

DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Propuesta de Decisión del Consejo sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades de los Estados miembros responsables de la seguridad interior y por Europol, con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves (COM(2005) 600 final)

(2006/C 97/03)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

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

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

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

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

Vista la solicitud de dictamen de conformidad con lo dispuesto en el artículo 28, apartado 2 del Reglamento (CE) nº 45/2001, presentada por la Comisión y recibida el 29 de noviembre de 2005,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1. INTRODUCCIÓN

1.1. Observación preliminar

La Propuesta de Decisión del Consejo sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades de los Estados miembros responsables de la seguridad interior y por Europol, con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves (en lo sucesivo «la propuesta») fue remitida por la Comisión al Supervisor Europeo de Protección de Datos (SEPD) mediante carta de 24 de noviembre de 2005. El SEPD entiende esta carta como una petición de asesoramiento a las instituciones y órganos comunitarios, tal y como está previsto en el

artículo 28, apartado 2 del Reglamento (CE) nº 45/2001. Según el SEPD, el presente dictamen deberá mencionarse en el preámbulo de la Decisión.

El SEPD considera importante dictaminar sobre este asunto sensible dado que esta propuesta sigue directamente la instauración del VIS, que será sometido a su supervisión y sobre la que ya emitió dictamen el 23 de marzo de 2005⁽¹⁾. En ese dictamen, ya se previó la hipótesis de acceso por parte de las autoridades policiales (véase más abajo); la creación de nuevos derechos de acceso al VIS repercutirá de manera determinante en el sistema en lo que se refiere a la protección de datos. Por ello, el hecho de dictaminar sobre la presente propuesta es una continuación necesaria del primer dictamen.

1.2. Importancia de la propuesta

a) Contexto

La presente propuesta no es importante sólo por sí misma, sino también por incluirse dentro de la tendencia general de conceder a las autoridades policiales el acceso a varios sistemas de información e identificación de amplio alcance. Lo anterior se menciona, entre otras cosas, en la Comunicación de la Comisión de 24 de noviembre de 2005 sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas en el ámbito de la Justicia y los Asuntos de Interior⁽²⁾, especialmente en su punto 4.6: «Por lo que se refiere al objetivo de luchar contra el terrorismo y la delincuencia, el Consejo considera ahora como una deficiencia la falta de acceso de las autoridades responsables de la seguridad interior a los datos del VIS. Se podría hacer la misma observación con respecto a los datos de inmigración contenidos en el SIS II y a los datos EURODAC».

Por ello, la presente propuesta podría considerarse como un precursor de instrumentos jurídicos análogos desarrollados dentro del contexto de otras bases de datos, por lo que resulta fundamental definir desde el principio los casos en los que podrá admitirse ese acceso.

⁽¹⁾ Dictamen del Supervisor Europeo de Protección de Datos sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (COM(2004)835 final).

⁽²⁾ COM (2005) 597 final.

b) *Impacto de un nuevo acceso al VIS*

El SEPD reconoce sin duda la necesidad de que las autoridades policiales aprovechen los mejores instrumentos que sea posible para identificar a los autores de actos terroristas u otros delitos graves. También es consciente de que los datos del VIS pueden suponer, en determinadas circunstancias, una fuente esencial de información para esas autoridades.

Con todo, la concesión de acceso a bases de datos del primer pilar a los organismos policiales, por más que esté justificada en la lucha contra el terrorismo, dista mucho de carecer de importancia. Debemos tener presente que el VIS es un sistema de información desarrollado para la aplicación de la política europea de visados y no como instrumento policial. Un acceso habitual significaría de hecho una importante violación del principio de limitación de la finalidad. Supondría una intromisión desproporcionada en la privacidad de los viajeros que aceptan que se traten sus datos para obtener un visado y esperan que sus datos sean recopilados, consultados y transmitidos sólo con ese objeto.

Dado que los sistemas de información se conforman con una finalidad específica, con garantías, seguridad y condiciones de acceso determinadas por esa finalidad, la concesión sistemática de acceso a efectos diferentes del original no sólo infringiría el principio de limitación de finalidad, sino que también podría acarrear que los elementos antes mencionados fueran inadecuados o insuficientes.

Dentro de esa misma línea, un cambio tan importante del sistema podría dejar sin efecto los resultados del estudio de evaluación de impacto (que versaba sobre el uso del sistema sólo para su finalidad original). Lo mismo puede decirse de los dictámenes de las autoridades de protección de datos. Puede afirmarse que la nueva propuesta cambia las premisas del análisis de conformidad que hicieron.

c) *Estricta limitación de este acceso*

A la vista de los comentarios precedentes, el SEPD quisiera insistir en que el acceso al VIS por parte de las autoridades policiales podría concederse sólo en circunstancias específicas, caso por caso, y junto con estrictas garantías. En otras palabras, la consulta que hagan las autoridades policiales deberá limitarse mediante los adecuados medios técnicos y jurídicos a casos específicos.

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

con las garantías que procedan, no podrá otorgarse un acceso sistemático.»

En conclusión, los requisitos esenciales podrían resumirse así:

- No debería concederse un acceso sistemático: la Decisión deberá garantizar en todo momento que se estudiará caso por caso la necesidad y la proporcionalidad del acceso por parte de autoridades del tercer pilar. En ese sentido, es capital una redacción precisa del instrumento jurídico para no hacer posible interpretaciones en sentido amplio, que acabarían suponiendo conceder acceso habitual.
- En los casos en los que se conceda acceso, se adoptarán las garantías y condiciones apropiadas, entre ellas un régimen de protección de datos global para el uso nacional de los datos teniendo en cuenta el tipo sensible de acceso.

1.3 Comentarios iniciales

El SEPD reconoce que es preciso prestar mucha atención a la protección de datos en este instrumento propuesto, sobre todo al limitar el acceso a casos específicos y sólo dentro del marco de la lucha contra delitos graves (!).

Entre otros elementos positivos, el SEPD desearía mencionar en especial:

- la limitación a determinadas formas de delincuencia, según se menciona en el Convenio Europol;
- la obligación de los Estados miembros de establecer una lista de autoridades que tengan acceso y de hacer públicas dichas listas;
- la existencia de un punto de acceso central por Estado miembro (y de una unidad especializada dentro de Europol), que permita un mejor filtrado de las solicitudes de acceso, así como una mejor supervisión;
- reglas estrictas para posterior transmisión de los datos, con arreglo al artículo 8, apartado 5, de la propuesta;
- la obligación de los Estados miembros y de Europol de dejar constancia de las personas responsables de la consulta de los datos.

2. ANÁLISIS DE LA PROPUESTA

2.1. Observación preliminar

A fin de conceder acceso a las autoridades con arreglo al tercer pilar, la principal propuesta VIS del primer pilar debería proporcionar una cláusula puente que habría de determinar básicamente el posible contenido de un instrumento jurídico del tercer pilar como el de esta propuesta. Cuando el SEPD emitió su dictamen sobre el VIS, dicha cláusula no se había introducido todavía y el SEPD no estaba en condiciones de comentarla. Por ello, todas las observaciones que se hacen a continuación deberán tomarse con la debida reserva respecto del contenido de la cláusula puente.

(!) Esto es también coherente con las conclusiones de los Consejos de marzo y julio de 2005, que pedían que el acceso al VIS se concediera a las autoridades encargadas de la seguridad interior «sólo dentro del estricto respeto de las normas relativas a la protección de datos de carácter personal».

2.2 Finalidad del acceso

A fin de garantizar la adecuada limitación de acceso, es importante definir claramente las condiciones de acceso al VIS. Estaría bien que, junto con la propia Decisión, la exposición de motivos y los considerandos (en particular el 7) dejen muy claro que la intención es proporcionar acceso sólo caso por caso.

Cabe hacer otro comentario sobre el artículo 5 de la propuesta, a fin de orientar su interpretación.

El artículo 5 restringe el alcance del acceso a condiciones sustanciales:

- b) el acceso para consultar el sistema deberá ser necesario a efectos de prevención, detección o investigación de delitos de terrorismo o de otros delitos graves;
- c) el acceso para consultar el sistema deberá ser necesario en casos específicos (...); y
- d) si existen motivos fundados, basados en indicios concretos, para considerar que la consulta de los datos del VIS contribuirá a la prevención, detección o investigación de cualquiera de los delitos de que se trata;

Estas condiciones se acumulan y el inciso b) es más una definición de ámbito *ratione materiae*. En la práctica significa que la autoridad que pretenda tener acceso deberá encontrarse con importantes actos delictivos, según se mencionan en el inciso b) la propuesta; deberá existir un caso específico según se menciona en el inciso c). Además, la autoridad deberá poder demostrar que, en ese caso específico, la consulta de los datos del VIS contribuirá a la prevención, detección o investigación de ese delito, tal y como se prevé en el inciso d).

Incluso con esta interpretación del artículo 5, al SEPD le preocupa la redacción flexible del inciso d): «contribuirá a» es más bien amplio. Hay muchos casos en los que los datos VIS podrán «contribuir a» la prevención o investigación de un delito grave. Para poder justificar el acceso a los datos del VIS, haciendo caso omiso al principio de limitación de finalidad, el SEPD opina que esta consulta deberá «contribuir sustancialmente a» la prevención, detección o investigación del delito grave de que se trate y sugiere modificar el artículo 5 en ese sentido.

El artículo 10 estipula que los registros deberán indicar el fin exacto del acceso. El «fin exacto» debería incluir los elementos que hicieran necesaria la consulta del VIS en el sentido del artículo 5, letra d). Lo anterior contribuiría a garantizar que se aplique una evaluación de la necesidad de todas las consultas del VIS y se redujera así el riesgo de acceso habitual.

2.3. Funciones de búsqueda en la base de datos VIS

En el artículo 5, apartados 2 y 3, se proporciona un acceso en dos fases a los datos del VIS, con un conjunto de datos sólo

accesibles si se ha producido una respuesta positiva en el primer conjunto de datos. Se trata de un planteamiento correcto en sí mismo. Con todo, el primer conjunto de datos parece demasiado amplio. En particular podría cuestionarse la relevancia de datos como los mencionados en el artículo 5, apartado 2, letras e) e i) para el primer conjunto de datos:

- El «motivo del viaje» parece ser una clave demasiado general como para permitir una consulta eficiente del sistema. Además, acarrea el riesgo de trazar un perfil de viajero basado en dicho elemento.
- En cuanto a «fotografías», es limitada la posibilidad de consultar una base de datos amplia basada en fotografías; los resultados producidos por esas búsquedas suponen, en el estado actual de la tecnología, una tasa inaceptable de respuestas falsas. Las consecuencias de una identificación errónea son muy graves para el afectado.

Por ello, el SEPD solicita que los datos mencionados en el artículo 5, apartado 2, letras e) e i) se consideren como información adicional accesible si la primera consulta mostrara que ya existen datos en el sistema y se trasladan al artículo 5, apartado 3).

Por otro lado, la posibilidad de consultar la base de datos sobre la base de fotografías debería someterse a una evaluación de esta técnica por parte del comité asesor y aplicarse sólo cuando la tecnología estuviera lo suficientemente evolucionada y fuera suficientemente fiable.

2.4. Aplicación a los Estados miembros a los que no se aplica el Reglamento VIS

El acceso al VIS para consulta podrán hacerlo las autoridades responsables de la seguridad interior de los Estados miembros que no sean parte del VIS. Estos servicios tendrán que efectuar la consulta mediante un Estado miembro participante, respetando las condiciones previstas en el artículo 5, apartado 1, letras b) a d) (es decir, caso por caso), y presentar una solicitud por escrito debidamente motivada.

El SEPD quisiera resaltar la necesidad de imponer algunas condiciones al tratamiento tras la consulta. La norma que se aplica a los Estados miembros participantes en el VIS es que, una vez que se hayan recuperado datos del VIS, deberán tratarse de acuerdo con la Decisión Marco de Protección de Datos del Tercer Pilar (véase más adelante). La misma condición deberá aplicarse a los Estados miembros en los que no se aplica el Reglamento VIS pero que consulten sus datos. Debería seguirse el mismo razonamiento a la conservación de registros para su futura supervisión. Por ello, el SEPD recomienda que se añada en el artículo 6 de la propuesta un párrafo en el sentido de que los artículos 8 y 10 de la Decisión se aplicarán también a los Estados miembros a los que no se aplique el Reglamento VIS.

2.5. Régimen de protección de datos

a) Aplicación de la Decisión Marco de Protección de Datos en el Tercer Pilar

Dado que el acceso de las autoridades responsables de la seguridad interior representa una excepción a la finalidad del VIS, ese acceso deberá estar sometido a un régimen de protección de datos coherente que garantice un alto nivel de protección de los datos extraídos del VIS y tratados por las autoridades nacionales o por Europol.

El artículo 8 de la propuesta establece que la Decisión marco del Consejo sobre la protección de datos de carácter personal tratados en el marco de la cooperación policial y judicial en materia penal (en lo sucesivo denominada «Decisión marco») se aplicará al tratamiento de datos efectuado con arreglo a la Decisión propuesta. Por lo que respecta a la protección de los datos, la presente propuesta debería considerarse, pues, como *lex specialis* que desarrolla o especifica la *lex generalis* (es decir, la Decisión marco). Por ejemplo, las normas sobre las transferencias sucesivas de datos a otros terceros países son más estrictas en esta propuesta y deberían seguirse. Lo mismo ocurre con los motivos para acceder a los datos.

b) Ámbito de aplicación

El SEPD se congratula del hecho de que el régimen de protección de datos de la Decisión marco se aplique a todo tratamiento de datos personales con arreglo a la Decisión propuesta. Ello significa que el nivel de protección de los datos será equivalente, cualesquiera que sean las autoridades que consulten los datos del VIS.

Como el artículo 2 se vale de un criterio funcional para definir a dichas autoridades («las autoridades de los Estados miembros que son responsables de la prevención, detección e investigación de los delitos de terrorismo y otros delitos graves»), esta definición podría abarcar a los servicios de inteligencia tanto como a las fuerzas y cuerpos de seguridad. Por tanto, los servicios de inteligencia que consulten el VIS están, en principio, sujetos a las mismas obligaciones en lo que respecta a la protección de datos, lo que constituye, naturalmente, un elemento positivo.

No obstante, como podrían albergarse algunas dudas respecto a esta interpretación sobre la aplicabilidad de la Decisión marco a los servicios de inteligencia cuando consultan los datos VIS, el SEPD sugiere una redacción alternativa, tal como:

«En los casos en que no sea de aplicación la Decisión marco (...), los Estados miembros dispondrán un nivel de protección de los datos al menos equivalente al que garantiza la Decisión marco».

c) Supervisión

En cuanto a la redacción del artículo 8, debería aclararse que el apartado 1 se refiere al tratamiento de datos dentro del territorio de los Estados miembros. Los apartados 2 y 3 aclaran su ámbito de aplicación (tratamiento de datos por Europol y por la Comisión) y debería explicitarse que el apartado 1 se refiere a otra hipótesis.

La distribución de competencias de supervisión atendiendo a las respectivas actividades de los distintos agentes es un planteamiento correcto. Sin embargo, se echa en falta un elemento: la necesidad de un enfoque coordinado de la supervisión. Como ya se declaró en el dictamen del SEPD sobre el VIS: «Por lo que se refiere a la supervisión del VIS, es importante destacar que las actividades de supervisión de las autoridades nacionales de control y del SEPD deberían coordinarse en cierta medida. Efectivamente, es necesario que la aplicación del Reglamento se haga de forma armonizada y que se intente alcanzar un enfoque común frente a problemas igualmente comunes.

Así, el artículo 35 [de la propuesta VIS] debería incluir una disposición en ese sentido, en la que se establezca que el SEPD convocará una reunión, al menos una vez al año, con todas las autoridades nacionales de control.»

Lo mismo ocurre con esta utilización específica del sistema VIS (en este caso participa también la Autoridad Común de Control de Europol). La supervisión debería ser plenamente coherente con la del «VIS del primer pilar», ya que constituye el mismo sistema. Además, las reuniones de coordinación convocadas por el SEPD con todos los participantes en la supervisión son el modelo que se ha escogido para la supervisión de otros sistemas de información a gran escala, como Eurodac.

El SEPD es consciente de que en la propuesta está prevista en cierto modo una coordinación, ya que se menciona el papel del futuro Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido en virtud del artículo 31 de la propuesta de Decisión Marco. No obstante, cabe reiterar que la supervisión en sí no queda englobada en la misión de dicho órgano consultivo.

El SEPD sugiere que se añada una disposición que establezca que los participantes en la reunión de coordinación convocada por él en el marco de la supervisión del «VIS del primer pilar» tendrán también competencia para los datos tratados en virtud de esta propuesta y que, a tal efecto, la Autoridad Común de Control de Europol tendría que estar representada.

2.6. Autoauditoría

El artículo 12 de la propuesta establece sistemas de supervisión para el VIS. El SEPD opina que esta supervisión no debe cubrir únicamente los aspectos de los resultados, la relación coste-eficacia y la calidad de los servicios, sino también el respeto de los requisitos legales, especialmente en el campo de la protección de datos. Por lo tanto, el artículo 12 debería modificarse en consecuencia.

Para realizar esta autoauditoría de la legalidad del tratamiento, la Comisión debe poder utilizar los registros conservados con arreglo al artículo 10 de la propuesta. Por tanto, el artículo 10 debe prever que dichos registros no sólo se conserven para supervisar la protección y la seguridad de los datos, sino también para realizar autoauditorías periódicas del VIS. Los propios informes de autoauditoría servirán de ayuda en la tarea de supervisión del SEPD y de los otros supervisores, que podrán así seleccionar mejor los ámbitos de supervisión prioritarios.

3. CONCLUSIÓN

En vista de lo anterior, el SEPD subraya que es crucial dar acceso a las autoridades competentes para la seguridad interior y a Europol, sólo en casos concretos y con garantías rigurosas. Este objetivo se consigue en la propuesta de forma globalmente satisfactoria, si bien pueden introducirse algunas mejoras, propuestas en el presente dictamen:

- Ha de ser condición del acceso al VIS en virtud del artículo 5 que la consulta vaya a contribuir de manera sustancial a la prevención, detección e investigación de delitos graves, y que los registros establecidos por el artículo 10 permitan evaluar esta condición en cada caso concreto.
- Dos funciones de búsqueda para el acceso al VIS que se mencionan en el artículo 5.2, «motivo del viaje» y «fotografías», deberían reconsiderarse y facilitarse como información suplementaria en caso de respuesta positiva.

- El nivel de protección de datos aplicable después de la consulta debería ser equivalente, independientemente de las autoridades que consulten los datos del VIS. Los artículos 8 y 10 deberían aplicarse también a los Estados miembros a los que no se aplica el Reglamento VIS.
- Debería garantizarse un planteamiento coordinado de la supervisión, también en lo que respecta al acceso al VIS que prevé esta propuesta.
- Las disposiciones sobre sistemas de seguimiento deberían garantizar asimismo la autoauditoría del cumplimiento de los requisitos de protección de datos.

Bruselas, a 20 de enero de 2006.

Peter HUSTINX
Supervisor Europeo de Protección de Datos