, esto se debe probablemente a la aplicabilidad de la Directiva 95/46/CE, que establece (en su artículo 13) posibilidades de introducir excepciones en el Derecho nacional. En cualquier caso, conviene destacar que el recurso al artículo 13 en el Derecho nacional para limitar el derecho de acceso siempre debe hacerse en cumplimiento del artículo 8 del CEDH, y sólo en casos limitados.

6.2.2. *Propuesta de Decisión*

La propuesta de Decisión recoge las restricciones del derecho de acceso que están previstas en el Convenio de Schengen. La propuesta de Decisión marco contiene en esencia los mismos límites al derecho de acceso; por lo tanto la adopción de este instrumento no aportaría ninguna diferencia notable sobre este punto.

Teniendo en cuenta que, en varios Estados miembros, el acceso a los datos de las fuerzas de seguridad es «indirecto» (es decir, se realiza a través de la autoridad nacional encargada de la protección de los datos), sería conveniente establecer que las autoridades encargadas de la protección de los datos deberán cooperar de forma activa en el ejercicio del derecho de acceso.

6.3. **Derecho de revisión o recurso de la decisión de introducir una descripción**

El apartado 3 del artículo 15 del Reglamento establece el derecho a obtener la revisión o a interponer un recurso ante una autoridad judicial respecto a la decisión de introducir una descripción adoptada por una autoridad administrativa. Este añadido con relación al actual Convenio de Schengen se acoge con satisfacción.

Se subraya así la necesidad de informar al interesado completa y rápidamente, tal como se indica en el apartado 6.1 *supr.*: sin esta información, este nuevo derecho seguiría siendo teórico.

6.4. **Vías de recurso**

El artículo 30 de la propuesta de Reglamento y el artículo 52 de la propuesta de Decisión establecen el derecho del interesado a interponer un recurso o a presentar una denuncia ante los órganos jurisdiccionales de un Estado miembro si se le deniega el derecho a acceder a los datos que le conciernen, rectificarlos o borrarlos, o el derecho a obtener información o reparación.

Los términos («Toda persona… en el territorio de cualquier Estado miembro») sugieren que el demandante debe encontrarse físicamente en el territorio para poder interponer recurso ante un órgano jurisdiccional. Esta restricción territorial no se justifica y podría vaciar de contenido el derecho a ejercer vías de recurso puesto que, con frecuencia, el interesado tiene que interponer una demanda precisamente porque no obtiene acceso al territorio Schengen. Además, por lo que se refiere a la propuesta de Reglamento, dado que la Directiva es *la lex generalis*, es necesario tener en cuenta su artículo 22, que establece que «toda persona» puede interponer un recurso jurisdiccional, independientemente de su lugar de residencia. La propuesta de Decisión marco tampoco implica una restricción territorial. El SEPD sugiere que se renuncie a la restricción territorial que figura en el artículo 30 y en el artículo 52 antes citados.

7. **CONTROL**

7.1. **Introducción: reparto de responsabilidades**

Las propuestas reparten la misión de control entre las autoridades de control nacionales [1] y el SEPD, según su ámbito de competencias, de acuerdo con el enfoque adoptado en las propuestas respecto a la legislación aplicable y a las responsabilidades relativas al funcionamiento y al uso del SIS II, así como a la necesidad de un control efectivo.

Por lo tanto, el SEPD se congratula por este enfoque, especificado en el artículo 31 de la propuesta de Reglamento y en el artículo 53 de la propuesta de Decisión. Sin embargo, para comprender mejor y precisar las tareas respectivas, el SEPD sugiere que se subdivida cada uno de estos artículos en varias disposiciones consagradas cada una a un nivel de control, como se hizo en la propuesta VIS.

[1] También participan las autoridades de control de Europol y Eurojust, pero en menor medida.

7.2. **Control por parte de las autoridades nacionales encargadas de la protección de datos**

Según el artículo 31 de la propuesta de Reglamento y el artículo 53 de la propuesta de Decisión, cada Estado miembro deberá velar por que una autoridad independiente controle la legalidad del tratamiento de los datos personales del SIS II.

Por otro lado, el artículo 53 de la propuesta de Decisión establece que cualquier persona tendrá derecho a solicitar a la autoridad de control que compruebe la legalidad del tratamiento de datos que se refieran a ella. No se ha introducido una disposición similar en la propuesta de Reglamento ya que la Directiva se aplica como *una lex generalis*. Por lo tanto, es necesario considerar que las autoridades nacionales encargadas de la protección de los datos pueden ejercer, respecto al SIS II, todas las competencias que les confiere el artículo 28 de la Directiva 95/46/CE, incluida la comprobación de la legalidad de una operación de tratamiento de datos. El artículo 31, apartado 1, del Reglamento describe su misión, pero no puede constituir una restricción de estos poderes. Debería precisarse claramente en el texto de la propuesta de Reglamento el reconocimiento de estas competencias.

En cuanto a la propuesta de Decisión, encomienda tareas más amplias a las autoridades de control nacionales porque su *lex generalis* es diferente. Sin embargo, no sería sensato que las autoridades de control tuvieran tareas y competencias diferentes en función de la categoría de los datos tratados, ya que en la práctica esto sería muy difícil de gestionar. Por lo tanto, conviene evitar esta situación, bien concediendo a estas autoridades los mismos poderes en el texto de la propuesta de decisión, bien remitiéndose a otra *lex generalis* (la Decisión marco relativa a la protección de datos en el marco del tercer pilar) que confiera más competencias a las autoridades encargadas de la protección de datos.

7.3. **Supervisión por parte del SEPD**

El SEPD supervisa que las actividades de tratamiento de datos de la Comisión se realicen en cumplimiento de los textos de las propuestas. Del mismo modo, debería poder ejercer todas las competencias que le atribuye el Reglamento 45/2001, teniendo en cuenta, no obstante, los poderes limitados que tiene la Comisión con respecto a los mismos datos.

Conviene añadir que, de conformidad con lo dispuesto en el artículo 46, letra f), del Reglamento 45/2001, el SEPD cooperará con las autoridades de control nacionales «en la medida necesaria para el ejercicio de sus deberes respectivos». La cooperación con los Estados miembros para el control del SIS II no se deriva solamente de las propuestas, sino también del Reglamento 45/2001.

7.4. **Control conjunto**

Las propuestas reconocen también la necesidad de coordinar las actividades de control de las distintas autoridades interesadas. El artículo 31 de la propuesta de Reglamento y el artículo 53 de la propuesta de Decisión disponen que las autoridades de control nacionales y el Supervisor Europeo de Protección de Datos «colaborarán entre sí. A tal fin, el Supervisor Europeo de Protección de Datos convocará una reunión al menos una vez al año.»

El SEPD acoge con satisfacción esta propuesta, que contiene en esencia los elementos necesarios para establecer la cooperación, realmente indispensable, entre las autoridades encargadas del control a nivel nacional y a nivel europeo. Conviene destacar que la reunión anual prevista en las propuestas debe ser considerada como un mínimo.

Sin embargo, estas disposiciones (el artículo 31 de la propuesta de Reglamento y el artículo 53 de la propuesta de Decisión) mejorarían si se aclarara el contenido de esta coordinación. La autoridad de control común existente es competente para examinar las dificultades de interpretación o aplicación del Convenio, para estudiar los problemas que puedan plantearse en el ejercicio de un control independiente o de un derecho de acceso, y para elaborar propuestas armonizadas que ofrezcan soluciones comunes a los problemas existentes.

Las nuevas propuestas no pueden resultar en una reducción del ámbito de aplicación actual del control común. Si bien no cabe duda de que las autoridades encargadas de la protección de datos pueden ejercer respecto al SIS II todas las competencias de control que les confiere la Directiva, la cooperación entre estas autoridades puede cubrir amplios aspectos del control del SIS II, incluidas las tareas desempeñadas por la autoridad de control común existente de conformidad con lo dispuesto en el artículo 115 del Convenio de Schengen.

No obstante, para que esto quede completamente claro, sería conveniente repetirlo explícitamente en el texto de las propuestas.

8. **SEGURIDAD**

La gestión y el mantenimiento de un nivel de seguridad óptimo para el SIS II constituye una exigencia fundamental para garantizar una protección suficiente de los datos personales almacenados en la base de datos. Para alcanzar este nivel satisfactorio de protección, es necesario establecer mecanismos de protección adecuados para hacer frente a los riesgos potenciales vinculados a la infraestructura del sistema y a las personas interesadas. Esta cuestión se aborda actualmente en distintos capítulos de la propuesta y requiere algunas mejoras.

Los artículos 10 y 13 de la propuesta abordan distintas medidas destinadas a garantizar la seguridad de los datos y enumeran los tipos de abuso que es necesario prevenir. El SEPD se congratula por la inclusión en estos artículos de disposiciones relativas al (auto) control sistemático de las medidas de seguridad.

Sin embargo, el artículo 59 de la propuesta de Decisión y el artículo 34 de la propuesta de Reglamento, que tratan sobre el seguimiento y la evaluación, no deberían referirse únicamente a los aspectos de producción, rentabilidad y calidad de los servicios, sino también al respeto de las condiciones jurídicas, en particular en el ámbito de la protección de datos. Por lo tanto, el SEPD recomienda que el ámbito de aplicación de estos artículos se amplíe al seguimiento y la elaboración de informes sobre la legalidad del tratamiento.

Además, como complemento a las disposiciones del artículo 10.1.f), o del artículo 18 de la propuesta de Decisión, y del artículo 17 de la propuesta de Reglamento sobre el acceso a los datos de las personas debidamente autorizadas, los Estados miembros (así como Europol y Eurojust) deberían también velar por que fueran accesibles perfiles de usuarios concretos (puestos a disposición de las autoridades de control nacionales para efectuar comprobaciones). Además de estos perfiles de usuarios, los Estados miembros deberán elaborar y actualizar permanentemente la lista completa de las identidades de los usuarios. Esto se aplica también *mutatis mutandis* a la Comisión.

Las medidas de seguridad mencionadas se completan mediante garantías en materia de seguimiento y organización. El artículo 14 de ambas propuestas define las condiciones y la finalidad del registro de todas las operaciones de tratamiento de datos efectuadas. Estos registros deben conservarse no sólo a efectos de seguimiento en materia de protección de datos y para garantizar la seguridad de los datos, sino también para autocontrol regular del SIS II que establece el artículo 10. Los informes de autocontrol contribuirán a que las autoridades de control cumplan con eficacia su misión de percibir los puntos débiles y se centren en ellos durante su propio procedimiento de comprobación.

Como ya se ha expuesto en el presente dictamen, la multiplicación de los puntos de acceso al sistema debe justificarse rigurosamente ya que aumenta automáticamente los riesgos de abuso. Por lo tanto el artículo 4.1.b), de las propuestas debería exigir que se demuestre concretamente la necesidad de un segundo punto de acceso.

Las propuestas no explican claramente la necesidad de copias nacionales del sistema central y levantan una seria inquietud sobre el nivel general de riesgo y la seguridad del sistema:

— la multiplicación de las copias aumenta el riesgo de abuso (teniendo en cuenta, en particular, la presencia de nuevos tipos de información, como los datos biométricos);

— no se definen claramente los datos a los que afectan estas copias;

— las exigencias de exactitud, calidad y disponibilidad mencionadas en el artículo 9 representan un reto técnico considerable e implican por lo tanto un aumento del coste vinculado al estado actual de la tecnología disponible;

— el control de estas copias por parte de las autoridades nacionales requerirá recursos humanos y financieros adicionales que podrían no estar disponibles todavía.

Considerando los riesgos que entrañan, el SEPD no está convencido ni de la necesidad de realizar copias nacionales (teniendo en cuenta las tecnologías disponibles), ni de las ventajas que su utilización pudiera tener. Recomienda que se suprima la posibilidad de que los Estados miembros utilicen copias nacionales.

No obstante, si debieran realizarse copias nacionales, el SEPD recuerda que su utilización a nivel nacional debe obedecer al principio de estricta limitación de la finalidad. Del mismo modo, la copia nacional no podrá consultarse según modalidades diferentes de las de la base de datos central.

La legalidad de una operación de tratamiento de datos personales se basa en el estricto respeto de la seguridad y la integridad de los datos. El SEPD efectuará un control eficaz sobre este tratamiento si puede controlar no sólo la seguridad de los datos, sino también su integridad mediante el examen de los registros de actividades (*logs*) disponibles. Por lo tanto, en el artículo 14, apartado 6, es necesario añadir «la integridad de los datos».

9. **COMITOLOGÍA**

Las propuestas prevén el recurso a la comitología en varios casos en los que deban adoptarse decisiones de carácter tecnológico para la aplicación o la gestión del SIS II. Tal como se indica en el dictamen sobre el VIS y por las mismas razones, estas decisiones tendrán una incidencia determinante en la aplicación adecuada de los principios de finalidad y proporcionalidad.

El SEPD recomienda que las decisiones que tengan una incidencia significativa en la protección de los datos, como las relativas al acceso a los datos o a su introducción, el intercambio de información adicional, la calidad de los datos y la compatibilidad entre descripciones y la conformidad técnica de las copias nacionales se adopten mediante un Reglamento o una Decisión, preferiblemente en el marco de un procedimiento de codecisión [1].

[1] En este mismo sentido, véase el apartado 3.12 del dictamen del SEPD sobre el Sistema de Información de Visados, y el apartado 60 del dictamen del SEPD sobre la propuesta de Directiva relativa a la conservación de datos tratados en el marco del suministro de servicios de comunicaciones electrónicos accesibles al público, de fecha 26 de septiembre de 2005.

Para las demás situaciones que tengan repercusiones en la protección de datos, el SEPD debería tener la posibilidad de formular un dictamen sobre las decisiones adoptadas por los comités.

En los artículos 60 y 61 de la Decisión y en el artículo 35 del Reglamento debería mencionarse el papel consultivo del SEPD.

En el caso más específico de las disposiciones técnicas que regulan la interconexión de inscripciones (artículo 26 del Reglamento y artículo 46 de la Decisión), es necesario explicar la necesidad de comitologías diferentes (consultiva en la Decisión y reglamentaria en el Reglamento).

10. **INTEROPERABILIDAD**

En ausencia de la Comunicación de la Comisión sobre la interoperabilidad de los sistemas emergentes de UE, resulta difícil evaluar correctamente las ventajas que entrañarían las sinergias previstas pero aún no precisadas.

A este respecto, el SEPD se remite a la Declaración del Consejo de 25 de marzo de 2004 sobre la lucha contra el terrorismo, en la que el Consejo solicita a la Comisión que presente propuestas destinadas a aumentar la interoperabilidad de las bases de datos europeas y a prever la creación de sinergias entre los sistemas de información actuales y futuros (SIS, VIS y EURODAC). Se remite también al debate en curso acerca del organismo al que podría encomendarse en el futuro la gestión de los distintos sistemas a gran escala (véase también a este respecto el apartado 3.8. del presente dictamen).

El SEPD ya declaró en su dictamen sobre el Sistema de Información de Visados que una condición previa fundamental y determinante para garantizar la eficacia de la explotación a gran escala de sistemas informáticos como el SIS II es garantizar la interoperabilidad, que permite reducir considerablemente el coste global y evitar las duplicaciones de elementos dispares.

— La interoperabilidad también puede contribuir a alcanzar el objetivo de mantener un alto nivel de seguridad en un espacio sin controles en las fronteras interiores entre Estados miembros mediante la aplicación de normas de procedimiento idénticas a todos los elementos de esta política. Sin embargo, es fundamental distinguir dos niveles de interoperabilidad:

  — es muy deseable garantizar la interoperabilidad de los sistemas de los Estados miembros de la UE; en efecto, las descripciones transmitidas por las autoridades de un Estado miembro deben ser compatibles con las que transmiten las autoridades de cualquier otro Estado miembro;

  — por el contrario, la conveniencia de garantizar la interoperabilidad entre sistemas que tienen fines diferentes, o con los sistemas de países terceros, es mucho más cuestionable.

Una de las precauciones que pueden tomarse para limitar el objetivo del sistema y evitar las desviaciones de uso consiste en utilizar normas tecnológicas diferentes. Además, toda forma de interacción entre dos sistemas distintos debería ser objeto de una documentación completa. La interoperabilidad no debería servir para que una autoridad no habilitada a consultar o explotar determinados datos pueda acceder a ellos por medio de otro sistema informático. Por ejemplo, según parece desprenderse de las propuestas, en los primeros años el SIS II no contendrá un sistema automático de identificación dactilar (SAID); sólo se menciona la creación de un futuro motor de búsqueda biométrico. Si se prevé que pueda utilizarse un SAID a partir de otros sistemas de UE, éste debería ser objeto de una descripción clara y tener en cuenta las precauciones que requieren este tipo de sinergias.

El SEPD desea subrayar una vez más que la interoperabilidad de los sistemas no puede instaurarse vulnerando el principio de restricción de la finalidad, y que cualquier propuesta sobre esta cuestión deberá serle presentada.

11. **RESUMEN DE LAS CONCLUSIONES**

11.1. **Observaciones de carácter general**

1. El SEPD acoge con satisfacción varios aspectos positivos de estas propuestas que, en determinados puntos, representan un progreso con relación a la situación actual. Reconoce que las disposiciones relativas a la protección de los datos se han redactado, en general, con gran cuidado.

2. El SEPD subraya que, a pesar de su complejidad, el nuevo régimen jurídico debería:

   — garantizar un elevado nivel de protección de los datos;

   — ser fiable tanto para los ciudadanos como para las autoridades que comparten sus datos;

   — ser coherente en su aplicación en distintos contextos (primer o tercer pilar).

3. Además, la adición de nuevos elementos al SIS II que aumentan su posible incidencia en la vida de las personas debería ir acompañada de medidas de salvaguardia más restrictivas, descritas en el dictamen. En concreto:

— no podrá concederse el acceso a los datos del SIS II a nuevas autoridades si no se justifica de forma rigurosa. Conviene también limitar este acceso en la medida de lo posible, tanto por lo que se refiere a los datos accesibles como a las personas autorizadas;

— la interconexión de las descripciones no podrá originar, siquiera indirectamente, una modificación de los derechos de acceso;

— una medida legislativa no adoptada no puede considerarse un motivo válido para introducir datos en el SIS II (inscripciones en la lista de no admisibles);

— procede volver a examinar la base jurídica para el acceso de las autoridades encargadas de expedir certificados de matriculación de vehículos, ya que este acceso está destinado principalmente a luchar contra la delincuencia;

— el SEPD reconoce que la utilización de los datos biométricos puede mejorar las prestaciones del sistema y ayudar a las víctimas de una usurpación de identidad. No obstante, parece que las incidencias de su introducción en el sistema no se han analizado de forma exhaustiva y que se ha sobrestimado la fiabilidad de estos datos.

11.2. **Observaciones particulares**

1. El SEPD se felicita de que la Comisión reconozca que el Reglamento (CE) nº 45/2001 se aplica a todas las actividades de tratamiento de datos de la Comisión en el SIS II, ya que esto contribuirá a garantizar una aplicación coherente y homogénea de las normas relativas a la protección de los derechos y libertades fundamentales respecto al tratamiento de los datos personales.

2. Para garantizar una limitación estricta del objetivo a nivel nacional, el SEPD recomienda introducir en las propuestas sobre el SIS II (concretamente en el artículo 21 de Reglamento y en el artículo 40 de la Decisión) disposiciones que tengan el mismo efecto que el actual artículo 102.4 del Convenio de Schengen, que limita las posibilidades de que los Estados miembros puedan hacer un uso de los datos que no esté previsto en los textos relativos al SIS II.

3. Para conceder el acceso a los datos del SIS II a cualquier autoridad deberán cumplirse condiciones estrictas, es decir:

— el acceso deberá ser compatible con el objetivo general del SIS II y conforme a su fundamento jurídico;

— deberá demostrarse la necesidad de acceder a los datos del SIS II;

— deberá precisarse explícitamente y de manera restrictiva la utilización que se hará de los datos;

— deberán definirse y limitarse las condiciones de acceso. En particular, debería existir una lista actualizada de las personas habilitadas para acceder al SIS II, incluso para Europol y Eurojust;

— la atribución del acceso al SIS II a estas autoridades no puede justificar en ningún caso el hecho de que introduzcan en el sistema o actualicen datos que no sean útiles para la descripción concreta de la que son parte;

— el periodo de conservación de los datos no podrá prolongarse cuando no sea necesario para los fines para los cuales se introdujeron estos datos.

4. En el caso particular de Europol y Eurojust, el SEPD insta a la Comisión a que defina de manera restrictiva las tareas cuya realización justificaría el acceso al SIS II. Por otro lado, el acceso de Europol y Eurojust debería limitarse a los datos relativos a aquellas personas cuyo nombre ya figura en sus expedientes. Se sugiere también que se conceda sólo un punto de acceso por lo que se refiere a Europol y Eurojust.

5. Por lo que se refiere a las descripciones que tienen por objeto la no admisión, las disposiciones basadas en medidas legislativas aún no adoptadas deberían bien retirarse, bien volver a formularse para que los interesados puedan saber, sobre la base de la legislación vigente, qué medidas pueden adoptar las autoridades exactamente con respecto a ellos.

6. Los períodos de conservación de los datos se han alargado sin aportar ninguna justificación seria. A falta de una motivación convincente, deberían recuperar su duración actual, en particular por lo que se refiere a las descripciones a efectos de vigilancia discreta o de controles específicos.

7. El papel de la Comisión se describe como el de responsable de la gestión operativa. Junto a la parte esencial que le corresponde en el desarrollo y el mantenimiento del sistema, debe considerarse como un papel de supervisor *sui generis*. Es una función que va mucho más allá del simple tratamiento, pero que también es más limitada que la de un supervisor ordinario, dado que la Comisión no tiene acceso a los datos tratados en el SIS II.

   En el marco de este papel, conviene añadir en el artículo 12 de ambas propuestas que la Comisión debería proponer regularmente la aplicación de nuevas tecnologías que representen el estado de la técnica en este ámbito, y que mejoren el nivel de protección de los datos y de seguridad.

8. Con respecto al papel de los Estados miembros, es necesario precisar qué autoridades asumen las funciones de supervisores.

9. En cuanto a la información sobre la persona en cuestión:

   — en la propuesta de Reglamento, procede añadir a la lista una serie de elementos de información: el período de conservación de los datos, la existencia del derecho a solicitar una revisión o de recurrir la decisión de introducir una descripción, la posibilidad de obtener asistencia de la autoridad encargada de la protección de los datos, así como la existencia de vías de recurso.

     Además, por lo que se refiere al momento en que se comunica esta información, sería necesario añadir la obligación de proporcionar información sobre la descripción, en la decisión en la que esté basada en primer lugar;

   — en la propuesta de Decisión, conviene modificar el artículo 50 para no supeditar el derecho a la información a una petición del interesado.

10. Se acoge favorablemente el establecimiento en las propuestas de plazos de respuesta a una solicitud de acceso. Pero procede precisar que, cuando el Derecho nacional fije también plazos, deberían aplicarse los más favorables al interesado.

    Además, sería conveniente establecer la obligación de que las autoridades encargadas de la protección de los datos cooperen de forma activa en el ejercicio del derecho de acceso.

11. Acerca del derecho de recurso, el SEPD sugiere suprimir la limitación territorial que figura en los artículos 30 y 52.

12. En lo relativo a las competencias de las autoridades nacionales encargadas de la protección de los datos:

   — en el Reglamento: es necesario prever que puedan ejercer respecto al SIS II todas las competencias que les confiere el artículo 28 de la Directiva 95/46/CE, y que se precise en el texto de la propuesta de Reglamento;

   — en la propuesta de Decisión: deberían concederse a las autoridades de control las mismas competencias que en el Reglamento y la Directiva.

13. A propósito de las competencias del SEPD: éste debería poder ejercer todas las competencias que le atribuye el Reglamento 45/2001, teniendo en cuenta, no obstante, los poderes limitados de la Comisión respecto a los mismos datos.

14. Con respecto al control coordinado: las propuestas también reconocen la necesidad de coordinar las actividades de control que ejercen las distintas autoridades interesadas. El SEPD se congratula de que contengan, en esencia, los elementos necesarios para establecer una cooperación entre las autoridades encargadas del control a nivel nacional y europeo. Sin embargo, estas disposiciones (artículo 31 de la propuesta de Reglamento y artículo 53 de la propuesta de Decisión) mejorarían si se aclarara el contenido de esta coordinación.

15. Los artículos 10 y 13 de la propuesta contienen distintas medidas en materia de seguridad de los datos; se acoge con satisfacción la inclusión de disposiciones relativas al (auto) control sistemático de las medidas de seguridad.

   — No obstante, el artículo 59 de la propuesta de Decisión y el artículo 34 de la propuesta de Reglamento, que tratan del control y la evaluación, no deberían referirse solamente a los aspectos relativos a la producción, la rentabilidad y la calidad de los servicios, sino también al respeto de las condiciones jurídicas, en particular en el ámbito de la protección de datos. Estas disposiciones deberían modificarse en este sentido.

   — Además, conviene completar el artículo 10.1.f) de la propuesta de Decisión y el artículo 17 de la propuesta de Reglamento añadiendo que los Estados miembros, Europol y Eurojust deberían velar por que sean accesibles determinados perfiles de usuarios (puestos a disposición de las autoridades de control nacionales para efectuar comprobaciones). Además de estos perfiles de usuarios, los Estados miembros deberán elaborar y actualizar permanentemente la lista completa de las identidades de los usuarios. Eso se aplica también a la Comisión.

   — La legitimidad de una operación de tratamiento de datos personales se basa en el estricto respeto de la seguridad y la integridad de los datos. El SEPD debería estar habilitado para comprobar no sólo la seguridad de los datos, sino también su integridad mediante el examen de los registros de actividades (*logs*) disponibles. Por lo tanto, conviene añadir «la integridad de los datos» en el artículo 14, apartado 6.

16. La utilización de copias nacionales es una fuente potencial de numerosos riesgos adicionales. El SEPD no está convencido ni de la necesidad de utilizar copias nacionales (teniendo en cuenta las tecnologías disponibles), ni de las ventajas que puedan aportar. Recomienda que se evite o al menos limite considerablemente la posibilidad de que los Estados miembros utilicen copias nacionales. Sin embargo, si éstas deben crearse, es necesario aplicar el principio de estricta restricción de la finalidad a su utilización a nivel nacional. Del mismo modo, la copia nacional no podrá en ningún caso consultarse según modalidades distintas a las fijadas para la base de datos central.

17. Acerca de la comitología: las decisiones que tengan una incidencia considerable en la protección de los datos deberían adoptarse por medio de un reglamento o una decisión, preferiblemente mediante un procedimiento de codecisión. Si se utiliza efectivamente el procedimiento de comitología, conviene mencionar el papel consultivo del SEPD en los artículos 60 y 61 de la Decisión y en el artículo 35 del Reglamento.

18. La interoperabilidad de los sistemas no puede aplicarse vulnerando el principio de restricción de la finalidad, y cualquier propuesta sobre este tema deberá presentarse al SEPD.

Hecho en Bruselas, el 19 de octubre de 2005.

Peter HUSTINX

Supervisor Europeo de Protección de Datos