DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la 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 (COM (2005) 475 final)

(2006/C 47/12)

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,

Vista la solicitud de dictamen con arreglo al apartado 2 del artículo 28 del 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,

HA ADOPTADO EL PRESENTE DICTAMEN:

I **CONSIDERACIONES PRELIMINARES**

Consulta del SEPD

1. La Comisión transmitió al SEPD la 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 mediante carta de 4 de octubre de 2005. El SEPD entiende que dicha carta constituye una solicitud de consulta de instituciones y organismos comunitarios a tenor del apartado 2 del artículo 28 del Reglamento n.º 45/2001/CE. El SEPD opina que el presente dictamen debería mencionarse en el preámbulo de la Decisión marco.

Importancia de la presente propuesta

2. El SEPD subraya la importancia de la presente propuesta, desde la perspectiva de los derechos y libertades fundamentales de las personas físicas en el sentido de que se protejan sus datos personales. La adopción de esta propuesta constituiría un avance considerable respecto de la protección de los datos personales, en un ámbito importante que requiere, señaladamente, un mecanismo coherente y eficaz de protección de los datos personales a escala de la Unión Europea.

3. En tales condiciones, el SEPD destaca la relevancia creciente que reviste la cooperación policial y judicial entre los Estados miembros, como elemento del establecimiento gradual de un espacio de libertad, seguridad y justicia. El Programa de La Haya introdujo el principio de disponibilidad con el fin de mejorar el intercambio transfronterizo de información policial y judicial. Conforme al Programa de La Haya ([1]), no debe bastar el mero hecho de que la información cruce las fronteras. La introducción del principio de disponibilidad refleja una tendencia más general a facilitar el intercambio de información policial (véanse, por ejemplo, el Tratado de Prüm ([2]) firmado por siete Estados miembros, y la propuesta sueca de una Decisión marco sobre la simplificación del intercambio de información e inteligencia entre los cuerpos de seguridad ([3])). Con la misma óptica cabe interpretar la muy reciente aprobación por el Parlamento Europeo de una Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos de comunicación ([4]). Esta evolución exige la adopción de un instrumento jurídico que garantice la protección efectiva de los datos personales en todos los Estados miembros de la Unión Europea, con arreglo a pautas comunes.

([1]) Página 18 del Programa.

([2]) Tratado entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal. Prüm (Alemania), 27 de mayo de 2005.

([3]) Iniciativa del Reino de Suecia con vistas a la adopción de un proyecto de Decisión marco sobre la simplificación del intercambio de información e inteligencia entre los cuerpos de seguridad de los Estados miembros de la Unión Europea, en particular en relación con delitos graves, incluidos los actos de terrorismo (DO C 281 de 18.11.2004, p. 5).

([4]) Basada en la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE (COM (2005) 438 final).

4. El SEPD pone de relieve que el actual marco general de protección de datos en este ámbito resulta insuficiente. En primer lugar, la Directiva 95/46/CE no se aplica al tratamiento de datos personales en el contexto de actividades ajenas al ámbito del Derecho comunitario, como las que prevé el título VI del Tratado de la Unión Europea (apartado 2 del artículo 3 de la Directiva). Si bien en la mayor parte de los Estados miembros el ámbito de aplicación de la legislación de incorporación es más amplio que el que exige la propia Directiva y no excluye el tratamiento de datos con fines policiales y judiciales, se registran importantes diferencias entre las diversas legislaciones nacionales. En segundo lugar, el Convenio nº 108 del Consejo de Europa ([1]), que obliga a todos los Estados miembros, no contempla la precisión necesaria de esta protección, como se reconoció ya en el momento de la adopción de la Directiva 95/46/CE. En tercer lugar, ninguno de estos dos instrumentos jurídicos tiene en cuenta las características particulares del intercambio de datos por parte de las autoridades policiales y judiciales ([2]).

Contribución al éxito de la propia cooperación

5. La protección eficaz de los datos personales no sólo reviste importancia para los propios sujetos a que se refieren los datos, sino que además contribuye al éxito de la propia cooperación policial y judicial. En muchos aspectos, ambos intereses públicos van de la mano.

6. Debe tenerse presente que –con bastante frecuencia– los datos personales de que se trata son de carácter sensible y han sido obtenidos por las autoridades policiales y judiciales como resultado de una investigación referida a personas. La voluntad de intercambiar tales datos con las autoridades de otros Estados miembros se incrementará si ese otro Estado miembro da garantías a la primera autoridad en cuanto al nivel de protección de los datos. El SEPD menciona, entre los elementos destacados de la protección de datos, su confidencialidad y seguridad así como las limitaciones de su acceso y su uso posterior.

7. Por otra parte, un nivel elevado de protección de datos puede ofrecer garantías de la exactitud y fiabilidad de los datos personales. Al intercambiarse datos entre autoridades policiales o judiciales, la exactitud y fiabilidad de los mismos asume una importancia aún mayor, en particular dado que, tras los intercambios y retransmisiones consecutivos de datos entre cuerpos y fuerzas de seguridad, en último término los datos serán tratados lejos de su punto de origen y fuera del contexto en que se obtuvieron y emplearon inicialmente. Por lo general, las autoridades receptoras desconocen totalmente las posibles circunstancias complementarias y deben atenerse exclusivamente a los propios datos en sí mismos.

8. Así pues, la armonización de las normas nacionales en materia de datos personales en la actuación policial y judicial –con inclusión de la adopción de adecuadas medidas de protección de dichos datos– puede servir de estímulo a la confianza recíproca y mejorar la eficacia del propio intercambio.

Respeto de los principios de la protección de datos, en combinación con un conjunto de normas complementarias

9. La necesidad y la importancia de la presente propuesta se han puesto de relieve en diversas ocasiones. En la Conferencia de Primavera celebrada en Cracovia en abril de 2005, las autoridades europeas encargadas de la protección de datos adoptaron una declaración y un documento de posición en los que abogaban por la adopción de un nuevo marco jurídico sobre la protección de datos aplicable a las actividades del tercer pilar. Este nuevo marco no sólo debería respetar los principios de la protección de datos establecidos en la Directiva 95/46/CE –es importante garantizar la coherencia de la protección de datos dentro de la Unión Europea– sino también aportar un conjunto de normas complementarias que respondan al carácter específico del ámbito de la actuación policial y judicial ([3]). El SEPD celebra que la presente propuesta tenga en cuenta estos puntos de partida: en ella se respetan los principios de protección de datos establecidos en la Directiva 95/46/CE y se aporta un conjunto de normas complementarias.

10. En el presente dictamen se analizará en qué medida es aceptable el resultado desde el punto de vista de la protección de datos, atendiendo debidamente al contexto particular de la protección de datos en el ámbito de la actividad policial. Por una parte, los datos en cuestión son a menudo de naturaleza sensible (véase el punto 6 del presente dictamen), y por otra, existe una fuerte presión para acceder a esos datos en aras de la eficacia de la actuación policial, actuación que puede abarcar la protección de la vida y la seguridad física de las personas. En opinión del SEPD, las normas de protección de datos deben obedecer a las necesidades justificadas de la actuación policial y judicial, sin menoscabo de la protección del sujeto a que se refieren los datos frente al tratamiento y el acceso injustificados a esos datos. Para ajustarse al principio de proporcionalidad, el resultado de las deliberaciones del legislador europeo debe reflejar el respeto de dos intereses públicos potencialmente contrapuestos. A este respecto, el SEPD reitera que en muchos casos ambos intereses van de la mano.

El contexto del título VI del Tratado de la Unión Europea

11. Por último, debe mencionarse que la presente propuesta se inscribe en el título VI del Tratado de la Unión Europea, el denominado tercer pilar. La intervención del legislador europeo está acotada por limitaciones claras: limitación de las competencias de la Unión a los asuntos mencionados en los artículos 30 y 31, limitaciones referidas al procedimiento legislativo, que no incluye la participación plena del Parlamento Europeo, y limitaciones en materia de control judicial, por cuanto las competencias del Tribunal de Justicia Europeo a tenor del artículo 35 del TUE son incompletas. Estas limitaciones exigen un análisis aún más minucioso del texto de la propuesta.

([1]) Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, 28 de enero de 1981.

([2]) En 1987, el Consejo de Europa emitió una Recomendación nº R (87) 15 dirigida a regular la utilización de datos de carácter personal en el sector de la policía, pero dicha Recomendación, por su naturaleza, no es vinculante para los Estados miembros.

([3]) En el mismo sentido, véase «El Supervisor Europeo de Protección de Datos como asesor de las instituciones comunitarias para las propuestas de legislación y documentos conexos» (18 de marzo de 2005), publicado en http://www.edps.eu.int/publications/policy_papers/policy_paper_advisor_ES.pdf.

II. CONTEXTO: INTERCAMBIO DE INFORMACIÓN CON ARREGLO AL PRINCIPIO DE DISPONIBILIDAD, CONSERVACIÓN DE DATOS Y MARCOS ESPECÍFICOS DEL SIS II Y EL VIS

II.1 Principio de disponibilidad

12. La propuesta guarda vínculos estrechos con la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (COM (2005) 490 final). Esta última propuesta pretende dar aplicación al principio de disponibilidad, y garantizar con ello que la información de que dispongan las autoridades competentes de un Estado miembro a efectos de la lucha contra la delincuencia se facilite a las autoridades equivalentes de otros Estados miembros. Esto debería llevar a la supresión de las fronteras interiores para el intercambio de este tipo de información, sometiendo dicho intercambio a condiciones uniformes en toda la Unión.

13. El estrecho vínculo entre ambas propuestas se deriva del hecho de que –en gran medida– la información policial y judicial se refiere a datos personales. No cabe adoptar normas jurídicas sobre el intercambio de información policial sin garantizar la adecuada protección de los datos personales. Cuando de una intervención a nivel de la Unión Europea se derive la supresión de las fronteras interiores para el intercambio de esta información, la protección de los datos personales ya no podrá corresponder de forma exclusiva al ámbito del Derecho nacional. La garantía de protección de los datos personales en todo el territorio de la Unión sin fronteras interiores se ha convertido en un cometido de las instituciones europeas. Este cometido se prevé de forma expresa en la letra b) del apartado 1 del artículo 30 del TUE, y es consecuencia de la obligación de la Unión de respetar los derechos fundamentales (artículo 6 del TUE). Por otra parte:

— En el apartado 2 del artículo 1 de la presente propuesta se prevé de forma expresa que los Estados miembros ya no podrán restringir ni prohibir la comunicación transfronteriza de información por motivos vinculados a la protección de datos personales.

— La propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad contiene varias referencias a la presente propuesta.

14. El SEPD señala que sólo debe adoptarse una Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad a condición de que se adopte igualmente una Decisión marco relativa a la protección de datos personales. Ahora bien, la presente propuesta de Decisión marco del Consejo relativa a la protección de datos posee una utilidad en sí misma y resulta necesaria aun en ausencia de un instrumento jurídico sobre disponibilidad. En la parte I del presente dictamen se ha sustentado esta opinión.

15. Así las cosas, el SEPD analizará las dos propuestas en dos dictámenes separados. Existe también para esto un motivo de orden práctico: no hay garantías de que el Consejo y el Parlamento Europeo vayan a tratar ambas propuestas de manera conjunta y con igual celeridad.

II.2 Conservación de datos

16. El 26 de septiembre de 2005, el SEPD presentó su dictamen sobre la propuesta de Directiva sobre la conservación de datos de comunicación ([1]). En su dictamen destacó algunas lagunas importantes de la propuesta y sugirió que se añadieran en la Directiva disposiciones específicas sobre el acceso de las autoridades competentes a los datos de tráfico y de localización y sobre la utilización posterior de los datos, así como la adición de otras salvaguardias adicionales para la protección de datos. El texto de la Directiva adoptada por el Parlamento Europeo y por el Consejo contiene una disposición limitada –pero en modo alguno suficiente– sobre protección de datos y seguridad de los mismos, y también una disposición aún más insuficiente en materia de acceso, que remite a la legislación nacional la definición de medidas sobre acceso a los datos conservados, teniendo en cuenta las disposiciones en la materia del Derecho de la Unión Europea o del Derecho internacional público.

17. La aprobación de la Directiva sobre la conservación de datos de comunicación acentúa la urgencia de establecer un marco jurídico sobre protección de datos en el tercer pilar. Al adoptar la Directiva, el legislador comunitario obliga a los proveedores de servicios de telecomunicaciones y de Internet a conservar datos para fines policiales, sin las necesarias y adecuadas salvaguardias para la protección de los interesados. Subsiste una brecha en la protección, por cuanto la Directiva no aborda (de manera suficiente) el acceso a los datos ni su ulterior utilización, una vez que las autoridades competentes policiales y judiciales han accedido a los mismos.

18. La presente propuesta colma una parte importante de esa brecha, ya que se aplica a la utilización posterior de los datos después del acceso por parte de las autoridades policiales. Ahora bien, el SEPD lamenta que la presente propuesta tampoco aborde la cuestión del acceso a dichos datos. En contra de lo que se prevé para los sistemas SIS II y VIS (véase la sección II.3 del presente dictamen), este asunto se deja a la discreción del legislador nacional.

II.3 Tratamiento en el marco del SIS II y del VIS

19. Actualmente, la Unión Europea utiliza o está elaborando diversos sistemas de información a gran escala (Eurodac, SIS II, VIS), y procura establecer sinergias entre ellos. Existe asimismo una tendencia cada vez mayor a conceder un acceso amplio a dichos sistemas para fines policiales. Con arreglo al Programa de La Haya, estas novedades de gran alcance deben tener en cuenta «la necesidad de lograr el equilibrio justo entre la aplicación de la ley y la salvaguarda de los derechos fundamentales individuales.»

([1]) Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE (COM(2005) 438 final), publicado en http://www.edps.eu.int.

20. En su dictamen de 19 de octubre de 2005 sobre las propuestas relativas a la segunda generación del Sistema de Información de Schengen (SIS II) ([1]), el SEPD subrayó algunos elementos relativos a la aplicación simultánea de normas generales (*lex generalis*) y de normas más específicas (*lex specialis*) en materia de protección de datos. Cabe considerar que la presente propuesta constituye una *lex generalis* que viene a sustituir al Convenio 108 en el marco del tercer pilar ([2]).

21. El SEPD destaca, a este respecto, que la propuesta proporciona asimismo un marco general de protección de datos para instrumentos específicos tales como la parte del SIS II correspondiente al tercer pilar y el acceso policial y judicial al Sistema de Información de Visados. ([3])

III. **CONTENIDO ESENCIAL DE LA PROPUESTA**

III.1 **Normas comunes aplicables a cualquier tratamiento de datos**

Punto de partida

22. A tenor del apartado 1 de su artículo 1, la propuesta pretende determinar normas comunes para garantizar la protección de las personas en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal. El apartado 1 del artículo 1 debe leerse juntamente con el apartado 1 del artículo 3, que declara que la propuesta se aplicará al tratamiento (...) de datos personales (...) por una autoridad competente, con fines de prevención, investigación, detección o enjuiciamiento de delitos.

23. De estas disposiciones se desprende que la propuesta de Decisión marco tiene dos características fundamentales: establece normas comunes y se aplica a cualquier tratamiento de datos a efectos de la aplicación de la legislación penal, aun cuando los datos no hayan sido transmitidos o facilitados por autoridades competentes de otros Estados miembros.

24. El SEPD subraya la importancia de estas dos características fundamentales. La presente propuesta debe tener el cometido de establecer un marco de protección de datos que complemente de forma plena el marco jurídico que ya existe para el primer pilar. Sólo si se cumple con este requisito plenamente la Unión Europea respeta su obligación con arreglo al apartado 2 del artículo 6 del TUE de respetar los derechos fundamentales garantizados por el CEDH.

Normas comunes

25. Por lo que atañe a la primera característica: la presente propuesta se encamina a garantizar que los principios vigentes de protección de datos se apliquen en el ámbito del tercer pilar. Proporciona asimismo normas comunes que especifican estos principios con miras a su aplicación en este ámbito. El SEPD recalca la importancia de estos aspectos de la propuesta, que reflejan el carácter particular y sensible del tratamiento de datos personales en este campo. El SEPD valora señaladamente la introducción del principio de distinción entre datos personales de determinadas categorías de personas como principio específico de la protección de datos en el ámbito de la cooperación policial y judicial en materia penal, además de los principios ya existentes de protección de datos (apartado 4 del artículo 4). En opinión del SEPD, el propio principio y sus consecuencias jurídicas para el interesado deberían precisarse *aún más* (véanse los puntos 88-92 del presente dictamen).

26. Las normas deben aplicarse a situaciones diversas, por lo que no pueden ser excesivamente detalladas. Por otra parte, es menester que proporcionen al ciudadano la necesaria seguridad jurídica, así como una adecuada protección de sus datos personales. El SEPD estima que en términos generales, la propuesta alcanza un equilibrio entre estos dos requisitos legislativos potencialmente contrapuestos. Las disposiciones prevén cierta flexibilidad allí donde se necesita, sin dejar de ser suficientemente precisas en la mayor parte de sus aspectos para dar protección al ciudadano.

27. Sin embargo, en algunos aspectos la propuesta resulta excesivamente flexible y no ofrece las garantías necesarias. Por ejemplo, en el apartado 1 del artículo 7 la propuesta contempla una exención general de las salvaguardias, supeditada exclusivamente a la condición «salvo que la legislación nacional disponga otra cosa». El mantenimiento de una facultad discrecional tan amplia de conservación de los datos durante más tiempo que el necesario para los fines previstos no sólo sería incompatible con el derecho fundamental a la protección de los datos, sino que sería además contraria a la necesidad básica de armonización de la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

28. Las exenciones –de ser necesarias– deben limitarse a las disposiciones nacionales o europeas destinadas a la protección de intereses públicos concretos. El apartado 1 del artículo 7 debería mencionar estos intereses.

29. Esto trae a colación otro aspecto. Toda vez que cualquier otro instrumento jurídico específico adoptado en el marco del título VI del Tratado UE contemple requisitos o restricciones más precisos para tratar los datos o acceder a los mismos, debería aplicarse esta legislación más específica en calidad de *lex specialis*. El artículo 17 de la propuesta prevé excepciones a los artículos 12, 13, 14 y 15 si una legislación específica adoptada en el marco del título VI del Tratado de la Unión Europea establece condiciones específicas para la transmisión de los datos. Esto es ilustrativo del alcance general de la propuesta (según se ha explicado anteriormente), pero no abarca

([1]) Punto 2.2.4 del dictamen.

([2]) Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, 28 de enero de 1981.

([3]) Propuesta de Decisión del Consejo relativa al acceso al Sistema de Información de Visados para su consulta por parte de las autoridades de los Estados miembros responsables de la seguridad interior y por parte de Europol con fines de prevención, descubrimiento e investigación de delitos terroristas y otras infracciones penales graves (COM (2005) 600 final), presentada el 24 de noviembre de 2005. El SEPD tiene intención de emitir un dictamen sobre dicha propuesta a comienzos de 2006.

todas las hipótesis posibles. En opinión del SEPD, el artículo 17:

— debería redactarse de manera más general: en caso de que exista legislación más específica que regule cualquiera de los aspectos del tratamiento de los datos (y no sólo su transmisión), será aplicable la legislación específica;

— debería contener una garantía de que las excepciones no podrán rebajar el nivel de protección.

Aplicables a todo tipo de tratamiento

30. Por lo que atañe a la segunda característica: el resultado ideal consistiría en que quedara cubierta cualquier obtención y tratamiento de datos personales en el marco del tercer pilar.

31. Es fundamental para el logro de su objetivo que la Decisión marco abarque todos los datos policiales y judiciales, aun cuando no hayan sido transmitidos ni facilitados por las autoridades competentes de otros Estados miembros.

32. Ello resulta aún más importante cuanto que cualquier limitación de los datos que se transmitan o faciliten a autoridades competentes de otros Estados miembros redundaría en que el ámbito de aplicación de la Decisión marco resultase especialmente inseguro e incierto, lo que se opondría a su objetivo esencial ([1]). Quedaría menoscabada la seguridad jurídica de las personas. En circunstancias normales, nunca se sabe con antelación –en el momento de la obtención de los datos personales– si dichos datos resultarán pertinentes a efectos de un intercambio con autoridades competentes de otros Estados miembros. El SEPD se remite, a este respecto, al principio de disponibilidad y a la supresión de las fronteras interiores para el intercambio de datos policiales y judiciales.

33. Por último, el SEPD observa que la propuesta no se aplica a:

— el tratamiento en el marco del segundo pilar del Tratado UE (política exterior y de seguridad común)

— el tratamiento de datos por parte de servicios de inteligencia y el acceso de dichos servicios a estos datos cuando sean tratados por autoridades competentes u otras partes (esto se desprende del artículo 33 del TUE).

En estos ámbitos, la legislación nacional deberá proporcionar la adecuada protección de los interesados. A la hora de valorar la propuesta es preciso tener en cuenta esta brecha de la protección en el plano de la UE: ([2]) puesto que no podrán cubrirse todos los tratamientos de datos en el ámbito policial y judicial, el legislador debe garantizar una protección aún más eficaz en los ámbitos a los que sí se aplica la propuesta.

([1]) El SEPD se remite al mismo razonamiento seguido por el Tribunal (entre otros asuntos) en su sentencia *Österreichischer Rundfunk* y otros, asuntos combinados C-465/00, C-138/01 y C-139/01, Rec. [2003], p. I-4989.

([2]) En el mismo sentido, véase el dictamen del SEPD de 26 de septiembre de 2005 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE, punto 33.

III.2 **Base jurídica**

34. En los considerandos de la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad se menciona una base jurídica concreta, la letra b) del apartado 1 del artículo 30. La presente propuesta, en cambio, no especifica qué disposiciones del artículo 30 o del artículo 31 constituyen la base jurídica.

35. Si bien no compete al SEPD, en su calidad de asesor en materia de legislación de la Unión Europea, escoger la base jurídica de una propuesta, resulta útil suponer que la presente propuesta pudiera basarse igualmente en la letra b) del apartado 1 del artículo 30. Además, podría basarse en la letra c) del apartado 1 del artículo 31, y debería aplicarse en su totalidad a las situaciones nacionales, toda vez que sea necesario para mejorar la cooperación policial y judicial entre los Estados miembros. A este respecto, el SEPD subraya nuevamente que todos los datos personales que hayan sido obtenidos, almacenados, tratados o analizados con fines policiales podrán, atendiendo en particular al principio de disponibilidad, ser objeto de intercambio con autoridades competentes de otro Estado miembro.

36. El SEPD comparte la opinión de que la letra b) del apartado 1 del artículo 30 y la letra c) del apartado 1 del artículo 31 del TUE constituyen una base jurídica para normas de protección de datos que no se limiten a la protección de los datos personales efectivamente intercambiados entre las autoridades competentes de los Estados miembros, sino que se apliquen igualmente a las situaciones de ámbito nacional. Concretamente:

— La letra b) del apartado 1 del artículo 30, que puede servir de base jurídica a normas sobre obtención, almacenamiento, tratamiento, análisis e intercambio de información pertinente, no se limita a la información que haya sido facilitada o transmitida a otros Estados miembros. La única limitación que impone la letra b) del apartado 1 del artículo 30 se refiere a la pertinencia de la información en el ámbito de la cooperación policial.

— Por lo que atañe a la cooperación judicial, la letra c) del apartado 1 del artículo 31 es todavía más explícita, por cuanto la acción en común incluirá «la consecución de la compatibilidad de las normas aplicables en los Estados miembros, en la medida necesaria para mejorar dicha cooperación».

— De la sentencia Pupino ([3]) se deduce que el Tribunal de Justicia aplica principios del Derecho comunitario en cuestiones del tercer pilar. Esta jurisprudencia refleja la evolución desde la mera cooperación entre las autoridades de los Estados miembros en el marco del tercer pilar hacia un espacio de libertad, seguridad y justicia, comparable al mercado interior establecido por el Tratado CE.

([3]) Sentencia del Tribunal de 16 de junio de 2005, Pupino, asunto C-105/03.

— A juicio del SEPD, el principio de eficacia supone que no se interprete el Tratado de tal manera que obstaculice el cumplimiento eficaz de sus funciones por parte de las instituciones de la Unión Europea. Ello incluye su función de protección de los derechos fundamentales.

— Como ya se ha dicho, la limitación a las situaciones transfronterizas no respetaría las consecuencias del principio de disponibilidad y menoscabaría la seguridad jurídica de las personas.

37. El SEPD desea referirse por separado al *intercambio de datos con terceros países*. Los Estados miembros utilizan datos personales obtenidos y tratados en terceros países que les son transmitidos con fines policiales, y transmiten datos personales que ellos mismos han obtenido o tratado a las autoridades competentes de terceros países y a organismos internacionales.

38. Los artículos 30 y 31 del TUE no exigen un trato diferenciado de los datos personales obtenidos por autoridades de terceros países respecto de los datos recabados inicialmente por autoridades competentes dentro de los Estados miembros. Los datos procedentes de terceros países, una vez recibidos, deben ajustarse a las mismas normas que los datos obtenidos en un Estado miembro. Ahora bien, no siempre resulta sencillo comprobar la calidad de los datos (lo que se abordará en el siguiente capítulo del presente dictamen).

39. Si se quiere ser rigurosos, la transmisión de datos personales a terceros países por parte de las autoridades competentes de los Estados miembros se sitúa fuera del ámbito de aplicación del título VI del Tratado UE. Ahora bien, si se pudiesen transmitir datos a terceros países sin que quedara garantizada la protección del interesado, ello supondría un quebrantamiento importante de la protección que prevé la presente propuesta dentro del territorio de la Unión Europea, por los motivos que se indican en la sección III.4 del presente dictamen. Resumiendo:

— Los derechos de los interesados garantizados por la presente propuesta se ven directamente afectados si la transmisión de los datos a terceros países no se somete a las normas de protección de datos.

— Existiría un riesgo de que las autoridades competentes soslayaran las estrictas normas de protección de datos.

40. En síntesis, la aplicabilidad de normas comunes de protección de datos a los datos personales intercambiados por las autoridades competentes de los Estados miembros con autoridades de terceros países y organizaciones internacionales es necesaria para que resulten eficaces las normas comunes sobre protección de datos personales entre las autoridades competentes de los Estados miembros, y es necesaria, por consiguiente, para mejorar la cooperación entre los Estados miembros. Los artículos 30 y 31 proporcionan la base jurídica necesaria.

III.3 **Observaciones específicas sobre el ámbito de aplicación de la propuesta**

Datos personales tratados por autoridades judiciales

41. No sólo las autoridades policiales tratan e intercambian datos personales; también lo hacen las autoridades judiciales. La propuesta, basada en los artículos 30 y 31 del Tratado UE, se aplica a la cooperación entre autoridades policiales y judiciales. Así las cosas, la propuesta tiene un ámbito de aplicación más amplio que la propuesta de Decisión marco sobre el intercambio de información, que se limita a la cooperación policial y se aplica exclusivamente a la información antes del inicio de un proceso judicial.

42. El SEPD celebra que la propuesta se haga extensiva a los datos personales tratados por las autoridades judiciales. Existen buenos motivos para reunir en la misma propuesta los datos policiales y judiciales tratados a efectos de garantizar el cumplimiento de la ley. En primer lugar, la organización de la cadena de investigación penal y enjuiciamiento difiere en los distintos Estados miembros. En segundo lugar, todos los datos personales de esta cadena son susceptibles de quedar incluidos en un expediente judicial. No resulta lógico aplicar regímenes diferentes a la protección de los datos en las fases anteriores.

43. Por lo que atañe, sin embargo, a la supervisión del tratamiento de los datos, es menester un planteamiento diferente. El artículo 30 de la propuesta enumera los cometidos de las autoridades de control. En su apartado 9 se dice que las competencias de la autoridad de control no afectarán a la independencia del poder judicial. El SEPD recomienda que se aclare en la propuesta que las autoridades de control no supervisan el tratamiento de los datos por las autoridades judiciales cuando actúan en el ejercicio de sus funciones jurisdiccionales. ([1])

Tratamiento de datos por parte de Europol y Eurojust (y el Sistema de Información Aduanero)

44. Con arreglo al apartado 2 del artículo 3 de la propuesta, la Decisión marco no se aplicará al tratamiento de datos personales por Europol, Eurojust y el Sistema de Información Aduanero ([2]).

([1]) Esta disposición podría ser semejante a la del artículo 46 del Reglamento (CE) nº 45/2001.

([2]) El Sistema de Información Aduanero es un sistema reducido pero bastante complejo compuesto por elementos nacionales y supranacionales, comparable al Sistema de Información de Schengen. Dada la importancia relativa de la presente propuesta en relación con el Sistema de Información Aduanero y habida cuenta de la complejidad del propio sistema, éste se dejará de lado en el presente dictamen. El SEPD abordará la cuestión del Sistema de Información Aduanero en otro contexto.

45. En rigor, esta disposición es innecesaria, al menos en lo que se refiere a Europol y Eurojust. Una decisión marco a tenor de la letra b) del artículo 34 del TUE sólo puede adoptarse para la aproximación de las disposiciones legales y reglamentarias de los Estados miembros, y no puede ir dirigida a Europol y Eurojust.

46. En cuanto al fondo, el apartado 2 del artículo 3 da pie a las siguientes consideraciones:

— La presente propuesta ofrece un marco general, que en principio debería ser aplicable a todas las situaciones que se inscriban en el tercer pilar. La coherencia del marco jurídico de la protección de datos es en sí misma un elemento que potencia la eficacia de dicha protección.

— En la actualidad, Europol y Eurojust cuentan con sistemas de protección de datos bien definidos, que incluyen un sistema de supervisión. Por tal motivo, no existe urgencia acuciante para adaptar las normas aplicables al texto de la presente propuesta.

— A más largo plazo, no obstante, las normas de protección de datos aplicables a Europol y a Eurojust deberían ponerse plenamente en consonancia con la presente Decisión marco.

— Ello es aún más importante cuanto que la presente propuesta de Decisión marco (con excepción de su capítulo III) se aplica a la obtención y el tratamiento de datos personales transmitidos a Europol y Eurojust por los Estados miembros.

III.4 **Estructura de la propuesta**

47. El SEPD, tras analizar la propuesta, ha llegado a la conclusión de que, en términos generales, ésta prevé una estructura de protección estratificada. Las normas comunes establecidas en el capítulo II de la propuesta (y, por lo que atañe a aspectos específicos, en los capítulos IV-VII) contienen dos estratos de protección:

— Transposición al tercer pilar de los principios generales de protección de datos establecidos en la Directiva 95/46/CE y en otros instrumentos jurídicos de las Comunidades Europeas, así como en el Convenio n.º 108 del Consejo de Europa.

— Normas adicionales sobre protección de datos, aplicables a cualquier tratamiento de datos personales en el marco del tercer pilar. Los apartados 3 y 4 del artículo 4 de la propuesta son ejemplos de tales normas adicionales.

48. El capítulo III añade un tercer estrato de protección para determinadas formas de tratamiento. Los títulos de las dos secciones del capítulo III y la formulación de varias de las disposiciones de la propuesta parecen dar a entender que este capítulo se aplica exclusivamente a los datos transmitidos o facilitados por las autoridades competentes de otros Estados miembros. Como consecuencia de ello, algunas disposiciones importantes a efectos de la protección de los datos personales no se aplicarían a tales datos en caso de que éstos no se intercambiaran entre Estados miembros. Dicho esto, el texto es ambiguo, dado que las mismas disposiciones parecen ir más allá de las actividades directamente relacionadas con los datos intercambiados. En cualquier caso, esta limitación del ámbito de aplicación no se explica ni justifica de forma expresa en la exposición de motivos, como tampoco en la evaluación del impacto.

49. El SEPD subraya la plusvalía que aporta esta estructura estratificada, que por sí misma puede brindar una protección óptima al interesado, atendiendo a las necesidades particulares de la actuación policial. Esta estructura es el reflejo de la necesidad de una adecuada protección de datos tal como se expresó en la Conferencia de Primavera celebrada en Cracovia en abril de 2005, y en principio se atiene al artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y al Convenio para la protección de los derechos humanos y de las libertades fundamentales, en particular a su artículo 8.

50. Sin embargo, del análisis del texto de la propuesta cabe extraer las observaciones que se exponen a continuación.

51. En primer lugar, debe velarse por que las normas adicionales de protección de datos del capítulo II (el segundo estrato mencionado en el punto 47) no se aparten de los principios generales de la protección de datos. En opinión del SEPD, las normas adicionales del capítulo II deben ofrecer a los interesados una protección adicional relacionada con el contexto específico del tercer pilar (información policial y judicial). Dicho de otro modo: estas normas adicionales no podrán dar lugar a un nivel de protección inferior.

52. De igual modo, el capítulo III, relativo a formas específicas de tratamiento (en el que aparece el tercer estrato de protección) no debe constituir una excepción respecto del capítulo II. A juicio del SEPD, las disposiciones del capítulo III deben ofrecer a los interesados una protección adicional en situaciones en que estén implicadas las autoridades competentes de más de un Estado miembro, pero no deben dar lugar a un nivel de protección inferior.

53. En segundo lugar, no deben incluirse en el capítulo III normas que tengan carácter general. El SEPD recomienda que tales disposiciones se trasladen al capítulo II. En el capítulo III deberán incluirse solamente disposiciones que se relacionen estrictamente con la protección de datos personales en el caso de intercambio de datos entre Estados miembros. Esto es todavía más importante cuanto que el capítulo III contiene disposiciones importantes con miras a un elevado nivel de protección del interesado en el contexto de la acción policial y judicial(-véase la sección IV.1 del presente dictamen).

IV. **ANÁLISIS DE LOS ELEMENTOS DE LA PROPUESTA**

IV.1 **Puntos de partida del análisis**

54. El SEPD, a la hora de analizar los diversos elementos sustantivos de la propuesta, tendrá en cuenta su estructura y contenido particulares. El SEPD no hará observaciones relativas a cada uno de los artículos de la propuesta.

55. En primer término, la mayor parte de las disposiciones de la propuesta son un calco de otros instrumentos jurídicos de la UE sobre protección de datos personales. Esas disposiciones son compatibles con el marco jurídico de protección de datos de la UE y resultan satisfactorias para proporcionar salvaguardias adecuadas en materia de protección de datos en el tercer pilar.

56. Ahora bien, el SEPD observa que algunas de las disposiciones que actualmente figuran en el capítulo III de la propuesta –relativas a aspectos particulares y, en términos generales (véase el punto 48 del presente dictamen), aplicables únicamente a los datos intercambiados con otros Estados miembros– integran principios generales y esenciales de la legislación de la UE sobre protección de datos. Así pues, esas disposiciones del capítulo III deberían trasladarse al capítulo II y hacerse aplicables a cualquier tratamiento de datos por parte de las autoridades policiales y judiciales. Tal es el caso de las disposiciones relativas al control de la calidad de los datos (apartados 1 y 6 del artículo 9) y las que regulan la utilización posterior de los datos personales (apartado 1 del artículo 11).

57. Algunos de los demás artículos del capítulo III de la propuesta no distinguen entre las condiciones adicionales que se relacionan específicamente con los intercambios de datos con otros Estados miembros (como el consentimiento de la autoridad competente del Estado miembro de transmisión) y las salvaguardias que son, en cambio, pertinentes y necesarias también respecto de los datos tratados en el interior de un Estado miembro. En tales casos, el SEPD recomienda que estas últimas sean de aplicación general, inclusive a los datos personales que no hayan sido transmitidos o facilitados por otro Estado miembro. Esta recomendación se refiere a:

— la transmisión de datos a particulares y a autoridades distintas de las autoridades policiales (letras a) y b) de los artículos 13 y 14), y a

— la transferencia a terceros países o a organismos internacionales (artículo 15, con excepción de su letra c)).

58. En esta parte del dictamen se señalarán asimismo a la atención del legislador algunas salvaguardias adicionales que no figuran en la presente propuesta. En opinión del SEPD, deberían ofrecerse estas salvaguardias adicionales por lo que respecta a las decisiones individuales automatizadas, a los datos personales recibidos de terceros países, al acceso a bases de datos de entidades privadas, al tratamiento de datos biométricos y a los perfiles de ADN.

59. Asimismo, en el análisis que aparece a continuación se formulan recomendaciones destinadas a mejorar el texto actual con miras a garantizar la eficacia de las disposiciones, la coherencia del texto y su compatibilidad con el actual marco jurídico de la protección de datos.

IV.2 **Limitación de los fines y tratamiento posterior**

60. En la letra b) del apartado 1 del artículo 4 se especifica que los datos deberán recogerse con fines determinados, explícitos y legítimos y no ser tratados posteriormente de manera incompatible con dichos fines. Normalmente los datos se recogerán en relación con un delito concreto (o, en determinadas circunstancias, para investigar a una banda o red delictiva, etc.). Podrán utilizarse para el fin inicial y posteriormente sufrir un tratamiento con otros fines, a condición de que sean compatibles con el inicial (por ejemplo, los datos obtenidos sobre una persona condenada por tráfico de drogas podrían utilizarse en el marco de una investigación relativa a una red de traficantes). Este planteamiento es un buen reflejo del principio de limitación de la finalidad, que también está consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, por lo que es compatible con la legislación vigente sobre protección de datos.

Tratamiento posterior para fines incluidos en el ámbito de aplicación de la Decisión marco

61. El SEPD observa que la propuesta no aborda de manera plenamente satisfactoria una situación que puede presentarse en la actividad policial: la necesidad de una utilización ulterior de los datos con un fin considerado incompatible con aquel para el que fueron recogidos. Los datos obtenidos por la policía podrían ser necesarios posteriormente para esclarecer un delito completamente distinto. A modo de ilustración cabe mencionar que los datos obtenidos para el enjuiciamiento por infracciones de tráfico pueden utilizarse con posterioridad para localizar y procesar a un ladrón de vehículos. El segundo fin, legítimo como es, no puede considerarse plenamente compatible con el fin de la recogida de los datos. Si no se permitiera a las autoridades policiales emplear los datos para este segundo fin, podrían verse tentadas a recoger los datos con fines vagos e indefinidos, en cuyo caso el principio de limitación de la finalidad perdería su sentido en lo tocante a la recogida. Asimismo, también se vería menoscabada la aplicación de otros principios, como la proporcionalidad, la exactitud y la fiabilidad (véanse las letras c) y d) del apartado 1 del artículo 4).

62. Conforme a la legislación de la UE sobre protección de datos, los datos personales deberán recogerse con fines determinados y explícitos, y no ser tratados posteriormente de manera incompatible con dichos fines. Sin embargo, el SEPD estima que debe admitirse cierta flexibilidad en cuanto a su utilización ulterior. Será más probable que se cumpla la limitación impuesta a la recogida si las autoridades responsables de la seguridad interior saben que podrán acogerse, con salvaguardias adecuadas, a una excepción de la limitación respecto del uso posterior.

63. Merece aclararse que esta necesidad de tratamiento posterior se reconoce en el artículo 11 de la propuesta, pero de manera relativamente insuficiente. El artículo 11 se aplica únicamente a los datos recibidos o facilitados por la autoridad competente de otro Estado miembro, y no prevé salvaguardias suficientes.

64. El SEPD recomienda que el apartado 1 del artículo 11 sea aplicable a todos los datos, con independencia de que se hayan recibido o no de otro Estado miembro. Lo que es más, deberían incluirse garantías más estrictas que las contempladas en su letra b): la utilización posterior para un fin considerado incompatible con el inicial sólo debería admitirse cuando resultase estrictamente necesaria, en un caso determinado, para la prevención, investigación, detección y enjuiciamiento de delitos penales o para la protección de los intereses o de los derechos fundamentales de una persona. En la práctica, el SEPD sugiere incluir esta disposición en un nuevo artículo 4 bis (y en todo caso, en el capítulo II de la propuesta).

65. Los apartados 2 y 3 del artículo 11 deberían seguir siendo aplicables tal como están; estos apartados proporcionan salvaguardias adicionales para los datos recibidos de otros Estados miembros. El SEPD observa que el apartado 3 del artículo 11 se aplicará al intercambio de datos a través del SIS II: el SEPD ya había mencionado en su dictamen sobre el SIS II que debería velarse por que efectivamente los datos del SIS no puedan utilizarse con fines distintos de los del propio sistema.

Tratamiento posterior para fines ajenos a la cooperación policial y judicial

66. En algunos casos, es menester tratar los datos para la protección de otros intereses importantes. En tales casos, podrían ser tratados incluso por otras autoridades distintas de las autoridades competentes a tenor de esta Decisión marco. Estas competencias de los Estados miembros podrían implicar un tratamiento que constituya una intrusión en la intimidad (por ejemplo, la investigación de una persona que no sea sospechosa), por lo que deberían acompañarse de condiciones muy rigurosas, como la obligación de que los Estados miembros adopten una legislación específica al respecto si desean acogerse a esta excepción. En el marco del primer pilar, esta cuestión se trató en el artículo 13 de la Directiva 95/46/CE, que estipula que se admitirán restricciones de algunas disposiciones de la Directiva en determinados casos. Los Estados miembros que apliquen tales restricciones deberán hacerlo ateniéndose al artículo 8 del CEDH.

67. Siguiendo la misma línea de razonamiento, la presente Decisión marco debería estipular en el capítulo II que deberá admitirse que los Estados miembros adopten medidas legislativas que permitan un tratamiento posterior cuando tales medidas sean necesarias para la salvaguardia de:

— la prevención de amenazas a la seguridad pública, la defensa o la seguridad del Estado

— la protección de un interés económico y financiero importante de un Estado miembro o de la Unión Europea

— la protección del interesado.

IV.3 **Criterios de legitimación del tratamiento de datos**

68. El artículo 5 de la propuesta dispone que las autoridades competentes sólo podrán tratar los datos en virtud de una ley que establezca que el tratamiento es necesario para el cumplimiento de las funciones legales de la autoridad en cuestión y con fines de prevención, investigación, detección y enjuiciamiento de delitos. El SEPD respalda los rigurosos requisitos impuestos por el artículo 5.

69. Sin embargo, el texto del artículo 5 subestima la necesidad de legitimar el tratamiento de datos, en determinadas circunstancias, con otros argumentos jurídicos. Es una disposición importante, que no debería imposibilitar el cumplimiento por parte de la policía de sus obligaciones conforme al Derecho nacional de revelar información a los servicios de inmigración o a las autoridades fiscales. Por consiguiente, el SEPD sugiere que el artículo 5 tenga en cuenta otros motivos legales justificados de tratamiento de datos personales, como la necesidad de cumplir con obligaciones legales a las que esté sujeto el responsable del tratamiento, el consentimiento inequívoco del interesado, siempre que el tratamiento se efectúe en interés del interesado, o la necesidad de proteger el interés vital del interesado.

70. El SEPD observa que el respeto de los criterios que legitiman el tratamiento de datos reviste especial importancia en relación con la cooperación policial y judicial, si se tiene en cuenta que la obtención ilegal de datos personales por parte de los servicios policiales podría tener la consecuencia de que esos datos no pudieran utilizarse como pruebas en el proceso judicial.

IV.4 **Necesidad y proporcionalidad**

71. Los artículos 4 y 5 de la propuesta pretenden asimismo garantizar –de un modo satisfactorio en líneas generales– que las restricciones a la protección de los datos personales sean necesarias y proporcionales, según lo exigen el Derecho de la Unión Europea, la jurisprudencia del Tribunal Europeo de Derechos Humanos y el artículo 8 del CEDH:

— La letra c) del apartado 1 del artículo 4 establece la norma general de que los datos sean adecuados, pertinentes y no excesivos en relación con los fines para los que se hubieran recabado o para los que se traten posteriormente.

— El artículo 5 precisa que el tratamiento debe ser *necesario* para el cumplimiento de las funciones legales de la autoridad en cuestión y con fines de prevención, investigación, detección y enjuiciamiento de delitos.

— El apartado 4 del artículo 4 declara que el tratamiento de datos personales únicamente se considerará necesario si se cumplen determinadas condiciones.

72. El SEPD observa que la formulación propuesta del apartado 4 del artículo 4 no se ajusta a los criterios fijados por la jurisprudencia del Tribunal Europeo de Derechos Humanos en relación con el artículo 8 del CEDH, según la cual sólo es legítimo imponer una restricción al respeto de la intimidad cuando resulte necesario en una sociedad democrática. A tenor de la propuesta, el tratamiento de datos se consideraría necesario no sólo cuando *posibilitara* el cumplimiento de las funciones de las autoridades policiales y judiciales, sino también cuando *existieran motivos razonables* para *creer* que los datos personales en cuestión sencillamente *facilitarían o acelerarían* la prevención, investigación, detección y enjuiciamiento de delitos.

73. Estos criterios no se ajustan a los requisitos del artículo 8 del CEDH, puesto que podría considerarse que cualquier tratamiento de datos personales serviría para facilitar las actividades de las autoridades policiales o judiciales, aun cuando los datos en cuestión no fuesen realmente necesarios para la realización de dichas actividades.

74. El texto actual del apartado 4 del artículo 4 daría pie a la recogida de datos personales en una escala excesiva, basada exclusivamente en la creencia de que los datos personales *pudieran facilitar* la prevención, investigación, detección y enjuiciamiento de delitos. Por el contrario, el tratamiento de datos personales deberá considerarse necesario únicamente si las autoridades competentes pueden demostrar efectivamente la necesidad del mismo, y a condición de que no se disponga de medidas que supongan una menor intrusión.

75. Por consiguiente, el SEPD recomienda que se modifique la redacción del primer inciso del apartado 4 del artículo 4 de modo tal que se respete la jurisprudencia (sobre el artículo 8 del CEDH). Por lo demás, por razones de sistematización, el SEPD sugiere que este apartado se traslade al final del artículo 5.

IV.5 **Tratamiento de categorías especiales de datos**

76. El artículo 6 establece –en principio– la prohibición del tratamiento de datos sensibles, es decir, datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, y la afiliación sindical, así como el tratamiento de los datos relativos a la salud o a la vida sexual. Esta prohibición dejará de aplicarse si el tratamiento está previsto por una ley y es absolutamente necesario para el ejercicio de las funciones legales de la autoridad en cuestión, con el fin de prevenir, investigar, detectar y enjuiciar delitos. Podrán igualmente tratarse datos sensibles si el interesado ha dado su consentimiento explícito a dicho tratamiento. En ambos casos, se establecerán garantías específicas adecuadas.

77. El texto del artículo 6 suscita dos observaciones. En primer lugar, este artículo se remite de forma excesivamente amplia al consentimiento del interesado. El SEPD subraya que sólo deberá permitirse el tratamiento de datos sensibles con base en el consentimiento explícito del interesado en la medida en que dicho tratamiento se efectúe en interés del interesado, y en que la negativa a dar ese consentimiento no redunde en consecuencias negativas para el interesado. El SEPD recomienda que se modifique consiguientemente el artículo 6, también para ponerlo en consonancia con la normativa vigente de la UE sobre protección de datos.

78. En segundo lugar, el SEPD estima que cabría tener en cuenta también otros motivos legales para el tratamiento, como la necesidad de proteger los intereses vitales del interesado o de otra persona (en caso de que el interesado no sea física o jurídicamente capaz de dar su consentimiento).

79. En el ámbito de la cooperación policial y judicial, el tratamiento de otras categorías de datos potencialmente sensibles, como los datos biométricos y los perfiles de ADN, reviste una importancia cada vez mayor. El artículo 6 de la propuesta no se refiere de forma expresa a ese tipo de datos. El SEPD invita al legislador de la UE a que dé pruebas de la máxima prudencia a la hora de desarrollar los principios generales de protección de datos expuestos en la presente propuesta mediante nueva legislación que implique el tratamiento de estas categorías especiales de datos. Ejemplo de ello es la actual propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (véanse los puntos 12-15 *supra*), en la que se contemplan de forma expresa el tratamiento y el intercambio de datos biométricos y perfiles de ADN (anexo II de dicha propuesta) pero no se menciona el carácter delicado ni la especificidad de estos datos desde el punto de vista de la protección de datos.

80. El SEPD recomienda que se prevean garantías específicas, en particular para asegurarse de que:

— sólo se utilicen datos biométricos y perfiles de ADN con arreglo a normas técnicas bien asentadas e interoperables

— se tenga muy en cuenta su grado de precisión, y el interesado pueda impugnarlos por medios de fácil accesibilidad, y

— se garantice plenamente el respeto de la dignidad de la persona.

Corresponde al legislador decidir si estas garantías deberán figurar en la presente Decisión marco o en los instrumentos jurídicos específicos que regulen la obtención y el intercambio de estas categorías especiales de datos.

IV.6 **Exactitud y fiabilidad**

81. La letra d) del apartado 1 del artículo 4 establece las normas generales aplicables a la calidad de los datos. Con arreglo a este texto, el responsable del tratamiento deberá asegurarse de que los datos sean exactos y, cuando sea necesario, actualizados. Deberá tomar todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que se hubieran recogido o para los que se traten posteriormente, sean suprimidos o rectificados. Esta disposición se ajusta a los principios generales de la legislación de la UE en materia de protección de datos.

82. En la tercera frase de la letra d) del apartado 1 del artículo 4 se dispone que los Estados miembros podrán prever el tratamiento de datos con niveles distintos de precisión y fiabilidad. El SEPD estima que esta disposición constituye una excepción al principio general de exactitud, y recomienda que se precise el carácter derogatorio de la misma añadiendo «sin embargo» o «no obstante» al comienzo de la tercera frase de la letra d) del apartado 1 del artículo 4. En tales casos, cuando no pueda garantizarse plenamente la exactitud de los datos, el responsable del tratamiento estará obligado a diferenciar los datos en función de su grado de exactitud y fiabilidad, remitiéndose en particular a la diferenciación fundamental entre datos basados en hechos y datos basados en opiniones y valoraciones personales. El SEPD recalca la importancia de esta obligación, tanto para los interesados como para las autoridades policiales, en especial cuando el tratamiento de los datos se efectúa lejos de su procedencia (véase el punto 7 del presente dictamen).

Control de la calidad de los datos

83. El principio general establecido en la letra d) del apartado 1 del artículo 4 se complementa con las garantías más específicas establecidas en el artículo 9, sobre control de la calidad de los datos. Concretamente, el artículo 9 dispone lo siguiente:

1. La calidad de los datos personales se controlará a más tardar antes de su transmisión o puesta a disposición. Además, deberá controlarse periódicamente la calidad de los datos puestos a disposición mediante acceso automatizado directo (apartados 1 y 2 del artículo 9).

2. Las resoluciones judiciales y las resoluciones de sobreseimiento deberán mencionarse en todas las transmisiones de datos y, antes de ser comunicados, deberán verificarse en la fuente los datos basados en opiniones o apreciaciones personales e indicarse su nivel de exactitud o fiabilidad (apartado 1 del artículo 9).

3. Los datos personales se marcarán, a petición del interesado, si éste niega que sean exactos y si no puede verificarse su exactitud o inexactitud (apartado 6 del artículo 9).

84. Así pues, la aplicación conjunta del apartado 1 del artículo 4 y el artículo 9 garantiza que se controle adecuadamente la calidad de los datos personales, tanto por parte del interesado como de las autoridades más próximas al origen de los datos sometidos a tratamiento, que están por tal motivo en mejor situación de controlarla.

85. El SEPD celebra la inclusión de estas disposiciones, ya que, al tiempo que se centran en las necesidades de las autoridades policiales, garantizan que cada tipo de datos se tenga en cuenta y se utilice convenientemente en función de su exactitud y fiabilidad, evitando así que el interesado se vea afectado de manera desproporcionada por la posible falta de precisión de algunos de los datos que le afecten.

86. El control de la calidad de los datos es un elemento esencial de protección del interesado, en especial en el caso de los datos personales tratados por la policía y las autoridades judiciales. Por tal motivo, el SEPD lamenta que la aplicabilidad del artículo 9 sobre control de la calidad de los datos se limite a los que se transmiten o ponen a disposición de otros Estados miembros. Esto es de lamentar por cuanto implica que la calidad de los datos personales –que también es esencial para los fines policiales y judiciales– únicamente estaría plenamente garantizada cuando los datos se transmitieran a otros Estados miembros o se pusieran a su disposición, pero no cuando el tratamiento se efectuara dentro de un Estado miembro ([1]). En lugar de ello, es indispensable, tanto en bien de los interesados como en interés de las autoridades competentes, velar por que se efectúe un control adecuado de la calidad de todos los datos personales, incluidos los que no hayan sido transmitidos o facilitados por otro Estado miembro.

87. Así pues, el SEPD recomienda suprimir en todo caso las limitaciones del ámbito de aplicación de los apartados 1 y 6 del artículo 9, trasladando estas disposiciones al capítulo II de la propuesta.

Distinción entre diversas categorías de datos

88. El apartado 3 del artículo 4 establece la obligación de que el responsable del tratamiento establezca una clara distinción entre los datos personales de diversas categorías de personas (sospechosos, condenados, testigos, víctimas, informantes, contactos, y otros). El SEPD aprueba este planteamiento. Si bien es cierto que las autoridades policiales y judiciales pueden verse en la necesidad de tratar datos correspondientes a categorías de personas muy diversas, es indispensable que esos datos se diferencien en función del diverso grado de implicación en un delito. Concretamente, las condiciones de obtención de los datos, los plazos, las condiciones para denegar al interesado el acceso o la información y las modalidades de acceso a los datos por parte de las autoridades competentes deberían reflejar las particularidades de las distintas categorías de datos tratados y los distintos fines con los que las autoridades policiales y judiciales obtienen tales datos.

89. A este respecto, el SEPD aboga por una especial atención en relación con los datos relativos a personas que no sean sospechosas. Se requieren condiciones y salvaguardias específicas para garantizar la proporcionalidad y evitar que se perjudique a personas sin participación activa en la comisión de delitos. Para esta categoría de personas, la propuesta debería contener disposiciones adicionales que restringieran la finalidad del tratamiento, fijaran plazos concretos y limitaran el acceso a los datos. El SEPD recomienda modificar la propuesta en tal sentido.

([1]) Por otra parte, esto no estaría en consonancia con la Recomendación nº R (87) 15 del Comité de Ministros del Consejo de Europa a los Estados miembros, dirigida a regular la utilización de datos de carácter personal en el sector de la policía. En particular, su Principio 7.2 dispone que deberán establecerse «controles regulares» de la calidad de los datos personales con el acuerdo de la autoridad de control o conforme a la legislación nacional.

90. El texto actual de la propuesta contiene una salvaguardia específica referida a los no sospechosos, a saber, el apartado 1 del artículo 7 de la misma. Según el SEPD, esta salvaguardia es importante sobre todo porque no se permite que los Estados miembros establezcan excepciones. Lamentablemente, el apartado 1 del artículo 7 sólo establece garantías más específicas por lo que atañe a los plazos, y su aplicabilidad se limita a la categoría de personas mencionadas en el último inciso del apartado 3 del artículo 4 de la propuesta. Por lo tanto, no ofrece garantías suficientes ni abarca la totalidad del grupo de personas no sospechosas. ([1])

91. También merecen atención los datos relativos a personas condenadas. Efectivamente, por lo que respecta a esos datos, deben tenerse debidamente en cuenta las iniciativas recientes y futuras sobre intercambio de ficheros de antecedentes penales y garantizarse la coherencia con las mismas. ([2])

92. Atendiendo a lo expuesto, el SEPD recomienda añadir un nuevo apartado al artículo 4 en el que figuren los siguientes elementos:

— disposiciones adicionales que restrinjan la finalidad del tratamiento, fijen plazos precisos y limiten el acceso a los datos cuando se refieran a personas no sospechosas

— la obligación de que los Estados miembros establezcan las consecuencias jurídicas de la diferenciación que habrá de hacerse entre los datos personales de las diversas categorías de personas, reflejando las particularidades de las distintas categorías de datos tratados y los distintos fines para los que las autoridades policiales y judiciales obtienen estos datos

— las consecuencias jurídicas deberán guardar relación con los requisitos para la recogida de datos, los plazos, la transmisión y utilización ulteriores de los mismos y las condiciones para denegar el acceso o la información al interesado.

IV.7 **Plazos de conservación de los datos personales**

93. Los principios generales por los que se rigen los plazos de conservación de los datos personales figuran en la letra e) del apartado 1 del artículo 4 y en el apartado 1 del artículo 7 de la propuesta. Como principio general, los datos personales deberán conservarse durante un período no superior al necesario para los fines para los que hubieran sido recogidos. Esto es coherente con la legislación de la UE sobre protección de datos. ([3])

94. No obstante, la disposición general del apartado 1 del artículo 7 sólo es aplicable «salvo que la legislación nacional disponga otra cosa». El SEPD señala que esta excepción es demasiado general y va más allá de las excepciones admisibles a tenor de la letra e) del apartado 1 del artículo 4. El SEPD propone que se suprima la excepción general del apartado 1 del artículo 7, o que al menos se restrinjan de forma expresa los intereses públicos que justifiquen el recurso a esta excepción por parte de los Estados miembros ([4]).

95. El apartado 2 del artículo 7 declara que la observancia de los plazos se garantizará con medidas procesales y técnicas adecuadas y se comprobará de forma regular. El SEPD, si bien expresa su satisfacción con esta disposición, recomienda que se disponga explícitamente que las medidas procesales y técnicas adecuadas deberán prever la supresión automática y regular de los datos personales al término de un plazo determinado.

IV.8 **Intercambio de datos personales con terceros países**

96. En grado cada vez mayor, la eficacia de la cooperación policial y judicial dentro de las fronteras de la UE depende de la cooperación con terceros países y organizaciones internacionales. En la actualidad se debaten o se prevén diversas iniciativas destinadas a mejorar la cooperación policial y judicial con terceros países u organizaciones internacionales, tanto a escala nacional como de la UE. ([5]) Es probable que la evolución de esta cooperación internacional se sustente en gran medida en el intercambio de datos personales.

97. Por consiguiente, resulta indispensable que los principios de tratamiento equitativo y legítimo (así como las garantías procesales en su conjunto) se apliquen igualmente a la recogida y el intercambio de datos personales más allá de las fronteras de la Unión, y que sólo se transmitan datos personales a terceros países u organizaciones internacionales si esas terceras partes implicadas garantizan un nivel adecuado de protección u ofrecen garantías adecuadas.

([1]) Véase, más concretamente, el punto 94 del presente dictamen.

([2]) La Decisión 2005/876/JAI del Consejo, relativa al intercambio de información de los registros de antecedentes penales, entró en vigor el 8 de diciembre. La Decisión completa y facilita los mecanismos existentes de transmisión de información sobre condenas con base en los convenios vigentes, como el Convenio Europeo de Asistencia Judicial en Materia Penal de 1959 y el Convenio de 2000 Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea. Este texto será sustituido más adelante por una decisión marco del Consejo que aporte mayor precisión. La Comisión prevé proponer una nueva decisión marco en esta materia.

([3]) Además de la disposición general sobre plazos de conservación de los datos personales que figura en el artículo 7, la propuesta contiene otras disposiciones específicas aplicables a los datos personales intercambiados con otros Estados miembros. En particular, el apartado 7 del artículo 9 dispone la supresión de los datos personales:
1. si los datos no debieran haberse transmitido, puesto a disposición o recibido;
2. al expirar un plazo comunicado por la autoridad que haya transmitido los datos, a menos que los datos personales sigan siendo necesarios para procedimientos judiciales;
3. si los datos no son o han dejado de ser necesarios para los fines para los que se transmitieron.

([4]) Cabría considerar su limitación a la lucha contra el terrorismo o a la protección de los intereses públicos concretos que se mencionan en la letra e) del apartado 1 del artículo 4: fines históricos, estadísticos o científicos.

([5]) Véase, por ejemplo, la reciente comunicación de la Comisión «Una estrategia relativa a la dimensión exterior del espacio de libertad, seguridad y justicia» (COM (2005) 491 final).

Transferencia de datos personales a terceros países

98. Con esta perspectiva, el SEPD expresa su satisfacción con el artículo 15 de la propuesta, que dispone la protección en caso de transferencia a las autoridades competentes de terceros países o a organismos internacionales. Ahora bien, esta disposición, incluida en el capítulo III de la propuesta, se aplica únicamente a los datos recibidos de autoridades competentes de otros Estados miembros o facilitados por tales autoridades. Como consecuencia de esta limitación, subsiste una carencia en el sistema de protección de datos a escala de la Unión Europea por lo que respecta a los datos que no se hayan recibido de autoridades competentes de otros Estados miembros. En opinión del SEPD, esta carencia es inadmisible por los motivos que se exponen a continuación.

99. En primer lugar, el nivel de protección que ofrece el Derecho de la UE en caso de transferencia a un país tercero no debe determinarse en función de la procedencia de los datos: un servicio policial interno del Estado miembro que transfiere los datos a un tercer país, o un servicio policial de otro Estado miembro.

100. En segundo lugar, debe observarse que las normas sobre transferencias de datos personales a terceros países representan un principio fundamental de la legislación sobre protección de datos. Este principio no sólo constituye una de las disposiciones fundamentales de la Directiva 95/46/CE, sino que está consagrado también en el Protocolo adicional al Convenio n.º 108 ([1]). No sería posible garantizar normas comunes para la protección de los datos personales, según se mencionan en el artículo 1 de la propuesta, si las normas comunes para la transferencia de datos personales a terceros países no abarcan la totalidad de las operaciones de tratamiento de tales datos. En consecuencia, los derechos de los interesados que la presente propuesta garantiza se verían directamente afectados si pudieran transmitirse datos personales a terceros países que no ofrecieran un nivel de protección adecuado.

101. En tercer lugar, la limitación del ámbito de estas normas a los «datos intercambiados» conllevaría la inexistencia de garantías por lo que atañe a los datos tratados exclusivamente en el interior de un país: paradójicamente se podrían transferir más «fácilmente» datos personales a terceros países –menospreciando la adecuada protección de esos datos personales– que a otros Estados miembros. Ello redundaría en la posibilidad de «blanqueo de información». Las autoridades competentes de los Estados miembros podrían soslayar las estrictas normas de protección de datos transmitiéndolos a terceros países u organizaciones internacionales, a partir de los cuales la autoridad competente de otro Estado miembro podría acceder a ellos o recibirlos.

102. Por lo tanto, el SEPD recomienda modificar la presente propuesta de manera que se garantice que el artículo 15 sea aplicable al intercambio de *todos* los datos personales efectuados con terceros países. Esta recomendación no afecta a la letra c) del apartado 1 del artículo 15, que por su propia naturaleza sólo puede referirse a los datos personales intercambiados con otros Estados miembros.

Transferencias excepcionales a países que no cuenten con un nivel de protección adecuado

103. El artículo 15 fija una serie de condiciones para la transferencia a las autoridades competentes de terceros países o a organizaciones internacionales, que son comparables a las que establece el artículo 25 de la Directiva 95/46/CE. Sin embargo, el apartado 6 del artículo 15 prevé la posibilidad de transferir datos a terceros países u organizaciones internacionales en los que no se garantice un nivel adecuado de protección de los datos, si resulta absolutamente necesario para proteger intereses esenciales de un Estado miembro o para evitar un peligro grave e inminente que suponga una amenaza para la seguridad pública o para una persona o personas específicas.

104. La aplicabilidad de la excepción prevista en el apartado 6 debe precisarse. Así pues, el SEPD recomienda lo siguiente:

— aclarar que esta excepción lo es únicamente respecto del requisito de «protección adecuada», pero no afecta a los demás requisitos establecidos en el apartado 1 del artículo 15;

— añadir que las transferencias de datos realizadas al amparo de esta excepción deberían someterse a condiciones adecuadas (como el requisito expreso de que los datos sólo se traten con carácter temporal y con fines concretos) y comunicarse a la autoridad de control competente.

Tratamiento de datos personales recibidos de terceros países

105. En el contexto de un intercambio cada vez más frecuente de datos personales con autoridades policiales y judiciales de terceros países, debe prestarse también especial atención a los datos personales «importados» de esos terceros países, cuando no estén garantizadas unas normas adecuadas de respeto de los derechos humanos, y en particular de protección de los datos personales.

([1]) El Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, relativo a las autoridades de control y los flujos de datos transfronterizos, se puso a la firma el 8.11.2001 y entró en vigor el 1.7.2004. Este instrumento jurídico internacional vinculante ha sido firmado hasta ahora por 11 Estados (9 de los cuales son Estados miembros de la UE). El apartado 1 del artículo 2 del Protocolo establece el principio general de que cada una de las Partes dispondrá que sólo pueda efectuarse la transferencia de datos personales a un destinatario sujeto a la jurisdicción de un Estado u organización que no sea Parte en el Convenio si dicho Estado u organización garantizan un nivel adecuado de protección para la transferencia considerada.

106. Desde un punto de vista más general. el SEPD considera que el legislador debería velar por que los datos personales recibidos de terceros países se ajusten al menos a las normas internacionales relativas al respeto de los derechos humanos. Por ejemplo, los datos obtenidos mediante la aplicación de torturas u otras violaciones de los derechos humanos, las listas negras fundadas exclusivamente en las convicciones políticas o en las preferencias sexuales no deberían tratarse ni tenerse en cuenta por parte de las autoridades policiales y judiciales, a no ser que se hiciese en beneficio del interesado. Por consiguiente, el SEPD recomienda que esto se precise al menos en un considerando de la propuesta, posiblemente remitiendo a los instrumentos internacionales pertinentes ([1]).

107. Por lo que se refiere concretamente a la protección de los datos personales, el SEPD señala que, cuando se transmitan datos personales procedentes de países en los que no existen normas ni garantías adecuadas de protección de tales datos, deberá evaluarse la posible falta de calidad de esos datos, a fin de evitar que las autoridades policiales de la UE se fíen erróneamente de esa información y prevenir perjuicios para los interesados.

108. Así pues, el SEPD recomienda añadir en el artículo 9 de la propuesta una disposición en el sentido de que deberá valorarse específicamente la calidad de los datos personales transmitidos desde terceros países tan pronto como se reciban, y deberá indicarse la exactitud y fiabilidad de esos datos.

IV.9 **Intercambios de datos personales con particulares y con autoridades distintas de las autoridades competentes**

109. En los artículos 13 y 14 de la propuesta se establece una serie de requisitos que deberán cumplirse en los casos en que se transmitan posteriormente datos personales a particulares y a autoridades distintas de las autoridades competentes. Como ya se ha mencionado, estos artículos complementan las normas más generales del capítulo II, que deberán cumplirse de todos modos.

110. El SEPD opina que, si bien en determinados casos puede ser necesaria la transmisión a particulares y a autoridades distintas de las autoridades competentes con fines de prevención y lucha contra la delincuencia, es menester aplicar condiciones específicas y rigurosas. Esto se ajusta al punto de vista expresado por las autoridades europeas encargadas de la protección de datos en el documento de posición de Cracovia ([2]).

111. Con esta perspectiva, el SEPD considera que las condiciones adicionales establecidas en los artículos 13 y 14 pueden considerarse satisfactorias, si se aplican juntamente con las normas generales previstas en el capítulo II, con inclusión de la aplicación rigurosa de las normas sobre tratamiento posterior (véase la sección IV.2 *supra*). Ahora bien, la propuesta en su redacción actual limita la aplicabilidad de los artículos 13 y 14 a los datos personales recibidos de las autoridades competentes de otro Estado miembro o puestos a disposición por dichas autoridades.

112. La aplicabilidad general de estas condiciones reviste una importancia aún mayor si se tiene en cuenta el incremento del intercambio de datos entre autoridades policiales y autoridades de otra índole o particulares también en el interior de los Estados miembros. Cabe citar, a modo de ejemplo, la asociación de los sectores público y privado en las actividades policiales ([3]).

113. Por consiguiente, el SEPD recomienda que se modifique la presente propuesta para garantizar que los artículos 13 y 14 se apliquen al intercambio de *todos* los datos personales, incluidos aquellos que no hayan sido transmitidos o facilitados por otro Estado miembro. Esta recomendación no se aplica a las respectivas letras c) de los artículos 13 y 14.

Acceso y utilización posterior de los datos personales controlados por particulares

114. El intercambio de datos personales con particulares se efectúa en ambas direcciones: implica igualmente, pues, la transmisión o la puesta a disposición de las autoridades policiales de datos que obran en poder de particulares.

115. En este caso, las autoridades públicas tienen acceso a datos personales obtenidos con fines comerciales (transacciones comerciales, mercadotecnia, prestación de servicios, etc.) y administrados por responsables privados, con fines bien distintos, de prevención, investigación, detección o enjuiciamiento de delitos. Además, cuando estos datos se utilicen con fines policiales o judiciales, será menester valorar minuciosamente la exactitud y la fiabilidad de los datos tratados con fines comerciales ([4]).

([1]) Convención de las Naciones Unidas contra la tortura y otros tratos o penas crueles, inhumanos o degradantes, firmada por todos los Estados miembros de la UE, que entró en vigor el 26 de junio de 1987. Su artículo 15, concretamente, dice así: «Todo Estado Parte se asegurará de que ninguna declaración que se demuestre que ha sido hecha como resultado de tortura pueda ser invocada como prueba en ningún procedimiento, salvo en contra de una persona acusada de tortura como prueba de que se ha formulado la declaración.»

([2]) *Position Paper on Law Enforcement and Information Exchange in the EU*, adoptado en la Conferencia de Primavera de las autoridades europeas encargadas de la protección de datos celebrada en Cracovia, 25 y 26 de abril de 2005.

([3]) Véase el Programa legislativo y de trabajo de la Comisión para 2006 (COM (2005) 531 final).

([4]) Por ejemplo, una factura telefónica resultará fiable para fines comerciales si en ella se consignan correctamente las llamadas efectuadas; en cambio, las autoridades policiales podrán no atribuirle la misma plena fiabilidad como prueba concluyente en cuanto a quién realizó una llamada determinada.

116. Un ejemplo muy reciente e importante de acceso a bases de datos privadas con fines policiales lo constituye el texto aprobado de la Directiva sobre la conservación de datos de comunicación (véanse los puntos 16-18 *supra*), conforme al cual los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones deberán conservar hasta dos años determinadas categorías de datos de comunicación, para asegurar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves. Según el texto aprobado, las cuestiones relativas al acceso a dichos datos rebasan el ámbito del Derecho comunitario y no pueden regularse en la propia Directiva. En su lugar, estas importantes cuestiones pueden estar sometidas a la legislación nacional o a una acción en virtud del título VI del TUE ([1]).

117. En su dictamen sobre la propuesta de esa Directiva, el SEPD defendió una interpretación más amplia del Tratado CE, dado que la limitación del acceso es necesaria para garantizar una adecuada protección del interesado cuyos datos de comunicación vayan a conservarse. Lamentablemente, el legislador europeo no incluyó en la citada Directiva normas relativas al acceso.

118. En el presente dictamen, el SEPD reitera su firme preferencia por que el Derecho de la UE contemple normas comunes en materia de acceso y utilización posterior por parte de las autoridades competentes. En la medida en que este aspecto no esté tratado en el primer pilar, un instrumento del tercer pilar podría ofrecer la protección necesaria. Vienen a respaldar esta posición del SEPD el incremento general de los intercambios de datos entre Estados miembros y la reciente propuesta sobre el principio de disponibilidad. Unas normas nacionales distintas en materia de acceso y utilización no serían compatibles con la propuesta de «libre circulación» de información policial en la totalidad de la UE, que incluye igualmente los datos procedentes de bases de datos privadas.

119. Así pues, el SEPD considera que deberían aplicarse normas comunes de acceso por parte de las autoridades policiales a los datos personales que obren en poder de particulares, con objeto de garantizar que sólo se permita el acceso con arreglo a condiciones y limitaciones bien definidas. Concretamente, sólo debería permitirse el acceso de las autoridades competentes en función de los casos individuales, en circunstancias especificadas, con fines especificados, y sujeto a control judicial dentro de los Estados miembros.

([1]) Según los considerandos de la Directiva, «Las cuestiones relativas al acceso por parte de las autoridades nacionales públicas a datos conservados con arreglo a la presente Directiva para las actividades contempladas en el artículo 3, apartado 2, guión 1, de la Directiva 95/46/CE, quedan fuera del ámbito de aplicación del Derecho comunitario. Sin embargo, pueden estar sometidos a la legislación nacional o a una acción como las previstas por las disposiciones del Título VI del Tratado de la Unión Europea, teniendo siempre presente que dichas leyes o acciones deben respetar plenamente los derechos fundamentales que se derivan de tradiciones constitucionales comunes de los Estados miembros y están garantizados por el CEDH. El artículo 8 del CEDH, según la interpretación del Tribunal Europeo de Derechos Humanos …».

IV.10 **Derechos del interesado**

120. El capítulo IV se refiere a los derechos del interesado de manera compatible –en general– con la actual legislación sobre protección de datos y con el artículo 8 de la Carta de los Derechos Fundamentales de la UE.

121. El SEPD expresa su satisfacción con estas disposiciones, que prevén un conjunto armonizado de derechos del interesado, al tiempo que atienden a las particularidades del tratamiento efectuado por las autoridades policiales y judiciales. Esto constituye un avance significativo, dado que la situación actual se caracteriza por una gran variedad de normas y usos, en especial por lo que respecta al derecho de acceso. Algunos Estados miembros no autorizan el acceso del interesado a sus propios datos, sino que tienen un sistema de «acceso indirecto» (que ejerce la autoridad nacional de protección de datos por cuenta del interesado).

122. Conforme a la propuesta, se armonizan las posibles excepciones al derecho de acceso directo. Esto reviste una gran importancia para que los ciudadanos –cuyos datos son tratados e intercambiados a una escala cada vez mayor por las autoridades competentes de distintos Estados miembros– dispongan, como interesados, de un conjunto armonizado de derechos, con independencia de cuál sea el Estado miembro en el que se recojan o traten los datos ([2]).

123. El SEPD reconoce la conveniencia de restringir los derechos de los interesados en los casos en que ello es necesario para los fines de prevención, investigación, detección o enjuiciamiento de delitos. Con todo, dado que esas limitaciones deben considerarse excepciones respecto de los derechos básicos de los interesados, habrá de aplicarse una rigurosa verificación de su proporcionalidad. Ello implica que las excepciones deberán estar limitadas y perfectamente definidas, y que en lo posible, las restricciones habrán de ser parciales y limitadas en el tiempo.

124. Con esta perspectiva, el SEPD desea señalar a la atención del legislador, en particular, la letra a) del apartado 2 de los artículos 19, 20 y 21, que establecen una excepción muy amplia y mal definida respecto de los derechos de los interesados, al disponer que podrán restringirse esos derechos cuando sea necesario para «permitir al responsable del tratamiento cumplir correctamente sus funciones legales». Además, esta excepción se añade a la de la letra b), que admite restricciones de los derechos de los interesados cuando sea necesario para «no perjudicar

([2]) En particular, el capítulo IV se refiere al derecho de información (artículos 19 y 20) y al derecho de acceso, rectificación, supresión o bloqueo (artículo 21). En general, estos artículos ofrecen a los interesados todos los derechos que normalmente garantiza la legislación de la UE sobre protección de datos, al tiempo que establecen una serie de excepciones destinadas a atender a las peculiaridades del tercer pilar. En particular, se admiten restricciones de los derechos de los interesados conforme a disposiciones prácticamente idénticas en lo tocante al derecho de información (apartados 2 respectivos de los artículos 19 y 20) y de acceso (apartado 2 del artículo 21).

investigaciones, indagaciones o procedimientos en curso, o el cumplimiento de las funciones legales de las autoridades competentes». Al tiempo que cabe considerar que esta segunda excepción está justificada, la primera parecería imponer una restricción desproporcionada de los derechos del interesado. Por consiguiente, el SEPD recomienda la supresión de la letra a) del apartado 2 de los artículos 19, 20 y 21.

125. Por otra parte, el SEPD recomienda las siguientes mejoras de los artículos 19, 20 y 21:

— Precisar que las restricciones de los derechos del interesado no son obligatorias, no se aplican durante un plazo indefinido y son admisibles «únicamente» en los casos concretos enumerados en los artículos.

— Tener en cuenta que el responsable del tratamiento debe facilitar información de manera espontánea y no a petición del interesado.

— Añadir, en la letra c) del apartado 1 del artículo 19, que también se deberá facilitar información sobre «los plazos de conservación de los datos».

— Velar (mediante una modificación del apartado 1 del artículo 20 en consonancia con otros instrumentos de protección de datos de la UE) por que se facilite información al interesado –cuando los datos no se hayan obtenido de él o se hayan obtenido sin su conocimiento– «a más tardar en el momento en que los datos se transmitan por primera vez».

— Velar por que el mecanismo de recurso contra la denegación o restricción de los derechos del interesado sea aplicable a los casos de restricción del derecho de información, y efectuar la consiguiente modificación del apartado 4 del artículo 19.

Decisiones individuales automatizadas

126. El SEPD lamenta que la propuesta no aborde en absoluto la importante cuestión de las decisiones individuales automatizadas. De hecho, la experiencia demuestra que las autoridades policiales recurren en un grado cada vez mayor al tratamiento automatizado de datos destinados a evaluar determinados aspectos personales de las personas, especialmente con el fin de valorar su fiabilidad y su comportamiento.

127. El SEPD –sin dejar de reconocer que estos sistemas pueden resultar necesarios en determinados casos para aumentar la eficacia de las actividades policiales– señala que las decisiones fundadas exclusivamente en el tratamiento automatizado de datos deberían estar sujetas a condiciones y garantías muy estrictas cuando generen efectos legales respecto a una persona o cuando afecten de manera significativa a una persona. Ello es todavía más importante en el contexto del tercer pilar, pues en este caso las autoridades tienen atribuida la fuerza pública coercitiva, por lo que existe la probabilidad de que sus decisiones o acciones afecten a las personas o den lugar a una intromisión mayor de la que se produciría cuando se tratase de decisiones o acciones de particulares.

128. En particular, y en consonancia con los principios generales de la protección de datos, sólo deberían admitirse estas decisiones o acciones cuando estuvieran expresamente autorizadas por la ley o por la autoridad de control competente, y las mismas deberían estar sujetas a medidas adecuadas destinadas a proteger los intereses legítimos del interesado. Además, el interesado debería contar con medios fácilmente accesibles que le permitieran exponer su punto de vista, y tener conocimiento del razonamiento en que se funda la decisión, salvo que ello sea incompatible con la finalidad del tratamiento de los datos.

129. Por lo tanto, el SEPD recomienda la introducción de una disposición específica sobre las decisiones individuales automatizadas, en consonancia con la legislación vigente de la UE sobre protección de datos.

IV.11 **Seguridad del tratamiento**

130. Por lo que respecta a la seguridad del tratamiento, el artículo 24 establece la obligación de que el responsable del tratamiento aplique las medidas técnicas y organizativas adecuadas, acordes con las disposiciones de otros instrumentos de protección de datos de la UE. Además, el apartado 2 contiene una lista amplia y pormenorizada de medidas que se aplicarán al tratamiento automatizado de datos.

131. El SEPD expresa su satisfacción con esta disposición; no obstante, con vistas a facilitar la eficacia del control por parte de las autoridades de control, sugiere que se añada a la lista de medidas del apartado 2 la siguiente medida adicional: «*k) aplicar medidas de seguimiento sistemático y elaboración de informes sobre la eficacia de estas medidas de seguridad (auditoría interna sistemática de las medidas de seguridad)*». [1]

Registro de datos

132. En el artículo 10 se dispone que se registre cada transmisión o recepción automatizadas de datos personales, o se documenten, en caso de transmisión no automatizada, para permitir la verificación posterior de la legalidad de la transmisión y el tratamiento de los datos. Esta información se pondrá a disposición de la autoridad de control competente, a petición de ésta.

[1] A este respecto, véase también el dictamen del SEPD 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), publicada en www.edps.eu.int

133. El SEPD aprueba esta disposición. Con todo, el SEPD observa que, para garantizar una supervisión exhaustiva y verificar la correcta utilización de los datos personales, debería registrarse o documentarse también el «acceso» a los datos. Esta información es fundamental, ya que el seguimiento eficaz del correcto tratamiento de datos personales no sólo habrá de centrarse en la legalidad de la transmisión de datos personales entre autoridades, sino también en la legalidad del acceso a los mismos por parte de dichas autoridades ([1]). Así pues, el SEPD recomienda que se modifique el artículo 10 para exigir que se registre o documente también el acceso a los datos.

IV.12 **Vías de recurso, responsabilidad y sanciones**

134. El capítulo VI de la propuesta trata de las vías de recurso (artículo 27), la responsabilidad (artículo 28) y las sanciones (artículo 29). En líneas generales, estas disposiciones son compatibles con la legislación vigente de la UE en materia de protección de datos.

135. En particular, por lo que se refiere a las sanciones, el SEPD celebra la precisión de que, en caso de incumplimiento de las disposiciones adoptadas con arreglo a la Decisión marco, las sanciones deberán ser eficaces, proporcionadas y disuasorias. Asimismo, en caso de infracciones intencionadas que impliquen una vulneración grave –especialmente de la confidencialidad y la seguridad del tratamiento– las sanciones penales garantizarán un mayor efecto disuasorio respecto a quebrantamientos más graves de la legislación sobre protección de datos.

IV.13 **Funciones de control, supervisión y asesoramiento**

136. Las disposiciones de la propuesta que tratan del control y supervisión del tratamiento de datos así como la consulta en asuntos relacionados con dicho tratamiento se asemejan en gran medida a las de la Directiva 95/46/CE. El SEPD celebra que la Comisión haya optado en la presente propuesta por mecanismos ya probados que funcionan correctamente, y hace especial hincapié en la introducción de un sistema (obligatorio) de control previo. Este sistema no sólo se prevé en la Directiva 95/46/CE, sino que además está incluido en el Reglamento (CE) nº 45/2001, y ha resultado ser un instrumento eficaz con que cuenta el SEPD en su labor de supervisión del tratamiento de datos por parte de las instituciones y organismos de las Comunidades Europeas.

137. Otro instrumento de control y supervisión del tratamiento de datos que ha dado prueba de su eficacia es el nombramiento de responsables de la protección de datos por parte del responsable del tratamiento. Este instrumento funciona en varios Estados miembros. El Reglamento (CE) nº 45/2001 le da carácter obligatorio, y es un instrumento que desempeña un papel esencial a nivel de las Comunidades Europeas. Los responsables de la protección de datos son administradores que garantizan de forma independiente, dentro de una organización, la aplicación interna de las disposiciones sobre protección de datos.

138. El SEPD recomienda que se añadan a la propuesta disposiciones relativas a responsables de la protección de datos. Estas disposiciones podrían ser análogas a los artículos 24-26 del Reglamento (CE) nº 45/2001.

139. La propuesta de Decisión marco va dirigida a los Estados miembros. Por consiguiente, es lógico que el artículo 30 de la misma prevea la supervisión por parte de autoridades de control independientes. La redacción de este artículo se asemeja a la del artículo 28 de la Directiva 95/46/CE. Estas autoridades nacionales deberán cooperar entre sí, así como con las autoridades de control que se creen en el marco del título VI del Tratado de la Unión Europea y con el SEPD. Por lo demás, el artículo 31 de la propuesta prevé la creación de un Grupo que habrá de desempeñar una función análoga a la que desempeña el Grupo del artículo 29 en cuestiones del primer pilar. En el artículo 31 de la propuesta se mencionan todos los actores pertinentes en el ámbito de la protección de datos.

140. Huelga decir que, en una propuesta que pretende mejorar la cooperación policial y judicial entre los Estados miembros, la cooperación entre todos los actores pertinentes en el ámbito de la protección de datos desempeña un papel importante. Así pues, el SEPD celebra el énfasis que pone la propuesta en la cooperación entre las autoridades de control.

141. Por lo demás, el SEPD destaca la importancia de un enfoque coherente en materia de protección de datos, al que podría contribuir el fomento de la comunicación entre el actual Grupo del artículo 29 y el Grupo creado en virtud de la presente propuesta de Decisión marco. El SEPD recomienda que se modifique el apartado 2 del artículo 31 de la propuesta con el fin de permitir que el presidente del Grupo del artículo 29 también participe o esté representado en las reuniones del nuevo Grupo.

142. El texto del artículo 31 de la presente propuesta contiene tan sólo una diferencia destacada con el artículo 29 de la Directiva 95/46/CE. El SEPD es miembro titular del Grupo del artículo 29. Esta pertenencia incluye el derecho de voto. La presente propuesta designa igualmente al SEPD como miembro del Grupo (en virtud del artículo 31), pero no prevé que cuente con derecho de voto. No quedan claros los motivos por los que la presente propuesta se aparta del artículo 29 de la Directiva 95/46/CE. En opinión del SEPD, el texto propuesto resulta ambiguo en cuanto al papel del SEPD, lo que podría menoscabar la eficacia de su participación en los trabajos del Grupo. Así pues, el SEPD recomienda mantener la coherencia con el texto de la Directiva.

([1]) Esto se atiene a lo dispuesto en el artículo 18 de la propuesta, a tenor del cual deberá informarse a la autoridad que haya enviado los datos, a petición de ésta, sobre el tratamiento posterior de los datos transmitidos o facilitados, y en el artículo 24, que desarrolla las medidas de seguridad, también a la luz de la auditoría interna sistemática de dichas medidas contemplada en la propuesta.

IV.14 **Otras disposiciones**

143. El capítulo VIII de la propuesta contiene algunas disposiciones finales por las que se modifica el Convenio de Schengen y otros instrumentos relativos al tratamiento y la protección de los datos personales.

Convenio de Schengen

144. El artículo 33 de la propuesta dispone que a efectos de las materias que entran en el ámbito de aplicación del Tratado UE, la presente Decisión marco sustituye a los artículos 126 a 130 del Convenio de Schengen. Los artículos 126 a 130 del Convenio de Schengen contienen las normas generales de protección para el tratamiento de datos transmitidos en aplicación del Convenio (pero al margen del Sistema de Información de Schengen).

145. El SEPD aprueba esta sustitución, por cuanto mejora la coherencia del régimen de protección de datos en el tercer pilar, y en algunos aspectos representa una mejora apreciable de la protección de datos, al aumentar, por ejemplo, las facultades de las autoridades de control. Ahora bien, en otros aspectos tiene la consecuencia involuntaria –y lamentable– de disminuir el nivel de protección de los datos. En efecto, algunas de las disposiciones del Convenio de Schengen son más rigurosas que las de la Decisión marco.

146. El SEPD se refiere, en particular, a la letra b) del apartado 3 del artículo 126 del Convenio de Schengen, en la que se dispone que los datos únicamente podrán ser utilizados por las autoridades judiciales, los servicios y los órganos que realicen una tarea o cumplan una función en el marco de los fines contemplados en el Convenio. Esta disposición parece excluir la transmisión a particulares, en tanto que la Decisión marco propuesta autorizaría dicha transmisión. Otro elemento es el hecho de que las disposiciones sobre protección de datos del Convenio de Schengen se aplican también a *todos* los datos transmitidos a partir de ficheros *no automatizados* o incluidos en los mismos (artículo 127), en tanto que los ficheros no estructurados se excluyen del ámbito de la Decisión marco propuesta.

Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea

147. El artículo 34 dispone que la presente Decisión marco sustituye al artículo 23 del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea. El SEPD observa que si bien en líneas generales esta sustitución proporciona una mejor protección de los datos personales intercambiados en el marco del Convenio, también podría dar lugar a ciertos problemas de compatibilidad entre ambos instrumentos.

148. En particular, el Convenio se refiere también a la asistencia judicial en el marco de la intervención de telecomunicaciones. En este caso, el Estado miembro requerido podrá dar su consentimiento a la intervención o a la transmisión del registro de las telecomunicaciones, supeditado a cualesquiera condiciones que deberían observarse en un caso nacional de características similares. A tenor del apartado 4 del artículo 23 del Convenio, si las condiciones adicionales se refieren a la utilización de datos personales, prevalecerán respecto de las normas de protección de datos previstas en el artículo 23. De modo análogo, el apartado 5 del artículo 23 determina la prevalencia de las normas adicionales de protección de la información obtenida por equipos conjuntos de investigación. El SEPD observa que si el artículo 23 se sustituye por la presente propuesta, no quedará claro si las mencionadas normas adicionales seguirían siendo aplicables. Por consiguiente, el SEPD recomienda que se aclare este punto, con miras a una evaluación exhaustiva de las consecuencias de la sustitución total del artículo 23 del Convenio por la presente Decisión marco.

Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

149. El apartado 2 del artículo 34 dispone que las referencias al Convenio n.º 108 se entenderán como referencias a la presente Decisión marco. La interpretación y la aplicabilidad concreta de esta disposición distan mucho de ser claras. En cualquier caso, el SEPD sobreentiende que esta disposición sólo se aplicará dentro del ámbito de aplicación *ratione materiae* de esta Decisión marco.

Observaciones finales

150. Por lo que atañe a la coherencia sistemática del texto, el SEPD observa que cabría encontrar un mejor emplazamiento para algunos de los artículos del texto de la propuesta.

Así pues, el SEPD sugiere:

1) trasladar el artículo 16 («Comité») del capítulo III («Formas específicas de tratamiento») a un nuevo capítulo;

2) trasladar los artículos 25 («Registro») y 26 («Controles previos») del capítulo V («Confidencialidad y seguridad del tratamiento») a un nuevo capítulo.

V. **CONCLUSIONES**

Un avance considerable

a) La adopción de la presente propuesta supondría un avance considerable en la protección de los datos personales, en un ámbito importante que exige, en particular, un mecanismo coherente y eficaz de protección de los datos personales a escala de la Unión Europea.

b) La protección eficaz de los datos personales no sólo es importante para los interesados, sino que contribuye asimismo al éxito de la propia cooperación policial y judicial. En muchos aspectos, ambos intereses públicos van de la mano.

Normas comunes

c) En opinión del SEPD, un nuevo marco de protección de datos no sólo debe respetar los principios de la protección de datos –es importante garantizar la coherencia de la protección de datos dentro de la Unión Europea–, sino proporcionar asimismo un conjunto adicional de normas que tenga en cuenta el carácter específico de la actividad policial.

d) La presente propuesta cumple estas condiciones: garantiza la aplicación en el ámbito del tercer pilar de los principios de protección de datos existentes en virtud de la Directiva 95/46/CE, puesto que la mayor parte de las disposiciones de la propuesta repiten las de otros instrumentos jurídicos de la UE en materia de protección de datos y son compatibles con dichos instrumentos. Por otra parte, aporta normas comunes que desarrollan esos principios, con miras a su aplicación en este ámbito, que en líneas generales resultan satisfactorias para proporcionar garantías adecuadas de protección de datos en el tercer pilar.

Aplicables a todos los tratamientos

e) Para que se logre el objetivo de la Decisión marco, es fundamental que ésta abarque la totalidad de los datos policiales y judiciales, aun cuando no sean transmitidos ni facilitados por las autoridades competentes de los Estados miembros.

f) La letra b) del apartado 1 del artículo 30 y la letra c) del apartado 1 del artículo 31 proporcionan una base jurídica para normas de protección de datos que no se limitan a la protección de los datos personales que efectivamente se intercambian entre las autoridades competentes de los Estados miembros, sino que son aplicables igualmente a las situaciones internas.

g) La propuesta no se aplica al tratamiento en el marco del segundo pilar del Tratado UE (política exterior y de seguridad común), ni al tratamiento de datos por parte de los servicios de inteligencia y al acceso de dichos servicios a esos datos cuando los mismos son tratados por autoridades competentes u otras partes (lo que se deriva del artículo 33 del TUE). En estos ámbitos, la adecuada protección de los interesados debe quedar garantizada por la legislación nacional. Esta brecha de la protección en el plano de la UE exige una protección aún más eficaz en los ámbitos que sí quedan cubiertos por la propuesta.

h) El SEPD celebra que la propuesta se haga extensiva a los datos personales tratados por las autoridades judiciales

En relación con otros instrumentos jurídicos

i) Toda vez que cualquier otro instrumento jurídico específico a tenor del título VI del Tratado UE prevea condiciones o restricciones más precisas para el tratamiento de datos o el acceso a los mismos, dicho instrumento jurídico específico se aplicaría como *lex specialis*.

j) La presente propuesta de Decisión marco sobre protección de datos reviste una utilidad propia, y resulta necesaria aun cuando no se adopte un instrumento jurídico sobre disponibilidad (con arreglo a la propuesta de la Comisión de 12 de octubre de 2005).

k) La aprobación por el Parlamento Europeo de la Directiva sobre la conservación de datos de comunicación hace que sea aún más urgente el establecimiento de un marco jurídico de protección de datos en el tercer pilar.

Estructura de la propuesta

l) Las normas adicionales del capítulo II (adicionales respecto de los principios generales de la Directiva 95/46/CE) deberían ofrecer una protección adicional a los interesados en relación con el contexto específico del tercer pilar, sin que pueda dar lugar a un nivel de protección inferior.

m) El capítulo III, dedicado a formas específicas de tratamiento (en el que se incluye el tercer estrato de protección), no puede suponer una excepción respecto del capítulo II: las disposiciones del capítulo III deben ofrecer a los interesados una protección adicional en situaciones en las que intervienen las autoridades competentes de más de un Estado miembro, sin que ello dé lugar a un nivel de protección inferior.

n) Las disposiciones sobre control de la calidad de los datos (apartados 1 y 6 del artículo 9) y las que regulan el tratamiento posterior de los datos (apartado 1 del artículo 11) deberían trasladarse al capítulo II y hacerse aplicables a cualquier tratamiento de datos por parte de las autoridades competentes, aunque los datos personales no hayan sido transmitidos ni facilitados por otro Estado miembro. Es fundamental, sobre todo, tanto en bien de los interesados como en interés de las autoridades competentes, velar por que se haga un adecuado control de la calidad de todos los datos personales.

Limitación de los fines

o) La propuesta no aborda de manera plenamente satisfactoria una situación que puede presentarse en la labor policial: la necesidad de un tratamiento posterior de los datos para un fin considerado incompatible con aquel para el que se obtuvieron.

p) De conformidad con la legislación de la UE en materia de protección de datos, los datos personales deben ser recogidos con fines determinados y explícitos, y no ser tratados posteriormente de manera incompatible con dichos fines. Ha de admitirse cierta flexibilidad en cuanto a su utilización posterior. Será más probable que se cumpla la limitación relativa a la recogida si las autoridades responsables de la seguridad del Estado saben que pueden esperar –ateniéndose a las garantías adecuadas– una excepción a la limitación del uso posterior.

q) La Decisión marco debería estipular en su capítulo II que se podrá permitir a los Estados miembros la adopción de medidas legislativas que autoricen un tratamiento posterior cuando tales medidas sean necesarias para la salvaguardia de:

— la prevención de amenazas a la seguridad pública, la defensa o la seguridad del Estado

— la protección de un interés económico o financiero importante de un Estado miembro

— la protección del interesado

Estas competencias de los Estados miembros podrían conllevar un tratamiento que invadiera la intimidad, por lo que deberían acompañarse de condiciones muy estrictas.

Necesidad y proporcionalidad

r) Los principios de necesidad y proporcionalidad de la propuesta deberían reflejar adecuadamente la jurisprudencia del Tribunal Europeo de Derechos Humanos, velando por que sólo se considere necesario el tratamiento de datos personales cuando las autoridades competentes estén en condiciones de demostrar una auténtica necesidad de efectuarlo, y a condición de que no se disponga de medidas que interfieran menos en la intimidad.

Intercambio de datos personales con terceros países

s) Si se pudieran transmitir datos personales a terceros países sin que se garantizara la protección del interesado, ello supondría un grave menoscabo de la protección que la presente propuesta prevé dentro del territorio de la Unión Europea. El SEPD recomienda modificar la presente propuesta haciendo que el artículo 15 sea aplicable al intercambio de *todos* los datos personales con terceros países. Esta recomendación no se aplica a la letra c) del apartado 1 del artículo 15.

t) Cuando se transmitan datos personales desde terceros países, deberá valorarse minuciosamente su calidad atendiendo al respeto de los derechos humanos y de las normas de protección de datos antes de su utilización.

Intercambio de datos personales con particulares y con autoridades distintas de las autoridades competentes

u) La transmisión a particulares y otros organismos públicos puede ser necesaria en determinados casos con fines de prevención de la delincuencia y lucha contra la misma, pero deberán aplicarse condiciones rigurosas y específicas. El SEPD recomienda que se modifique la presente propuesta para que los artículos 13 y 14 sean aplicables al intercambio de *todos* los datos personales, incluidos los que no se hayan recibido de otro Estado miembro o hayan sido puestos a disposición por otro Estado miembro. Esta recomendación no se aplica a las respectivas letras c) de los artículos 13 y 14.

v) Las autoridades policiales deberían aplicar normas comunes a los datos personales que obren en poder de particulares, con el fin de velar por que sólo se permita el acceso con arreglo a condiciones y limitaciones bien definidas.

Categorías especiales de datos

w) Deberían preverse garantías específicas, en particular con el fin de velar por que:

— sólo se utilicen datos biométricos y perfiles de ADN conforme a normas técnicas bien establecidas e interoperables

— se tenga cuidadosamente en cuenta su grado de precisión, y el interesado pueda impugnarlos con medios fácilmente accesibles, y

— quede plenamente garantizado el respeto de la dignidad de las personas.

Distinción entre diferentes categorías de datos

x) Los datos personales correspondientes a diferentes categorías de personas (sospechosos, condenados, víctimas, testigos, etc.) deberían tratarse conforme a condiciones y garantías diferentes y adecuadas. Por consiguiente, el SEPD propone añadir al artículo 4 un nuevo apartado que contenga los siguientes elementos:

— la obligación de que los Estados miembros establezcan las consecuencias legales de las distinciones que deberán efectuarse entre los datos personales de diferentes categorías de personas

— disposiciones adicionales que restrinjan los fines del tratamiento, establezcan límites temporales precisos y limiten el acceso a los datos, en la medida en que se refieran a personas no sospechosas.

Decisiones individuales automatizadas

y) Las decisiones fundadas únicamente en el tratamiento automatizado de datos deberían someterse a condiciones muy rigurosas cuando generen efectos respecto de una persona o afecten de forma significativa a una persona. Por consiguiente, el SEPD recomienda la inclusión de disposiciones específicas sobre decisiones individuales automatizadas, análogas a las de la Directiva 95/46/CE.

Selección de otras recomendaciones

z) El SEPD recomienda lo siguiente:

— Modificar la redacción del primer guión del apartado 4 del artículo 4 para garantizar el respeto de la jurisprudencia relativa al artículo 8 del CEDH, ya que la formulación propuesta del apartado 4 del artículo 4 no cumple los criterios de la jurisprudencia del Tribunal Europeo de Derechos Humanos relativa al artículo 8 del CEDH.

— Suprimir la amplia excepción prevista en el apartado 1 del artículo 7, o al menos restringir de forma expresa los intereses públicos que justificarían su uso por los Estados miembros.

— Modificar el artículo 10 disponiendo que también quede registrado o documentado el acceso a los datos.

— Suprimir la letra a) del apartado 2 de los artículos 19, 20 y 21.

— Añadir a la propuesta disposiciones sobre responsables de la protección de datos. Estas disposiciones podrían ser análogas a los artículos 24-26 del Reglamento (CE) nº 45/2001.

— Modificar el apartado 2 del artículo 31 de la propuesta para que se faculte también al presidente del Grupo del artículo 29 a participar o estar representado en las reuniones del nuevo Grupo.

Hecho en Bruselas, el 19 de diciembre de 2005.

Peter HUSTINX

Supervisor Europeo de Protección de Datos