



**00664/11/ES
WP 181**

Dictamen 10/2011 relativo a la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves

Adoptado el 5 de abril de 2011

Este grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. Sus tareas se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.

La secretaría la facilita la Dirección D (Derechos Fundamentales y Ciudadanía) de la Comisión Europea, Dirección General de Justicia, Libertad y Seguridad, B-1049 Bruselas, Bélgica, despacho MO-59 06/036.

Sitio de Internet: http://ec.europa.eu/justice/policies/privacy/index_en.htm

El Grupo de Trabajo de protección de las personas físicas en lo que respecta al tratamiento de datos personales

Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995,

Vistos el artículo 29 y el artículo 30, apartados 1, letra a), y 3, de dicha Directiva, y el artículo 15, apartado 3, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, y visto su Reglamento interno,

Ha adoptado el presente Dictamen.

1. Introducción

El 2 de febrero de 2011, la Comisión Europea publicó su propuesta de Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves. El Grupo de Trabajo había emitido un dictamen sobre la anterior propuesta de PNR de la UE (Propuesta de Decisión Marco del Consejo sobre utilización de registros de nombres de los pasajeros (PNR: *passenger name records*) a efectos de aplicación de la ley), presentada por la Comisión el 6 de noviembre de 2007¹. El Grupo de Trabajo ha comentado también ampliamente en diversos dictámenes distintos acuerdos vigentes entre la UE y países terceros y el enfoque avanzado por la Comisión en su Comunicación de 21 de septiembre de 2010². Amén de ello, el Grupo de Trabajo ha subrayado su inquietud por aspectos del PNR en diversas cartas al Comisario Barrot, a la Comisaria Malmström, al Director General Faull y a la Comisión LIBE del Parlamento Europeo.

El presente Dictamen se dirige a las instancias que participan en la discusión y el desarrollo de la última propuesta, a saber, la Comisión, el Grupo de Trabajo GENVAL del Consejo y el Parlamento Europeo.

2. Necesidad y proporcionalidad

La propuesta de 2011 se acompaña de una evaluación de impacto orientada a exponer más detalladamente el fundamento subyacente a la propuesta y a sus disposiciones. El Grupo de Trabajo considera que la lucha contra el terrorismo y el crimen organizado es necesaria y legítima y que los datos personales, especialmente algunos datos de pasajeros, pueden ser valiosos para evaluar riesgos y prevenir y combatir el terrorismo y el crimen organizado. No obstante, en relación a un sistema de PNR europeo debe justificarse bien la limitación de los derechos y libertades fundamentales y demostrarse claramente la necesidad de tal limitación para lograr un justo equilibrio entre las demandas de protección de la seguridad pública y la restricción del derecho a la intimidad.

El Grupo de Trabajo ha puesto en duda con argumentos la necesidad y proporcionalidad de los sistemas de PNR y continúa haciéndolo en relación con la propuesta de 2011. Sin dejar de apreciar la mayor elaboración que muestra la evaluación de impacto, consideramos que no aporta una evaluación adecuada de la utilización del PNR ni demuestra la necesidad de lo que

¹ WP 145 – Dictamen conjunto con el Grupo de Trabajo sobre Policía y Justicia.

² Dictámenes WP 103 (Canadá); WP 138 (EE.UU.); WP 151 (EE.UU.- Información a los pasajeros); y WP 178 (Enfoque global de la Comisión).

propone. La propuesta debe clarificar si el objetivo es combatir la delincuencia grave (transnacional), incluido el terrorismo, o si el objetivo es combatir solo el terrorismo y la delincuencia relacionada con el terrorismo.

El capítulo 3.2 de la evaluación de impacto, «Respeto de los derechos fundamentales», se limita a declarar que se ha utilizado la Lista de control de derechos fundamentales, pero no dice nada más que justifique las conclusiones. Además, el razonamiento expuesto en el capítulo sobre la interferencia con el derecho a la intimidad del artículo 8 del Convenio Europeo de Derechos Humanos y los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea es un razonamiento circular. La condición jurídica previa de interferencia con dichos derechos es que sea «necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás» amén de ser «necesaria en una sociedad democrática» y estar «sujeta al principio de proporcionalidad». Que el objeto de la propuesta sea la prevención del terrorismo y la delincuencia grave no implica que cumpla claramente con estos requisitos: aún quedan por probar la necesidad y la proporcionalidad. En el propio panorama general que hace la Comisión de los sistemas de información³ se señala:

«Necesidad

La interferencia entre una autoridad pública y el derecho a la intimidad puede ser necesaria en interés de la seguridad nacional, la seguridad pública o la prevención de delitos. La jurisprudencia del Tribunal Europeo de Derechos Humanos establece tres condiciones con las cuales pueden justificarse estas restricciones: si son lícitas, si persiguen una finalidad legítima y si son necesarias en una sociedad democrática. La interferencia con el derecho a la intimidad se considera necesaria si responde a una necesidad social acuciante, si guarda proporción con el objetivo perseguido y si las razones expuestas por la autoridad pública para justificarla son pertinentes y suficientes. En todas las propuestas políticas futuras, la Comisión evaluará el impacto que se espera pueda producir la iniciativa sobre el derecho de las personas a la intimidad y a la protección de los datos personales y expondrá por qué ese impacto es necesario y por qué la solución propuesta guarda proporción con el fin legítimo de mantener la seguridad interior de la Unión Europea, prevenir los delitos o gestionar la migración».

El Grupo de Trabajo no cree que la Comisión haya cumplido con los compromisos antes suscritos en relación con la propuesta de PNR de la UE. Hay además otras consideraciones sobre los argumentos de necesidad y proporcionalidad que se exponen a continuación.

2.1. Refuerzo de la seguridad

La propuesta y la evaluación de impacto afirman que un sistema de PNR de la UE garantizaría la seguridad y evitaría las lagunas creadas al eliminarse los controles en las fronteras interiores debido al Convenio de Schengen. Bien motivado, este sería un objetivo legítimo, pero el Grupo de Trabajo tiene aún que ver pruebas satisfactorias de que procesar los datos PNR en todos los Estados miembros vaya a evitar las lagunas de seguridad derivadas de procesar dichos datos únicamente en unos pocos Estados miembros.

³ Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia COM(2010)385 final.

A nivel de la UE hay ya sistemas y herramientas que compensan la eliminación de controles fronterizos entre los países de Schengen basados en el llamado acervo de Schengen, de modo que, si subsistieran huecos de seguridad, lo que primero habría que hacer es analizar el funcionamiento correcto de los sistemas vigentes.

2.2. Sistemas, instrumentos y cooperación existentes

El panorama general de la gestión de la información que hace la Comisión en materia de libertad, seguridad y justicia, no evalúa la eficacia de los distintos sistemas en uso ni examina si, en conjunto, proporcionan los instrumentos adecuados para combatir el terrorismo y el crimen organizado o, si tal no fuera el caso, dónde se sitúan los fallos. El Grupo de Trabajo considera que dicha evaluación es necesaria antes de implantar otras medidas similares, como un sistema de PNR de la UE. La propuesta de PNR acarreará un solapamiento de obligaciones para las empresas de transporte, al ser ya posible por otros sistemas la recogida de datos, y supone un riesgo grave de lento corrimiento de funciones. Por ejemplo, la Directiva API obliga a las empresas de transporte a comunicar por adelantado datos de los pasajeros y el uso de los datos no se limita a los controles fronterizos sino que se extiende a las actividades de mantenimiento del orden público. Aunque el Grupo de Trabajo ha planteado varias veces a la Comisión el problema, aún no ha visto que se haya evaluado adecuadamente la eficacia de la Directiva API ni su transposición nacional, y el Grupo pone en cuestión que siga siendo necesaria si se introduce un sistema de PNR paneuropeo.

El Grupo de Trabajo se plantea si el conjunto de medidas de cooperación policial y judicial implantadas en la UE para prevenir y perseguir la delincuencia, que incluyen la lucha contra el terrorismo y la delincuencia grave, no suponen ya instrumentos adecuados para el objetivo que pretende alcanzar la propuesta de PNR de la UE. La evaluación de impacto no lleva a cabo este análisis.

El Grupo de Trabajo reconoce que algunos Estados miembros ajenos al espacio Schengen no pueden beneficiarse de algunos de los instrumentos y sistemas vigentes, lo que puede influir en la prueba de necesidad que se realice en dichos países. Pero dichos Estados miembros pueden aplicar y de hecho aplican la directiva API y lo que debe estudiarse es si el uso de los sistemas existentes y la mejora de la cooperación entre Estados miembros y otros pudiera realmente aportar la información necesaria al efecto. Cabe también observar que el hecho de que los datos PNR se vayan a utilizar como herramienta inteligente, como se apunta en la evaluación de impacto, incrementa también el nivel de requisitos necesarios para garantizar la protección de datos.

2.3. Proporcionalidad

De acuerdo con la propuesta, se recogerá una enorme cantidad de datos personales sobre todos los pasajeros que vuelen hacia o desde la UE, se trate o no de sospechosos. La recogida y el tratamiento de datos PNR en la lucha contra el terrorismo y la delincuencia grave no deben posibilitar el rastreo y la vigilancia de todos los viajeros. El Grupo de Trabajo lo considera desproporcionado y, por ello, estima que recoger y retener todos los datos de todos los viajeros de todos los vuelos no se ajusta al artículo 8 de la Carta de los Derechos Fundamentales. Como ya se ha dicho, la evaluación de impacto no incluye justificación convincente al respecto. Las propuestas realizadas a nivel de la UE deben ser específicas y

orientadas a un objetivo concreto y, en el contexto presente, toda propuesta debe centrarse en los riesgos planteados por el terrorismo y la delincuencia grave.

El Grupo de Trabajo duda seriamente de que aplicar sistemáticamente a todos los pasajeros ciertos criterios predeterminados y verificar los datos en «bases de datos pertinentes» que no se especifican, sea una medida proporcional. No está claro cómo se van a definir dichos criterios predeterminados y dichas bases de datos pertinentes, ni si los datos PNR se utilizarán para crear o actualizar los criterios ni en qué medida todas las comprobaciones quedarán automáticamente sujetas a investigaciones adicionales. El Grupo de Trabajo desearía también recordar que, en algunos Estados miembros, métodos similares de control solo son constitucionales y consiguientemente viables para la policía con autorización judicial y en circunstancias específicas, como una amenaza específica. El sistema PNR propuesto convertiría esta excepcionalidad en un instrumento corriente del trabajo policial.

Implantar medidas que no supongan protección de los derechos y libertades de los viajeros solo es algo proporcionado cuando se hace como recurso temporal ante una amenaza específica, lo que no es el caso de esta propuesta. En la lucha contra el terrorismo y la delincuencia grave, la invasión de la intimidad de los viajeros debe ser proporcional a los beneficios. El Grupo de Trabajo no ha visto aún estadísticas que demuestren la relación entre el número de viajeros inocentes cuyos PNR se han recogido y el número de soluciones de orden público derivados de dichos datos.

En suma, el Grupo de Trabajo considera aún que sigue sin demostrarse que el sistema sea necesario y que las medidas propuestas no responden al principio de proporcionalidad. No obstante, el Grupo de Trabajo considera constructivo comentar también otros aspectos de la Directiva propuesta, que se exponen a continuación.

3. Objetivos

La propuesta de Directiva establece dos objetivos generales al tratamiento de datos con cuatro actividades específicas. Los datos PNR solo pueden tratarse a fines de:

- prevenir, detectar, investigar y enjuiciar delitos terroristas y delitos graves examinando a los pasajeros antes de su salida o llegada, verificando sus datos en bases de datos pertinentes (objetivo 1, actividad 1) y respondiendo a demandas de las autoridades competentes en casos específicos (objetivo 1, actividad 2); y
- prevenir, detectar, investigar y enjuiciar delitos terroristas y delitos transnacionales graves examinando a los pasajeros antes de su salida o llegada con arreglo a criterios específicos (objetivo 2, actividad 3) y analizando los datos de PNR para actualizar o crear nuevos criterios (objetivo 2, actividad 4).

No queda claro qué significan estos criterios en la práctica. El objetivo 1, actividad 1 parece querer decir que se verifiquen los datos en listas de alerta rápida, SIS u otras bases de datos nacionales o de la UE. El objetivo 1, actividad 2 parece significar que se comparta la información, caso por caso, cuando medie una demanda específica. El objetivo 2, actividad 3 parece indicar que se comparen los datos con perfiles de delitos específicos; y el objetivo 2, actividad 4 parece indicar que los datos PNR se usen para elaborar dichos perfiles.

Un principio básico de la protección de datos es que se definan estrictamente los objetivos y las actividades. Las «bases de datos pertinentes» deben también definirse con más detalle,

sumándolas quizás también a la lista de autoridades competentes que cada Estado miembro deberá presentar a la Comisión. En todo caso, las bases de bases utilizadas deben ser las creadas con iguales propósitos, es decir, la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves. Además, la legislación al uso debe ser clara en lo que atañe a las restricciones de uso de estas bases de datos. El Grupo de Trabajo reitera también la importancia de garantizar que todo criterio de evaluación aplicado por los Estados miembros para analizar los datos sea específico, esté justificado y se revise periódicamente.

3.1. Definiciones

La propuesta define los «delitos de terrorismo» como delitos tipificados en el Derecho nacional a que se refieren los artículos 1 a 4 de la Decisión marco 2002/475/JAI. Los «delitos graves» y los «delitos transfronterizos graves» se definen como delitos según el Derecho nacional a que se refiere el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI. El Grupo de Trabajo subraya la importancia de contar con decisiones precisas en esta materia, pero la definición de delito grave es demasiado amplia y cuestionamos la necesidad y proporcionalidad de usar datos PNR para algunos de esos delitos.

En relación con ello, el considerando 12 de la propuesta determina que los Estados miembros pueden excluir delitos menores si consideran desproporcionado incluirlos, pero es una opción que depende de cada Estado miembro. Esto pudiera llevar a una situación en que un Estado miembro incluye unos delitos y otro no. No está claro quién decide sobre la proporcionalidad de una medida ni si dicha decisión debe comunicarse a la Comisión, que podría garantizar la coherencia y la aplicación correcta del principio de proporcionalidad.

Las dudas del Grupo de Trabajo sobre el ámbito potencialmente amplio de la definición de delito grave se aplican también a las disposiciones que se proponen en la Directiva para compartir datos con otras autoridades de dentro y fuera de la UE.

4. Retención

Los plazos de retención propuestos se reducen claramente en comparación con la propuesta anterior y los distintos acuerdos de PNR adoptados a nivel de la UE. No obstante, el Grupo de Trabajo sigue considerando desproporcionada la propuesta de retener datos durante cinco años, aunque sea enmascarándolos. Desde siempre se ha procurado en los sistemas de PNR que todos los datos de todos los viajeros se guardaran durante el mismo periodo de tiempo; y este plazo de retención es de por sí desproporcionado. El Grupo de Trabajo no tiene pruebas satisfactorias que demuestren que haya que retener los datos de todos los viajeros; o que la retención deba ser de cinco años.

4.1. Enmascaramiento de datos

Aunque, de acuerdo con la propuesta, los datos vayan a enmascarse al cabo de 30 días y, en general, solo vayan a poder acceder a ellos determinados miembros del UEP encargados de elaborar perfiles y patrones de viaje, un acceso pleno a todos los datos seguiría siendo posible durante todo el plazo de retención. Aunque el enmascaramiento pretenda minimizar los datos y controlar el acceso a estos, que son principios importantes de la protección de datos, el Grupo de Trabajo sigue cuestionando que se precisen todos los datos de todos los funcionarios, y considera que los datos de los viajeros no sospechosos deben borrarse.

Si el legislador decidiera retener los datos durante un plazo limitado de tiempo, los datos deberían protegerse de modo que no se revelaran los detalles de la identificación. Esta medida de protección debería efectuarse como muy tarde a la llegada del vuelo. El acceso a los datos protegidos para localizar detalles de identificación debería depender de una decisión judicial caso por caso para investigaciones criminales específicas.

El Grupo de Trabajo desearía también recalcar con firmeza la necesidad de utilizar un lenguaje preciso que no confunda o se preste a equívocos. La propuesta menciona tanto «enmascaramiento» como «anonimización». Estos términos no son iguales y es evidente que el objetivo es el enmascaramiento, no la anonimización, pues los datos de identificación de una persona siguen pudiendo localizarse fácilmente. La propuesta, intencionadamente o no, no debe confundir o prestarse a equívocos ni tampoco prometer lo que no pueda cumplirse.

5. Derechos de protección de datos individuales

La propuesta contiene disposiciones que se refieren específicamente a la protección de datos. El Grupo de Trabajo considera necesario que toda propuesta de la UE que incida en los derechos y libertades de las personas incluya disposiciones sobre los derechos individuales de acceso, corrección, indemnización y recurso judicial. No obstante, los derechos de esta propuesta son los de la Decisión marco 2008/977/JAI, no los de la Directiva 95/46/CE. Por ello, los derechos están más limitados. No está claro si los derechos se aplican exclusivamente a los datos transferidos a otra autoridad o si incluyen los datos retenidos por la autoridad nacional. En algunos Estados miembros que utilizan actualmente datos PNR, el Derecho nacional de aplicación de la Directiva 95/46 reconoce los derechos de acceso, corrección y reclamación de los individuos; estos derechos quedarán reducidos si entra en vigor la propuesta de Directiva PNR.

Hay también un riesgo de discriminación derivado del trabajo de elaboración de perfiles pues el sistema considera a los pasajeros de las líneas aéreas como grupo. A los pasajeros no se les da información alguna sobre los criterios con arreglo a los cuales se les evalúa, lo que incide en el ejercicio de derechos de las personas directamente afectadas por el trabajo de elaboración de perfiles.

El Grupo de Trabajo recuerda la importancia de que se incluyan medidas adecuadas de protección de datos y salvaguardias en las propuestas de la UE que incidan en los derechos y libertades de las personas, como reglas de confidencialidad y tratamiento de seguridad, obligación de informar a las personas o prohibición de transmitir los datos a instancias privadas, y de que las decisiones no se adopten exclusivamente a partir de un tratamiento automatizado. El Grupo de Trabajo resalta también la importancia de incluir autoridades de control nacionales que, a nivel nacional, se ocupen de la aplicación de la legislación de la UE.

Respecto de los datos sensibles, la propuesta establece que el filtrado y borrado de los mismos los realice la UEP. En dictámenes sobre diversos acuerdos PNR de la UE con terceros países, el Grupo de Trabajo ha apoyado siempre la prohibición de tratar los datos sensibles en este contexto y recalcado con firmeza su opinión, ya antigua, de que el proceso de filtrado debe realizarlo la empresa de transporte antes de remitir los datos a la autoridad receptora.

El Grupo de Trabajo resalta la importancia de asegurar que las propuestas de la UE que incidan en los derechos y libertades de las personas incluyan requisitos de control y revisión

tales como el tratamiento de registros y las solicitudes de datos para permitir verificar la legalidad del tratamiento, el autocontrol y la garantía de la integridad y seguridad de los datos por parte de las autoridades nacionales de protección de datos. Sin embargo, es importante entender cómo van a funcionar en la práctica estos sistemas y cómo un registro y una documentación eficaces van a satisfacer los principios de minimización de datos antes mencionados.

6. Elementos informativos

A diferencia de los datos API, los datos PNR no se verifican, por lo que tienen menos fiabilidad. Los elementos informativos que figuran como anexo de esta propuesta son los mismos 19 elementos de los acuerdos UE-EE.UU. y UE-Canadá. El Grupo de Trabajo reitera su postura de que no hay pruebas suficientes que sugieran qué campos resultan necesarios y que, por consiguiente, tal lista es desproporcionada. Las categorías son generales y varias incluyen a su vez subconjuntos de datos. Aunque se prohibiera el tratamiento de datos personales sensibles, la lista de elementos informativos incluye el campo «observaciones generales», que puede contener toda clase de información, como preferencias de comidas, peticiones de servicios especiales, etc. Al Grupo de Trabajo no le consta que haya pruebas satisfactorias que muestren qué elementos de PNR han resultado necesarios o se han utilizado con éxito en soluciones policiales. Además, no todas las empresas de transporte recogen datos PNR.

7. Autoridades competentes y envíos a terceras partes

La propuesta dispone que los Estados miembros tienen que notificar a la Comisión la lista de sus autoridades competentes en el plazo de los doce meses siguientes a la entrada en vigor de la Directiva, lista que se publicará en el Diario Oficial. El Grupo de Trabajo respalda las medidas de transparencia que den una visión clara de las instancias que puedan recibir y tratar los datos. Pero las funciones (responsable del control/ responsable del tratamiento) de las autoridades competentes y los UEP no quedan claras.

El Grupo de Trabajo reitera su preocupación por la amplia definición que se hace de «delito grave», especialmente en relación con envíos a terceras partes dentro y fuera de la UE.

8. Revisión y reciprocidad

Según la propuesta, la Directiva se revisará a los cuatro años de su entrada en vigor. A los dos años de la entrada en vigor de la Directiva se hará una revisión especial para estudiar la posibilidad de ampliar su ámbito de aplicación a los vuelos intracomunitarios. El Grupo de Trabajo subraya la necesidad de que los procesos de revisión legislativa de la UE incluyan criterios claros en relación con los cuales pueda la revisión evaluar la necesidad y eficacia de un sistema. El Grupo de Trabajo reitera también la importancia de incluir autoridades nacionales de protección de datos en todo proceso de revisión, especialmente porque esto se prescribe en otros instrumentos de la UE, como los acuerdos PNR de la UE con terceros países.

Al desarrollar las propuestas de la UE, el Grupo de Trabajo subraya la importancia de tener en cuenta las implicaciones de eventuales requisitos de reciprocidad. Un modelo de PNR europeo podría llevar a que requisitos similares se plantearan recíprocamente por parte de países no democráticos o países que no cuenten con un nivel adecuado de protección de

derechos y libertades fundamentales, incluidos datos personales e intimidad. Es evidente que, si tales países recibieran datos PNR de la UE, podrían derivarse consecuencias graves para las personas.

9. Conclusión

El Grupo de Trabajo considera que aún no se ha demostrado la necesidad de un sistema de PNR de la UE y que las medidas propuestas no responden al principio de proporcionalidad, sobre todo porque el sistema plantea la recogida y retención de todos los datos de todos los viajeros de todos los vuelos. El Grupo de Trabajo tiene también serias dudas sobre la proporcionalidad de que los datos de todos los pasajeros se analicen sistemáticamente según criterios predeterminados.

El Grupo de Trabajo recomienda que antes se evalúen los sistemas y métodos de cooperación y el modo en que se ensamblan para detectar lagunas de seguridad. Si las hubiera, el paso siguiente sería analizar el mejor modo de paliarlas, lo que no implica necesariamente la introducción de un sistema nuevo entero. Los mecanismos actuales podrían seguir explotándose y mejorándose.

Si la presente propuesta de Directiva entrara en vigor, debería garantizar medidas y garantías de protección de datos apropiadas y adecuadas. La Comisión debiera también consiguientemente considerar la posibilidad de derogar algunos de los sistemas vigentes, como la Directiva API, para evitar solapamientos.

El Grupo de Trabajo continuará observando con atención la evolución de este asunto y agradecerá cualquier oportunidad de presentar y seguir elaborando su posición a las distintas partes implicadas en la presente propuesta. El Grupo de Trabajo continuará también aportando los dictámenes que sean apropiados y necesarios.

Bruselas, 5 de abril de 2011

*Por el Grupo de Trabajo
El Presidente
Jacob KOHNSTAMM*