I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos acerca de la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* — PNR) con fines represivos

(2008/C 110/01)

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 [1],

Visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [2], y en particular su artículo 41,

Vista la solicitud de dictamen remitida por la Comisión Europea con arreglo al artículo 28.2 del Reglamento (CE) nº 45/2001 y recibida el 13 de noviembre de 2007,

HA ADOPTADO EL PRESENTE DICTAMEN:

I. INTRODUCCIÓN

Consulta al Supervisor Europeo de Protección de Datos (SEPD)

1. De conformidad con el artículo 28.2 del Reglamento (CE) nº 45/2001 (denominado en lo sucesivo «el Reglamento»), la Comisión ha remitido al SEPD, para consulta, la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* — PNR) con fines represivos (en lo sucesivo denominada «la propuesta»).

2. La propuesta se refiere al tratamiento de datos del PNR dentro de la UE, y está estrechamente relacionada con otros sistemas de recogida y utilización de datos de los viajeros, en particular el acuerdo que la UE y Estados Unidos celebraron en julio de 2007. Estos sistemas revisten gran interés para el SEPD, que ya ha tenido ocasión de remitir algunas observaciones preliminares sobre el cuestionario que la Comisión envió a las partes interesadas [3] en diciembre de 2006 en relación con el sistema PNR previsto para la UE. El SEPD se congratula de la consulta de la Comisión, y considera que el presente dictamen debería mencionarse en el preámbulo de la Decisión del Consejo.

La propuesta en su contexto

3. La propuesta tiene por objeto armonizar las disposiciones que regulan en los Estados miembros las obligaciones de las compañías aéreas que vuelan hacia o desde el territorio de uno o varios Estados miembros en materia de transmisión de datos del PNR a las autoridades competentes, con el fin de prevenir y combatir el terrorismo y la delincuencia organizada.

4. La UE ha celebrado ya acuerdos de transmisión de datos del PNR con fines similares, tanto con Estados Unidos como con Canadá. El primer acuerdo, celebrado con Estados Unidos en mayo de 2004, fue sustituido por otro

[1] DO L 281 de 23.11.1995, p. 31.
[2] DO L 8 de 12.1.2001, p. 1.

[3] En particular los Estados miembros, las autoridades de protección de datos y las asociaciones de compañías aéreas. La Comisión Europea elaboró este cuestionario para preparar la evaluación de impacto de la propuesta.

nuevo en julio de 2007 ([1]), y en julio de 2005 se celebró un acuerdo similar con Canadá ([2]). La UE proyecta iniciar negociaciones con Australia para celebrar un acuerdo sobre el intercambio de datos del PNR; también Corea del Sur está pidiendo que se le transmitan datos del PNR de los vuelos hacia su territorio, aunque no hay previstas aún negociaciones al respecto a escala europea.

5. Dentro de la UE, la propuesta viene a añadirse a la Directiva 2004/82/CE del Consejo ([3]) sobre la obligación de los transportistas de comunicar los datos procedentes del sistema de información anticipada sobre pasajeros (datos API), con el fin de combatir la inmigración ilegal y de mejorar el control de fronteras. Esta Directiva debería haberse incorporado al ordenamiento jurídico interno de los Estados miembros a más tardar el 5 de septiembre de 2006, pero su aplicación no está aún garantizada en todos los Estados miembros.

6. Contrariamente a lo que ocurre con los datos procedentes del sistema de información anticipada sobre pasajeros (API), cuya finalidad es ayudar a identificar a los viajeros, los datos del PNR mencionados en la propuesta que nos ocupa se emplearían para realizar evaluaciones del riesgo que presentan las personas, obtener información analítica y establecer relaciones entre personas conocidas y desconocidas.

7. Los elementos principales de la propuesta son los siguientes:

   — la propuesta dispone que las compañías aéreas pongan los datos del PNR a disposición de las autoridades competentes de los Estados miembros, con el fin de prevenir y combatir los atentados terroristas y la delincuencia organizada,

   — la propuesta dispone que se designe, en principio en cada Estado miembro, una Unidad de Información sobre Pasajeros, encargada de recopilar los datos del PNR de las compañías aéreas (o de los intermediarios designados) y de realizar una evaluación del riesgo que entrañan los pasajeros,

   — la información así evaluada se remitiría a las autoridades competentes de cada Estado miembro, y se comunicaría a los demás Estados miembros, en función de las circunstancias de cada caso, para los fines antes mencionados,

   — la transferencia de esta información a países no pertenecientes a la UE estaría supeditada a condiciones adicionales,

   — los datos se conservarían durante trece años, ocho de ellos en una base de datos inactiva,

   — el tratamiento de la información se regiría por las disposiciones del (proyecto) 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 (en lo sucesivo denominada «la Decisión marco relativa a la protección de datos») ([4]),

   — un comité compuesto por representantes de los Estados miembros asistiría a la Comisión para la adopción de protocolos, normas de cifrado y requisitos y prácticas de evaluación del riesgo,

   — la Decisión se examinaría a los tres años de su entrada en vigor.

Aspectos en los que se centra el presente dictamen

8. La propuesta sobre la cual se ha consultado al SEPD representa un paso más dentro de la tendencia a recoger de forma habitual datos de personas que, en principio, no son sospechosas de haber cometido infracción alguna. Como se ha indicado antes, esta evolución se está produciendo tanto a escala internacional como europea.

9. El SEPD observa que también el Grupo de Trabajo del artículo 29 y el Grupo «Policía y Justicia» han presentado sobre esta propuesta un dictamen conjunto ([5]) que el SEPD apoya. El presente dictamen hace hincapié en varios aspectos adicionales y los desarrolla.

10. El SEPD analizará en el presente dictamen todos los aspectos pertinentes de la propuesta, pero centrándose de manera especial en cuatro grandes cuestiones:

    — la primera de ellas es la legitimidad de las medidas propuestas: se evaluarán la finalidad, necesidad y proporcionalidad de la propuesta a la luz de los criterios del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea,

    — en el dictamen se analizará también la legislación aplicable a las operaciones de tratamiento de datos propuestas. Se prestará especial atención en este contexto a la cuestión del ámbito de aplicación de la Decisión marco relativa a la protección de datos en relación con la legislación sobre protección de datos del primer pilar. Se discutirán también las consecuencias del régimen de protección de datos aplicable en el ejercicio de los derechos del interesado,

([1]) Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007) (DO L 204 de 4.8.2007, p. 18).

([2]) Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros y de los expedientes de pasajeros (DO L 82 de 21.3.2006, p. 15).

([3]) Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas (DO L 261 de 6.8.2004, p. 24).

([4]) La última versión de esta propuesta, que lleva la signatura 16397/07, puede consultarse en el registro de documentos del Consejo.

([5]) Dictamen conjunto sobre la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (PNR) con fines represivos (presentada por la Comisión el 6 de noviembre de 2007), adoptado por el Grupo de Trabajo del artículo 29 el 5 de diciembre de 2007 y por el Grupo «Policía y Justicia» el 18 de diciembre de 2007 (doc. WP 145 y WPPJ 01/07, respectivamente).

— el dictamen se centrará a continuación en la naturaleza de los destinatarios de los datos a escala nacional: la naturaleza de las Unidades de Información sobre Pasajeros, de los intermediarios y de las autoridades competentes designados para realizar la evaluación de riesgos y analizar los datos de los pasajeros suscita especial inquietud, ya que la propuesta no contiene precisiones al respecto,

— la cuarta cuestión se refiere a las condiciones de transferencia de datos a terceros países: no está claro qué condiciones se aplicarán a tales transferencias cuando se superpongan varios cuerpos de normas, como las condiciones de transferencia establecidas por la propuesta que nos ocupa, las de la Decisión marco relativa a la protección de datos y los acuerdos internacionales existentes (con Estados Unidos y Canadá).

11. En la parte final se hará referencia a otras cuestiones importantes, como las medidas positivas de protección de datos o los motivos adicionales de inquietud que supone la propuesta.

II. LEGITIMIDAD DE LAS MEDIDAS PROPUESTAS

12. Para analizar la legitimidad de las medidas propuestas de conformidad con los principios fundamentales de protección de datos, en particular el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y los artículos 5 a 8 del Convenio nº 108 del Consejo de Europa ([1]), es necesario determinar claramente la finalidad del tratamiento de datos previsto por la propuesta y evaluar su necesidad y su proporcionalidad. Es preciso garantizar que no existan otros medios menos invasivos para alcanzar el objetivo perseguido.

Determinación de la finalidad de las medidas

13. Del enunciado de la propuesta y de la evaluación de su impacto se desprende que la finalidad de la propuesta no consiste simplemente en identificar a terroristas conocidos o delincuentes conocidos del mundo de la delincuencia organizada mediante la comparación de sus nombres con los de las listas gestionadas por las autoridades represivas. Antes bien, se trata de reunir información analítica sobre el terrorismo y la delincuencia organizada y, más concretamente, «proceder a evaluaciones del riesgo que puedan entrañar las personas, obtener información y establecer vínculos entre personas conocidas y desconocidas» ([2]). En este sentido, el objetivo enunciado en el artículo 3.5 de la propuesta consiste, en primer lugar, en «identificar a las personas que estén *o puedan estar* implicadas en un delito de terrorismo o de delincuencia organizada, *así como a sus cómplices*».

14. Ésta es la razón alegada para explicar que los datos del sistema de información anticipada sobre pasajeros (API) no bastan para alcanzar el objetivo perseguido. En efecto, como ya se ha señalado, los datos del API deben servir, en principio, para ayudar a identificar a los viajeros, mientras que los datos del PNR no tienen por objeto la identificación, sino ayudar a realizar evaluaciones del riesgo que presentan las personas, obtener información analítica y establecer relaciones entre personas conocidas y desconocidas.

15. Las medidas previstas no persiguen únicamente la captura de personas *conocidas*, sino también la localización de personas que *puedan* cumplir los criterios de la propuesta.

El análisis de riesgos y la determinación de pautas de comportamiento son el instrumento fundamental que el proyecto propone para la identificación tales personas. El considerando 9 de la propuesta indica expresamente que estos datos han de conservarse «durante un período suficiente para que puedan elaborarse indicadores de riesgo y diseñarse esquemas de desplazamiento y de comportamiento».

16. La finalidad de la propuesta puede describirse, pues, a dos niveles: el primero se refiere al objetivo global de combatir el terrorismo y la delincuencia organizada, mientras que el segundo abarca los medios y medidas inherentes a la consecución de dicho objetivo. Si la lucha contra el terrorismo y la delincuencia organizada es un fin claro y legítimo, los medios empleados para alcanzarlo son discutibles.

Determinación de pautas y evaluación del riesgo

17. La propuesta no contiene indicaciones sobre la forma en que se determinarán las pautas de comportamiento y se evaluarán los riesgos. En lo que se refiere a la forma en que se emplearán los datos del PNR, la evaluación de impacto precisa que se compararán los datos de los viajeros «con una combinación de características y pautas de comportamiento, a fin de realizar una evaluación de riesgo. Si un pasajero encaja en una evaluación de riesgos determinada, puede ser identificado como un pasajero de alto riesgo» ([3]).

18. La determinación de las personas sospechosas podría hacerse sobre la base de elementos concretos que justifiquen una sospecha y que formen parte de sus datos en el PNR (por ej., contacto con una agencia de viajes sospechosa, referencia de una tarjeta de crédito robada), y sobre la base de unas pautas o de un perfil abstracto. En efecto, se podrían construir diferentes perfiles estándar en función de las pautas de viaje, para «viajeros normales» o «viajeros sospechosos». Estos perfiles permitirían realizar una investigación más detenida de aquellos viajeros que no pertenezcan a la «categoría de viajeros normales», en particular si su perfil está asociado a otros elementos sospechosos como una tarjeta de crédito robada.

19. Aunque no se puede dar por sentado que los pasajeros vayan a ser seleccionados en función de su religión o de otros datos sensibles, sí parece que serían objeto de investigación sobre la base de una combinación de elementos de información *concretos* y *abstractos*, *entre ellos* pautas estándar y perfiles abstractos.

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

([2]) Exposición de motivos de la propuesta, sección 1.

([3]) Evaluación de impacto, sección 2.1: «*Description of the problem*».

20. La posibilidad de calificar semejante tipo de investigación de «caracterización de perfiles» es discutible. La caracterización de perfiles podría definirse como en «un método informatizado que, mediante la prospección en un gran banco de datos, permita o tenga por objeto permitir clasificar a una persona en una categoría determinada, con cierta probabilidad (y por tanto, con cierto margen de error), a fin de tomar respecto de ella decisiones individualizadas» ([1]).

21. El SEPD es consciente de que la definición del concepto de caracterización de perfiles está siendo actualmente objeto de debate. El que se reconozca o no oficialmente que la propuesta tiene por objetivo la *caracterización de los perfiles* de los viajeros es secundario, ya que lo que nos ocupa aquí no es un problema de definiciones, sino de repercusiones en las personas.

22. El aspecto más inquietante para el SEPD es el hecho de que se adopten, sobre la base de pautas y criterios establecidos utilizando los datos del conjunto de los pasajeros, decisiones que afectarán a personas: se podrá adoptar una decisión sobre una persona tomando como referencia (al menos parcialmente) pautas derivadas de los datos de *otras* personas. Las decisiones se tomarán, pues, en relación con un contexto abstracto, lo cual puede afectar sobremanera a los interesados, que encontrarán además enormes dificultades para defenderse de tales decisiones.

23. Por otra parte, la evaluación de riesgos se realizará sin que existan principios uniformes de identificación de sospechosos. El SEPD tiene serias dudas sobre la seguridad jurídica de todo el proceso de filtrado, dada la indefinición de los criterios que se aplicarán para el examen de cada viajero.

24. EL SEPD recuerda que, según la jurisprudencia del Tribunal Europeo de Derechos Humanos, la legislación nacional debe ser suficientemente precisa como para indicar al ciudadano las circunstancias y condiciones que facultan a las autoridades públicas para almacenar y utilizar datos sobre su vida privada. La legislación debe «ser accesible para el interesado y sus efectos han de ser previsibles». Una norma es previsible «si está formulada con suficiente precisión como para que cualquier persona pueda regular su conducta, si es preciso con el asesoramiento adecuado» ([2]).

25. En conclusión, la propuesta que nos ocupa requiere un examen detenido sobre todo por los tipos de riesgo mencionados. El objetivo general de combatir el terrorismo y la delincuencia organizada es, en sí mismo, claro y legítimo, pero los elementos fundamentales del tratamiento que han de implantarse no parecen estar suficientemente circunscritos y justificados. El SEPD insta pues al legislador de la UE a tratar con claridad esta cuestión antes de que se adopte la Decisión marco.

Necesidad

26. Las consideraciones anteriores muestran que las medidas son claramente invasivas; sin embargo, su utilidad no está en modo alguno demostrada.

27. La evaluación del impacto de la propuesta está centrada en la mejor manera de establecer un PNR de la Unión Europea, más que en la necesidad de dotarse de semejante registro. Se hace alusión en dicha evaluación ([3]) a los registros de nombres de los pasajeros existentes en otros países, concretamente Estados Unidos y el Reino Unido. Cabe lamentar, sin embargo, la ausencia de hechos y cifras precisos sobre tales registros. Se indica que se han realizado «numerosas detenciones» en relación con «diversos delitos» en el marco del sistema *Semaphore* del Reino Unido, pero no se precisa el vínculo entre tales detenciones y el terrorismo o la delincuencia organizada. Tampoco se dan precisiones acerca del programa estadounidense, salvo que «la UE ha podido evaluar la utilidad de los datos del PNR y darse cuenta de las posibilidades que ofrece a efectos represivos».

28. No es sólo en *la propuesta* donde falta información precisa sobre los resultados concretos de los sistemas PNR, sino también en los informes publicados por *otros organismos*, como la oficina del Congreso estadounidense encargada de fiscalizar al Gobierno —*Government Accountability Office* (GAO)—, que no confirman de momento la eficacia de las medidas ([4]).

([1]) Esta definición procede de un estudio reciente del Consejo de Europa sobre la caracterización de perfiles: *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, noviembre de 2007 (no publicado aún). Véase también la definición de Lee Bygrave: «En términos generales, la caracterización de perfiles es el proceso que permite inferir un conjunto de características (relativas normalmente al comportamiento) sobre una persona o colectivo y aplicar a continuación a esa persona o colectivo (o a otras personas o colectivos) un trato determinado por esas características. Como tal, el proceso de caracterización de perfiles tiene dos componentes: i) la generación de perfiles, es decir, el proceso de inferencia de un perfil, y ii) la aplicación de perfiles, es decir, el proceso de aplicación a personas o colectivos de un trato determinado por dicho perfil», en L. A. BYGRAVE, «*Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling*», en *Computer Law & Security Report*, 2001, vol. 17, pp. 14-24:
http://www.austlii.edu.au/au/journals/PLPR/2000/40.html

([2]) Rotaru/Rumanía, sentencia nº 28341/95, apdos. 50, 52 y 55.
Véase también Amann/Suiza, sentencia nº 27798/95, apdos. 50 *y ss.*

([3]) Sección 2.1, «*Description of the problem*».

([4]) Véase, por ejemplo, el informe de publicado en mayo de 2007 por la *Government Accountability Office* de Estados Unidos en respuesta a la solicitud de miembros del Congreso: «*Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain*»:
http://www.gao.gov/new.items/d07346.pdf

29. El SEPD considera que las técnicas encaminadas a evaluar el riesgo que presenta una persona utilizando herramientas de prospección de datos y pautas de comportamiento requieren una valoración más detenida, y que su utilidad debe demostrarse claramente en el marco de la lucha contra el terrorismo antes de que puedan emplearse a tan gran escala.

Proporcionalidad

30. Para determinar si hay equilibrio entre la intrusión que la medida supone en la vida privada del interesado y la necesidad de la medida ([1]) se tienen en cuenta los siguientes elementos:

— las medidas se aplican a todos los viajeros sin distinción, estén siendo investigados o no por las autoridades policiales o judiciales. Se trata de una investigación anticipatoria cuya escala no tiene precedentes,

— las decisiones que se tomen sobre las personas pueden basarse en perfiles abstractos, y tener por tanto un margen de error significativo,

— las medidas que hayan de tomarse sobre la persona son de naturaleza represiva: suponen, por tanto, una intrusión mucho mayor, en términos de exclusión o coerción, que las que puedan adoptarse en otros contextos, como el de los delitos relacionados con las tarjetas de crédito o el de la comercialización.

31. El respeto del principio de proporcionalidad no implica sólo que la medida propuesta sea eficaz, sino también que la finalidad perseguida no pueda alcanzarse por medios que supongan una menor injerencia en la intimidad. La eficacia de las medidas propuestas no se ha demostrado. Es preciso estudiar cuidadosamente si existen alternativas antes de que puedan implantarse medidas adicionales o nuevas de tratamiento de datos personales. A juicio del SEPD, no se ha realizado ese análisis global.

32. El SEPD recuerda que existen ya, dentro de la UE o en sus fronteras, otros sistemas de gran alcance para el control de los movimientos de las personas, algunos de los cuales están ya en funcionamiento o a punto de ser implantados, en particular el Sistema de Información de Visados ([2]) y el Sistema de Información de Schengen ([3]). Aunque el objetivo principal de estos instrumentos no es la lucha contra el terrorismo o la delincuencia organizada, las autoridades policiales y judiciales tienen o tendrán en cierta medida acceso a ellos en el marco más general de la lucha contra la delincuencia ([4]).

33. El Tratado de Prüm, que se firmó en mayo de 2005 y que se está haciendo extensivo a todos los Estados miembros de la UE, permite también, por ejemplo, acceder a los datos personales (en especial en lo que respecta a los datos biométricos) incluidos en las bases de datos policiales nacionales ([5]).

34. Todos estos instrumentos tienen un punto en común, a saber, que permiten un control global, desde diferentes perspectivas, de los movimientos de las personas. Su posible contribución a la lucha contra determinados tipos de delitos, entre ellos el terrorismo, debe ser analizada en profundidad y de forma exhaustiva antes de decidir establecer nuevas formas de investigación sistemática de todas las personas que entran o salen de la UE en avión. El SEPD recomienda que la Comisión realice ese análisis, que es un paso necesario dentro del proceso legislativo.

Conclusión

35. En vista de lo que antecede, la conclusión del SEPD acerca de la legitimidad de las medidas propuestas es la siguiente: la acumulación de diferentes bases de datos sin una visión global de sus resultados y carencias concretos:

— es contraria a una política legislativa racional, que exige que no se adopten nuevos instrumentos antes de que los existentes hayan sido plenamente implantados y hayan demostrado ser insuficientes ([6]),

— puede, por lo demás, conducirnos a una sociedad basada en una vigilancia total.

36. Indudablemente, la lucha contra el terrorismo puede constituir un motivo legítimo para aplicar excepciones a los derechos fundamentales a la intimidad y la protección de datos. Sin embargo, para que tales excepciones sean

([1]) Según el artículo 9 del Convenio 108, «Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presenté Convenio cuando tal excepción prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:
1) para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;
2) para la protección de la persona concernida y de los derechos y libertades de otras personas.».

([2]) Decisión 2004/512/CE del Consejo, de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (DO L 213 de 15.6.2004, p. 5); 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; propuesta de Decisión del Consejo sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades de los Estados miembros responsables de la seguridad interior y por Europol, con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves, COM(2005) 600 final.

([3]) Véase, en particular, la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 205 de 7.8.2007).

([4]) Véase a este respecto el dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades de los Estados miembros responsables de la seguridad interior y por Europol, con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves [COM(2005) 600 final] (DO C 97 de 25.4.2006, p. 6).

([5]) Véanse los dictámenes del SEPD sobre las Decisiones Prüm: dictamen de 4 de abril de 2007 sobre la iniciativa de quince Estados miembros con vistas a la adopción de la Decisión del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (DO C 169 de 21.7.2007, p. 2); y dictamen de 19 de diciembre de 2007 sobre la iniciativa de la República Federal de Alemania encaminada a la adopción de una Decisión del Consejo relativa a la ejecución de la Decisión 2007/…/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, disponible en el sitio: http://www.edps.europa.eu

([6]) El SEPD ha hecho alusión a este aspecto en varias ocasiones, la última de ellas en su dictamen de 25 de julio de 2007 acerca de la aplicación de la Directiva sobre protección de datos (DO C 255 de 27.10.2007, p. 1).

válidas, la necesidad de la injerencia debe estar justificada por elementos claros e indiscutibles, y debe demostrarse la proporcionalidad del tratamiento de datos propuesto. Estos requisitos son especialmente necesarios en el caso de una injerencia generalizada en la intimidad de las personas como la prevista en la propuesta.

37. Estos elementos justificativos no están presentes en la propuesta, que no supera tampoco las pruebas de necesidad y proporcionalidad.

38. El SEPD insiste en que las pruebas de necesidad y proporcionalidad desarrolladas *supra* son esenciales: constituyen una *condición indispensable* para la entrada en vigor de esta propuesta. Todas las demás observaciones formuladas por el SEPD en el presente dictamen deben apreciarse a la luz de esta condición preliminar.

III. **LEGISLACIÓN APLICABLE — EJERCICIO DE LOS DERECHOS DEL INTERESADO**

Legislación aplicable

39. El análisis que figura a continuación está centrado en tres puntos:

— una descripción de los diferentes pasos del tratamiento de datos previsto en la propuesta, con miras a determinar la legislación aplicable en cada etapa,

— las limitaciones (en términos de ámbito de aplicación y de derechos de los interesados) de 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,

— un análisis más general de la medida en que un instrumento del tercer pilar puede aplicarse al tratamiento de datos por agentes privados en el contexto del primer pilar.

Legislación aplicable en las diferentes etapas del tratamiento de datos

40. Según el artículo 11 de la propuesta «Los Estados miembros garantizarán que la Decisión marco […] del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal sea aplicable al tratamiento de datos personales con arreglo a la presente Decisión marco».

41. Ahora bien, a pesar de esta disposición, no está claro en qué medida la Decisión marco relativa a la protección de datos —un instrumento del tercer pilar del Tratado de la UE— será aplicable a los datos tratados por las compañías aéreas, recogidos por las Unidades de Información sobre Pasajeros y utilizados a continuación por otras autoridades competentes.

42. La primera etapa del tratamiento de datos personales previsto en la propuesta la efectúan las compañías aéreas, que están obligadas a facilitar a las Unidades de Información sobre Pasajeros los datos del PNR, en general mediante un sistema de exportación de los datos («sistema *push*»). De la formulación de la propuesta y la evaluación de impacto ([1]) se desprende que las compañías aéreas también pueden transmitir los datos en bloque a los intermediarios. Las compañías aéreas trabajan principalmente en un contexto comercial y están sujetas a la legislación nacional de protección de datos por la que se incorpora al ordenamiento jurídico interno la Directiva 95/46/CE ([2]). Cuando los datos recopilados se utilicen para fines represivos, se plantearán problemas en lo que se refiere a la legislación aplicable ([3]).

43. Los datos serían filtrados a continuación por un intermediario (a fin de formatearlos y de excluir los datos del PNR que no figuren en la lista de datos exigidos por la propuesta) o bien enviados directamente a las Unidades de Información sobre Pasajeros. Los intermediarios podrían también ser agentes del sector privado, como ocurre en el caso de la sociedad SITA, que es la que desempeña estas funciones en el marco del Acuerdo PNR con Canadá.

44. Cuando los datos llegan a las Unidades de Información sobre Pasajeros, que han de realizar la evaluación de riesgo de la totalidad de los datos, no está claro a quién incumbe la responsabilidad del tratamiento, en el que podrían participar las autoridades aduaneras y fronterizas, y no necesariamente las autoridades policiales o judiciales.

45. La posterior transmisión de los datos filtrados a las autoridades «competentes» se produciría probablemente en un contexto represivo. La propuesta establece que las «autoridades competentes serán exclusivamente las autoridades responsables de prevenir o combatir los delitos de terrorismo y la delincuencia organizada».

46. A medida que se va avanzando de una etapa del proceso de tratamiento a otra, va estrechándose también el vínculo de los agentes que intervienen y de la finalidad perseguida con la cooperación policial y judicial en materia penal. Sin embargo, la propuesta no indica expresamente a partir de qué momento es aplicable la Decisión marco relativa a la protección de datos. Su formulación podría incluso llevar a pensar que ésta se aplica a la totalidad del proceso de tratamiento, incluidas las compañías aéreas ([4]). Sin embargo, la Decisión marco relativa a la protección de datos personales adolece en sí misma de ciertas limitaciones.

([1]) Véanse el artículo 6.3 de la propuesta y el anexo A de la evaluación de impacto, «*Method of transmission of the data by the carriers*».

([2]) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

([3]) A este respecto, véanse las consecuencias de la sentencia PNR: sentencia del Tribunal de Justicia, de 30 de mayo de 2006, Parlamento Europeo/Consejo (C-317/04) y Comisión (C-318/04), asuntos acumulados C-317/04 y C-318/04, apartado 56, Rec. 2006, p. I-4721.

([4]) Véase el artículo 11 de la propuesta, así como el considerando 10 del preámbulo, que reza como sigue: «La Decisión marco […] del Consejo relativa a la protección de datos personales en el marco de la cooperación policial y judicial en materia penal debería ser aplicable al tratamiento de todos los datos personales efectuado en virtud de la presente Decisión marco. Los derechos de las personas afectadas por el tratamiento de datos, como el derecho a la información, el derecho de acceso, el derecho de rectificación, supresión y bloqueo de los datos, así como los derechos de indemnización y recurso judicial deberían ser los que establece dicha Decisión marco.».

47. En este contexto, el SEPD pone en entredicho fundamentalmente que el título VI del Tratado de la UE pueda utilizarse como base jurídica para imponer obligaciones jurídicas, de forma habitual y para fines represivos, a agentes del sector privado. Por otra parte, es procedente preguntarse si el título VI del Tratado de la UE puede servir de base jurídica para la imposición de obligaciones jurídicas a autoridades públicas que, en principio, están fuera del marco de la cooperación policial y judicial. Estas cuestiones se desarrollan más adelante.

Limitaciones de la Decisión marco relativa a la protección de datos

48. El texto de 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 adolece al menos de dos limitaciones que son pertinentes por lo que respecta a su ámbito de aplicación.

49. En primer lugar, el ámbito de aplicación de la propuesta de Decisión marco del Consejo relativa a la protección de datos se define claramente en su texto: se aplica exclusivamente «a los datos recogidos y tratados por las autoridades competentes para la prevención, la investigación, la detección y la represión de infracciones penales y la ejecución de sanciones penales» ([1]).

50. En segundo lugar, dicha Decisión marco no está concebida para aplicarla a los datos objeto de tratamiento a escala exclusivamente nacional, sino que se limita a los datos intercambiados entre Estados miembros y transmitidos a terceros países ([2]).

51. La Decisión marco relativa a la protección de datos presenta también ciertos inconvenientes, comparada con la Directiva 95/46/CE, en particular una excepción de gran alcance al principio de limitación de la finalidad del tratamiento de datos. En lo que se refiere a este principio de finalidad, la propuesta limita claramente la finalidad del tratamiento a la lucha contra el terrorismo y la delincuencia organizada. Sin embargo, permite el tratamiento para fines más generales. En tales casos, la *lex specialis* (la propuesta que nos ocupa) debe prevalecer sobre la *lex generalis* (la Decisión marco relativa a la protección de datos) ([3]). Este extremo debería indicarse expresamente en el texto de la propuesta.

52. Por esta razón, el SEPD recomienda que se añada a la propuesta la disposición siguiente: «Los datos personales transmitidos por las compañías aéreas en virtud de la presente Decisión marco no podrán ser objeto de tratamiento para fines distintos de la lucha contra el terrorismo y la delincuencia organizada. No serán de aplicación las excepciones al principio de finalidad previstas en la Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.».

53. En conclusión, el SEPD señala que existe una grave inseguridad jurídica en lo que respecta al régimen de protección de datos aplicable a los diferentes agentes que intervienen en el tratamiento según la propuesta, en particular las compañías aéreas y demás agentes del primer pilar: pueden aplicarse bien las normas de la propuesta, bien las normas de la Decisión marco relativa a la protección de datos, o bien la legislación nacional de aplicación de la Directiva 95/46/CE. El legislador debe aclarar en qué etapa precisa del tratamiento se aplican estas diferentes normas.

Condiciones de aplicación de las normas del primer y del tercer pilar

54. El SEPD tiene serias dudas de que un instrumento del tercer pilar pueda crear obligaciones jurídicas, de forma habitual y para fines represivos, aplicables a agentes del sector público o privado que, en principio, están al margen de la cooperación policial y judicial.

55. Podría establecerse una comparación con otros dos casos de intervención del sector privado en la conservación o transmisión de datos a efectos represivos:

— *el caso del PNR estadounidense, en el que se preveía que las compañías aéreas transmitieran sistemáticamente datos del PNR a las autoridades policiales y judiciales*. El Tribunal de Justicia dictaminó, en su sentencia sobre el asunto PNR, que la Comunidad no tenía competencia para celebrar el acuerdo PNR. Uno de los motivos que empleó para justificar su fallo fue que la transferencia de datos del PNR al Servicio de aduanas y protección de fronteras de Estados Unidos (CBP) constituía una operación de tratamiento relacionada con la seguridad pública y las actividades del Estado en materia penal ([4]). En este caso, la operación de tratamiento era la transferencia *sistemática* al CBP, que es el elemento que distingue este asunto del que se menciona a continuación,

— *la conservación general de datos por los operadores de comunicaciones electrónicas*. En lo que respecta a la competencia de la Comunidad para establecer el periodo de conservación, este caso difiere del asunto anterior dado que la Directiva 2006/24/CE ([5]) sólo establece una obligación de conservación, permaneciendo los datos bajo el control de los operadores: no se prevé ninguna transferencia sistemática de datos a las autoridades policiales y judiciales. Cabe concluir que, dado que los datos quedan bajo el control de los proveedores de servicios, es a éstos a quien compete velar por que se respeten las obligaciones de protección de datos personales respecto del interesado.

([1]) Considerando 5 *bis* de la propuesta de Decisión marco relativa a la protección de datos (texto del 11 de diciembre de 2007).
([2]) Véase el artículo 1.
([3]) A este respecto, habría que analizar y debatir cuidadosamente el texto del artículo 27 *ter* de la última versión de la propuesta de Decisión marco relativa a la protección de datos en el tercer pilar.
([4]) Sentencia del Tribunal de Justicia, de 30 de mayo de 2006, Parlamento Europeo/Consejo (C-317/04) y Comisión (C-318/04), asuntos acumulados C-317/04 y C-318/04, apartado 56, Rec. 2006, p. I-4721.
([5]) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105 de 13.4.2006, p. 54).

56. En la propuesta que nos ocupa, las compañías aéreas tienen que facilitar sistemáticamente datos del PNR relativos a todos los pasajeros. Sin embargo, estos datos no se transfieren directamente y en bloque a las autoridades policiales y judiciales: pueden ser transmitidos a un intermediario, y son evaluados por un tercero, cuya condición jurídica no está clara, antes de que la información seleccionada sea remitida a las autoridades competentes.

57. La parte principal del proceso de tratamiento se produce en una zona gris que está relacionada a la vez con el primer y el tercer pilar. Como se verá en la sección IV del presente dictamen, la naturaleza de los agentes que se ocupan del tratamiento de los datos no está clara. Lo que sí está claro es que las compañías aéreas no son autoridades con funciones represivas, y que los intermediarios pueden ser agentes del sector privado. Incluso en lo que se refiere a las Unidades de Información sobre Pasajeros, que serían autoridades públicas, es importante destacar que no todas las autoridades públicas tienen la condición jurídica y las competencias necesarias para realizar de forma rutinaria funciones de carácter represivo.

58. Hasta la fecha, ha existido siempre una separación clara entre las actividades del sector privado y las de las autoridades represivas: estas últimas son realizadas por autoridades específicamente designadas para ello, en particular la policía, pudiéndose pedir a los agentes del sector privado que, en función de las circunstancias de cada caso, comuniquen datos personales a las autoridades represivas. Se observa actualmente una tendencia a imponer de forma sistemática a los agentes del sector privado obligaciones de cooperación para fines represivos, tendencia que plantea la cuestión de cuál es el régimen de protección de datos (primer o tercer pilar) que regula las condiciones de tal cooperación: ¿deben basarse las normas en la naturaleza del responsable del tratamiento de los datos (sector privado) o en la finalidad del tratamiento (represiva)?

59. El SEPD ha mencionado ya el riesgo de que se produzca un vacío jurídico entre las actividades del primer y el tercer pilar ([1]). En efecto, no está nada claro si las actividades de las empresas privadas que están conectadas de alguna manera con la aplicación del Derecho penal se encuentran dentro del ámbito de actuación del legislador de la Unión Europea según los artículos 30, 31 y 34 del Tratado de la UE.

60. Si no se aplicara el régimen general (primer pilar), los proveedores de servicios se verían obligados a establecer complejas distinciones dentro de sus bases de datos. Con arreglo al régimen actual, está claro que el responsable del tratamiento de los datos debe respetar las mismas normas de protección de datos para todos los interesados, con independencia de los fines que motiven la conservación de los datos. Debería evitarse por ello toda situación que dé lugar a la aplicación de diferentes regímenes de protección de datos a las operaciones de tratamiento de datos realizadas con distintos fines por los proveedores de servicios.

([1]) Véase el dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos (DO C 255 de 27.10.2007, p. 1). Véase también el Informe anual de 2006, p. 47.

Ejercicio de los derechos del interesado

61. Los diferentes regímenes jurídicos que se apliquen a escala nacional tendrían consecuencias importantísimas principalmente en el ejercicio de los derechos del interesado.

62. En el preámbulo de la propuesta se indica que los derechos de información, acceso, rectificación, supresión y bloqueo de los datos, y los derechos de indemnización y recurso judicial deben ser los que establece la Decisión marco relativa a la protección de datos. Sin embargo, tal indicación no permite determinar a quién corresponde atender a las peticiones del interesado.

63. La información sobre el tratamiento podría ser comunicada por las compañías aéreas, pero el acceso y la rectificación de los datos resultan más complejos, ya que estos derechos están restringidos con arreglo a la Decisión marco relativa a la protección de datos. Como se ha indicado antes, es dudoso que se pueda obligar a un proveedor de servicios como una compañía aérea a otorgar, en función de la finalidad perseguida (comercial o represiva), derechos diferenciados de acceso a los datos que conserva y de rectificación de éstos. Cabría aducir que tales derechos han de ejercerse ante la Unidad de Información sobre Pasajeros o ante las autoridades competentes designadas. Sin embargo, la propuesta no da indicaciones a este respecto y, como se ha señalado ya, tampoco está claro que las mencionadas autoridades (al menos las Unidades de Información sobre Pasajeros) vayan a ser autoridades con funciones represivas, que son las que se encargan normalmente de los procedimientos de acceso restringidos (y quizá indirectos).

64. Por otra parte, el interesado puede tener que enfrentarse al problema de que haya más de un destinatario de sus datos, en lo que se refiere a las Unidades de Información sobre Pasajeros: en efecto, los datos son remitidos a las unidades del país de salida y de llegada de los vuelos, pero pueden remitirse también, en determinados casos, a las unidades de otros Estados miembros. Por lo demás, es posible que varios Estados miembros decidan establecer o designar a una sola Unidad de Información sobre Pasajeros común. En tal caso, el interesado podría tener que ejercer su derecho de reparación ante una autoridad de otro Estado miembro. Una vez más, no está claro si se aplicarían las normas nacionales de protección de datos (que, en principio, deberían estar armonizadas dentro de la UE), o si habría que tener en cuenta una legislación específica en materia policial o judicial (dado que, en el tercer pilar, no hay una armonización global a escala nacional).

65. El mismo problema se plantea en lo que respecta al acceso a los datos tratados por los intermediarios, cuya condición jurídica no está clara, y podría darse también con las compañías aéreas de diferentes países de la UE.

66. El SEPD lamenta la incertidumbre de que adolece la propuesta en lo que se refiere al ejercicio de estos derechos fundamentales del interesado. Destaca que esta situación se debe principalmente al hecho de que se hayan encomendado semejantes responsabilidades a agentes que no tienen como función principal el mantenimiento de la ley.

Conclusión

67. El SEPD considera que la propuesta debería aclarar qué régimen jurídico se aplica en cada etapa del tratamiento de datos y especificar ante qué agente o autoridad se ejercerán los derechos de acceso y reparación. Recuerda que, con arreglo al artículo 30.1, letra b) del Tratado de la UE, las disposiciones sobre protección de datos deberían ser adecuadas y aplicarse a la totalidad de las operaciones de tratamiento que establece la propuesta. No basta con hacer una simple referencia a la Decisión marco relativa a la protección de datos porque ésta tiene un ámbito de aplicación limitado y prevé restricciones de los derechos que establece. En lo que respecta a las autoridades policiales y judiciales, las normas de la mencionada Decisión marco deberían aplicarse, como mínimo, al conjunto de las operaciones de tratamiento previstas en la propuesta, a fin de garantizar la coherencia con la aplicación de los principios de protección de datos.

IV. NATURALEZA DE LOS DESTINATARIOS DE LOS DATOS

68. El SEPD observa que la propuesta no contiene indicación alguna acerca de la naturaleza de los destinatarios de los datos personales recopilados por las compañías aéreas, ya se trate de los intermediarios, de las Unidades de Información sobre Pasajeros o de las autoridades competentes. Hay que destacar que la naturaleza del destinatario está directamente relacionada con el tipo de garantías de protección de datos que se aplica al destinatario. Se ha hecho referencia ya a la diferencia entre las garantías previstas por las normas del primer y del tercer pilar. Es indispensable que el régimen aplicable esté claro para todos los agentes que intervienen en el proceso, incluidos los gobiernos nacionales, los servicios con funciones represivas, las autoridades de protección de datos, los responsables del tratamiento y los titulares de los datos.

Intermediarios

69. La propuesta no contiene indicación alguna acerca de la naturaleza de los intermediarios ([1]). Tampoco especifica cuál es su función como responsables del tratamiento o encargados del tratamiento. Por experiencia, parece que no habría problema alguno en asignar a una entidad del sector privado (ya se trate de un sistema informatizado de reservas o de otra entidad) el cometido de recopilar los datos del PNR directamente a partir de las compañías aéreas y de transmitirlos a las Unidades de Información sobre Pasajeros. Ésa es, en efecto, la forma en que se efectúa el tratamiento de datos con arreglo al Acuerdo PNR con Canadá: SITA ([2]) es la empresa encargada del tratamiento de la información. La función del intermediario es decisiva, ya que podría ser responsable de filtrar los datos que transmiten en bloque las compañías aéreas o de cambiar su formato ([3]). Incluso si los intermediarios están obligados a suprimir la información tratada después de transmitirla a las Unidades de Información sobre Pasajeros, el proceso de tratamiento es en sí muy delicado: una consecuencia de la intervención de intermediarios es la creación de una base de datos adicional con cantidades ingentes de datos que, según la propuesta, pueden comprender incluso datos sensibles (que los intermediarios deben suprimir después). Por estas razones, el SEPD recomienda que ningún intermediario intervenga en el proceso de tratamiento de los datos de los viajeros, a menos que su naturaleza y su cometido estén estrictamente especificados.

Unidades de Información sobre Pasajeros

70. Estas unidades desempeñan un papel fundamental en la identificación de personas que están o pueden estar implicadas en delitos de terrorismo o de delincuencia organizada o ser cómplices en ellos. Según la propuesta, se encargarán de crear indicadores de riesgo y de facilitar información sobre pautas de viaje ([4]). Cuando la evaluación del riesgo se basa en pautas de viaje estandarizadas y no en pruebas materiales vinculadas a un caso concreto, el análisis que realizan puede considerarse una investigación anticipatoria. El SEPD insiste que este tipo de tratamiento está, en principio, estrictamente regulado (cuando no prohibido) por la legislación de los Estados miembros, y que su realización corresponde a autoridades públicas específicas cuyo funcionamiento está también estrictamente regulado.

71. Las Unidades de Información sobre Pasajeros se encargan, pues, de un proceso de tratamiento de datos muy delicado, sin que la propuesta precise su naturaleza ni las condiciones en las que ejercerían esta competencia. Aunque es probable que esta tarea sea realizada por un órgano público (como la administración aduanera o los servicios de control de fronteras), la propuesta no impide expresamente que los Estados miembros encomienden su ejecución a servicios de inteligencia o incluso a cualquier tipo de entidad de tratamiento de datos. El SEPD destaca que la transparencia y las garantías exigidas a los servicios de inteligencia no son siempre idénticas a las que se aplican a los servicios represivos tradicionales. Es indispensable que se precise la naturaleza de las Unidades de Información sobre Pasajeros, porque tendrá consecuencias directas en el régimen jurídico aplicable y en las condiciones de supervisión. El SEPD considera que la propuesta debe incluir disposiciones adicionales sobre las particularidades de dichas unidades.

([1]) Véase el artículo 6 de la propuesta.

([2]) La sociedad SITA fue creada en 1949 por once compañías aéreas. Presta servicios de valor añadido al sector del transporte aéreo a través de su rama comercial, SITA INC (información, redes e informática), y servicios de red a través de su cooperativa SITA SC.

([3]) Evaluación de impacto, anexo A, «*Method of transmission of the data by the carriers*».

([4]) Véase el artículo 3 de la propuesta.

Autoridades competentes

72. Del artículo 4 de la propuesta se desprende que cualquier autoridad responsable de prevenir o combatir el terrorismo y la delincuencia organizada puede recibir los datos. La finalidad está claramente definida, pero no hay precisiones sobre la naturaleza de estas autoridades. La propuesta no establece en ningún momento que los destinatarios de los datos sólo puedan ser autoridades con funciones represivas.

Como se ha indicado ya en lo que se refiere a las Unidades de Información sobre Pasajeros, es fundamental que el tratamiento de la información sensible de que se trata se realice en un entorno jurídico claro. Esta claridad es siempre mucho mayor en el caso de las autoridades con funciones represivas que en lo tocante a los servicios de inteligencia. Si se tienen en cuenta los elementos de prospección de datos y de investigación anticipatoria que contiene la propuesta, no cabe excluir que tales servicios de inteligencia u otros tipos de autoridades participen en el tratamiento de datos.

Conclusión

73. Como observación general, el SEPD señala que la implantación de un registro de nombres de pasajeros de la UE se ve aún más dificultada por el hecho de que las autoridades represivas tienen competencias diferentes según la legislación nacional de cada Estado miembro, con independencia de que se incluya o no en esta categoría de autoridades a los servicios de inteligencia, la administración aduanera, los servicios de inmigración o la policía. Ésta es, sin embargo, una razón más para recomendar que la propuesta sea mucho más precisa en lo que respecta a la naturaleza de los agentes mencionados y a las garantías de control de la ejecución de sus funciones. Habría que añadir a la propuesta disposiciones que especifiquen de manera rigurosa las competencias y obligaciones jurídicas de los intermediarios, las Unidades de Información sobre Pasajeros y las demás autoridades competentes.

V. CONDICIONES DE TRANSMISIÓN A TERCEROS PAÍSES

74. La propuesta establece algunas salvaguardias en relación con la transmisión de los datos del PNR a terceros países ([1]). En particular, dispone expresamente que este tipo de transferencias está sujeto a la Decisión marco relativa a la protección de datos, limita de manera expresa los fines para los cuales pueden emplearse los datos y estipula que el Estado miembro que transfirió los datos debe dar su consentimiento para que éstos puedan transferirse a otro país tercero, además de establecer que la transferencia debe cumplir las disposiciones de la legislación nacional del Estado miembro de que se trate y las de cualesquiera acuerdos internacionales aplicables.

75. Sin embargo, quedan abiertas muchas cuestiones, en particular en relación con la forma del consentimiento, las condiciones de aplicación de la Decisión marco relativa a la protección de datos y la cuestión de la «reciprocidad» en las transferencias de datos a terceros países.

([1]) Véase el artículo 8 de la propuesta.

Forma del consentimiento

76. El Estado miembro de origen debe dar su consentimiento expreso para que los datos puedan ser transferidos de un país tercero a otro. La propuesta no especifica en qué condiciones debe darse este consentimiento y a quién corresponde darlo, ni indica si las autoridades nacionales de protección de datos deben intervenir en la decisión. El SEPD considera que la forma en que se dará el consentimiento debe ser, como mínimo, conforme con las leyes nacionales que regulen las condiciones de transmisión de datos personales a terceros países.

77. Por otra parte, el consentimiento del Estado miembro no debe prevalecer sobre el principio de que el país destinatario de los datos ha de garantizar un nivel adecuado de protección para el tratamiento de que se trate. Estas condiciones deben ser acumulativas, como ocurre en la Decisión marco relativa a la protección de datos (artículo 14). El SEPD sugiere por ello que se añada en el artículo 8.1 una letra c) con el siguiente texto: «y c) el país tercero garantiza un nivel adecuado de protección para el tratamiento de datos previsto». El SEPD recuerda, a este respecto, que deben implantarse mecanismos que garanticen la existencia de normas comunes y decisiones coordinadas en lo que respecta a la idoneidad de la protección ([2]).

Aplicación de la Decisión marco relativa a la protección de datos

78. La propuesta remite a las condiciones y garantías contenidas en la Decisión marco relativa a la protección de datos, al tiempo que precisa expresamente ciertas condiciones, en particular el consentimiento antes mencionado del Estado miembro del que proceden los datos, y limita la finalidad del tratamiento de los datos a la prevención y lucha contra el terrorismo y la delincuencia organizada.

79. La Decisión marco relativa a la protección de datos supedita la transferencia de datos personales a terceros países a una serie de condiciones, entre ellas la limitación de la finalidad del tratamiento, la naturaleza de los destinatarios, el consentimiento del Estado miembro y el principio de idoneidad. Sin embargo, prevé también excepciones a estas condiciones de transmisión: la existencia de intereses superiores legítimos, en particular intereses públicos importantes, puede ser motivo suficiente para que los datos se transfieran aunque no se cumplan las condiciones mencionadas.

80. Como se ha indicado en la sección III del presente dictamen, el SEPD considera que es necesario estipular expresamente en el texto de la propuesta que las garantías más precisas de ésta prevalecen sobre las condiciones —y excepciones— generales de la Decisión marco relativa a la protección de datos, cuando ésta sea de aplicación.

([2]) Dictamen del SEPD de 26 de junio de 2007 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, apartados 27 a 30 (DO C 139 de 23.6.2007, p. 1).

Reciprocidad

81. La propuesta aborda la posibilidad de que un país pida a la UE, a título de «represalia», datos del PNR sobre vuelos que se dirigen a su territorio desde la UE. Cuando la UE solicita información de las bases de datos de las compañías aéreas de tales países terceros respecto de un vuelo que sale de la UE o se dirige a la UE, este tercer país podría pedir la misma información (incluidos datos de ciudadanos de la UE) de compañías aéreas establecidas en la UE. La Comisión considera que esta posibilidad es «muy remota», pero la ha previsto. La propuesta señala a este respecto que los acuerdos celebrados con Estados Unidos y Canadá establecen esta reciprocidad, «que puede aplicarse automáticamente» ([1]). El SEPD tiene dudas acerca de la relevancia de esta reciprocidad automática y de la aplicación de salvaguardias a tales transferencias, teniendo en cuenta, en particular, la existencia de un nivel adecuado de protección en los países en cuestión.

82. Debería establecerse una distinción entre los países terceros que han celebrado ya un acuerdo con la UE y los que no lo han hecho.

Países que no han celebrado un acuerdo con la UE

83. El SEPD observa que la reciprocidad puede dar lugar a la transmisión de datos personales a países en los que no hay garantías de aplicación de normas democráticas ni niveles adecuados de protección.

84. La evaluación de impacto ofrece más elementos de juicio acerca de las condiciones de la transmisión de datos a terceros países: se hace hincapié en las ventajas del sistema PNR de la UE, en el que los datos son filtrados por las Unidades de Información sobre Pasajeros; sólo los datos seleccionados de personas sospechosas (y no los datos en bloque) se transmitirían a las autoridades competentes de los Estados miembros y, es de suponer, de terceros países ([2]). El SEPD recomienda que se aclare este punto en el texto de la propuesta. Una simple indicación en la evaluación de impacto no proporciona la protección necesaria.

85. Si bien la selección de datos contribuiría a minimizar la repercusión de la propuesta en la intimidad de los pasajeros, debe recordarse que los principios de protección de datos van mucho más allá de la minimización de las transferencias de datos e incluyen principios como la necesidad, la transparencia y el ejercicio de los derechos del interesado, todos los cuales deben tenerse en cuenta a la hora de determinar si un país tercero proporciona un nivel adecuado de protección.

Países que han celebrado un acuerdo bilateral con la UE

86. La evaluación de impacto indica que el proceso de tratamiento elegido dará a la UE la posibilidad «de insistir en determinadas normas y de velar por la coherencia en estos acuerdos bilaterales con terceros países. Permitirá asimismo pedir un trato de reciprocidad a países terceros con los que la UE tiene un acuerdo, cosa que no es posible hoy por hoy» ([3]).

87. Estas observaciones llevan a plantearse cuáles serán las repercusiones de la propuesta en los acuerdos existentes con Canadá y Estados Unidos. Las condiciones de acceso a los datos previstas en esos acuerdos son, en efecto, mucho menos estrictas, dado que los datos no son objeto de un proceso de selección similar antes de su transmisión a dichos países.

88. La evaluación de impacto indica que «si la UE ha celebrado acuerdos internacionales con terceros países para intercambiar con ellos o transmitirles datos del PNR, es necesario tener debidamente en cuenta tales acuerdos. Las compañías aéreas deberían enviar datos del PNR a las Unidades de Información sobre Pasajeros aplicando las prácticas normales con arreglo a las medidas vigentes. La Unidad de Información sobre Pasajeros que reciba tales datos los transmitirá a la autoridad competente del país tercero con el que se haya celebrado el acuerdo» ([4]).

89. Aunque la propuesta parece encaminada a que *sólo* se transfieran datos *seleccionados* a las autoridades competentes (de dentro y fuera de la UE), tanto la evaluación de impacto como la propia propuesta, en su preámbulo (considerando 21) y en su artículo 11, recuerdan que los acuerdos existentes deben tenerse debidamente en cuenta. Esto podría llevar a la conclusión de que el filtrado sólo sería una medida válida para los acuerdos que se celebren en el futuro. De ello podría inferirse que la norma de acceso de las autoridades estadounidenses, por ejemplo, a los datos del PNR seguirá siendo el acceso a los datos en bloque, de conformidad con lo dispuesto en el acuerdo entre la UE y Estados Unidos, pero que, paralelamente a esta norma y en función de las circunstancias de cada caso, se podría transferir a Estados Unidos información específica determinada por las Unidades de Información sobre Pasajeros que contenga otros datos además de los relacionados con vuelos con destino en Estados Unidos.

90. El SEPD lamenta que este aspecto crucial de la propuesta no esté claro. Considera que es de capital importancia que las condiciones de transferencia de datos del PNR a terceros países sean coherentes y que se aplique a este respecto un nivel armonizado de protección. Por otra parte, por razones de seguridad jurídica, habría que incluir en la propuesta (y no sólo en la evaluación de impacto, como ocurre actualmente) precisiones sobre las garantías aplicables a la transferencia de datos.

([1]) Exposición de motivos de la propuesta, sección 2.
([2]) Evaluación de impacto, sección 5.2, «*Protection of privacy*».
([3]) Evaluación de impacto, sección 5.2, «*Relations with third countries*».
([4]) Evaluación de impacto, anexo A, «*Bodies receiving data from the Passenger Information Units*».

VI. OTROS ASPECTOS SUSTANTIVOS

Tratamiento automatizado de datos

91. El SEPD observa que la propuesta excluye expresamente la posibilidad de que las Unidades de Información sobre Pasajeros y las autoridades competentes de los Estados miembros tomen medidas represivas basadas únicamente en los resultados del tratamiento automatizado de los datos del PNR o en el origen racial o étnico de una persona, sus convicciones religiosas o filosóficas, sus opiniones políticas o su orientación sexual ([1]).

92. El SEPD se congratula de estas precisiones, ya que limitan el riesgo de que se tomen medidas arbitrarias contra personas. Sin embargo, observa que estas precisiones se limitan a las *medidas represivas* de las Unidades de Información sobre Pasajeros y de las autoridades competentes. No se aplican, según el enunciado actual, al filtrado automatizado de los datos de las personas en función de perfiles estándar, ni impiden que se confeccionen de forma automatizada listas de sospechosos a los que se apliquen medidas de vigilancia especial, por ejemplo, siempre y cuando tales medidas no se consideren «represivas».

93. El SEPD considera que el concepto de *medida represiva* es demasiado impreciso y que, por principio, el tratamiento automatizado de los datos de una persona, *por sí solo*, no debería permitir tomar *decisión alguna* sobre ella ([2]). El SEPD recomienda que se modifique el texto en consecuencia.

Idoneidad de los datos

94. El artículo 5.2 de la propuesta ofrece una precisión importante, a saber, que las compañías aéreas no están obligadas a recoger o conservar más datos que los que recopilen en el contexto de su actividad comercial normal.

95. Sin embargo, varios aspectos del tratamiento de estos datos merecen observaciones adicionales:

— los datos que han de facilitarse, según la lista del anexo I de la propuesta, son muy numerosos; esta lista es similar a la lista de datos a los que tiene acceso Estados Unidos con arreglo al acuerdo celebrado entre la UE y este país. Diversas fuentes, entre ellas el Grupo de Trabajo del artículo 29 ([3]), han cuestionado ya en varias ocasiones la idoneidad de algunos de los datos solicitados,

— de la formulación de la evaluación de impacto ([4]) y del artículo 6.3 de la propuesta parece deducirse que las compañías aéreas también podrían transmitir los datos en bloque a los intermediarios. En esta primera fase, los datos transmitidos a terceros ni siquiera tendrían que limitarse a datos del PNR indicados en la lista del anexo I de la propuesta,

— por lo que respecta al tratamiento de datos sensibles, aunque éstos puedan ser filtrados antes de su transmisión por los intermediarios, está por demostrar que resulte estrictamente necesario que las compañías aéreas transmitan el campo abierto.

El SEPD apoya las observaciones formuladas a este respecto por el Grupo de Trabajo del artículo 29.

Método de transferencia de los datos del PNR

96. Las compañías aéreas establecidas fuera de la UE están obligadas a emplear el método de exportación («método *push*») para transmitir los datos a las Unidades de Información sobre Pasajeros o a los intermediarios, siempre y cuando dispongan de los medios técnicos necesarios para ello. De lo contrario, deben permitir que los datos se obtengan por extracción («método *pull*»).

97. La coexistencia de métodos diferentes de comunicación de los datos en función de las compañías aéreas sólo hará que resulte más complejo controlar el cumplimiento de las normas de protección de datos durante las transferencias de datos del PNR. Además, esa coexistencia podría distorsionar la competencia entre las compañías aéreas de la UE y las demás.

98. El SEPD recuerda que el método de exportación de los datos, que permite a las compañías aéreas conservar el control sobre la idoneidad de los datos que se transfieren y las circunstancias de su transmisión, es el único admisible si se quiere respetar el principio de proporcionalidad del tratamiento de los datos. Por otra parte, la transmisión debe realizarse mediante una exportación efectiva, es decir, los datos no deben enviarse en bloque al intermediario, sino filtrados ya en esta primera etapa del proceso de tratamiento. No es admisible que se transmitan a terceros datos innecesarios (ni datos que no figuren en el anexo I de la propuesta), aunque vayan a ser suprimidos inmediatamente por sus destinatarios.

Conservación de datos

99. El artículo 9 de la propuesta dispone que los datos del PNR se conserven durante un periodo de 5 años, al que se añade otro periodo de 8 años durante el cual los datos permanecerán en una base de datos inactiva, a la que se podrá acceder sólo en determinadas condiciones.

([1]) Considerando 20 y artículos 3.3 y 3.5, respectivamente, de la propuesta.

([2]) Véase, a este respecto, el artículo 15.1 de la Directiva 95/46/CE. La Directiva prohíbe tales decisiones automatizadas siempre que vayan a tener efectos sobre la persona objeto de la medida. En el contexto de la propuesta, es probable que toda decisión adoptada en un marco represivo afecte siempre gravemente al interesado. Por otra parte, el hecho de ser objeto de controles adicionales puede afectar al interesado, en especial si estas medidas se le aplican repetidamente.

([3]) Véase, en particular, su dictamen nº 5/2007, de 17 de agosto de 2007, relativo al nuevo Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por parte de las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, celebrado en julio de 2007, WP 138.

([4]) Evaluación de impacto, anexo A, «*Method of transmission of the data by the carriers*».

100. El SEPD considera discutible la diferencia entre estos dos tipos de bases de datos: es discutible que la base de datos inactiva constituya un archivo real, con métodos diferentes de almacenamiento y recuperación de los datos. En efecto, la mayoría de las condiciones a las que está supeditado el acceso a la base de datos inactiva corresponden a requisitos de seguridad que podrían aplicarse igualmente al periodo de conservación de 5 años.

101. La duración total del periodo de almacenamiento (13 años) es en cualquier caso excesiva. Se ha justificado en la evaluación de impacto aludiendo a la necesidad de elaborar indicadores de riesgo y establecer pautas de viaje y de comportamiento ([1]); la eficacia de tales indicadores y pautas está aún por demostrar. Si bien es obvio que los datos pueden conservarse tanto tiempo como sea necesario en casos concretos, mientras se realizan las investigaciones correspondientes, no hay motivo alguno que permita justificar la conservación de los datos de todos los viajeros durante 13 años cuando no existe sospecha alguna.

102. El SEPD observa asimismo que este periodo de conservación no concuerda con las respuestas de los Estados miembros al cuestionario de la Comisión, ya que éstos consideraron que el periodo medio de conservación necesario sería de 3,5 años ([2]).

103. Por otra parte, este periodo de 13 años es similar al periodo de conservación que se fijó en el último acuerdo celebrado con Estados Unidos (15 años). Ahora bien, el SEPD tenía entendido que ese largo periodo se había aceptado únicamente debido a las fuertes presiones del gobierno estadounidense, que quería un periodo muy superior a 3,5 años, y no porque lo hubieran defendido en ningún momento el Consejo o la Comisión. No hay razón para incorporar a un instrumento jurídico interno de la UE esta transacción, que se ha presentado siempre como un resultado necesario de las negociaciones.

Función del Comité de Estados miembros

104. El Comité de Estados miembros al que se refiere el artículo 14 de la propuesta será competente para tratar cuestiones de seguridad, como protocolos y normas de cifrado de los datos del PNR, pero también para dar orientaciones sobre los requisitos generales comunes, los métodos y las prácticas relacionados con la evaluación del riesgo.

105. Aparte de estas indicaciones, la propuesta no contiene ningún elemento o criterio relativo a las condiciones concretas o al contexto del proceso de evaluación del riesgo. La evaluación de impacto indica que los criterios dependerán en última instancia de la información analítica de que disponga cada Estado miembro, y ésta no es un dato constante. La evaluación de riesgo se realizará sin normas uniformes de identificación de sospechosos. Es discutible, pues, que el Comité de Estados miembros pueda desempeñar un papel a este respecto.

Seguridad

106. La propuesta detalla una serie de medidas de seguridad ([3]) que han de tomar las Unidades de Información sobre Pasajeros, los intermediarios y otras autoridades competentes a fin de proteger los datos. Dada la importancia de la base de datos y los problemas que plantea el tratamiento de éstos, el SEPD considera que, además de las medidas previstas, habría que obligar a la entidad que realice el tratamiento a notificar oficialmente todo quebrantamiento de la seguridad.

107. El SEPD está al tanto del proyecto de establecer un procedimiento de notificación de esta índole en el sector de las comunicaciones electrónicas a escala europea. Recomienda que se incluya esta salvaguardia en la propuesta, y remite a este respecto al sistema establecido por Estados Unidos para combatir el quebrantamiento de la seguridad en sus organismos oficiales ([4]). Pueden darse problemas de seguridad en cualquier ámbito de actividad, tanto en el sector público como en el privado, como demuestra, por poner un ejemplo reciente, la pérdida por la administración del Reino Unido de una base de datos completa sobre los ciudadanos británicos ([5]). Este tipo de sistemas de alerta debe aplicarse prioritariamente a las bases de datos de gran envergadura, como la prevista en la propuesta.

Cláusula de examen y cláusula de extinción

108. El SEPD toma nota de que la Decisión marco que nos ocupa debe ser examinada, a los tres años de su entrada en vigor, sobre la base de un informe elaborado por la Comisión. Reconoce que en ese examen, basado en la información facilitada por los Estados miembros, se prestará especial atención a las garantías de protección de datos, a la aplicación del método de exportación de datos, a la conservación de éstos y a la calidad de la evaluación de riesgos. Para ser exhaustivo, este examen debería incluir los resultados de un análisis de los datos estadísticos elaborados a partir del tratamiento de la información del PNR. Tales estadísticas deberían incluir, además de los elementos mencionados en el artículo 18 de la propuesta, datos estadísticos sobre la identificación de personas de alto riesgo, como los criterios para tal identificación y los resultados concretos de las medidas represivas adoptadas como consecuencia de la identificación.

([1]) Evaluación de impacto, anexo A, «*Data retention period*».
([2]) Evaluación de impacto, anexo B.
([3]) Véase el artículo 12 de la propuesta.
([4]) Véanse, en particular, los trabajos de la comisión especial estadounidense sobre la suplantación de identidad (*Identity Theft Task Force*): http://www.idtheft.gov/
([5]) Véase el enlace al sitio de la Administración de Hacienda y Aduana del Reino Unido: http://www.hmrc.gov.uk/childbenefit/update-faqs.htm
Véase también: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

109. El SEPD ha insistido ya en el presente dictamen en la ausencia de elementos concretos que demuestren la necesidad del sistema propuesto. No obstante, considera que, en caso de que la Decisión marco tuviera que entrar en vigor, debería completarse, como mínimo, con una cláusula de extinción. Al final del periodo de tres años, la Decisión marco debería ser derogada si no ha aparecido ningún elemento que demuestre la conveniencia de que siga vigente.

Efectos en otros instrumentos jurídicos

110. En sus disposiciones finales, la propuesta supedita la continuación de la aplicación de los acuerdos o convenios bilaterales o multilaterales ya existentes a la condición de que sean compatibles con los objetivos de la Decisión marco propuesta.

111. El SEPD tiene dudas sobre el alcance de esta disposición. Como ya se ha mencionado en la sección V en relación con la reciprocidad, no está claro qué repercusiones tendrá esta disposición en el contenido de acuerdos con terceros países como el celebrado con Estados Unidos. Por otra parte, tampoco está claro si esta disposición puede influir en las condiciones de aplicación de instrumentos cuyo ámbito de aplicación es mayor, como el Convenio nº 108 del Consejo de Europa. Es importante evitar todo riesgo de malinterpretación, por improbable que pueda parecer dado que se trata de agentes y contextos institucionales diferentes; para ello, debe aclararse en la propuesta que ésta no afecta en modo alguno a los instrumentos que tienen un ámbito de aplicación más amplio, en particular los que tienen por objeto la protección de los derechos fundamentales.

VII. **CONCLUSIÓN**

112. El SEPD destaca que la propuesta tendrá enormes repercusiones en la protección de datos. Se ha centrado en su análisis en los cuatro problemas principales que suscita la propuesta, e insiste en que las cuestiones que se han planteado deben resolverse de forma global. En las circunstancias actuales, la propuesta vulnera ciertos derechos fundamentales, en particular el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, y no debe ser adoptada.

113. Para solventar los problemas mencionados *supra*, especialmente la prueba de legitimidad, se han formulado en el presente dictamen algunas propuestas de redacción que el legislador debería tener en cuenta. Se trata, concretamente, de las indicadas en los apartados 67, 73, 77, 80, 90, 93, 106, 109 y 111 del dictamen.

Legitimidad de las medidas propuestas

114. Si bien el objetivo general de combatir el terrorismo y la delincuencia organizada es en sí mismo claro y legítimo, los aspectos fundamentales del tratamiento de datos que debe implantarse no están suficientemente circunscritos y justificados.

115. El SEPD considera que, antes de que puedan aplicarse a gran escala técnicas encaminadas a evaluar el riesgo que representa una persona sobre la base de instrumentos de prospección de datos y pautas de comportamiento, es preciso aquilatarlas mejor y demostrar claramente su utilidad en el marco de la lucha contra el terrorismo.

116. La acumulación de diferentes bases de datos sin una visión global de sus resultados concretos y sus carencias:

— es contraria a una política legislativa racional, que exige que no se adopten nuevos instrumentos antes de que los existentes hayan sido plenamente implantados y hayan demostrado ser insuficientes,

— puede, por lo demás, conducirnos a una sociedad basada en una vigilancia total.

117. Indudablemente, la lucha contra el terrorismo puede constituir un motivo legítimo para aplicar excepciones a los derechos fundamentales a la intimidad y la protección de datos. Sin embargo, para que tales excepciones sean válidas, la necesidad de la injerencia debe basarse en elementos claros e indiscutibles, y debe demostrarse la proporcionalidad del tratamiento de datos propuesto. Estos requisitos son especialmente necesarios en el caso de una injerencia generalizada en la intimidad de las personas como la prevista en la propuesta.

118. Estos elementos justificativos no están presentes en la propuesta, que no supera tampoco las pruebas de necesidad y proporcionalidad.

119. El SEPD insiste en que las pruebas de necesidad y proporcionalidad desarrolladas *supra* son esenciales: constituyen una *condición indispensable* para la entrada en vigor de esta propuesta.

Marco jurídico aplicable

120. El SEPD señala que existe una grave inseguridad jurídica en lo que respecta al régimen de protección de datos aplicable a los diferentes agentes que intervienen en el tratamiento según la propuesta, en particular las compañías aéreas y demás agentes del primer pilar. A estos agentes se les pueden aplicar bien las normas de la propuesta, bien las normas de la Decisión marco relativa a la protección de datos, o bien la legislación nacional de aplicación de la Directiva 95/46/CE. El legislador debe aclarar en qué etapa precisa del tratamiento se aplican estas diferentes normas.

121. La tendencia actual a imponer de forma sistemática a los agentes del sector privado obligaciones de cooperación para fines represivos plantea la cuestión de cuál es el régimen de protección de datos (primer o tercer pilar) que regula las condiciones de tal cooperación: no está claro si las normas deben basarse en la naturaleza del responsable del tratamiento de los datos (sector privado) o en la finalidad del tratamiento (represiva).

122. El SEPD ha mencionado ya el riesgo de que se produzca un vacío jurídico entre las actividades del primer y el tercer pilar ([1]). En efecto, no está nada claro si las actividades de las empresas privadas que están conectadas de alguna manera con la aplicación del Derecho penal se encuentran dentro del ámbito de actuación del legislador de la Unión Europea según los artículos 30, 31 y 34 del Tratado de la UE.

123. Debe evitarse toda situación que dé lugar a la aplicación de diferentes regímenes de protección de datos a las operaciones de tratamiento de datos realizadas con distintos fines por los proveedores de servicios, sobre todo por las dificultades que semejante situación supondría para el ejercicio de los derechos de los interesados.

Naturaleza de los destinatarios de los datos

124. La propuesta debe especificar la naturaleza de los destinatarios de los datos personales recopilados por las compañías aéreas, ya se trate de los intermediarios, de las Unidades de Información sobre Pasajeros o de las autoridades competentes.

125. La naturaleza del destinatario, que puede ser en ciertos casos un agente del sector privado, está directamente relacionada con el tipo de garantías de protección de datos que se aplica al destinatario. Es indispensable que el régimen aplicable esté claro para todos los agentes que intervienen en el proceso, incluidos el legislador, las autoridades de protección de datos, los responsables del tratamiento y los titulares de los datos.

Transmisión de datos a terceros países

126. El SEPD destaca la necesidad de asegurarse de que el país destinatario de los datos garantice un nivel adecuado de protección. Cuestiona asimismo la pertinencia del principio de reciprocidad mencionado en la propuesta, y su aplicación a países ya vinculados por un acuerdo con la UE, como Canadá o Estados Unidos. Considera que es de capital importancia que las condiciones de transferencia de datos del PNR a terceros países sean coherentes y que se aplique a este respecto un nivel armonizado de protección.

Otros aspectos sustantivos

127. El SEPD señala también a la atención del legislador varios aspectos específicos de la propuesta que requieren mayor precisión o una consideración más adecuada del principio de protección de datos. Se trata, en particular, de los siguientes:

— es necesario restringir las condiciones en que pueden tomarse decisiones automatizadas,

— debe reducirse el número de categorías de datos que pueden ser objeto de tratamiento,

— la transferencia de datos debe hacerse únicamente mediante exportación («*push*»),

— el periodo de conservación de los datos es excesivo y no está justificado,

— se podría precisar más la función de orientación que incumbe al Comité de Estados miembros en lo que se refiere a la evaluación de riesgos,

— las medidas de seguridad deberían incluir un procedimiento de notificación de los quebrantamientos de la seguridad,

— la disposición relativa al examen de la Decisión marco debe incluir una cláusula de extinción,

— hay que aclarar en la propuesta que ésta no afecta en modo alguno a los instrumentos cuyo ámbito de aplicación es más amplio y que tienen por objeto, en particular, la protección de los derechos fundamentales.

Observaciones finales

128. El SEPD observa que la propuesta de que se trata se presenta en un momento en que la arquitectura institucional de la Unión Europea está a punto de sufrir profundas modificaciones. Las consecuencias del Tratado de Lisboa en el proceso decisorio serán fundamentales, en particular en lo que se refiere a la función del Parlamento Europeo.

129. Considerando que la propuesta tendrá unas repercusiones sin precedentes en lo tocante a los derechos fundamentales, el SEPD recomienda que, en lugar de adoptarla en el marco del Tratado vigente, se vele por que se le aplique el procedimiento de codecisión establecido en el nuevo Tratado. Este proceder permitirá reforzar los fundamentos jurídicos en los que se basaría la adopción de las decisivas medidas que prevé la propuesta.

([1]) Véase el dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos (DO C 255 de 27.10.2007, p. 1). Véase también el Informe anual de 2006, p. 47.