COMISIÓN EUROPEA

Bruselas, 2.2.2011
COM(2011) 32 final

2011/0023 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves

{SEC(2011) 132 final}
{SEC(2011) 133 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

- **Motivación y objetivos de la propuesta**

En la última década, la UE y otras zonas del mundo han visto incrementarse la delincuencia organizada y otros delitos graves como la trata de seres humanos[1] y el tráfico de drogas[2]. Según la recopilación de estadísticas sobre la delincuencia y la justicia penal, en 2007 se cometieron aproximadamente 14 000 delitos por 100 000 habitantes en los Estados miembros de la UE (excluidos Italia y Portugal, sobre los que no hay datos disponibles), que oscilaron entre 14 465 delitos en Suecia y 958 en Chipre. En la Evaluación de la Amenaza de la Delincuencia Organizada (OCTA) en la UE realizada por Europol en 2009 se señala que la mayoría de los delitos cometidos por la delincuencia organizada implican viajes internacionales dedicados por lo general al tráfico de personas, drogas o mercancías ilícitas en la UE.

Al mismo tiempo, los terroristas y las organizaciones terroristas se encuentran dentro y fuera de las fronteras de la UE. Los atentados terroristas de 2001 en los Estados Unidos, el atentado terrorista frustrado de agosto de 2006 de hacer explotar varios aviones en el trayecto del Reino Unido a los Estados Unidos y la tentativa de atentado terrorista a bordo de un vuelo de Ámsterdam a Detroit en diciembre de 2009, han puesto de manifiesto la capacidad de los terroristas para organizar atentados contra vuelos internacionales en cualquier país. Si bien la actividad terrorista disminuyó en la UE en 2009, de acuerdo con el Informe 2010 de Europol sobre la situación y las tendencias del terrorismo en la UE, la amenaza del terrorismo sigue siendo real y grave. La mayoría de los actos terroristas tiene carácter transnacional e implica viajes internacionales[3] con destino, entre otros, a campos de entrenamiento fuera de la UE, lo que exige una cooperación creciente entre los servicios con funciones coercitivas.

Los delitos graves y los delitos terroristas causan graves daños a sus víctimas, provocan perjuicios económicos a gran escala y socavan la sensación de seguridad sin la cual las personas no pueden ejercitar eficazmente su libertad y los derechos individuales.

Un estudio publicado en 2009[4] para la Organización Internacional del Trabajo estimó que, en las economías industrializadas, la explotación económica resultante de la trata de seres humanos en 2007 supuso un coste de 2 508 368 218 dólares USA, mientras que el total mundial fue de 19 598 020 343 dólares USA.

El informe anual 2010 sobre la situación del problema de las drogas en Europa del Observatorio Europeo de las Drogas y las Toxicomanías, señala el carácter global del problema de las drogas y los daños graves y crecientes que causa. Al socavar el desarrollo social y alimentar la corrupción y la delincuencia organizada, representa una amenaza real para la Unión Europea. Anualmente se producen en la UE alrededor de 1 000 fallecimientos relacionados con la cocaína. Según un cálculo prudente, el número de consumidores de opiáceos en Europa es de 1, 35 millones. En cuanto a las repercusiones económicas y sociales

---

1 Evaluación de la Amenaza de la Delincuencia Organizada en la UE por Europol, 2009.
2 Eurostat 36/2009.
3 Informe 2010 de Europol sobre Situación y tendencias del terrorismo en la UE.
4 *Measuring the costs of coercion to workers in forced labour*- Vinogradova, De Cock, Belser.

de las drogas, 22 Estados miembros comunicaron en 2008 un gasto total de 4 200 millones de euros relativo a drogas ilícitas.

Otro estudio, procedente del Ministerio del Interior del Reino Unido[5], calculó costes generados antes del delito como los gastos defensivos, costes resultantes del delito como las secuelas físicas y psíquicas para la víctima y el valor de los bienes robados, así como costes generados como respuesta al delito, incluidos los del sistema judicial penal. Estos costes se fijaron en 36 166 000 000 £ en 2003.

Al mismo tiempo, cuatro de cada cinco europeos desean que la UE refuerce su acción contra la delincuencia organizada y el terrorismo[6].

Como respuesta a la amenaza que suponen los delitos graves y el terrorismo, y a la supresión de los controles fronterizos interiores en virtud del Convenio de Schengen, la UE adoptó medidas para la recogida y el intercambio de datos personales entre los servicios con funciones coercitivas y otras autoridades. Estas medidas han demostrado su utilidad, si bien tienden a centrarse en datos relativos a personas que ya son sospechosas, es decir, personas que son «conocidas» por los servicios con funciones coercitivas. El Sistema de Información de Schengen (SIS)[7], el Sistema de Información de Schengen de segunda generación (SIS II)[8], el Sistema de Información de Visados (VIS)[9], y el sistema de entrada y salida anticipado, son ejemplos de dichas medidas.

En su «Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia»[10] la Comisión incluyó un análisis de dichas medidas y subrayó la necesidad de intensificar la cooperación entre los servicios con funciones coercitivas en lo que respecta a los pasajeros de vuelos internacionales con destino a o procedentes de los Estados miembros, incluida una utilización más sistemática de los datos del registro de nombres de los pasajeros (*Passenger Name Record- PNR*) con fines coercitivos. El «Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano»[11] insta a la Comisión a presentar una propuesta sobre la utilización de datos PNR para prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves.

Los datos PNR consisten en información no verificada suministrada por los pasajeros que es recogida y conservada en los sistemas de control de reservas y salidas de las compañías aéreas para sus propios fines comerciales. Los diversos tipos de información que contienen son las fechas de viaje e itinerario, datos del billete, datos de contacto, la agencia de viajes que reservó el vuelo, medios de pago utilizados, número de asiento y datos del equipaje.

Los servicios con funciones coercitivas pueden utilizar los datos PNR de diferentes maneras:

---

5 *The economic and social costs of crime against individuals and households* 2003/04.

6 Eurobarómetro estándar 71, p. 149 del anexo.

7 Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes (DO L 239 de 22.9.2000, p. 19).

8 Reglamento (CE) nº 1987/2006, Reglamento (CE) nº 1986/2006.

9 Decisión 2004/512/CE del Consejo, Reglamento (CE) nº 767/2008, Decisión 2008/633/JAI del Consejo. Véase también la Declaración sobre la lucha contra el terrorismo, Consejo Europeo, 25.3.2004.

10 COM(2010) 385.

11 Documento del Consejo nº 17024/09 de 2.12.2009.

reactiva: utilización en investigaciones, enjuiciamientos, desmantelamiento de redes tras la comisión de un delito. Para que los servicios con funciones coercitivas puedan remontarse suficientemente en el tiempo, es necesario un periodo adecuado de conservación de datos por los servicios con funciones coercitivas.

en tiempo real: utilización anterior a la llegada o salida de los pasajeros con objeto de prevenir un delito, vigilar o detener a personas antes de la comisión de un delito o porque se ha cometido o se está cometiendo un delito. En tales casos los datos PNR son necesarios para contrastar determinados criterios de evaluación, con el fin de identificar a los sospechosos previamente «desconocidos» y contrastar diversas bases de datos de personas y objetos buscados.

proactiva: utilización de los datos para el análisis y el establecimiento de criterios de evaluación que podrán utilizarse posteriormente en la evaluación previa a la llegada y la salida de pasajeros. Para llevar a cabo ese análisis pertinente para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, será necesario en tales casos un periodo adecuado de conservación de datos por los servicios con funciones coercitivas.

La recogida, utilización y conservación más sistemáticas de los datos PNR relativos a los vuelos internacionales, con arreglo a unas garantías de protección de datos estrictas, reforzarán la prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos graves y, como se ha explicado anteriormente, son necesarias para responder a las amenazas contra la seguridad y reducir los daños causados.

No obstante, en la actualidad la utilización de datos PNR no está regulada en el ámbito de la UE. Aunque sólo un número reducido de Estados miembros ha establecido un sistema PNR hasta la fecha, la mayoría de ellos utiliza los datos PNR para prevenir, detectar, investigar y enjuiciar los delitos graves y los delitos terroristas de forma no sistemática o en virtud de poderes generales conferidos a la policía y otras autoridades. En el ámbito de la UE, el Reino Unido ya dispone de un sistema PNR, mientras que Francia, Dinamarca, Bélgica, Suecia y los Países Bajos han aprobado la normativa necesaria o están probando actualmente la utilización de datos PNR. Otros Estados miembros están considerando establecer sistemas PNR. Estas medidas nacionales difieren en varios aspectos como la finalidad del sistema, el periodo de conservación de datos, la estructura del sistema, el ámbito geográfico y los modos de transporte tratados. También es muy probable que, una vez adoptado el marco normativo completo sobre la utilización de datos PNR en los Estados miembros, haya normas divergentes sobre protección de datos y las medidas de seguridad aplicables a las transferencias de datos. Podrían crearse hasta 27 sistemas considerablemente divergentes. El resultado serían unos niveles de protección desigual de los datos personales en toda la UE, diferencias en la seguridad, costes crecientes e inseguridad jurídica tanto para las compañías aéreas como para los pasajeros.

La propuesta se propone, por tanto, armonizar las disposiciones de los Estados miembros relativas a la obligación de las compañías aéreas que efectúan vuelos entre un tercer país y el territorio de al menos un Estado miembro de transmitir los datos PNR a las autoridades competentes con la finalidad de detectar, investigar y enjuiciar los delitos terroristas y los delitos graves. No exige a las compañías aéreas recoger información adicional de los pasajeros ni conservar ningún dato, ni exige a los pasajeros facilitar datos adicionales a los ya previstos a las compañías aéreas.

Es necesario imponer dichas obligaciones legales a las compañías aéreas por las razones siguientes:

En primer lugar, los datos PNR permiten a los servicios con funciones coercitivas identificar a personas que previamente eran «desconocidas», es decir, personas que previamente no eran sospechosas de estar implicadas en un delito terrorista o delito grave pero que un análisis de los datos indica que pueden estar implicadas en dicho delito y, por tanto, deben ser objeto de un nuevo examen por las autoridades competentes. La identificación de esas personas ayuda a los servicios con funciones coercitivas a prevenir y descubrir delitos graves, incluidos actos terroristas. Para lograrlo, los servicios con funciones coercitivas deben utilizar los datos PNR tanto en tiempo real para contrastarlos con los criterios de evaluación predeterminados que indican cuales son las personas previamente «desconocidas» que requieren ser examinadas de nuevo, como de forma proactiva para el análisis y la creación de criterios de evaluación.

Por ejemplo, el análisis de datos PNR puede dar indicaciones sobre las rutas de viaje más habituales de los traficantes de personas o de drogas que pueden encajar en los criterios de evaluación. El control de datos PNR en tiempo real con arreglo a tales criterios puede prevenir o detectar delitos. Un ejemplo concreto proporcionado por un Estado miembro es un asunto en el que el análisis de datos PNR descubrió un grupo de traficantes de personas que viajaba siempre por la misma ruta. Utilizaban documentos falsos para facturar en un vuelo interior de la UE y al mismo tiempo usaban documentos auténticos para facturar en otro vuelo destinado a un tercer país. Una vez en la sala de espera del aeropuerto, embarcaban en el vuelo interior de la UE. Sin los datos PNR habría sido imposible desmantelar esta red de tráfico de personas.

Así, la utilización proactiva y en tiempo real combinadas de los datos PNR puede permitir a los servicios con funciones coercitivas enfrentarse a la amenaza de delitos terroristas y delitos graves desde una perspectiva distinta del tratamiento de otras categorías de datos personales: como se explica más adelante, el tratamiento de los datos personales disponibles para los servicios con funciones coercitivas a través de medidas de ámbito de la UE existentes y previstas como la Directiva sobre la información previa sobre pasajeros[12], el Sistema de Información de Schengen (SIS), y el Sistema de Información de Schengen de segunda generación (SIS II), no permiten a los servicios con funciones coercitivas identificar a los sospechosos «desconocidos» del mismo modo que el análisis de datos PNR.

En segundo lugar, los datos PNR ayudan a los servicios con funciones coercitivas a prevenir, detectar, investigar y enjuiciar delitos graves, incluidos los actos terroristas, después de la comisión de un delito. Para lograrlo, los servicios con funciones coercitivas deben utilizar los datos PNR en *tiempo real* para contrastarlos con diversas bases de datos de personas «conocidas» y objetos buscados. También deben utilizar los datos PNR de manera reactiva para elaborar pruebas y, en su caso, descubrir a los cómplices de los delincuentes y desmantelar las redes delictivas.

Por ejemplo, la información de la tarjeta de crédito que forma parte de los datos PNR puede permitir a los servicios con funciones coercitivas identificar y demostrar los vínculos entre una persona y una organización delictiva o un delincuente conocido. Un ejemplo proporcionado por un Estado miembro se refiere al tráfico de personas y drogas a gran escala que afecta a un Estado miembro y terceros países. Los cárteles importaban drogas a diversos

[12] Directiva 2004/82/CE de 29 de agosto de 2004.

destinos en Europa. Utilizaban a personas que ingerían la droga y que a su vez eran víctimas de la trata. Su identificación por medio de los PNR fue posible porque habían comprado el billete con tarjetas de crédito robadas. Esto condujo a detenciones en los Estados miembros. De esta forma se creó un criterio de evaluación que a su vez condujo a realizar varias detenciones adicionales en otros Estados miembros y terceros países.

Por último, la utilización de datos PNR antes de la llegada permite a los servicios con funciones coercitivas realizar una evaluación y un control más detallado únicamente de las personas que, según el criterio de evaluación objetivo y la experiencia previa, pueden suponer una amenaza para la seguridad. Así se facilita el viaje a los demás pasajeros y se reduce el riesgo de que éstos sean examinados al entrar en la UE con criterios ilegales como la nacionalidad o el color de la piel que los servicios con funciones coercitivas, incluidos los guardias fronterizos y de aduanas, pueden asociar erróneamente con riesgos para la seguridad.

Las medidas propuestas suponen la recogida y el tratamiento de datos PNR por los servicios con funciones coercitivas y, por tanto, afectan a los derechos a la intimidad y la protección de datos. Para garantizar el cumplimiento del principio de proporcionalidad, se ha limitado cuidadosamente el alcance de la propuesta, que contiene garantías estrictas de protección de datos.

La necesidad de utilizar datos PNR, de manera limitada y con garantías estrictas de protección de datos, se basa en una serie de elementos de hecho que se recogen en la evaluación de impacto que acompaña a la presente propuesta. En ausencia de disposiciones armonizadas sobre la recogida y el tratamiento de datos PNR en el ámbito de la UE, no se dispone de estadísticas detalladas sobre la medida en que dichos datos contribuyen a prevenir, detectar, investigar y perseguir delitos graves y de terrorismo. La necesidad de utilizar datos PNR ha sido confirmada por la información procedente de los terceros países y los Estados miembros que ya utilizan datos PNR con fines coercitivos.

La experiencia de estos países muestra que la utilización de datos PNR ha permitido realizar progresos fundamentales en la lucha contra la droga, la trata de seres humanos y el terrorismo, así conocer mejor la composición y el funcionamiento de las redes terroristas y otras redes delictivas. En lo que respecta a las drogas, los Estados miembros han indicado que la mayoría de las incautaciones se han realizado mediante el uso de datos PNR en *tiempo real* y de forma *proactiva.* Bélgica informó de que el 95 % del total de las incautaciones de drogas en 2009 se debió exclusivamente o de forma determinante al tratamiento de datos PNR. Suecia informó de que el 65-75 % del total de las incautaciones de drogas en 2009 se debió exclusivamente o de forma determinante al tratamiento de datos PNR. Esto representó 278,9 kilos de cocaína y cantidades adicionales de heroína y otras drogas. Los Estados Unidos informaron de que en un periodo de 6 meses en 2010 se incautaron 212 kilos de cocaína y 20 kilos de heroína debido exclusivamente o de forma determinante al tratamiento de datos PNR.

- **Contexto general**

El 6 de noviembre de 2007 la Comisión adoptó 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[13] (denominada en lo sucesivo «la propuesta de 2007»). La propuesta se debatió ampliamente en los grupos de trabajo del Consejo y los progresos realizados en los debates fueron apoyados por el Consejo de Justicia y Asuntos de Interior en

[13] COM(2007) 654.

enero, julio y noviembre de 2008. Los debates sobre la propuesta que tuvieron lugar en los grupos de trabajo permitieron alcanzar un consenso sobre la mayoría de sus disposiciones[14].

Al entrar el vigor el Tratado de Funcionamiento de la Unión Europea (TFUE) el 1 de diciembre de 2009, la propuesta de la Comisión, que todavía no había sido aprobada por el Consejo, quedó obsoleta. La propuesta actual sustituye a la propuesta de 2007 y se basa en las disposiciones del TFUE. Tiene en cuenta las recomendaciones del Parlamento Europeo contenidas en su Resolución de noviembre de 2008[15], y refleja el estado de los últimos debates de los grupos de trabajo del Consejo en 2009. Asimismo tiene en cuenta los dictámenes del Supervisor Europeo de Protección de Datos[16], del Grupo de trabajo del artículo 29 sobre protección de datos[17] y de la Agencia Europea de Derechos Fundamentales[18].

- **Disposiciones vigentes en el ámbito de la propuesta**

Los datos PNR son diferentes de la información previa sobre pasajeros (*Advance Passenger Information*, API) y no deben confundirse con ésta. Los datos API son información biográfica que figura en la parte de lectura óptica del pasaporte y se refieren al nombre y apellidos, el lugar de nacimiento, la nacionalidad de la persona, el número de pasaporte y su fecha de expiración. Por tanto, son distintos y de alcance más limitado que los datos PNR.

En la UE la utilización de la información API está regulada por la Directiva API[19]. La Directiva establece que los datos API deben ponerse a disposición de las autoridades de control de fronteras, a instancia de cada Estado miembro, en el caso de los vuelos que entren en el territorio de la UE, con el fin de mejorar los controles fronterizos y combatir la inmigración clandestina. Aunque la Directiva permite utilizar estos datos para fines coercitivos, esto sólo es posible si se cumplen los criterios específicos. Así, aunque en algunos casos los servicios con funciones coercitivas utilizan los datos API para identificar a sospechosos y personas buscadas, estos datos se utilizan principalmente como un instrumento de control de identidad y gestión fronteriza. Además, los datos API no permiten a los servicios con funciones coercitivas realizar una evaluación de los pasajeros y, por tanto, no facilitan la detección de delincuentes o terroristas hasta entonces «desconocidos».

El objetivo del **Sistema de Información de Schengen** (SIS) es mantener la seguridad pública, incluida la seguridad nacional, en el espacio Schengen. El SIS es un sistema de información centralizado que consta de una parte nacional en cada Estado participante y una unidad de apoyo técnico en Francia. Los Estados miembros pueden introducir descripciones de las personas buscadas para su detención a efectos de entrega o extradición; de extranjeros a los que se deniega la entrada; personas desaparecidas; testigos o personas objeto de una citación judicial; personas y vehículos sujetos a controles adicionales; vehículos, documentos y armas de fuego perdidos o robados; y billetes de banco sospechosos.

El **Sistema de Información de Visados** (VIS) trata de abordar ambas cuestiones. Su objetivo es ayudar a aplicar una política de visados común facilitando el examen de las solicitudes de

---

14 Documento del Consejo nº 5618/2/09 REV 2 de 29.6.2009.
15 P6_TA (2008) 0561.
16 DO C 110 de 1.5.2008.
17 Dictamen nº 145 de 5.12.2007.
18 http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf.
19 Directiva 2004/82/CE de 29 de agosto de 2004.

visado y los controles en las fronteras exteriores, y contribuyendo al mismo tiempo a prevenir las amenazas para la seguridad interior de los Estados miembros. Es un sistema de información centralizado que incluye una parte nacional en cada Estado participante y una función de apoyo técnica en Francia. El VIS usará un sistema de correspondencias biométricas para garantizar unas comparaciones fidedignas de las impresiones dactilares y verificar la identidad de los titulares de visado en las fronteras exteriores. En él se incluirán datos sobre las solicitudes de visados, fotografías, impresiones dactilares, decisiones relacionadas de las autoridades responsables de los visados y enlaces entre aplicaciones relacionadas.

Por lo tanto, al igual que el sistema API, el SIS y el VIS se utilizan principalmente para verificar la identidad y como instrumentos de gestión fronteriza, y sólo son útiles si se conoce la identidad del sospechoso. Estos instrumentos no son útiles para realizar evaluaciones de personas ni para detectar delincuentes o terroristas «desconocidos».

La UE, los Estados Unidos, Canadá y Australia han celebrado acuerdos de transmisión de datos PNR, limitados a los viajes por avión, en el contexto de la lucha contra el terrorismo y los delitos transnacionales graves. Estos acuerdos exigen a las compañías aéreas, que recopilan datos PNR de los pasajeros para sus propios fines comerciales, que transmitan estos datos a las autoridades competentes de los Estados Unidos, Canadá y Australia. Los tres acuerdos deberán renegociarse durante 2011. Otros países como Corea del Sur y Japón han solicitado también negociar este tipo de acuerdos. La Comisión presentó los elementos esenciales de la política de la UE en esta materia en su Comunicación de 21 de septiembre de 2010 «Sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países»[20]. La presente propuesta es plenamente coherente con la política establecida en esa Comunicación.

- **Coherencia con otras políticas y objetivos de la Unión**

El Sistema de Información de Schengen (SIS)[21], el Sistema de Información de Schengen de segunda generación (SIS II)[22], el Sistema de Información de Visados (VIS)[23], el sistema de entrada y salida anticipado y el programa de viajeros registrados, son medidas de la UE relacionadas directamente con acciones que tienen lugar físicamente en las fronteras.

Aunque los PNR son datos de los pasajeros relativos al viaje, se utilizan más como instrumento de investigación penal que como instrumento de control fronterizo. Se utilizan antes del cruce de frontera, no en el momento del cruce de frontera. El objetivo principal que se persigue con la utilización de los datos PNR es luchar contra el terrorismo y los delitos graves más que luchar contra la inmigración clandestina y facilitar los controles fronterizos.

La propuesta no cambiará ni interferirá con las actuales normas de la UE sobre la forma en que se realizan los controles ni con las normas de la UE que regulan la entrada y salida en el

---

20 COM(2010) 492.

21 Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes (DO L 239 de 22.9.2000, p. 19).

.

22 Reglamento (CE) nº 1987/2006, Decisión 2007/533/JAI, Reglamento (CE) nº 1986/2006.

23 Decisión 2004/512/CE del Consejo, Reglamento CE) nº 767/2008, Decisión 2008/633/JAI del Consejo. Véase también la Declaración sobre la lucha contra el terrorismo, Consejo Europeo, 25.3.2004.

territorio de la Unión. La propuesta más bien coexistirá con estas normas, que se mantendrán intactas.

- **Impacto en los derechos fundamentales**

La propuesta coincide plenamente con el objetivo global de crear un espacio europeo de libertad, seguridad y justicia. Dado el carácter de las disposiciones propuestas, la presente propuesta ha sido objeto de un examen exhaustivo para garantizar la compatibilidad de sus disposiciones con los derechos fundamentales y, en particular, con el derecho a la protección de datos personales consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la UE, tal como se refleja en la evaluación de impacto que acompaña a la presente propuesta. La propuesta también se ajusta al artículo 16 del TFUE, que garantiza el derecho de todos a la protección de datos personales.

La propuesta es compatible con los principios de protección de datos y sus disposiciones concuerdan con la Decisión marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal[24] («Decisión marco 2008/977/JAI»). Esto implica reconocer el derecho de las personas al acceso, el derecho de rectificación, supresión y bloqueo, así como el derecho a la indemnización y a un recurso judicial. Además, con el fin de cumplir el principio de proporcionalidad, en algunas materias la propuesta establece normas de protección de datos más estrictas que la Decisión marco 2008/977/JAI.

El alcance de la propuesta se limita estrictamente y los servicios con funciones coercitivas sólo pueden utilizar los datos PNR para combatir los delitos graves especificados en una lista exhaustiva, que además pueden ser castigados con penas de supresión de libertad de al menos tres años en el Estado miembro. Por otra parte, para garantizar el tratamiento más limitado posible de datos de personas inocentes y no sospechosas, algunos aspectos del ámbito de la propuesta relativos a la creación y aplicación de criterios de evaluación se han limitado especialmente a los delitos graves que tienen también carácter transnacional, es decir, que están intrínsecamente relacionados con los viajes, de ahí el tipo de datos tratados. La propuesta permite conservar los datos PNR durante un periodo no superior a 5 años, tras el cual deberán suprimirse. Además, los datos PNR deben mantenerse anónimos después de un periodo muy breve de 30 días, dado que pueden utilizarse de forma proactiva una vez transcurrido este periodo. Se prohíbe la recogida y utilización de datos sensibles que revelen directa o indirectamente la raza o el origen étnico, las creencias religiosas o filosóficas, las opiniones políticas, la pertenencia a un sindicato, la salud o la orientación sexual de la persona. Además, la propuesta dispone que una decisión adoptada por una autoridad competente de un Estado miembro que produzca efectos jurídicos adversos o afecte gravemente a una persona, no debe adoptarse únicamente sobre la base del tratamiento automatizado de datos PNR. Por otra parte, dicha decisión no debe basarse en ningún caso en el origen racial o étnico, las creencias religiosas o filosóficas, las opiniones políticas, la pertenencia a un sindicato, la salud o la orientación sexual de la persona. Además, las compañías deben transmitir los datos PNR exclusivamente por el método *push*, lo que significa que los Estados miembros no tendrán acceso directo a los sistemas informáticos de las compañías. Los datos PNR sólo se podrán transferir por los Estados miembros a los terceros países en circunstancias muy limitadas y en cada caso concreto. Para garantizar la eficiencia y un alto nivel de protección de datos, se exige a los Estados Miembros que se

[24] DO L 350 de 30.12.2008 de p. 60.

aseguren de que una autoridad nacional de control independiente (autoridad de protección de datos) se responsabilice del asesoramiento y el control del tratamiento de datos PNR. También se pide a los Estados miembros que creen una unidad única designada (Unidad de Información sobre Pasajeros) responsable de la gestión y protección de datos. El tratamiento de datos PNR debe ser registrado y documentado en su totalidad por la Unidad de Información sobre Pasajeros con el fin de verificar la legalidad del tratamiento de datos, ejercer el autocontrol y garantizar adecuadamente la integridad de los datos y la seguridad de su tratamiento. Los Estados miembros también deben asegurarse de que se informe con claridad y precisión a los pasajeros de la recogida de datos PNR y de los derechos que les corresponden.

En consecuencia, además de conformarse a las normas y principios existentes en materia de protección de datos, la propuesta contiene una serie de garantías para el pleno cumplimiento del principio de proporcionalidad y garantiza un alto nivel de protección de los derechos fundamentales.

2. CONSULTA DE LAS PARTES INTERESADAS Y EVALUACIÓN DE IMPACTO

- **Consulta de las partes interesadas**

Métodos de consulta utilizados, principales sectores de consulta y perfil general de los consultados

Al preparar la propuesta de 2007, la Comisión consultó en diciembre de 2006 a todas las partes interesadas mediante un cuestionario. El cuestionario fue enviado a todos los Estados miembros, las autoridades de protección de datos de los Estados miembros, el Supervisor Europeo de Protección de Datos, la Asociación de Compañías Aéreas Europeas (ACAE), la *Air Transport Association of America* (ATA, asociación de transporte aéreo de los EE.UU.), la Asociación Internacional de Chárters Aéreos (IACA), la Asociación Europea de las Compañías Regionales de Aviación (ERA) y la Asociación de Transporte Aéreo Internacional (IATA). Las respuestas se recogieron en la evaluación de impacto que acompañó a la propuesta de 2007. A continuación, la Comisión convocó a los Estados miembros a una reunión en la que los representantes de éstos tuvieron la oportunidad de intercambiar sus puntos de vista.

Tras la adopción de la propuesta de 2007, las partes interesadas publicaron sus posturas al respecto. El Parlamento Europeo adoptó una Resolución sobre la propuesta el 20 de noviembre de 2008[25]. Los Estados miembros expusieron sus posturas en los debates de los grupos de trabajo del Consejo[26]. También emitieron sus dictámenes respectivos el Supervisor Europeo de Protección de datos[27], el Grupo de trabajo del artículo 29 sobre protección de datos[28] y la Agencia de Derechos Fundamentales[29].

---

25 P6_TA (2008) 0561.

26 Documento del Consejo nº 17024/09 de 2.12.2009.

27 DO C 110 de 1.5.2008.

28 Dictamen conjunto sobre 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, presentada por la Comisión el 6 de noviembre de 2007 (DT 145 de 5.12.2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_en.pdf.

29 http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf.

Resumen de las respuestas

La principal crítica contenida en la Resolución del Parlamento Europeo se basaba en que la necesidad de las acciones propuestas no había sido suficientemente demostrada. El Parlamento cuestionaba que la propuesta cumpliera los requisitos necesarios que justifican interferir en el derecho de protección de datos. La Resolución manifestaba la preocupación del Parlamento por el hecho de que no se había evaluado el valor añadido de la propuesta en el contexto de otras iniciativas en materia de fronteras. En cuanto a la protección de datos, el Parlamento pedía una clara limitación de la finalidad y subrayó que únicamente determinadas autoridades específicas tendrían acceso a los datos PNR. Por último, el Parlamento manifestó su preocupación porque el método propuesto de evaluación automatizada de datos PNR mediante criterios de evaluación predeterminados y basados en hechos supone una utilización muy amplia de los datos, e insistió en que dicha evaluación no debería conducir en ningún caso a la elaboración de perfiles (*profiling*) basados en datos sensibles.

El Grupo del artículo 29 sobre la protección de datos consideró que la propuesta era desproporcionada y podía vulnerar el derecho a la protección de datos. Puso en tela de juicio el régimen de protección de datos al no regular la Decisión marco 2008/977/JAI el tratamiento de datos a nivel nacional. Consideró que la necesidad de la propuesta no había quedado demostrada suficientemente, que el periodo de conservación de datos (13 años) era desproporcionado y que sólo debería usarse el método *push* de transferencia de datos.

El Supervisor Europeo de Protección de Datos cuestionó que se hubiera demostrado la necesidad y la proporcionalidad de la propuesta dado que ésta afecta a la recogida de datos de personas inocentes. Criticó la propuesta porque contribuye a establecer una sociedad vigilada y puso en tela de juicio el régimen de protección de datos porque la Directiva marco 2008/977/JAI no regula el tratamiento de datos a nivel nacional. El Supervisor propuso específicamente que se definieran mejor las autoridades que tendrían acceso a los datos PNR y las condiciones de transferencia de datos a los terceros países.

La Agencia de Derechos Fundamentales también opinó que no se había demostrado la necesidad ni la proporcionalidad de la propuesta y consideró que deberían incluirse más garantías en la misma con el fin de evitar la elaboración de perfiles basados en datos sensibles.

Algunas asociaciones de compañías aéreas y, en particular, la Asociación de Transporte Aéreo Internacional (IATA) y la Asociación de Compañías Aéreas Europeas (ACAE), expusieron sus opiniones sobre la propuesta. Criticaron sobre todo la estructura descentralizada de ésta y subrayaron que la recogida centralizada de datos tendría ventajas financieras para las compañías. También criticaron la elección del método *push* y pidieron que se dejara a las compañías aéreas elegir el método de transferencia.

El proceso de consulta influyó considerablemente en la propuesta legislativa. Aunque algunas partes interesadas no estaban convencidas de la necesidad de utilizar los datos PNR, todas estuvieron de acuerdo en que es preferible una normativa en el ámbito de la UE al desarrollo de sistemas PNR nacionales divergentes. Las consultas también llevaron a limitar la finalidad de la utilización de los datos a la lucha contra los delitos graves y los delitos terroristas, así como a limitar el alcance de la propuesta al transporte aéreo. Se ha optado por un régimen de protección de datos exigente con un periodo específico de conservación y la prohibición de utilizar datos sensibles como los que revelan la raza, el origen étnico, las creencias religiosas o filosóficas, las opiniones políticas, la pertenencia a un sindicato, la salud y la orientación

sexual. Se ha preferido el método *push*, así como las limitaciones estrictas a las transferencias ulteriores de datos a los terceros países.

- **Obtención y utilización de asesoramiento técnico**

No se precisó asesoramiento técnico externo.

- **Evaluación del impacto**

La Comisión realizó la evaluación de impacto prevista en el Programa de Trabajo[30].

En la evaluación de impacto se examinaron cuatro opciones, cada una de las cuales contiene dos variantes:

Opción estratégica A: abstenerse de tratar el asunto a nivel de la UE y mantener el *statu quo.*

Opción estratégica B: establecer la estructura de un sistema de recogida y tratamiento de datos PNR, con una opción B.1: recogida y tratamiento descentralizados de datos por los Estados miembro, y una opción B.2: recogida y tratamiento centralizados de datos a nivel de la UE.

Opción estratégica C: limitación de la finalidad de las medidas propuestas, con una opción C.1: acceso para la prevención, detección, investigación y enjuiciamiento de delitos graves y delitos terroristas únicamente, y opción C.2: acceso para la prevención, detección, investigación y enjuiciamiento de delitos graves y delitos terroristas, y para otros objetivos estratégicos.

Opción estratégica D: determinar los modos de transporte a los que se aplicarán las medidas propuestas, con una opción D.1: sólo las compañías aéreas, y una opción D.2: compañías aéreas, marítimas y de ferrocarril.

Las opciones se evaluaron con arreglo a los siguientes criterios: seguridad en la UE, protección de datos personales, costes para los servicios públicos, costes para las compañías aéreas/competencia en el mercado interior y promoción de un enfoque global.

La evaluación de impacto llegó a la conclusión de que una propuesta legislativa aplicable a los viajes por vía aérea con una recogida descentralizada de los datos PNR con la finalidad de prevenir, detectar, investigar y enjuiciar los delitos terroristas y otros delitos graves era la mejor opción estratégica (combinación de B1, C1 y D1). Esto mejorará la seguridad en la UE, al mismo tiempo que limitará al mínimo el impacto en la protección de datos personales y mantendrá unos niveles de costes aceptables.

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

- **Resumen de la medida propuesta**

La propuesta se propone armonizar las disposiciones de los Estados miembros sobre la obligación de las compañías aéreas que efectúan vuelos entre un tercer país y el territorio de al menos un Estado miembro de transmitir los datos PNR a las autoridades competentes con la finalidad de prevenir, detectar, investigar y enjuiciar los delitos terroristas y otros delitos

[30] SEC(2011) 132.

graves. El tratamiento de datos PNR con arreglo a la presente propuesta cumplirá las normas de protección de datos establecidas en la Decisión marco 2008/977/JAI.

- **Base jurídica**

El TFUE y, en particular, su artículo 82, apartado 1, letra d), y su artículo 87, apartado 2, letra a).

- **Principio de subsidiariedad**

A los servicios con funciones coercitivas se les deberá dotar de instrumentos eficaces para la lucha contra el terrorismo y los delitos graves. La mayoría de los actos de terrorismo y delitos graves implica algún viaje internacional, por lo que las autoridades deben utilizar los datos PNR para proteger la seguridad interior de la UE. Por otra parte, las investigaciones encaminadas a prevenir, detectar, investigar y enjuiciar delitos terroristas y delitos graves realizadas por las autoridades competentes de los Estados miembros dependen en gran medida de la cooperación internacional y transfronteriza.

Dada la libre circulación de personas en el espacio Schengen, es necesario que todos los Estados miembros recojan, traten e intercambien datos PNR con el fin de evitar diferencias en la seguridad. Actuando de forma coherente y colectiva, esta medida contribuirá a aumentar la seguridad en la UE.

La acción a nivel de la UE contribuirá a la armonización de las disposiciones que garantizan la protección de datos en los Estados miembros. Los diferentes sistemas de los Estados miembros que ya han establecido mecanismos similares o lo harán en el futuro pueden repercutir negativamente en las compañías aéreas, ya que tendrán que cumplir diversos requisitos nacionales posiblemente divergentes y relativos, por ejemplo, a los tipos de datos que deberán transmitirse y las condiciones de su suministro a los Estados miembros. Estas diferencias también pueden ser perjudiciales para la cooperación efectiva entre los Estados miembros a efectos de prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves.

Considerando que los objetivos de la presente propuesta no pueden alcanzarse suficientemente por los Estados miembros y pueden lograrse mejor a nivel de la Unión, se puede concluir que la UE está legitimada para actuar y está en mejores condiciones para actuar que los Estados miembros de forma independiente. Por tanto, la propuesta cumple el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea.

- **Principio de proporcionalidad**

La propuesta recogida, el análisis y la conservación de carácter más sistemático de los datos PNR relativos a los vuelos procedentes de terceros países y con destino a la UE, con arreglo a unas garantías de protección de datos rigurosas, reforzarán la prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos graves, y son necesarios para responder a las amenazas contra la seguridad.

El ámbito de la propuesta se limita a los elementos que requieren un enfoque armonizado de la UE, es decir, la definición de las formas de utilización de los PNR por los Estados miembros, los elementos de los datos que deberán recogerse, las finalidades para las cuales la información podrá utilizarse, la comunicación de datos entre las unidades PNR de los Estados miembros y las condiciones técnicas necesarias para dicha comunicación.

La medida propuesta es una directiva. Optar por un sistema descentralizado significa que los Estados miembros podrán elegir cómo crear su sistema PNR y decidir sus aspectos técnicos.

De conformidad con el principio de proporcionalidad establecido en el artículo 5 del Tratado de la Unión Europea, la presente propuesta no excede de lo necesario y proporcionado para alcanzar sus objetivos.

- **Instrumento elegido**

Instrumento propuesto: directiva.

No proceden otros instrumentos por la siguiente razón:

El objetivo de la medida es la aproximación de las legislaciones de los Estados miembros, por lo que no sería adecuado ningún instrumento distinto de la directiva.

4. REPERCUSIONES PRESUPUESTARIAS

La propuesta no tiene ninguna incidencia en el presupuesto de la UE.

5. INFORMACIÓN ADICIONAL

- **Simulación, fase piloto y período transitorio**

Habrá un período transitorio para la propuesta consistente en un periodo de aplicación de dos años. También habrá una recogida transitoria de datos PNR para completar la recogida de datos relativos a todos los vuelos en los seis años siguientes a la entrada en vigor de la Directiva.

- **Ámbito de aplicación territorial**

Los destinatarios de la propuesta serán los Estados miembros. La aplicación de la Directiva al Reino Unido, Irlanda y Dinamarca se determinará de conformidad con lo dispuesto en los Protocolos nº 21 y 22 anejos al Tratado de Funcionamiento de la Unión Europea.

- **Cláusula de reexamen/de revisión/de expiración**

La propuesta incluye una cláusula que prevé reexaminar el funcionamiento de la Directiva a los cuatro años de la fecha de su transposición y el reexamen especial de la posible ampliación del ámbito de la Directiva para regular los datos PNR de los pasajeros de vuelos internos de la UE.

2011/0023 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 82, apartado 1, letra d), y su artículo 87, apartado 2, letra a),

Vista la propuesta de la Comisión,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[31],

Visto el dictamen del Comité de las Regiones[32],

Tras haber consultado al Supervisor Europeo de Protección de Datos,

Actuando de conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) El 6 de noviembre de 2007, la Comisión adoptó 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[33]. No obstante, al entrar en vigor el Tratado de Lisboa el 1 de diciembre de 2009, la propuesta de la Comisión, que en esta fecha todavía no había sido aprobada por el Consejo, quedó obsoleta.

(2) El «Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano»[34] insta a la Comisión a presentar una propuesta sobre la utilización de datos PNR para prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves.

(3) La Comisión presentó algunos elementos esenciales de la política de la Unión en esta materia en su Comunicación de 21 de septiembre de 2010 «Sobre el enfoque global de

---

31 DO C, p.
32 DO C, p.
33 COM(2007) 654.
34 Documento del Consejo nº 17024/09 de 2.12.2009.

las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países»[35].

(4) La 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[36] regula la comunicación previa por los transportistas a las autoridades nacionales competentes de los datos de las personas transportadas con objeto de mejorar los controles fronterizos y combatir la inmigración ilegal.

(5) Los datos PNR son necesarios para prevenir, detectar, investigar y enjuiciar eficazmente los delitos terroristas y los delitos graves y para mejorar, en consecuencia, la seguridad interior.

(6) Los datos PNR ayudan a los servicios con funciones coercitivas a prevenir, detectar, investigar y enjuiciar delitos graves, incluidos actos terroristas, al compararlos en las diversas bases de datos de personas y objetos buscados, para elaborar pruebas y, en su caso, descubrir a los cómplices de los delincuentes y desmantelar redes delictivas.

(7) Los datos PNR permiten a los servicios con funciones coercitivas identificar a personas que previamente eran «desconocidas», es decir, que previamente no eran sospechosas de estar implicadas en un delito terrorista o delito grave pero que un análisis de datos indica que pueden estar implicadas en dicho delito y, por tanto, deben ser objeto de un nuevo examen por las autoridades competentes. Mediante la utilización de datos PNR los servicios con funciones coercitivas pueden responder a la amenaza del terrorismo y los delitos graves desde una perspectiva distinta del tratamiento de otras categorías de datos personales. No obstante, para garantizar el tratamiento más limitado posible de datos de personas inocentes y no sospechosas, estos aspectos de la utilización de datos PNR relativos a la creación y aplicación de criterios de evaluación deberían verse aún más limitados a los delitos graves que también tienen carácter transnacional, es decir, que están intrínsecamente relacionados con los viajes y, por tanto, con el tipo de datos tratados.

(8) El tratamiento de datos personales debe ser proporcional al objetivo específico de seguridad que persigue la presente Directiva.

(9) La utilización de datos PNR junto con datos de información anticipada sobre pasajeros en determinados casos ha aportado un valor añadido a la verificación por los Estados miembros de la identidad de un individuo, aumentando así su valor para los servicios con funciones coercitivas.

(10) Por consiguiente, para prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves es fundamental que todos los Estados miembros introduzcan disposiciones que impongan obligaciones a las compañías aéreas que realizan vuelos internacionales desde o hacia el territorio de uno o varios Estados miembros de la Unión Europea.

(11) Las compañías aéreas ya recogen y tratan datos PNR de sus pasajeros para sus fines comerciales propios. La presente Directiva no debería imponer ninguna obligación a

---

35 COM(2010) 492.

36 DO L 261 de 6.8.2004 de p. 24.

las compañías aéreas de recoger o conservar datos adicionales de los pasajeros ni ninguna obligación a los pasajeros de facilitar datos adicionales a los ya previstos a las compañías aéreas.

(12) Deben utilizarse las definiciones de delitos terroristas contenidas en los artículos 1 a 4 de la Decisión marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo[37]. La definición de delito grave que se utiliza es la del artículo 2 de la Decisión marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros[38]. Ahora bien, los Estados miembros pueden excluir los delitos menores para los que, habida cuenta de sus respectivos sistemas de justicia penal, el tratamiento de datos PNR conforme a la presente Directiva no se ajuste al principio de proporcionalidad. La definición de delito transnacional grave se toma del artículo 2 de la Decisión marco 2002/584/JAI y de la Convención de las Naciones Unidas sobre la Delincuencia Organizada Transnacional.

(13) Los datos PNR deben transferirse a una unidad única designada (Unidad de Información sobre Pasajeros) en el Estado miembro pertinente, a fin de garantizar la claridad y reducir los costes de las compañías aéreas.

(14) El contenido de las listas de datos PNR que deben enviarse a la Unidad de Información sobre Pasajeros debería elaborarse con el objetivo de reflejar la legítima exigencia de las autoridades públicas de prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves, a fin de mejorar la seguridad interior en la Unión y la protección de los derechos fundamentales de los ciudadanos y, en particular, el derecho a la intimidad y la protección de datos personales. Dichas listas no deben incluir datos personales que pudieran revelar el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato o datos sobre la salud u orientación sexual de los interesados; los datos PNR deben contener la información detallada sobre la reserva y el itinerario de viaje del pasajero que permita a las autoridades competentes identificar a los pasajeros por vía aérea que representan una amenaza para la seguridad interior.

(15) En la actualidad se dispone de dos métodos de transferencia de datos: el método *pull*, en el que las autoridades competentes del Estado que solicita los datos pueden llegar hasta (acceder) el sistema de reserva de la compañía aérea y extraer (*pull*) una copia de los datos requeridos, y el método *push* en el que las compañías aéreas transfieren (*push*) los datos PNR solicitados a la autoridad requirente, lo que permite a las compañías aéreas mantener el control de los datos suministrados. Se considera que el método *push* ofrece un grado mayor de protección de datos y debería ser obligatorio para todas las compañías aéreas.

(16) La Comisión apoya las directrices de la Organización de Aviación Civil Internacional (OACI) sobre los datos PNR. Estas directrices deberían ser la base para la adopción de los formatos de datos admitidos para la transferencia de datos PNR por las compañías aéreas a los Estados miembros. Esto justifica que dichos formatos de datos admitidos y los protocolos aplicables a la transferencia de datos de las compañías aéreas deban

---

37 DO L 164 de 22.6.2002, p. 3. Decisión modificada por la Decisión nº 2008/919/JAI del Consejo, de 28 noviembre 2008 (DO L 330 de 9.12.2008, p. 21).

38 DO L 190 de 18.7.2002, p. 1.

adoptarse de conformidad con el procedimiento consultivo previsto en el Reglamento (UE) nº del Parlamento Europeo y del Consejo [……..]..

(17) Los Estados miembros deberían tomar todas las medidas necesarias para que las compañías aéreas puedan cumplir sus obligaciones con arreglo a la presente Directiva. Los Estados miembros deben imponer sanciones disuasorias, efectivas y proporcionadas, incluidas las pecuniarias, contra las compañías aéreas que incumplan sus obligaciones de transferencia de datos PNR. En caso de infracciones graves y repetidas que pudieran ser perjudiciales para los objetivos fundamentales de la presente Directiva, las sanciones podrían incluir, en casos excepcionales, medidas como la inmovilización, el embargo o la incautación de los medios de transporte, la suspensión provisional o la retirada de la licencia de explotación.

(18) Cada Estado miembro debería ser responsable de evaluar las amenazas potenciales relacionadas con los delitos terroristas y los delitos graves.

(19) Tomando plenamente en consideración el derecho a la protección de datos personales y el derecho a la no discriminación, las autoridades competentes de los Estados miembros no deberían tomar ninguna decisión que pudiera tener efectos jurídicos adversos para una persona o afectarle gravemente en razón únicamente del tratamiento automatizado de datos PNR. Por otra parte, dicha decisión no debería adoptarse en ningún caso en razón del origen racial o étnico, las creencias religiosas o filosóficas, las opiniones políticas, la pertenencia a un sindicato, la salud o la orientación sexual de la persona.

(20) Los Estados miembros deberían compartir con otros Estados miembros los datos PNR que reciban, siempre que esa transferencia sea necesaria para la prevención, detección, investigación o persecución de delitos terroristas o delitos graves. Las disposiciones de la presente Directiva se entienden sin perjuicio de otros instrumentos de la Unión relativos al intercambio de información entre autoridades policiales y judiciales, incluida la Decisión 2009/371/JAI del Consejo, de 6 de abril de 299, por la que se crea la Oficina Europea de Policía (Europol)[39] y la Decisión marco 2006/960/JAI del Consejo, de 18 de septiembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea[40]. Este intercambio de datos PNR entre los servicios con funciones coercitivas y judiciales debería regirse por las normas de cooperación policial y judicial.

(21) El periodo durante el cual deben conservarse los datos PNR debería ser proporcional a las finalidades de prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos graves. Dada la naturaleza de los datos y su utilización, es necesario que los datos PNR se conserven durante un periodo suficientemente largo para realizar análisis y utilizarlos en las investigaciones. Para evitar una utilización desproporcionada es necesario que, después de un periodo inicial, los datos se archiven y sólo sean accesibles en condiciones muy estrictas y limitadas.

(22) Cuando se transfieran datos PNR específicos a las autoridades competentes y estos se utilicen en el contexto del enjuiciamiento o de investigaciones penales específicas, la

---

39 DO L 121 de 15.5.2009, p. 37.

40 DO L 386 de 29.12.2006, p. 89.

conservación de dichos datos por las autoridades competentes debería regirse por la legislación nacional del Estado miembro, con independencia de los periodos de conservación fijados en la presente Directiva.

(23) En cada Estado miembro, el tratamiento interno de los datos PNR por la Unidad de Información sobre Pasajeros y las autoridades competentes debería respetar las normas de protección de datos personales previstas en la legislación nacional que sean conformes a la Decisión marco 2008/977/JAI, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal[41] (Decisión marco 2008/977/JAI).

(24) Considerando el derecho a la protección de datos personales, los derechos de los interesados al tratamiento de sus datos PNR, tales como el derecho de acceso, el derecho de rectificación, supresión y bloqueo, así como los derechos de reparación y a un recurso judicial, deberían ser conformes con la Decisión marco 2008/977/JAI.

(25) Teniendo en cuenta el derecho de los pasajeros a ser informados del tratamiento de sus datos personales, los Estados miembros deberían garantizar que reciban información precisa sobre la recogida de datos PNR y su transferencia a la Unidad de Información sobre Pasajeros.

(26) Las transferencias de datos PNR por los Estados miembros a los terceros países sólo deberían permitirse en cada caso y de conformidad con la Decisión marco 2008/977/JAI. Para garantizar la protección de datos personales, dichas transferencias deberían cumplir requisitos adicionales relativos a la finalidad de la transferencia, la categoría de la autoridad receptora y las garantías aplicables a los datos personales transferidos al tercer país.

(27) La autoridad nacional de control que se ha establecido en aplicación de la Decisión marco 2008/977/JAI también debería ser responsable de asesorar sobre la aplicación y ejecución de las disposiciones de la presente Directiva y de controlar dicha aplicación y ejecución.

(28) La presente Directiva no afecta a la posibilidad de que los Estados miembros establezcan, con arreglo a sus legislaciones nacionales, un mecanismo para recoger y tratar los datos PNR con finalidades distintas de las especificadas en la presente Directiva, o que los transportistas que no sean los mencionados en ella hagan lo mismo con respecto a los vuelos internos siempre que cumplan las disposiciones de protección de datos aplicables y las normativas nacionales respeten el acervo de la Unión. La cuestión de la recogida de datos PNR sobre vuelos interiores debería ser objeto de una reflexión particular en el futuro.

(29) Como consecuencia de las diferencias jurídicas y técnicas entre las disposiciones nacionales sobre el tratamiento de datos personales, incluidos los datos PNR, las compañías aéreas se enfrentan y se enfrentarán a requisitos diferentes en cuanto al tipo de información que deben transferir, así como en cuanto a las condiciones en que debe suministrarse la información a las autoridades nacionales competentes. Estas diferencias pueden ser perjudiciales para la efectiva cooperación entre las autoridades

[41] DO L 350 de 30.12.2008, p. 60.

nacionales competentes a efectos de prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves.

(30) Dado que los objetivos de la presente Directiva no pueden ser alcanzados de manera suficiente por los Estados miembros y pueden lograrse mejor a escala de la Unión, ésta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar estos objetivos.

(31) La presente Directiva respeta los derechos fundamentales y los principios de la Carta de los Derechos Fundamentales de la Unión Europea. En particular, el derecho de protección de datos personales, el derecho a la intimidad y el derecho a la no discriminación reconocidos en los artículos 8, 7 y 21 de la Carta, y debe aplicarse en consecuencia. La Directiva es compatible con los principios de protección de datos y sus disposiciones concuerdan con la Decisión marco 2008/977/JAI del Consejo. Además, con el fin de cumplir el principio de proporcionalidad, la Directiva, en determinadas materias, contendrá normas de protección de datos más estrictas que la Decisión marco 2008/977/JAI.

(32) Se ha limitado en lo posible el ámbito de la Directiva, que permite conservar datos PNR durante un periodo máximo de 5 años, tras el cual los datos deben ser suprimidos; los datos deben ser anónimos tras un periodo muy breve, y se prohíbe la recogida y utilización de datos sensibles. Para garantizar la eficiencia y un alto nivel de protección de datos, se exige a los Estados miembros que garanticen que una autoridad nacional de control independiente sea responsable de asesorar y controlar el tratamiento de datos PNR. El tratamiento de datos PNR debe registrarse o documentarse a efectos de verificación de la legalidad de los datos tratados y de autocontrol, así como para garantizar adecuadamente la integridad y seguridad de los datos tratados. Los Estados miembros también deben asegurarse de que los pasajeros reciban una información clara y precisa sobre la recogida de datos PNR y sus derechos.

(33) [De conformidad con el artículo 3 del Protocolo (nº 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, estos Estados miembros han notificado su intención de participar en la adopción y aplicación de la presente Directiva] O BIEN [Sin perjuicio de lo dispuesto en el artículo 4 del Protocolo (nº 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, estos Estados miembros no participarán en la adopción de la presente Directiva y no estarán vinculados ni sujetos a su aplicación].

(34) De conformidad con lo dispuesto en los artículos 1 y 2 del Protocolo (nº 22) sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la adopción de la presente Directiva y no está vinculada por ella ni sujeta a su aplicación.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Directiva regula la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros de vuelos internacionales hacia o desde los Estados miembros, así como el tratamiento de dichos datos, incluidas su recogida, utilización y conservación por los Estados miembros y su intercambio entre ellos.

2. Los datos del registro de nombres de los pasajeros recogidos de conformidad con la presente Directiva sólo podrán tratarse para los fines siguientes:

   a) prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos graves con arreglo al artículo 4, apartado 2, letras b) y c); y

   b) prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos transnacionales graves con arreglo al artículo 4, apartado 2, letras a) y d).

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

a) «compañía aérea»: empresa de transporte aéreo con una licencia de explotación válida o similar que le permite llevar a cabo el transporte por vía aérea de pasajeros;

b) «vuelo internacional»: cualquier vuelo programado o no programado por una compañía aérea para aterrizar en el territorio de un Estado miembro procedente de un tercer país o para salir del territorio de un Estado miembro con destino final en un tercer país, incluidos en ambos casos las transferencias y los vuelos de tránsito;

c) «registro de nombres de los pasajeros» o «datos PNR»: una relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas (DCS) o en sistemas equivalentes que posean las mismas funcionalidades;

d) «pasajero»: toda persona transportada o que va a ser transportada a bordo de un avión, distinta de los miembros de la tripulación, con el consentimiento de la compañía aérea;

e) «sistemas de reserva»: el sistema de control interno de la compañía aérea en el cual se recaban los datos PNR para el tratamiento de las reservas;

f) «método *push*», método por el cual las compañías aéreas transmiten los datos PNR requeridos a la base de datos de la autoridad requirente;

g) «delitos terroristas», los delitos con arreglo a las legislaciones nacionales a que se refieren los artículos 1 a 4 de la Decisión marco 2002/475/JAI del Consejo;

h) «delitos graves»: los delitos con arreglo a las legislaciones nacionales a que se refiere el artículo 2, apartado 2, de la Decisión marco 585/2002/JAI del Consejo si son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo a la legislación nacional de un Estado miembro. No obstante, los Estados miembros pueden excluir los delitos menores para los que, habida cuenta de sus respectivos sistemas de justicia penal, el tratamiento de datos PNR conforme a la presente Directiva no se ajuste al principio de proporcionalidad.

i) «delitos graves transnacionales»: los delitos con arreglo a las legislaciones nacionales a que se refiere el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI del Consejo, si son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo a la legislación nacional de un Estado miembro, y siempre que:

i) se cometan en más de un Estado;

ii) se cometan en un Estado pero una parte considerable de su preparación, planificación, dirección o control tenga lugar en otro Estado;

iii) se cometan en un Estado pero con la intervención de un grupo delictivo organizado que esté implicado en actividades delictivas en un Estado; o

iv) se cometan en un Estado pero produzcan efectos considerables en otro Estado.

CAPÍTULO II

RESPONSABILIDADES DE LOS ESTADOS MIEMBROS

Artículo 3

Unidad de Información sobre Pasajeros

1. Cada Estado miembro creará o designará una autoridad competente para la prevención, detección, investigación o enjuiciamiento de los delitos terroristas y delitos graves o una rama de esa autoridad para actuar como su «Unidad de Información sobre Pasajeros» responsable de la recogida de datos PNR de las compañías aéreas, su almacenamiento, análisis y transmisión de los resultados del análisis a las autoridades competentes mencionadas en el artículo 5. Su personal podrá ser enviado en comisión de servicios por las autoridades competentes.

2. Dos o más Estados miembros podrán establecer o designar una autoridad única para que actúe como su Unidad de Información sobre Pasajeros. Esta Unidad de Información sobre Pasajeros se establecerá en uno de los Estados miembros participantes y se considerará la Unidad de Información sobre Pasajeros de todos los Estados miembros participantes. Los Estados participantes acordarán las normas detalladas de funcionamiento de la Unidad de Información sobre Pasajeros y respetarán los requisitos establecidos en la presente Directiva.

3. Cada Estado miembro notificará a la Comisión la Unidad de Información sobre Pasajeros en el plazo de un mes desde su creación, y podrá actualizar su declaración en cualquier momento. La Comisión publicará esta información, así como las eventuales actualizaciones, en el *Diario Oficial de la Unión Europea*.

Artículo 4

Tratamiento de los datos PNR

1. Los datos PNR transferidos por las compañías aéreas, con arreglo al artículo 6, relativos a vuelos internacionales que aterricen en el territorio de cada Estado miembro o salgan del mismo, serán recopilados por la Unidad de Información sobre Pasajeros del Estado miembro en cuestión. Si los datos PNR transferidos por las compañías aéreas incluyeran datos distintos de los enumerados en el anexo, la Unidad de Información sobre Pasajeros los suprimirá inmediatamente en el momento de su recepción.

2. La Unidad de Información sobre Pasajeros tratará los datos PNR sólo para los fines siguientes:

   (a) realizar una evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro a fin de identificar a toda persona que pueda estar implicada en un delito terrorista o delito transnacional grave y deba ser examinada posteriormente por las autoridades competentes a que se refiere el artículo 5. Al realizar dicha evaluación, la Unidad de Información sobre Pasajeros podrá tratar los datos PNR con arreglo a criterios predeterminados. Los Estados miembros garantizarán que todo resultado positivo de dicho tratamiento automatizado sea revisado individualmente por medios no automatizados para determinar la necesidad o no de que la autoridad competente mencionada en al artículo 5 emprenda una acción.

   (b) Realizar una evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro a fin de identificar a toda persona que pueda estar implicada en un delito terrorista o delito grave y deba ser examinada de nuevo por las autoridades competentes a que se refiere el artículo 5. Al realizar la evaluación, la Unidad de Información sobre Pasajeros podrá comparar los datos PNR con otras bases de datos pertinentes, incluidas las bases de datos nacionales o internacionales o las bases nacionales que reproduzcan las bases de datos de la Unión, siempre que se hayan establecido conforme al Derecho de la Unión con respecto a personas u objetos buscados o descritos, de conformidad con las normas nacionales, internacionales y de la Unión aplicables a tales ficheros. Los Estados miembros velarán por que se revise manualmente cualquier resultado positivo que arroje ese tratamiento

automatizado, con el fin de comprobar si es necesario que las autoridades competentes a que hace referencia el artículo 4 emprendan una acción;

(c) responder, en cada caso particular, a las peticiones debidamente razonadas de las autoridades competentes de que se suministren y traten datos PNR en casos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos transnacionales graves, y facilitar a las autoridades competentes los resultados de dicho tratamiento; así como

(d) analizar los datos PNR con el fin de actualizar o establecer nuevos criterios para realizar las evaluaciones a fin de identificar a toda persona que pueda estar implicada en un delito terrorista o delito grave transnacional conforme a la letra a).

3. La evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro mencionado en el apartado 2, letra a), se realizará de forma no discriminatoria con arreglo a criterios de evaluación establecidos por su Unidad de Información sobre Pasajeros. Los Estados miembros se asegurarán de que las Unidades de Información sobre Pasajeros, en cooperación con las autoridades competentes mencionadas en el artículo 5, establezcan los criterios de evaluación. Los criterios de evaluación no se basarán en ningún caso en el origen racial o étnico, las creencias religiosas o filosóficas, las opiniones políticas, la pertenencia a un sindicato, la salud o la orientación sexual de la persona.

4. La Unidad de Información sobre Pasajeros de un Estado miembro transferirá los datos PNR o los resultados del tratamiento de datos PNR de las personas identificadas con arreglo al apartado 2, letras a) y b), a las autoridades competentes del mismo Estado miembro para su ulterior examen. Tales transferencias sólo se harán caso por caso.

Artículo 5

Autoridades competentes

1. Cada Estado miembro elaborará la lista de autoridades competentes para solicitar o recibir datos PNR o los resultados del tratamiento de datos PNR de las Unidades de Información sobre Pasajeros a fin de examinar de nuevo esa información o de tomar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves.

2. Las autoridades competentes serán las autoridades responsables de prevenir, detectar, investigar o enjuiciar los delitos terroristas y los delitos graves.

3. Cada Estado miembro notificará la lista de sus autoridades competentes a la Comisión a los doce meses de la entrada en vigor de la presente Directiva, a más tardar, y podrá actualizar su declaración en todo momento. La Comisión publicará esta información, así como las eventuales actualizaciones, en el *Diario Oficial de la Unión Europea*.

4. Los datos PNR de los pasajeros y los resultados del tratamiento de datos PNR recibidos por la Unidad de Información sobre Pasajeros podrán ser tratados de nuevo

por las autoridades competentes de los Estados miembros únicamente con el fin de prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves.

5. El apartado 4 se entiende sin perjuicio de las facultades judiciales o coercitivas nacionales en el caso de que, en el curso de la acción ejercida después del tratamiento, se detecten otros delitos o indicios de delitos.

6. Las autoridades competentes no adoptarán ninguna decisión que produzca efectos jurídicos adversos para una persona o que afecte significativamente a una persona únicamente en razón del tratamiento automatizado de datos PNR. En ningún caso se adoptarán decisiones en razón del origen racial o étnico, las creencias religiosas o filosóficas, las opiniones políticas, la pertenencia a un sindicato, la salud o la orientación sexual de la persona.

Artículo 6

Obligaciones de las compañías aéreas

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las compañías aéreas transfieran *(push)* los datos PNR definidos en el artículo 2, letra c), y especificados en el anexo, en la medida en que ya los hayan recopilado, a la base de datos de la Unidad de Información sobre Pasajeros nacional del Estado miembro en cuyo territorio aterrizará o de cuyo territorio saldrá el vuelo internacional. En los casos en que el código de un vuelo internacional es compartido por una o más compañías aéreas, la obligación de transferir los datos PNR de todos los pasajeros de dicho vuelo recaerá en la compañía aérea que explote el vuelo de que se trate Si es un vuelo con escalas múltiples en los aeropuertos de los Estados miembros, las compañías aéreas transferirán los datos PNR a las Unidades de Información sobre Pasajeros de todos los Estados miembros interesados.

2. Las compañías aéreas transferirán los datos PNR por medios electrónicos utilizando los protocolos y los formatos de datos comunes que deberán adoptarse conforme al procedimiento de los artículos 13 y 14 o, en caso de fallo técnico, por cualquier otro medio adecuado que garantice un nivel adecuado de seguridad de los datos:

   a) 24 a 48 horas antes de la hora de salida programada del vuelo;

   así como

   b) inmediatamente después del cierre, es decir, una vez que los pasajeros hayan embarcado en el avión en preparación de la salida y no sea posible embarcar a otros pasajeros.

3. Los Estados miembros podrán permitir a las compañías aéreas que limiten la transferencia a que se refiere el apartado 2, letra b), a actualizaciones de la transferencia a que se refiere el apartado 2, letra a).

4. En cada caso particular, a petición de una Unidad de Información sobre Pasajeros conforme a la legislación nacional, las compañías aéreas transferirán datos PNR en caso de que sea necesario un acceso más rápido que el previsto en el apartado 2, letra

a), para ayudar a responder a una amenaza real y concreta relacionada con delitos terroristas o delitos graves.

Artículo 7

Intercambio de información entre los Estados miembros

1. En lo que respecta a las personas identificadas por una Unidad de Información sobre Pasajeros de conformidad al artículo 4, apartado 2, letras a) y b), los Estados miembros garantizarán que el resultado del tratamiento de los datos PNR sea transmitido por dicha Unidad a las Unidades de Información sobre Pasajeros de otros Estados miembros en los que la primera Unidad considere que la transferencia es necesaria para la prevención, detección, investigación o enjuiciamiento de delitos terroristas o delitos graves. Las Unidades de Información sobre Pasajeros de los Estados miembros receptores transmitirán dichos datos PNR o el resultado de su tratamiento a las autoridades competentes.

2. La Unidad de Información sobre Pasajeros de un Estado miembro tendrá derecho a solicitar, en caso necesario, a la Unidad de Información sobre Pasajeros de cualquier otro Estado miembro, que le suministre los datos PNR almacenados en la base de datos de este último de conformidad con el artículo 9, apartado 1, así como, si fuera necesario, el resultado del tratamiento de los datos PNR. La solicitud de tales datos podrá basarse en un elemento o una combinación de elementos de los datos, según estime necesario la Unidad de Información sobre Pasajeros requirente en cada caso concreto para prevenir, detectar, investigar o enjuiciar delitos terroristas o delitos graves. Las Unidades de Información sobre Pasajeros suministrarán lo antes posible los datos solicitados y también los resultados del tratamiento de datos PNR, si ya estuviera preparado según lo previsto en el artículo 4, apartado 2, letras a) y b).

3. La Unidad de Información sobre Pasajeros de un Estado miembro tendrá derecho a solicitar, en caso necesario, a la Unidad de Información sobre Pasajeros de cualquier otro Estado miembro, que le suministre los datos PNR almacenados en la base de datos de este último de conformidad con el artículo 9, apartado 2, así como, si fuera necesario, los resultados del tratamiento de los datos PNR. La Unidad de Información sobre Pasajeros podrá solicitar el acceso a datos PNR específicos conservados por la Unidad de Información sobre Pasajeros de otro Estado miembro en su forma integral y sin máscaras únicamente en circunstancias excepcionales como respuesta a una amenaza específica o a una investigación o enjuiciamiento específico relacionado con delitos terroristas o delitos graves.

4. Únicamente en los casos en que sea necesario para la prevención de una amenaza grave e inmediata para la seguridad pública podrán las autoridades competentes de un Estado miembro solicitar directamente a la Unidad de Información sobre Pasajeros de cualquier otro Estado miembro que le facilite los datos PNR almacenados en la base de datos de este último de conformidad con el artículo 9, apartados 1 y 2. Tales solicitudes se referirán al enjuiciamiento o las investigaciones específicas de delitos terroristas o delitos graves y serán motivadas. Las Unidades de Información sobre Pasajeros responderán a dichas solicitudes con carácter prioritario. En todos los demás casos las autoridades competentes canalizarán sus solicitudes a través de la Unidad de Información sobre Pasajeros de su propio Estado miembro.

5. Excepcionalmente, cuando sea necesario disponer de acceso rápido para responder a una amenaza específica y real relacionada con delitos terroristas o delitos graves, la Unidad de Formación sobre Pasajeros de un Estado miembro tendrá derecho a solicitar a la Unidad de Información sobre Pasajeros de otro Estado miembro que le suministre datos PNR de los vuelos que aterrizan o salen del territorio de este último en cualquier momento.

6. El intercambio de información previsto en el presente artículo podrá realizarse utilizando cualquiera de las vías existentes de cooperación internacional entre servicios con funciones coercitivas. Para la solicitud y el intercambio de información se utilizará la lengua aplicable a la vía de cooperación utilizada. Los Estados miembros, al efectuar sus notificaciones de conformidad con el artículo 3, apartado 3, informarán también a la Comisión de los datos detallados de las personas de contacto a las que se podrán enviar las solicitudes en casos de emergencia. La Comisión comunicará las notificaciones recibidas a los Estados miembros.

Artículo 8

Transferencias de datos a los terceros países

Un Estado miembro podrá transferir datos PNR y los resultados del tratamiento de datos PNR a un tercer país sólo en casos concretos y si:

a) se cumplen las condiciones establecidas en el artículo 13 de la Decisión marco 2008/977/JAI del Consejo;

b) la transferencia es necesaria para los fines de la presente Directiva especificados en el artículo 1, apartado 2, y

c) el tercer país acuerda transferir los datos a otro tercer país únicamente si fuera necesario para los fines de la presente Directiva especificados en el artículo 1, apartado 2, y sólo con la autorización expresa del Estado miembro.

Artículo 9

Período de conservación de los datos

1. Los Estados miembros se asegurarán de que los datos PNR suministrados por las compañías aéreas a la Unidad de Información sobre Pasajeros se conserven en una base de datos en la Unidad de Información sobre Pasajeros durante un período de 30 días a partir de su transferencia a la Unidad de Información sobre Pasajeros del primer Estado miembro en cuyo territorio aterrice o de cuyo territorio salga el vuelo internacional.

2. Al expirar el período de 30 días a partir de la transferencia de los datos PNR a la Unidad de Información sobre Pasajeros a que se refiere el apartado 1, los datos se conservarán en la Unidad de Información sobre Pasajeros por otro período de cinco años. Durante este periodo, se enmascararán todos los elementos de los datos que puedan servir para identificar al pasajero al que se refieren los datos PNR. Estos datos PNR anónimos serán únicamente accesibles a un número limitado de miembros

del personal de la Unidad de Información sobre Pasajeros expresamente autorizados para realizar análisis de datos PNR y elaborar criterios de evaluación con arreglo al artículo 4, apartado 2, letra d). El acceso a la totalidad de los datos PNR sólo lo autorizará el Jefe de la Unidad de Información sobre Pasajeros para los fines del artículo 4, apartado 2, letra c), siempre que se considere razonable por necesidades de una investigación y en respuesta a una amenaza o riesgo real, o bien a una investigación o enjuiciamiento específico.

A efectos de la presente Directiva, los elementos de los datos que podrían servir para identificar al pasajero al que se refieren los datos PNR, y que deberían filtrarse y enmascararse son los siguientes:

– nombre y apellido(s), incluidos los nombres y apellidos de otros pasajeros que figuran en el PNR y el número de personas que viajan juntas que figuran en el PNR;

– dirección y datos de contacto;

– observaciones generales, en la medida en que contengan información que pueda servir para identificar al pasajero al que se refiere el PNR; así como

– toda la información previa sobre pasajeros (API) recopilada.

3. Los Estados miembros se asegurarán de que los datos PNR sean suprimidos al expirar el periodo especificado en el apartado 2. Esta obligación se entenderá sin perjuicio de aquellos casos en que se hayan transferido datos PNR específicos a una autoridad competente para su utilización en el marco de investigaciones o enjuiciamientos penales, en cuyo caso la conservación de los datos por la autoridad competente se regirá por la legislación nacional del Estado miembro.

4. Los resultados de la evaluación a que se refiere el artículo 4, apartado 2, letras a) y b), los conservará la Unidad de Información sobre Pasajeros únicamente durante el tiempo necesario para informar de un resultado positivo a las autoridades competentes. Cuando la operación de evaluación automática, tras un examen individual por medios no automatizados, arroje un resultado negativo, éste también se almacenará para evitar «falsos» resultados positivos futuros durante un periodo máximo de tres años, a menos que los datos de base no se hubieran eliminado con arreglo al apartado 3 al expirar esos cinco años, en cuyo caso el registro se conservará hasta la supresión de los datos de base.

Artículo 10

Sanciones contra las compañías aéreas

Los Estados miembros, de conformidad con sus legislaciones nacionales, se asegurarán de prever sanciones disuasorias, eficaces y proporcionadas, incluidas pecuniarias, contra las compañías aéreas que no transmitan los datos exigidos por la presente Directiva, en la medida en que ya los hayan recopilado, o no lo hagan en el formato exigido, o bien vulneren las disposiciones nacionales adoptadas con arreglo a la presente Directiva.

Artículo 11

Protección de datos personales

1. Cada Estado miembro establecerá que, en lo que respecta al tratamiento de datos personales con arreglo a la presente Directiva, todo pasajero tendrá los mismos derechos de acceso, rectificación, supresión y bloqueo, indemnización y recurso judicial que los reconocidos en el marco de la legislación nacional en aplicación de los artículos 17, 18, 19 y 20 de la Decisión marco 2008/977/JAI del Consejo. Se aplicarán, por lo tanto, las disposiciones de los artículos 17, 18, 19 y 20 de la Decisión marco 2008/977/JAI del Consejo.

2. Cada Estado miembro establecerá que las disposiciones adoptadas en el marco de la legislación nacional en aplicación de los artículos 21 y 22 de la Decisión marco 2008/977/JAI del Consejo sobre la confidencialidad del tratamiento y la seguridad de los datos se aplicarán también a todo tratamiento de datos con arreglo a la presente Directiva.

3. Se prohibirá el tratamiento de datos PNR que revele el origen racial o étnico, las creencias religiosas o filosóficas, las opiniones políticas, la pertenencia a un sindicato, la salud o la orientación sexual de una persona. En el caso de que la Unidad de Información sobre Pasajeros reciba datos PNR que revelen tal información, los suprimirá inmediatamente.

4. El tratamiento de datos PNR por las compañías aéreas, las transferencia de datos PNR por las Unidades de Información sobre Pasajeros y las solicitudes de las autoridades competentes o las Unidades de Información sobre Pasajeros de otros Estados miembros y terceros países, incluidas las rechazadas, serán registradas o documentadas por la Unidad de Información sobre Pasajeros y las autoridades competentes con el fin de verificar la legalidad del tratamiento de datos, ejercer el autocontrol y garantizar adecuadamente la integridad de los datos y la seguridad de su tratamiento, especialmente por las autoridades nacionales de protección de datos. Los registros se conservarán durante un periodo de cinco años, a menos que los datos de base no se hubieran suprimido ya con arreglo al artículo 9, apartado 3, al expirar esos cinco años, en cuyo caso los registros se conservarán hasta la supresión de los datos de base.

5. Los Estados miembros se asegurarán de que las compañías aéreas, sus agentes y otros vendedores de billetes de transporte aéreo de pasajeros informen a los pasajeros de vuelos internacionales en el momento de reservar un vuelo y en el momento de la compra del billete, de manera clara y precisa, del suministro de datos PNR a la Unidad de Información sobre Pasajeros, las finalidades de su tratamiento, el periodo de conservación de datos, su utilización posible para prevenir, detectar, investigar o enjuiciar delitos terroristas y delitos graves, la posibilidad de intercambiar y compartir esos datos y de sus derechos de protección de datos y, en particular, el derecho a reclamar ante una autoridad nacional de protección de datos. Los Estados miembros pondrán la misma información a disposición del público en general.

6. Se prohibirá cualquier transferencia de datos PNR por las Unidades de Información sobre Pasajeros y las autoridades competentes a partes privadas en los Estados miembros o los terceros países.

7. Sin perjuicio de lo dispuesto en el artículo 10, los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de lo dispuesto en la presente Directiva y establecerán, en particular, sanciones eficaces, proporcionadas y disuasorias, que deberán aplicarse en caso de incumplimiento de las disposiciones adoptadas con arreglo a la presente Directiva.

Artículo 12

Autoridad nacional de control

Cada Estado miembro preverá que la autoridad nacional de control establecida en aplicación del artículo 25 de la Decisión marco 2008/977/JAI también sea responsable de asesorar sobre y controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros con arreglo a la presente Directiva. Se aplicarán las nuevas disposiciones del artículo 25 de la Decisión marco 2008/977/JAI.

CAPÍTULO IV

DISPOSICIONES DE APLICACIÓN

Artículo 13

Protocolos comunes y formatos de datos admitidos

1. Todas las transferencias de datos PNR por las compañías aéreas a las Unidades de Información sobre Pasajeros a efectos de la presente Directiva se efectuarán por medios electrónicos o, en caso de fallo técnico, por cualquier otro medio adecuado, durante un periodo de un año a partir de la adopción de los protocolos comunes y formatos de datos admitidos de conformidad con el artículo 14.

2. Una vez transcurrido el periodo de un año desde la fecha de adopción de los protocolos comunes y los formatos de datos admitidos, todas las transferencias de datos PNR por las compañías aéreas a las Unidades de Información sobre Pasajeros a efectos de la presente Directiva se efectuarán electrónicamente utilizando métodos seguros en forma de protocolos comunes aceptados que serán comunes a todas las transferencias para garantizar la seguridad de los datos durante la transferencia, y en un formato de datos admitido que garantice su legibilidad por todas las partes interesadas. Se exigirá a todas las compañías aéreas que seleccionen e indiquen a la Unidad de Información sobre Pasajeros el protocolo común y el formato de datos que se proponen utilizar en las transferencias.

3. Se elaborará una lista de los protocolos comunes aceptados y los formatos de datos admitidos que, en caso necesario, la Comisión adaptará de conformidad con el procedimiento previsto en el artículo 14.

4. Mientras no se disponga de los protocolos comunes aceptados y los formatos de datos admitidos a que se refieren los apartados 2 y 3, será de aplicación el apartado 1.

5. Cada Estado miembro se asegurará de que se adopten las medidas técnicas necesarias para poder utilizar los protocolos y formatos de datos comunes en el plazo de un año desde la fecha de adopción de los protocolos comunes y los formatos de datos admitidos.

Artículo 14

Comitología

1. La Comisión estará asistida por un comité (en adelante «el Comité») conforme al Reglamento […/2011/EU] de 16 de febrero de 2011.

2. Cuando se haga referencia al presente apartado, se aplicará el artículo 4 del Reglamento […/2011/EU] de 16 de febrero de 2011.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 15

Transposición

1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar dos años después de su entrada en vigor. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones, así como una tabla de correspondencias entre las mismas y la presente Directiva.

   Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 16

Disposiciones transitorias

En la fecha mencionada en el artículo 15, apartado 1, es decir, dos años después de la entrada en vigor de la presente Directiva, los Estados miembros se asegurarán de que se hayan recogido los datos PNR de al menos el 30 % de los vuelos a que se refiere el artículo 6, apartado 1. Hasta dos años después de la fecha mencionada en el artículo 15, los Estados miembros se asegurarán de que se hayan recogido los datos PNR de al menos el 60 % de los vuelos a que se refiere el artículo 6, apartado 1. Los Estados miembros se asegurarán de que a

partir de cuatro años desde la fecha mencionada en el artículo 15 se hayan recogido los datos PNR de todos los vuelos a que se refiere el artículo 6, apartado 1.

Artículo 17

Revisión

Con arreglo a la información suministrada por los Estados miembros, la Comisión:

a) examinará la viabilidad y necesidad de incluir los vuelos internos en el ámbito de aplicación de la presente Directiva, a la vista de la experiencia adquirida por los Estados miembros que recopilan datos PNR sobre vuelos internos. La Comisión presentará un informe al Parlamento Europeo y al Consejo en el plazo de dos años a partir de la fecha mencionada en el artículo 15, apartado 1;

b) realizará una revisión del funcionamiento de la presente Directiva y presentará un informe al Parlamento Europeo y al Consejo en el plazo de cuatro años desde la fecha mencionada en el artículo 15, apartado 1. La revisión abarcará todos los elementos de la presente Directiva y, especialmente, el cumplimiento de la norma de protección de datos personales, la duración del periodo de conservación de datos y la calidad de las evaluaciones. También contendrá la información estadística recopilada con arreglo al artículo 18.

Artículo 18

Datos estadísticos

1. Los Estados miembros prepararán el conjunto de la información estadística sobre los datos PNR comunicados a las Unidades de Información sobre Pasajeros. Estas estadísticas abarcarán como mínimo el número de identificaciones de personas que pueden estar implicadas en delitos terroristas o delitos graves de conformidad con el artículo 4, apartado 2, y el número de medidas represivas subsiguientes que se hayan adoptado utilizando datos PNR por compañía aérea y destino.

2. Las estadísticas no contendrán datos personales. Se transmitirán anualmente a la Comisión.

Artículo 19

Relación con otros instrumentos

1. Los Estados miembros podrán seguir aplicando los acuerdos bilaterales o los acuerdos o disposiciones que mantengan entre ellos sobre el intercambio de información entre las autoridades competentes, en vigor cuando se adopte la presente Directiva, siempre que dichos acuerdos o disposiciones sean compatibles con la presente Directiva.

2. La presente Directiva se entiende sin perjuicio de las obligaciones y compromisos de la Unión en virtud de acuerdos bilaterales o multilaterales con terceros países.

Artículo 20

Entrada en vigor

La presente Directiva entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Los destinatarios de la presente Directiva serán los Estados miembros de conformidad con lo dispuesto en los Tratados.

Hecho en Bruselas, el [...]

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*

ANEXO

Datos del registro de nombres de los pasajeros recopilados por las compañías aéreas

(1) Localizador de registro PNR

(2) Fecha de reserva/emisión del billete

(3) Fecha o fechas de viaje previstas

(4) Nombre(s) y apellido(s)

(5) Dirección y datos de contacto (número de teléfono, dirección de correo electrónico)

(6) Todos los datos de pago, incluida la dirección de facturación

(7) Itinerario completo del viaje para el PNR específico

(8) Información sobre viajeros asiduos

(9) Agencia de viajes/operador de viajes

(10) Situación de vuelo del pasajero: confirmaciones y paso por el mostrador de facturación, no comparecencia o pasajeros de última hora sin reserva

(11) Información PNR escindida/dividida

(12) Observaciones generales (incluida la información disponible sobre menores de 18 años no acompañados como nombre y sexo del menor, edad, idioma o idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculos con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculos con el menor, agente en el lugar de salida y de llegada)

(13) Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes de ida solo y la indicación de la tarifa de los billetes electrónicos (*Automatic Ticket Fare Quote*, ATFQ)

(14) Datos del asiento, incluido el número

(15) Información sobre códigos compartidos

(16) Toda la información relativa al equipaje

(17) Número de viajeros y otros nombres de viajeros que figuran en el PNR

(18) Cualquier información recogida en el sistema de información previa sobre los pasajeros (sistema API)

(19) Todo el historial de cambios de los datos PNR indicados en los números 1 a 18.