



I

Conforme indica su disposición final cuarta mediante el Anteproyecto sometido a informe se incorpora al Derecho español la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, que regula, conforme a su artículo 1.1 la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE y el tratamiento de estos datos, incluida su recogida, utilización y conservación por los Estados miembros, así como el intercambio de los mismos entre dichos Estados miembros.

Como es sabido, la citada Directiva se aprobó en la misma fecha que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y que la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, formando con ambas lo que se conoce como el paquete de reforma de protección de datos.

La existencia de una Directiva específica reguladora de la materia a la que se refiere el Anteproyecto de Ley se funda en el hecho de que mientras el Reglamento General de Protección de Datos y la Directiva 2016/680 delimitan claramente dos ámbitos subjetivos diferenciados de aplicación, la Directiva 2016/681 establece un régimen de obligaciones en materia de protección de datos aplicable en ciertos preceptos a las compañías y operadores aéreos, así como otros sujetos obligados, sometidos en general a las previsiones del Reglamento General de Protección de Datos, y en otras normas aplicable a los órganos competentes para la prevención, investigación, detección o enjuiciamiento de infracciones penales, sometidos con carácter general a la Directiva.



El comentario que acaba de efectuarse resulta especialmente relevante, toda vez que las disposiciones concretas del Anteproyecto deben interpretarse de forma armonizada para cada uno de los sujetos incluidos en su ámbito de aplicación con las disposiciones generales que les son de aplicación. Por este motivo, el artículo 13 de la Directiva diferencia el derecho aplicable, teniendo en cuenta las normas vigentes en el momento de su entrada en vigor, estableciendo en sus apartados 1 a 3 que:

“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 protección de sus datos personales, derechos de acceso, rectificación, supresión y restricción y derechos de indemnización y recurso judicial que los establecidos en el derecho de la Unión y nacional y en aplicación de los artículos 17, 18, 19 y 20 de la Decisión marco 2008/977/JAI. Se aplicarán, por lo tanto, dichos artículos.

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

3. La presente Directiva se entenderá sin perjuicio de la aplicabilidad de la Directiva 95/46/CE del Parlamento Europeo y del Consejo al tratamiento de datos personales por las compañías aéreas, en particular sus obligaciones de tomar las medidas técnicas y de organización adecuadas para proteger la seguridad y la confidencialidad de los datos personales.”

Por otra parte, y aun cuando el artículo 18.1 de la Directiva 2016/681 (en adelante “Directiva PNR”) establece que los Estados miembros deberán proceder a su trasposición al derecho interno a más tardar el 25 de mayo de 2018, teniendo en cuenta el estado de tramitación del Anteproyecto sometido a informe, se omitirán, en lo que a las obligaciones de quienes deben facilitar información se refiere, toda referencia a la Ley Orgánica 15/1999, que queda desplazada del ordenamiento en cuanto no sea conforme al Reglamento General de Protección de Datos, que será la norma de referencia que se tomará en consideración en el presente informe, dado que su entrada en vigor tendrá lugar el mencionado 25 de mayo de 2018. Del mismo modo, en lo que pudiera resultar pertinente, y aun cuando se trate de una norma en trámite de aprobación, se hará referencia al Proyecto de Ley Orgánica de Protección de Datos, por el que se adapta el derecho español al mencionado Reglamento General.



En este sentido, y para concluir esta primera consideración preliminar, debe recordarse que el citado Proyecto de Ley contiene una cautela en relación con la normativa aplicable a los tratamientos sometidos a la Directiva 2016/680, al establecer su disposición transitoria cuarta que “Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva”.

Como segunda consideración previa, es preciso recordar que el régimen de comunicación de los datos contenidos en los registros de nombres de pasajeros a las autoridades competentes para la prevención, investigación, detección o enjuiciamiento de infracciones penales, así como su posible transferencia a terceros Estados en virtud de convenios internacionales concluidos por la Unión Europea ha sido objeto de un largo debate en el seno de las instituciones de la Unión así como en el marco de la actividad de las autoridades de protección de datos a lo largo de los últimos quince años, habiéndose adoptado diversos dictámenes por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, tales como la Opinión 7/2010 sobre la Comunicación de la Comisión 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, adoptado el 12 de noviembre de 2010.

Igualmente, esta cuestión, aunque desde el plano de la transferencia de los datos del PNR a terceros Estados ha sido objeto de análisis por el dictamen 1/2017, de 26 de julio, del Tribunal de Justicia de la Unión Europea que analiza el Convenio de la Unión con Canadá para la transmisión de dichos datos, a instancia del Parlamento Europeo. En este sentido, y tomando en consideración el citado dictamen debe tenerse en cuenta la doctrina sentada por el Tribunal en sus sentencias de 8 de abril de 2014 (asunto Digital Rights Ireland) y de 21 de diciembre de 2016 (asunto Tele2 Sverige), por cuanto la comunicación de los datos PNR puede considerarse, tal y como indican los apartados 124 y 126 del dictamen 1/2017 una injerencia en los derechos a la intimidad y a la protección de datos de carácter personal, consagrados por los artículos 7 y 8 de la Carta de Derechos de la Unión Europea.

Como última consideración previa, debe señalarse que habida cuenta del objeto del Anteproyecto sometido a informe será preciso que el mismo se extienda a la práctica totalidad de su articulado, al encontrarse el mismo vinculado al régimen de protección de datos de carácter personal. No obstante,



se dedicará un análisis más detallado a aquellos preceptos que pudieran revestir una mayor complejidad en su análisis conjunto con las normas de protección de datos que resultan de aplicación.

II

Entrando ya en el análisis del articulado del Anteproyecto sometido a informe, el Capítulo I, bajo la rúbrica “disposiciones generales”, regula su objeto y ámbito de aplicación, clarificando el alcance de las referencias a los “delitos graves” y los datos del registro PNR y especificando quiénes se encuentran sometidos a las obligaciones de transmisión previstas en el texto.

Respecto de la delimitación del alcance de los delitos graves cuya prevención, investigación, detección o enjuiciamiento podrá justificar la aplicación de las disposiciones del Anteproyecto, así como de los datos PNR a los que el mismo se refiere, y sin perjuicio respecto de estos últimos de lo que posteriormente se indicará, el Anteproyecto se limita a reproducir, respectivamente los Anexos II y I de la Directiva 2016/681, por lo que no cabe efectuar comentario adicional alguno.

Por otra parte, en cuanto al objeto y ámbito de aplicación del Anteproyecto, el artículo 2 prevé que la norma será de aplicación tanto a vuelos comerciales como a vuelos privados, añadiendo determinados supuestos en que se excluye su aplicación, tales como “los vuelos realizados por aeronaves de Estado, trabajos aéreos, aviación general que no tenga por objeto el transporte de personas, servicios aeroportuarios, servicios de navegación aérea, vuelos relacionados con la producción de aeronaves civiles, vuelos de entrenamiento de tripulaciones, vuelos de traslado para mantenimiento y revisión y vuelos relacionados con funciones regulatorias”.

Igualmente, se indica que dichos vuelos serán, según el apartado 1, “tanto interiores como exteriores de la Unión Europea, que tengan programada su salida del territorio español o la llegada al mismo, o que hagan escala en él”. A ello añade el artículo 2.3 que la norma “será de aplicación a las rutas o los vuelos concretos de carácter nacional, que tengan su origen o destino programado en territorio español y que no efectúen escalas en ningún otro Estado, siempre que exista una clara, cierta y contrastada situación de riesgo, con la finalidad de prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves”.

Esta última previsión se complementa con la disposición adicional segunda, que prevé que “Las rutas o los vuelos concretos de carácter nacional a los que será de aplicación esta ley en virtud del artículo 2.3 serán determinados por el Secretario de Estado de Seguridad, que podrá delegar esta competencia en el Director del Centro de Inteligencia contra el Terrorismo

y el Crimen Organizado”, dada la condición de éste como Unidad de Información de Pasajeros (en adelante UIP)

Ciertamente, la Directiva 2016/681 se limita a hacer referencia a lo largo de su articulado a la aplicación de sus disposiciones en relación con las obligaciones y actuación de las compañías aéreas, lo que aparentemente podría implicar que las disposiciones de su norma de trasposición únicamente fueran aplicables a los vuelos comerciales y no a los vuelos privados. Tampoco se establece una disposición que habilite expresamente a los Estados miembros a ampliar su ámbito de aplicación a los vuelos privados, lo que podría reincidir en la conclusión alcanzada.

Sin embargo, es preciso tener en cuenta cuál es el objeto del régimen establecido por la Directiva, que puede resumirse claramente en el primer inciso de su considerando 10, cuando indica que “Para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves, es fundamental que todos los Estados miembros introduzcan disposiciones que impongan a las compañías aéreas que realizan vuelos exteriores de la UE, la obligación de transferir todos los datos PNR que recojan, incluidos los datos API”.

Es decir, se persigue con la regulación establecida en la citada Directiva la posibilidad de que las autoridades competentes para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo o delitos graves mencionados en su Anexo II puedan conocer qué personas han utilizado el transporte aéreo, dentro de los límites establecidos en la propia Directiva, a fin de, por una parte, poder acceder a esa información y, por otra, poder establecer modelos de conducta que permitan una mayor prevención de tales conductas delictivas.

Pues bien, el efecto útil perseguido por la Directiva se vería limitado si las obligaciones de información y la posibilidad de acceso a la información facilitada quedase limitada a los vuelos comerciales, dado que es posible que existan determinados modelos de conducta que partan, precisamente, del uso de aviación no comercial, particularmente vinculado a determinadas actividades delictivas y al crimen organizado.

De este modo, la limitación del alcance del texto sometido a informe a la aviación comercial podría perjudicar el efecto útil de la Directiva, por lo que su adecuada trasposición debería incluir también los vuelos privados.

Evidentemente, esta ampliación sin embargo podría implicar la asunción en el ámbito de la aviación privada de nuevas obligaciones derivadas de la necesidad de recopilar todos los datos PNR contenidos en el Anexo I de la Directiva. Sin embargo el Anteproyecto tiene en cuenta esta circunstancia y establece una limitación en lo que afecta a los datos respecto de los que existirá



la obligación de comunicación en el caso de los vuelos privados. En este sentido, el artículo 5.3 dispone que “Los datos PNR de los pasajeros de los vuelos privados así como de la tripulación y del resto de las personas referidas en el segundo párrafo del apartado 1, que deberán ser cedidos a la Unidad de Información sobre Pasajeros, son los recogidos en los párrafos p) y r) del apartado anterior”. De este modo, en los supuestos de vuelos privados únicamente procederá la comunicación de datos del sistema de información anticipada de pasajeros (datos API, en los términos previstos en el artículo 3.2 de 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) y la información relativa al equipaje, pero ninguna otra información adicional. De este modo, queda garantizado el cumplimiento del objeto de la Directiva 2016/681 y al propio tiempo no se imponen cargas adicionales respecto de la aviación privada.

En cuanto a las rutas respecto de las que habrá de facilitarse la información, el artículo 2 de la Directiva PNR dispone en su apartado 1 que “En caso de que un Estado miembro decida aplicar la presente Directiva a los vuelos interiores de la UE, lo notificará por escrito a la Comisión”, lo que implica la posibilidad de aplicación de las disposiciones a los vuelos intracomunitarios, tal y como prevé el artículo 2.1 del Anteproyecto al referirse a vuelos interiores de la Unión.

A su vez, el artículo 2.3 de la Directiva añade que “Cada Estado miembro podrá decidir aplicar la presente Directiva exclusivamente a vuelos interiores de la UE seleccionados. Al adoptar tal decisión, el Estado miembro deberá elegir los vuelos que considere necesarios a fin de perseguir los objetivos de la presente Directiva. El Estado miembro podrá decidir modificar la selección de vuelos interiores de la UE en todo momento”.

De este modo, no cabe oponer objeción a la posibilidad de que el ámbito de aplicación del Anteproyecto se extienda, en determinadas circunstancias a rutas o vuelos, a vuelos domésticos, tal y como prevé el artículo 2.3 del Anteproyecto.

No obstante, el precepto mencionado, y su conexión con la disposición adicional segunda del Anteproyecto plantean algunas dudas interpretativas que deberían ser resueltas en la versión final del texto.

Así, en primer lugar, se plantea si no existiría algún tipo de redundancia en la delimitación que el artículo 2.3 realiza de lo que debe entenderse por vuelos de carácter nacional, dado que se indica que la extensión de los efectos de la Ley se aplicará a “vuelos concretos de carácter nacional, que tengan su origen o destino programado en territorio español y que no efectúen escalas en ningún otro Estado”. Esta clarificación podría resultar redundante, dado que serán vuelos nacionales los que tengan origen y destino en territorio español,

pudiendo establecerse la delimitación que efectúa el último inciso haciendo referencia a “vuelos concretos de carácter nacional que no efectúen escalas en ningún otro Estado”.

El principal problema se plantea en cuanto a la delimitación de los criterios y la fijación de la competencia para determinar los vuelos nacionales a los que podrá extenderse esta habilitación.

En efecto, el artículo 2.3 de la Directiva PNR impone que en caso de optarse por su aplicación a vuelos internos de la Unión Europea, el Estado “deberá elegir” los que considere necesarios para el cumplimiento de los objetivos de la misma. Ello supone que la delimitación de cuáles habrán de ser esos vuelos deberá haberse adoptado, con carácter previo a la solicitud de la información, y sobre la base de un contenido reglado, cual es la vinculación de las rutas con los objetivos de la Directiva.

Ciertamente, el artículo 2.3 establece un criterio delimitador de las rutas relacionado con la consecución de los objetivos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo o delitos graves, basado en el hecho de que “exista una clara, cierta y contrastada situación de riesgo”. Sin embargo, este criterio parece ser poco coherente con lo previsto en la Directiva, que parece partir de una previa determinación de los supuestos en que procederá aplicar las obligaciones previstas en aquélla, toda vez que la amenaza, además de clara y contrastada debería ser cierta.

Ello, además, se vincula con la ya reproducida disposición adicional segunda, en que se indica que la delimitación de los vuelos a los que será aplicable el precepto se llevará a cabo por el Secretario de Estado de Seguridad, que podrá delegar la competencia en el Director del Centro de Inteligencia contra el terrorismo y el crimen organizado, lo que parece estar vinculado a su condición de UIP nacional.

A este respecto, debe indicarse, en primer lugar, que esta disposición debería formar parte del articulado del Proyecto, dado que, teniendo en cuenta el margen otorgado por el artículo 2.3 de la Directiva PNR, sería preciso establecer un mínimo procedimiento que especifique el modo en que se procederá a la delimitación de las rutas nacionales a las que será de aplicación el Anteproyecto. Esta disposición debería especificar el modo en que se apreciaría la posible concurrencia de las excepcionales circunstancias mencionadas en el precepto, que en ningún caso podría fundarse en la mera inmediatez.

Al propio tiempo, debe señalarse que no parece que se encuentre en el espíritu de la Directiva la habilitación a las UIP nacionales, cuyas funciones en relación con el PNR aparecen claramente delimitadas en el texto, la competencia para establecer, aunque sea por delegación, las rutas nacionales



a las que debería aplicarse el Anteproyecto. En todo caso, esta función debería ser la de propuesta al órgano competente de tales rutas al apreciar, a la vista de la información recabada y la actuación de inteligencia que se desarrollase con dicha información la posible concurrencia de las circunstancias que justifiquen la ampliación del ámbito de aplicación del texto a este tipo de rutas.

Por todo ello, se considera que sería preciso dar nueva redacción al artículo 2.3 del Anteproyecto, en los siguientes términos.

“Además, será de aplicación a las rutas o los vuelos concretos de carácter nacional que no efectúen escalas en ningún otro Estado, siempre que existan **indicios suficientes de** una clara y contrastada situación de riesgo, con la finalidad de prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves.

Estas rutas o vuelos **se determinarán mediante resolución del** Secretario de Estado de Seguridad **a propuesta del** Director del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.”

III

El Capítulo I también delimita los sujetos respecto de los que se recabarán los datos PNR. Así, el artículo 1.1 a) hace referencia, dentro del objeto de la Ley a “La transferencia de datos del registro de nombres de los pasajeros, de la tripulación y de cualquier otra persona a bordo del vuelo (datos PNR)”.

Añade el artículo 5.1 que “Los datos PNR son el conjunto de datos relativos al viaje de un pasajero, reservado por él o en su nombre, que recoge la información necesaria para la gestión de la reserva”, señalando en su párrafo segundo que “a efectos de esta ley, tendrán la consideración de datos PNR los datos de los miembros de la tripulación que cumplen sus obligaciones profesionales en relación al vuelo, y de cualquier otra persona que viaje a bordo del mismo”.

La Directiva PNR define en su artículo 3.5 el registro de nombres de los pasajeros o PNR como “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 utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades”.

Quiere ello decir, que el alcance de la Directiva se limita a información referida a los pasajeros del vuelo. A tal efecto, el artículo 3.4 de la Directiva



define como tales “toda persona, incluidos los pasajeros en tránsito o en conexión y exceptuados los miembros de la tripulación, transportada o que vaya a ser transportada a bordo de una aeronave con el consentimiento de la compañía aérea, lo cual se manifiesta en la inclusión de la persona en la lista de pasajeros”.

De este modo, la Directiva excluye de su ámbito de aplicación cualquier información referida a quienes no ostenten la condición de pasajeros, lo que excluiría de la misma y de su transposición los datos de los miembros de la tripulación, así como los de cualquier otra persona que no tenga la condición de pasajeros.

Al propio tiempo, de la definición contenida en la Directiva parece deducirse que la misma únicamente contempla la posibilidad en que a bordo de una aeronave puedan hallarse durante el viaje dos categorías de personas: los pasajeros y los tripulantes. De ello parece deducirse que toda persona que no pertenezca a la tripulación, incluyendo las mencionadas tanto en el artículo 1.1 a) como en el artículo 5.1, párrafo segundo del Anteproyecto deberá tener la condición de pasajero, lo que podría incluir al personal de seguridad de la línea aérea, las personas que pudieran, por diversas circunstancias embarcarse en el vuelo, incluso gratuitamente, en caso de existir disponibilidad para ello o el persona de las Fuerzas y Cuerpos de Seguridad, que en definitiva tendrían esa condición.

Por ello, la primera conclusión que cabe alcanzar es que, no siendo posible, desde la perspectiva de la Directiva, la existencia de personas a bordo distintas de los pasajeros y tripulantes, **no parece lógico hacer referencia a “cualquier otra persona que viaje a bordo” de la aeronave, que debería suprimirse de los artículos 1.1 a) y 5.1 del Proyecto.**

Por otra parte, como se ha dicho, el régimen de la Directiva únicamente es aplicable a los pasajeros, lo que, por una mera interpretación sistemática parece lógico, si se tiene en cuenta que la misma se refiere a la información del “registro de nombres de pasajeros”, siendo así que los tripulantes no ostentan esta condición ni un gran número de las informaciones establecidas en el artículo 5.2 pueden ir referidas a los mismos.

Ciertamente, y en aras a lograr el efecto útil de la Directiva puede tener sentido que la UIP pueda conocer la información esencial acerca de los tripulantes de la aeronave. Sin embargo ello no permite que los datos de los mismos puedan asimilarse, directa o indirectamente al PNR.

Sin embargo, como se ha indicado, el Anteproyecto crea en su artículo 5.1 la ficción de que la información referida a la tripulación “tendrá la consideración de datos PNR” a los efectos de la Ley, si bien en el artículo 5.3 indica que los únicos datos que deberán ser objeto de cesión a la UIP serán

los recogidos en los párrafos p) y r) del artículo 5.2; es decir, los datos API y la información referida al equipaje.

A nuestro juicio sería recomendable que se modificase el tenor del Anteproyecto para clarificar el alcance de las previsiones a las que se refiere el artículo 5.3 y hacerlas más acordes con lo establecido en la Directiva que, como se ha indicado ahora para el caso de tripulantes y terceras personas, y se señaló en un lugar anterior respecto de los datos relativos a vuelos privados, no aparecen expresamente regulados por la citada norma de Derecho de la Unión aun cuando la obtención de estos datos con la finalidad de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves recogidos en el Anexo II de la Directiva puedan contribuir a lograr el efecto útil de dicha norma.

Ello exigiría no considerar datos PNR los datos referentes a los mencionados colectivos y los citados vuelos, sino indicar en el Anteproyecto que serán de aplicación las mismas obligaciones a los datos contenidos en el sistema de información anticipada de pasajeros así como las informaciones referidas al equipaje de los tripulantes y, en caso de existir tal colectivo, las terceras personas mencionadas en el texto, así como los procedentes de vuelos privados.

De este modo, sería preciso modificar diversos preceptos del Anteproyecto, a fin de ajustarlos a lo que acaba de mencionarse. De este modo, sería preciso modificar el artículo 1.1 a), redactándolo en los siguientes términos:

“La transferencia de datos del registro de nombres de los pasajeros (datos PNR), así como la información referida a la tripulación prevista en el artículo 5.3 de esta Ley, correspondientes a vuelos internacionales y nacionales, en los términos y a los efectos previstos en el capítulo II.”

Del mismo modo, sería preciso suprimir el segundo párrafo del artículo 5.1, modificando a su vez el artículo 5.3, quedando redactado en los siguientes términos.

“Las disposiciones de esta Ley Orgánica serán igualmente aplicables a los datos de la tripulación que se contuvieran en el sistema de información anticipada sobre los pasajeros (sistema API), así como la información relativa al equipaje de los miembros de la tripulación y de los pasajeros y tripulantes de los vuelos privados.”

IV



Por último, dentro de las previsiones del Capítulo I del Anteproyecto, debe hacerse ahora referencia a lo dispuesto en el artículo 4, referido a los sujetos obligados a la comunicación de la información. En el apartado 1 de dicho precepto se señala que serán sujetos obligados las compañías aéreas, reproduciendo el concepto que de las mismas da el artículo 3.1 de la Directiva PNR, si bien **debería incluirse la mención efectuada por la Directiva a que se trate de transporte “de pasajeros”**.

Junto con dicha referencia, el artículo 4.1 señala que en el caso de vuelos privados el sujeto obligado será el titular de la aeronave, debiendo tenerse en cuenta lo ya señalado

Finalmente, conforme al artículo 4.2 serán sujetos obligados “las entidades de gestión de reserva de vuelos, entendiendo como tales a cualquier entidad que gestione reservas de vuelos de pasajeros y recabe datos PNR de los mismos, cualesquiera que sean los medios utilizados para ello, tales como los operadores turísticos o las agencias de viajes

En este sentido, debe recordarse que el considerando 33 de la Directiva PNR indica que la misma “no afecta a la posibilidad de que los Estados miembros establezcan en su derecho nacional un mecanismo para recoger y tratar los datos PNR proporcionados por operadores económicos que no sean compañías aéreas, tales como agencias de viaje y operadores turísticos que prestan servicios relacionados con los viajes, como la reserva de vuelos, para los cuales recogen y tratan datos PNR, o de los transportistas que no sean los mencionados en él, siempre que el derecho nacional de que se trate respete el derecho de la Unión”. De este modo, esta posibilidad se encuentra expresamente reconocida por la Directiva.

No obstante, sería preciso que se plantease el problema que podría surgir en caso de discrepancia entre los datos PNR facilitados por las compañías aéreas y los sujetos mencionados en el artículo 4.2, teniendo en particularmente que la última versión actualizada de los datos será la que remita la compañía aérea en el momento de cierre del embarque.

Este problema parece solucionarse cuando el artículo 7.2 del Anteproyecto establece que “Las entidades de gestión de reservas de vuelos enviarán todos los datos PNR de los que dispongan en el transcurso normal de su actividad, correspondientes a los vuelos incluidos en el ámbito de aplicación de esta ley, a la compañía aérea explotadora del vuelo de que se trate”.

Sin embargo, los términos en que se establece este precepto, aun no resultando contradictorios con el artículo 4.2 del Anteproyecto podría inducir al equívoco de considerar que estos sujetos están obligados a la comunicación de los datos PNR no a las compañías aéreas, sino a la Unidad de Información sobre pasajeros.



Por ello, **sería conveniente que se clarificase en el artículo 4.2 del Anteproyecto que los sujetos a los que el mismo se refiere se encuentran obligados en los términos establecidos en el artículo 7.3.**

V

El Capítulo II del Anteproyecto, bajo la rúbrica “tratamiento de los datos PNR”, regula el cuerpo de obligaciones impuestas tanto a los sujetos obligados en el artículo 4 de aquél como a los distintos órganos públicos intervinientes en el sistema (UIP y autoridades competentes), trasponiendo las previsiones contenidas en los artículos 4 a 14 de la Directiva PNR.

Dicho Capítulo regula en primer lugar la Unidad de Información sobre pasajeros, que, según se indica “se encuentra encuadrada” en el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (en adelante CITCO), dependiente de la Secretaría de Estado de Seguridad, que desarrollará las funciones enumeradas en el artículo 6.2. Dicha UIT contará con un responsable de la protección de los datos PNR, que “velará por que se adopten las medidas oportunas para controlar el tratamiento de estos datos, y por que se apliquen las garantías en materia de protección de datos”, para lo que habrá de contar “con los medios necesarios para el desempeño de sus funciones de manera eficaz e independiente”, actuando como punto de contacto único al que cualquier interesado podrá dirigirse para todas las cuestiones relativas al tratamiento de sus datos PNR. El artículo

Sin embargo, el artículo 6.4 no considera responsable del tratamiento a la propia UIT, integrada en el CITCO, sino al propio Centro, indicando que “podrá encomendar el tratamiento de todos o de algunos datos PNR, respecto de todas o de algunas operaciones de tratamiento, a un encargado, que actuará siempre por cuenta de aquel”, si bien ese tratamiento sólo podrá llevarse a cabo, conforme al artículo 4.5 “en lugares seguros dentro del territorio nacional”.

A nuestro juicio, podría apreciarse la existencia de una contradicción entre los apartados 3 y 4 de este precepto, dado que si bien por una parte, de la enumeración de las funciones establecidas en el apartado 2 y la obligación de designación de un responsable de protección de datos en el apartado 3 se derivaría que la UIP tiene por sí misma la consideración de responsable del tratamiento de los datos PNR, el apartado 4 señala terminantemente que esta condición de responsable no recae en la propia Unidad, sino en el CITCO en que la misma se encuentra integrada.

El artículo 2.3 c) del Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, regula el CITCO como órgano de coordinación dependiente de la Secretaría de Estado



de Seguridad “al que corresponde la recepción, integración y análisis de la información estratégica disponible en la lucha contra todo tipo de delincuencia organizada o grave, terrorismo y radicalismo violento, el diseño de estrategias específicas contra estas amenazas y su financiación, así como, en su caso, el establecimiento de criterios de actuación y coordinación operativa de los organismos actuantes en los supuestos de coincidencia o concurrencia en las investigaciones”, refiriéndose a continuación a una serie de materias competencia del citado Centro:

“1.º Recibir, integrar y analizar informaciones y análisis operativos que sean relevantes o necesarios para elaborar la correspondiente inteligencia criminal estratégica y de prospectiva, tanto en su proyección nacional como internacional, integrando y canalizando a las Fuerzas y Cuerpos de Seguridad del Estado toda la información operativa que reciba o capte.

2.º Dictar, determinar y establecer, en los supuestos de intervención conjunta o concurrente, los criterios de coordinación y de actuación de las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado, y la de éstos con otros organismos intervinientes, en función de sus competencias propias o de apoyo a la intervención.

3.º Elaborar informes anuales, así como una evaluación periódica de la amenaza.

4.º Elaborar, en coordinación con el Gabinete de Coordinación y Estudios, las informaciones estadísticas no clasificadas relacionadas con estas materias, en especial la estadística oficial sobre drogas.

5.º Proponer, en el ámbito de sus competencias, las estrategias nacionales y actualizarlas de forma permanente, coordinando y verificando su desarrollo y ejecución.

6.º Establecer, en el ámbito de sus competencias, las relaciones correspondientes con otros centros o unidades similares de la Unión Europea, sus Estados miembros o terceros países.”

De la descripción de estas funciones se desprende la necesidad de diferenciar la UIP, como órgano integrado en el CITCO, cuyas funciones deberán corresponderse con las recogidas, con un carácter bastante más restrictivo, en el artículo 6 de la Directiva PNR, del CITCO, en que dicha Unidad se encontrará integrada, y cuyas funciones, más extensas no podrían en principio referirse sin más a los datos PNR salvo que se encuentran expresamente amparadas por el citado artículo 6.



Debe recordarse que la existencia de una unidad separada encargada de la recepción de los datos PNR y su transmisión a las autoridades competentes es uno de los aspectos esenciales de la Directiva PNR, actuando esa Unidad como sujeto interpuesto entre las compañías aéreas y dichas autoridades, que podrá además llevar a cabo actuaciones específicas de análisis dentro de los límites establecidos en la Directiva.

En este sentido, el considerando 13 se refiere expresamente a las unidades, indicando que “Los datos PNR deberán transmitirse a una unidad única de información sobre los pasajeros («UIP») designada en el Estado miembro de que se trate, a fin de garantizar la claridad y reducir los costes de las compañías aéreas. La UIP puede disponer de distintas sucursales dentro de un Estado miembro, y los Estados miembros también podrán establecer conjuntamente una UIP. Los Estados miembros deberán intercambiar mutuamente la información a través de las correspondientes redes de intercambio de información para facilitar dicho intercambio y garantizar la interoperabilidad”

Por este motivo, deberá ser la propia UIP y no el CITCO, aun cuando la Unidad se integre en su estructura orgánica, el responsable del tratamiento de los datos, debiendo además establecerse determinadas limitaciones a la utilización de los datos PNR por parte del CITCO, dado que la realización de labores de inteligencia y análisis debería limitarse a lo establecido expresamente en la Directiva, sin que sea posible una extensión de dichas actuaciones mediante el cruce de los datos PNR con cualesquiera bases de datos, cuestión a la que se hará referencia posteriormente.

En consecuencia, debería modificarse el apartado 4 del artículo 6 del Anteproyecto sometido a informe, indicando lo siguiente:

“La Unidad de Información sobre Pasajeros, en su condición de responsable del tratamiento de los datos PNR podrá encomendar el tratamiento de todos o de algunos datos PNR, respecto de todas o de algunas operaciones de tratamiento, a un encargado, que actuará siempre por cuenta de aquel”.

Por lo demás, las funciones encomendadas a la UIP en el apartado 2 del artículo 6 del Anteproyecto responden a las establecidas en los artículos 4.2, 6.2 y 6.3 de la Directiva PNR, aun cuando **es aconsejable que dichas funciones se recogiesen expresamente con el mismo grado de detalle que se establece en dichos preceptos, a fin de evitar que puedan considerarse amparados por el Anteproyecto tratamientos de datos que excedan de los que traen cobertura de la Directiva** lo que podría implicar una extralimitación del principio de limitación de finalidad, consagrado por el artículo 4.1 b) de la Directiva 2016/680. Al propio tiempo, estas funciones deben estudiarse de

forma conjunta con las establecidas en el artículo 8 del Anteproyecto, tal y como se hará en un lugar posterior.

Finalmente, el apartado 3 del artículo 6 del Anteproyecto resulta ajustado a las exigencias establecidas por el artículo 5 de la Directiva PNR, no siendo preciso efectuar ningún otro comentario respecto del mismo

VI

El artículo 7 del Anteproyecto regula, conforme a lo establecido en el artículo 8 de la Directiva PNR, las obligaciones de comunicación de los datos PNR por parte de los sujetos obligados, estableciendo en sus apartados 1 y 2 la obligación genérica de comunicación, en su apartado 3 el formato en que dicha comunicación podrá tener lugar, en su apartado 4 el momento en que deberá facilitarse la información y en su apartado 5 la posibilidad de que la información pueda ser requerida al margen de los momentos establecidos en el apartado 4.

Al margen de lo ya indicado en la última parte del apartado IV de este informe, cabe efectuar las siguientes consideraciones en relación con el artículo 7 del Anteproyecto.

1) El primer párrafo del apartado 1 señala que en caso de vuelos privados “los datos PNR deberán ser remitidos por el piloto de la aeronave”.

Como primera consideración, ya se indicó en un lugar anterior que en el caso de los vuelos privados no se procederá a la comunicación de los datos PNR, dado que como tales no existen. Del mismo modo, se indicó que resulta preferible especificar los datos que habrán de facilitarse y no establecer una suerte de equivalencia real de los datos a facilitar con los datos PNR. Por este motivo, **sería necesario suprimir la expresión PNR de este último inciso del párrafo primero.**

Al propio tiempo, el Anteproyecto otorga en su artículo 4.1b) la condición de sujeto obligado al titular de la aeronave, por lo que la referencia al piloto de la misma, establecida en el artículo 7.1 podría introducir cierta confusión, al generar la apariencia de que es el piloto y no el titular el sujeto obligado.

Si se considera necesario establecer esta **especificación debería resultar claro que la misma no convierte al piloto en sujeto obligado**, del mismo modo que no lo serán las personas a cargo de la compañía aérea encargadas de garantizar el cumplimiento por la misma de las obligaciones previstas en el Anteproyecto.

2) En segundo lugar, el artículo 7.1 prevé en su párrafo segundo que “Estas entidades informarán a las personas a las que se refieran dichos datos



del motivo de su recogida y de su destinatario, ante quien podrán ejercitar sus derechos”.

Sería necesario que la obligación prevista en el precepto correspondiese a los sujetos obligados y no a “estas entidades”, toda vez que el párrafo primero del artículo 7.1 no se refiere a entidades en todos los supuestos, al incluir, como se ha indicado, sujetos obligados y personas que dentro del sujeto obligado han de facilitar la información.

Por otra parte, en cuanto al alcance de la obligación, es preciso indicar que las compañías aéreas y los titulares de los vuelos privados en su condición de responsables del tratamiento se encuentran sometidos al Reglamento 2016/679, cuyo artículo 13 regula el principio de transparencia y el derecho a la información sobre el tratamiento, imponiendo a los responsables una serie de obligaciones de información mucho más amplias que las mencionadas en el párrafo segundo del artículo 7.1.

Por este motivo, sería necesario modificar la redacción de este segundo párrafo, resultando la siguiente:

“Dentro del cumplimiento de sus obligaciones de información, y sin perjuicio de lo establecido en el Reglamento (UE) 2016/679, los sujetos obligados informarán a las personas a las que se refieran **los datos PNR** del motivo de su recogida y de su destinatario, ante quien podrán ejercitar sus derechos.”

3) El párrafo tercero del artículo 7.1 se refiere a los vuelos con código compartido, disponiendo en su primer inciso que “los casos en que existan varias compañías aéreas relacionadas con un mismo vuelo, la obligación de transmitir los datos recaerá en la compañía aérea que actúe como explotadora o comercializadora principal del mismo”.

La Directiva PNR se refiere a estas situaciones en su artículo 8.1, estableciendo que “En los casos en que el código de un vuelo internacional sea compartido con una o más compañías aéreas, la obligación de transmitir los datos PNR de todos los pasajeros de dicho vuelo recaerá en la compañía aérea que explote el vuelo”.

Pues bien, siendo claro el concepto establecido en la Directiva, no se alcanza a comprender el motivo por el que el Anteproyecto sometido a informe diferencia entre la compañía que explota el vuelo y la comercializadora principal, siendo así que podría darse el caso de que no recayendo ambas circunstancias en la misma compañía se plantease la duda de cuál de las dos es la obligada. Por el contrario, si dicha discrepancia no tuviera lugar en ningún supuesto tampoco parece lógico modificar en este punto el tenor de la Directiva PNR, que se refiere exclusivamente a la compañía explotadora del vuelo.



Por ello, **procedería suprimir la expresión “o comercializadora principal” en el párrafo tercero del artículo 7.1.**

4) El apartado 4 regula los momentos en que podrán facilitarse los datos. A tal efecto, dispone el último inciso de la letra b) de este apartado en relación con la información que habrá de facilitarse en el momento en que se cierre el embarque de la aeronave, que deberán “transmitirse todos los datos PNR correspondientes al vuelo, de manera completa, incluidos los datos modificados o nuevos respecto a los transmitidos de acuerdo al párrafo anterior”.

En este punto, debe recordarse que el artículo 8.4 de la Directiva PNR dispone que “Los Estados miembros permitirán a las compañías aéreas que limiten la transmisión a que se refiere el apartado 3, letra b), a actualizaciones de la transmisión a que se refiere la letra a) de dicho apartado”.

Como puede comprobarse, el citado precepto no establece una habilitación para que los Estados miembros determinen si únicamente deberá facilitarse la información que haya sido objeto de actualización o si, por el contrario, la información debe transmitirse en su integridad. Por el contrario, se impone expresamente a los Estados Miembros la obligación de permitir que los sujetos obligados faciliten únicamente los datos en que se haya modificado la información PNR que hubo de ser transmitida en el período comprendido entre las 24 y 48 horas anteriores a la salida del vuelo, garantizando así el cumplimiento del principio de exactitud de los datos.

De este modo, la imposición de una regla que impide a los sujetos obligados optar por facilitar únicamente la información actualizada de los datos PNR resultaría contraria a la Directiva.

Por ello, **procedería suprimir el inciso “debiendo transmitirse todos los datos PNR correspondientes al vuelo, de manera completa, incluidos los datos modificados o nuevos respecto a los transmitidos de acuerdo al párrafo anterior” del artículo 7.4 b) del Anteproyecto o reemplazarlo por “pudiendo transmitir únicamente los datos modificados o nuevos respecto a los transmitidos de acuerdo al párrafo anterior”.**

Por otra parte, el apartado 4 incluye un segundo párrafo en que se indica que los sujetos obligados “deberán transmitir, inmediatamente, cualquier modificación de los datos previamente enviados que se produzca durante el vuelo”.

Esta obligación no aparece recogida en ningún precepto de la Directiva PNR, resultando además confuso que dicha información, dentro del concepto de datos PNR contenido en la propia Directiva sea posible, toda vez que en caso de producirse alguna modificación no lo será en dichos datos, sino en la

información referida al propio vuelo, como sucedería, por ejemplo, en caso de que fuese previsto realizar una escala técnica o la aeronave debiera aterrizar en un aeropuerto distinto al de destino por cualquier motivo.

Sin lo que se pretende es indicar que las compañías deberán facilitar esa información **sería necesario desvincularla de los datos PNR, que por su propia definición no podrían modificarse una vez iniciado el vuelo.**

5) Resta por último hacer referencia al apartado 5 del artículo 7 del Anteproyecto, según el cual “cuando sea necesario acceder a los datos PNR para responder a una amenaza real y concreta relacionada con delitos de terrorismo o con delitos graves, todos los sujetos obligados, caso por caso, deberán transmitir a la Unidad de Información sobre Pasajeros dichos datos o permitirán su acceso a los datos PNR de que se trate, con carácter inmediato al requerimiento recibido”.

Este precepto pretende ser la trasposición al derecho español del artículo 8.5 de la Directiva PNR, que establece que “Cuando sea necesario acceder a los datos PNR para responder a una amenaza concreta y real relacionada con delitos de terrorismo o delitos graves, las compañías aéreas, caso por caso, transmitirán los datos PNR en momentos distintos de los mencionados en el apartado 3, a petición de una UIP y de conformidad con el derecho nacional”.

La razón de ser de este precepto de la Directiva resulta plenamente ajustada al objeto de la misma y, en consecuencia, a la finalidad del tratamiento, dado que son las circunstancias extraordinarias las que justifican una solicitud expresa de los datos PNR, que habrán de ser transmitidos de modo inmediato por los sujetos obligados a fin de lograr la adecuada prevención, detección, investigación o enjuiciamiento de los delitos enumerados en el Anexo II de la Directiva.

Sin embargo, el Anteproyecto introduce una sensible modificación respecto del régimen de la Directiva, por cuanto no sólo se prevé, aunque dada la redacción del precepto un tanto implícita, la solicitud de los datos por la UIP, y la obligación de su transmisión inmediata, sino que se establece que los sujetos obligados permitirán el acceso por la Unidad a los datos PNR de que se trate.

Como es suficientemente conocido, una de las cuestiones que mayores debates ha planteado en relación con el posible uso y acceso a los datos PNR a lo largo de los últimos quince años ha sido la referida al sistema de acceso a la información. En relación con esta cuestión señala el considerando 16 de la Directiva PNR que “En la actualidad se dispone de dos métodos de transferencia de datos: el método de extracción, en el que las autoridades competentes del Estado miembro que solicita los datos PNR pueden acceder al



sistema de reserva de la compañía aérea y obtener («extraer») una copia de los datos PNR deseados, y el método de transmisión, en el que las compañías aéreas envían («transmiten») los datos PNR a la autoridad solicitante, lo que permite a las compañías aéreas mantener el control de los datos suministrados», concluyendo inequívocamente que “Se considera que el «método de transmisión» ofrece un nivel mayor de protección de los datos y que debe ser obligatorio para todas las compañías aéreas”.

Sin embargo, a través de la previsión a la que acaba de hacerse referencia, el Anteproyecto prevé la posibilidad de acudir al sistema de extracción por parte de la UIP en determinadas circunstancias, lo que resulta contrario a la propia norma de derecho de la Unión que, como se ha indicado, prevé que el método de acceso a los datos PNR deberá ser siempre el de transmisión. De este modo, la citada previsión resulta contraria a la Directiva PNR.

Por ello, **procedería suprimir el inciso “o permitirán su acceso a los datos PNR de que se trate,” del artículo 7.5 del Anteproyecto.**

VII

El artículo 8 del Anteproyecto tiene por finalidad esencial la trasposición de lo previsto en el artículo 6 de la Directiva PNR, si bien las previsiones de dicho precepto son igualmente tenidas en cuenta por el artículo 6 del Anteproyecto, referido a la propia UIP, tal y como se ha indicado anteriormente. En este sentido, sería aconsejable que las disposiciones de trasposición del artículo 6 se unificasen en un solo precepto del Anteproyecto por motivos de sistemática.

Dentro de las previsiones del artículo 6, y aparte de las observaciones que podrían ser consecuencia de consideraciones ya efectuadas con anterioridad, tales como la referencia a las personas que se hallen a bordo de la aeronave dentro del colectivo del que se tomarán los datos, cabe efectuar dos consideraciones de distinta relevancia.

1) En primer lugar, el apartado 2 b) indica que la UIP tratará los datos para “Responder en cada caso particular a las peticiones de las autoridades competentes, debidamente motivadas y con suficiente base, así como facilitar a dichas autoridades los datos PNR solicitados o los resultados de su tratamiento o ambas cosas”.

Esta previsión deriva del artículo 6.6 de la Directiva PNR, a cuyo tenor “La UIP de un Estado miembro transmitirá los datos PNR de las personas identificadas con arreglo al apartado 2, letra a), o los resultados del tratamiento de esos datos PNR a las autoridades competentes pertinentes a que hace referencia el artículo 7 del mismo Estado miembro para su ulterior examen.



Dicha transmisión solo se llevará a cabo tras un análisis de cada caso y, en caso de tratamiento automatizado de los datos PNR, tras una revisión individualizada por medios no automatizados”.

Al propio tiempo, el artículo 9.2 del Anteproyecto prevé que “Las peticiones de datos realizadas por las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas”.

Finalmente, el artículo 8.4 del Anteproyecto, en relación con el artículo 6.5 de la Directiva PNR dispone que “Todo resultado positivo que arroje el tratamiento automatizado de los datos PNR, con arreglo al apartado 2.a), se revisará individualmente por la Unidad de Información sobre Pasajeros a través de medios no automatizados, con el fin de comprobar la necesidad de que las autoridades competentes realicen un examen ulterior o emprendan las acciones o inicien los procedimientos oportunos”.

Tomando en cuenta las previsiones que acaban de reproducirse, sería conveniente que el artículo 8.2 b) del Anteproyecto recogiese en su texto las cautelas derivadas de los mismos, clarificando que las cesiones de datos a las autoridades competentes lo serán tras una revisión individualizada y no automatizada de los resultados y que las transmisiones en ningún caso serán masivas.

Ciertamente se puede argumentar que tales cautelas aparecen recogidas en otros lugares del texto sometido a informe. Sin embargo, como ya se ha indicado anteriormente la propia Directiva PNR se refiere a estas cuestiones en distintos lugares de su articulado. Además, no debe olvidarse que la obligación de realizar un análisis individualizado y por medios no automatizados se impone por la Directiva PNR a las UIP, por lo que es en el precepto referido a las mismas donde debería incluirse esta circunstancia. Es decir, sería preciso que el Anteproyecto complementase la cautela establecida en el apartado 4 del artículo 8 con una expresa referencia en el apartado 2 b) a la existencia del análisis individualizado, en los mismos términos en que se recoge en los apartados 5 y 6 de la Directiva PNR.

En consecuencia, **sería preciso incluir en el artículo 8.2 b) del Anteproyecto una remisión a la exigencia del análisis individualizado y no automatizado previsto en el artículo 8.4 como requisito previo a la remisión de los datos que se prevé en aquél.**

2) Por otra parte, el artículo 8.3 a) del Anteproyecto sometido a informe dispone que “Al realizar la evaluación a que se refiere el apartado 2.a), la Unidad de Información sobre Pasajeros someterá los datos PNR a las siguientes operaciones: a) Comparará los datos PNR con todos los ficheros

disponibles a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves”.

Este precepto parece trasponer al derecho interno lo previsto en el artículo 6.3 a) de la Directiva PNR, a cuyo tenor “Al realizar la evaluación a que se refiere el artículo 2, letra a), la UIP podrá: a) comparar los datos PNR con las bases de datos pertinentes a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, incluidas las bases de datos sobre personas u objetos buscados o bajo alerta, de acuerdo con las normas de la Unión, internacionales y nacionales aplicables a dichas bases de datos”.

No obstante, se aprecia una diferencia sustancial entre ambos textos, dado que mientras la Directiva habilita el acceso y cotejo de los datos con las bases de datos “las bases de datos pertinentes” a los efectos previstos en la propia Directiva, el Anteproyecto modifica la expresión, refiriéndose a “todos los ficheros disponibles” a tales efectos.

Como cuestión previa, debe clarificarse que el concepto de fichero se encuentra en la actualidad superado a los efectos de la aplicación de la normativa de protección de datos, toda vez que la misma es aplicable a cualquier tratamiento total o parcialmente automatizado, quedando en la práctica el concepto de fichero limitado a los de carácter no automatizado, con los que probablemente no vaya a tener lugar el cotejo al que se está haciendo referencia. Por ello, resulta de una mayor propiedad desde el punto de vista técnico hacer referencia a “bases de datos” y no a “ficheros”.

Pero aún más relevante es la segunda modificación introducida, dado que frente al acceso a las bases pertinentes el Anteproyecto prevé el acceso a todas las bases disponibles, siendo así que este concepto es enormemente más amplio que el previsto en la Directiva PNR.

La noción de pertinencia se vincula claramente al principio de proporcionalidad, limitando el acceso a lo que sea “adecuado, pertinente y no excesivo” para el cumplimiento de la finalidad perseguida por el tratamiento, tal y como establece el artículo 4.1 c) de la Directiva 2016/680. Por el contrario, el concepto de disponibilidad hace caso omiso de la aplicación de la citada regla de proporcionalidad, refiriéndose a la posibilidad de acceso a cuanta información pueda hallarse a disposición de la UIP, sin aplicar el test de proporcionalidad exigido por la Directiva PNR. Ello se agrava aún más cuando no sólo se hace referencia a la información disponible, sino que a ello se le añade el adverbio “toda”.

Debe además tenerse en cuenta lo ya señalado en un lugar anterior en relación con el encuadramiento orgánico de la UIP que lleva a cabo el Anteproyecto, dado que al encontrarse dicha unidad en el CITCO y ejercer éste



las funciones que ya se han reproducido en un lugar anterior, el alcance de la disponibilidad que se prevé en el Anteproyecto se incrementa exponencialmente. De este modo, si por una parte la dependencia orgánica de la UIP hace que la misma pierda el carácter de estanqueidad pretendido por la Directiva PNR y por otra se incrementa la posibilidad de acceso a bases de datos “disponibles” y no solamente “pertinentes” se altera sustancialmente la finalidad perseguida por la Directiva, que pretende conciliar la actividad de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y delitos graves con las mayores garantías de protección del derecho a la protección de datos de los pasajeros, teniendo en cuenta que, como se indica al comienzo de este informe, el tratamiento descrito en la Directiva supone necesariamente una injerencia en este derecho fundamental.

Por este motivo, **se considera imprescindible la modificación del artículo 8.3 a) del Anteproyecto, reemplazando la expresión “todos los ficheros disponibles” por “las bases de datos pertinentes”.**

VIII

Dentro de las disposiciones del artículo 8 del Anteproyecto debe ahora llamarse la atención sobre el último inciso del apartado 5, que establece, en términos similares a los establecidos en el artículo 6.7 de la Directiva PNR que el responsable de protección de datos de la UIP podrá remitir, si lo estima oportuno, las cuestiones de que tuviera conocimiento, relacionadas con un tratamiento ilícito de los datos PNR “a la Autoridad nacional de Control”.

Nada cabe objetar al tenor del precepto, si bien es preciso valorar si la la referencia final debería hacerse, de forma abstracta a la autoridad nacional de control o a esta Agencia Española de Protección de Datos.

En este sentido, la disposición adicional primera del Anteproyecto sometido a informe establece lo siguiente:

“Se designa como Autoridad Nacional de Control a la Agencia Española de Protección de Datos, y como tal le corresponderá realizar las siguientes funciones:

a) Asesorar, previa solicitud, a cualquier interesado en el ejercicio de los derechos establecidos en esta ley

b) Conocer de las reclamaciones presentadas contra los tratamientos realizados al amparo de esta ley y dar respuesta a las mismas en un plazo de tiempo razonable.

c) Verificar la legalidad de los tratamientos, por propia iniciativa o como consecuencia de una reclamación, para lo cual podrá realizar



investigaciones, inspecciones y auditorías, de acuerdo con lo dispuesto en su normativa reguladora.”

Por su parte, la referencia a la Autoridad Nacional de Control aparece recogida, además de en el citado artículo 8.5, en los apartados 2, 4 y 5 del artículo 14, referido a la protección de datos de carácter personal, y cuyo análisis se desarrollará en un lugar posterior de este informe.

Pues bien, siendo inequívoca la designación de la Agencia Española de Protección de Datos como autoridad nacional de control a los efectos del Anteproyecto sería necesario que las referencias que los artículos 8 y 14 del mismo se realizan de dicha autoridad nacional lo fueran de la propia Agencia, que será quien ostente esa condición, reemplazando la expresión “autoridad nacional de control” por “Agencia Española de Protección de Datos”.

Podría plantearse que ello plantearía ciertos problemas de denominación en la norma que traspusiera al derecho español el artículo 15 de la Directiva PNR, lo que el Anteproyecto lleva a cabo mediante la disposición adicional primera.

Sin embargo, a nuestro juicio, y siguiendo la propia estructura de la Directiva sería coherente que dicha trasposición se llevase a cabo en el articulado de la norma y no en una disposición adicional. Del mismo modo, nada impediría que la redacción de dicho artículo, que debería ser el siguiente al artículo 14, mantuviese una estructura parcialmente similar a la de la disposición adicional primera.

En este sentido, debe tenerse en cuenta que la Agencia Española de Protección de Datos no sólo tiene la condición de autoridad nacional de control a los efectos de la Directiva PNR, sino también a los previstos en el Reglamento 2016/679 y en la Directiva 2016/680, siendo dichas disposiciones aplicables, respectivamente, a los sujetos obligados y a la UIP y las autoridades competentes.

De este modo, la norma que regulase las competencias de la Agencia a los efectos de la trasposición de la Directiva PNR debería reconocer las citadas competencias, recogiendo posteriormente las que a las autoridades nacionales de control atribuye el artículo 15 de la Directiva PNR.

Por este motivo, se considera que procedería introducir un nuevo artículo, que se numeraría entre los artículos 14 y 15 del Anteproyecto, con el siguiente tenor:

“Artículo 14 bis. Competencias de la Agencia Española de Protección de Datos.



Además, de las competencias que le otorga su normativa específica, la Agencia Española de Protección de Datos, en su condición de autoridad nacional de control a los efectos previstos en la presente Ley Orgánica ejercerá las siguientes:

- a) Asesorar, previa solicitud, a cualquier interesado en el ejercicio de los derechos establecidos en esta ley
- b) Conocer de las reclamaciones presentadas contra los tratamientos realizados al amparo de esta ley y dar respuesta a las mismas en un plazo de tiempo razonable.
- c) Verificar la legalidad de los tratamientos, por propia iniciativa o como consecuencia de una reclamación, para lo cual podrá realizar investigaciones, inspecciones y auditorías, de acuerdo con lo dispuesto en su normativa reguladora.”

IX

EL artículo 9 del Anteproyecto se refiere a las autoridades competentes, siguiendo lo establecido en el artículo 7 de la Directiva PNR. A tal efecto, el apartado 1 enumera dichas autoridades, el apartado segundo se refiere a los requisitos de las solicitudes que deberán dirigirse a la UIP, el artículo 4 limita las finalidades del tratamiento de los datos y el apartado 5 se refiere al derecho del interesado en relación con las decisiones automatizadas adoptadas por las autoridades competentes.

En relación con este punto, debe hacerse referencia al apartado 2 del artículo 9, a cuyo tenor “Las peticiones de datos realizadas por las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas”.

Ya se ha indicado en un lugar anterior que la sistemática de la Directiva PNR bica este precepto entre las obligaciones de las UIP, que no deben aceptar solicitudes masivas de datos y que deben valorar la fundamentación de las que se le dirijan. El Anteproyecto, por el contrario, ubica estas previsiones en el artículo dedicado a las autoridades competentes.

La cuestión que no obstante debería plantearse, a la luz de la doctrina del Tribunal de Justicia de la Unión Europea en las sentencias recaídas en los asuntos Digital Rights Ireland y Tele2 Sverige es la de si los únicos requisitos formales que han de exigirse a las solicitudes son los de que las mismas sean “debidamente motivadas y con suficiente base” o si sería necesaria la existencia de algún tipo de exigencia formal adicional.



A tal efecto, no debe olvidarse que, como se viene indicando a lo largo de este informe, y se desprende de la jurisprudencia que se acaba de mencionar, el tratamiento llevado a cabo por la UIP, que recogerá la información de todos los vuelos internacionales así como de determinados vuelos nacionales que se establezcan supone, una clara intromisión en los derechos fundamentales de los pasajeros y tripulantes a los que los datos se refieren y, particularmente, de su derecho fundamental a la protección de datos de carácter personal.

Evidentemente nada cabe objetar de las solicitudes que se lleven a cabo por la autoridad judicial o por el Ministerio Fiscal, amparadas actualmente en el artículo 11.2 d) de la Ley Orgánica 15/1999 y en el nuevo marco normativo en la obligación legal a la que se refiere el artículo 6.1 c) del Reglamento 2016/679.

La cuestión se plantea en los restantes supuestos, en que sería precisa la existencia de algún tipo de requerimiento adicional previo al acceso a los datos.

Así, esta Agencia, en lo que se refiere a las Fuerzas y Cuerpos de Seguridad, tanto estatales como autonómicos, ha venido señalando que podría ser posible sin necesidad de autorización judicial expresa el acceso a los datos de carácter personal que resulte necesario para el desempeño por los mismos de sus funciones de policía judicial, siempre y cuando se cumplan una serie de requisitos que reiteradamente se han venido señalando, entre los que resulta esencial la comunicación posterior de los datos a los órganos judiciales o al Ministerio Fiscal.

Teniendo en cuenta lo antedicho, **debería plantearse si no sería necesario el establecimiento de algún requisito adicional para que pueda llevarse a cabo una solicitud de datos PNR por las Fuerzas y Cuerpos de Seguridad.**

Por otra parte, el apartado 5 del artículo 9 establece en su primer párrafo que “Las decisiones de las autoridades competentes que produzca efectos jurídicos adversos para una persona o que la afecte significativamente no se adoptarán únicamente en razón del tratamiento automatizado de los datos PNR”.

Se traspone así lo dispuesto en el primer inciso del artículo 7.6 de la Directiva PNR, a cuyo tenor “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”.

Si bien ambos preceptos pueden ser interpretados de un modo similar, ciertamente la redacción del contenido en el Anteproyecto podrá resultar más confusa, dado que al tomar como sujeto a las decisiones de las autoridades y no a las propias autoridades parece reconocer la existencia, como punto de partida, de decisiones negativas, aun cuando no sean automáticas. Por este motivo, **podría considerarse deseable el establecimiento de una redacción más cercana en su estructura a la del primer inciso del artículo 7.5 de la Directiva.**

X

Aun cuando ello suponga no seguir estrictamente la sistemática del Anteproyecto sometido a informe, procede ahora entrar en el estudio del artículo 13 del mismo, referido a la conservación de los datos y su despersonalización, a fin de trasponer al derecho español lo previsto en el artículo 12 de la Directiva PNR.

Con carácter general, el precepto mantiene la sistemática del citado artículo 12 de la Directiva, reproduciendo los plazos de conservación y enmascaramiento que la misma prevé, así como las reglas para la suspensión permanente de los datos y de los resultados de su tratamiento previstos en los apartados 4 y 5 del citado precepto.

No obstante, como primera cuestión a tener en cuenta sería preciso introducir ciertas mejoras técnicas en el apartado 2 del artículo 13, referido a la despersonalización por enmascaramiento de los datos.

Ciertamente, el precepto reproduce el tenor del artículo 12.2 de la Directiva. Sin embargo la misma introduce un concepto de la despersonalización en su artículo 1.10 que, por el contrario, no incluye el precepto. Dado que el citado término es desconocido en nuestro derecho, sería conveniente, aun no incluyendo en el Anteproyecto un artículo de definiciones, incorporar ese concepto en el propio artículo 13.2.

Por otra parte, debe recordarse que el sistema no sólo incorporará los datos PNR de los pasajeros, sino también la información API de los tripulantes y, si procediera, tal y como ya se analizó, de terceras personas. Por este motivo sería conveniente hacer referencia a los afectados y no a los pasajeros, a fin de englobar todos los sujetos a los que la información puede referirse.

De este modo, se propone dar al artículo 13.2 la siguiente redacción:

“Transcurrido un plazo de seis meses desde su recepción, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento, **de manera que resulten invisibles para un usuario**, de los siguientes



elementos que podrían servir para identificar directamente a **los afectados.**”

Por otra parte, dado el carácter taxativo de los elementos que habrán de ser objeto de enmascaramiento, **debería ajustarse la redacción del artículo 13.2 a) al tenor de la Directiva PNR, haciendo referencia a “los nombres y apellidos, incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas”.**

EL precepto que plantea una mayor complejidad dentro del artículo 13 del Anteproyecto es el incluido en su apartado 3, referido a los supuestos en que será posible la transmisión de datos sometidos previamente al procedimiento de despersonalización por enmascaramiento.

Tras indicarse en la letra a) del precepto que será posible dicha transmisión cuando, en primer lugar, el supuesto se encuentre amparado por el artículo 8.2 b) del Anteproyecto, lo que resulta coincidente con el artículo 6.2 b) de la Directiva PNR, el Anteproyecto añade que será igualmente necesario que la transmisión “Haya sido aprobada por una autoridad judicial o por el responsable del tratamiento de los datos”, si bien “En este último caso, se informará al responsable de la protección de datos de la Unidad de Información sobre Pasajeros, quien podrá llevar a cabo una revisión posterior de dicha transmisión”.

EL artículo 12.3 b) de la Directiva PNR, en relación con este segundo requisito para la transmisión de los datos, la supedita a que “haya sido aprobado por: i) una autoridad judicial, u ii) otra autoridad nacional competente para verificar si se cumplen las condiciones para la divulgación conforme al derecho nacional, con sujeción a la información y revisión *a posteriori* del responsable de la protección de datos de la UIP”.

Como puede comprobarse, la trasposición que de dicho precepto realiza el Anteproyecto sometido a informe genera la necesaria conclusión de que la “responsable del tratamiento de los datos”; es decir, en los términos actualmente previsto el CITCO y en los propuestos por esta Agencia la UIP, tendrá la condición de “autoridad nacional competente para verificar si se cumplen las condiciones para la divulgación”.

Quiere ello decir que el Anteproyecto toma en consideración un sistema en que sería la propia Unidad de Información sobre Pasajeros la que determinaría, por sí sola, si no existiese autorización judicial, la procedencia o improcedencia de acceder a los solicitado, no actuando solamente como tenedora y suministradora de los datos, sino como órgano administrativo competente para supervisar la validez de las solicitudes que le sean formuladas.



En este sentido, debe traerse nuevamente a colación lo señalado en el apartado IX de este informe, toda vez que dentro de las funciones establecidas en la Directiva en ningún momento se otorga a las UIP la capacidad de resolver por sí solas acerca de las solicitudes a menos que las mismas no cumplan con los requisitos legalmente exigidos, lo que incluiría la autorización judicial o administrativa pertinente, pero no la competencia para actuar como autoridad administrativa que autoriza el acceso a los datos.

Por este motivo, y tal como se indicaba en el apartado IX de este informe **debería analizarse si existirá otra autoridad distinta de la judicial que pueda autorizar el acceso en estos supuestos, siendo claro que la misma no podría ser la propia UIP, lo que exige o bien la supresión del artículo 13.3 b) del Anteproyecto en su totalidad o bien únicamente la de su primer inciso, en caso de que pueda determinarse otra autoridad distinta de la judicial y la UIP “responsable del tratamiento de los datos”.**

XI

Los artículos 10 a 12 del Anteproyecto se refieren al intercambio de información PNR con otros Estados Miembros, así como su transmisión a EUROPOL y a terceros Estados, resultando en gran medida ajustadas a las previsiones de los artículos 9 a 11 de la Directiva PNR, lo que permite su estudio conjunto en el presente informe. No obstante, es preciso efectuar las siguientes consideraciones:

Ante todo, y en relación con lo señalado en el artículo 10.4 del Proyecto, referido a la comunicación a otras UIP de Estados Miembros de datos sometidos a la previa despersonalización por enmascaramiento, es preciso reiterar lo que acaba de señalarse en el apartado anterior de este informe, en el sentido de que la decisión acerca de la procedencia del acceso no debe quedar en manos de la propia UIP responsable del tratamiento ni, en los términos en que aparece ahora recogido en el texto, en manos del CITCO.

En segundo lugar, en cuanto al acceso por la UIP española a los datos recopilados por las Unidades de otros Estados Miembros, el artículo 10.2 dispone que “La Unidad de Información sobre Pasajeros española solicitará, en cada caso concreto, para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves, a la Unidad de Información sobre Pasajeros de cualquier otro Estado miembro que le suministre los datos PNR almacenados en su base de datos, así como, si fuera necesario, el resultado de cualquier tratamiento de los mismos. La solicitud deberá ser debidamente motivada”.

En relación con este punto, el artículo 9.2 de la Directiva PNR dispone en su inciso primero que “La UIP de un Estado miembro tendrá derecho a solicitar, en caso necesario, a la UIP de cualquier otro Estado miembro que le

suministre los datos PNR almacenados en la base de datos de esta última y que aún no hayan sido despersonalizados mediante enmascaramiento de elementos de los datos, de conformidad con el artículo 12, apartado 2, así como, si fuera necesario, el resultado de cualquier tratamiento de los mismos, si este ya se hubiera realizado de conformidad con el artículo 6, apartado 2, letra a)”

De este modo, sería preciso clarificar en el artículo 10.2 que el acceso podrá tener lugar en relación con los datos que no hayan sido sometidos a un previo proceso de despersonalización, debiendo estar a su derecho interno para el acceso a aquéllos que ya lo hubieran sido, del mismo modo que se exige para terceros Estados que soliciten el acceso a los datos PNR de la UIP española.

Por ello, sería en primer lugar preciso modificar el apartado resultando el siguiente tenor:

“La Unidad de Información sobre Pasajeros española solicitará, en cada caso concreto, para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves, a la Unidad de Información sobre Pasajeros de cualquier otro Estado miembro que le suministre los datos PNR almacenados en su base de datos **y que no hayan sido despersonalizados mediante enmascaramiento**, así como, si fuera necesario, el resultado de cualquier tratamiento de los mismos. La solicitud deberá ser debidamente motivada”.

Además, habría de añadirse un segundo párrafo que indique lo siguiente:

“En el caso de que los datos a los que se pretenda acceder hayan sido despersonalizados mediante enmascaramiento el acceso podrá tener lugar de conformidad con el derecho nacional aplicable en el Estado de la Unidad de Información sobre Pasajeros requerida.”

En tercer lugar, en relación con el artículo 11, **sería conveniente clarificar en su primer párrafo que la motivación de la solicitud de EUROPOL debería referirse a las causas que justifican la necesidad de la comunicación para apoyar y reforzar la acción de un Estado Miembro**, en los términos que aparecen ya previsto en este párrafo.

Dentro de este mismo artículo, el párrafo segundo dispone que “la Unidad de Información sobre Pasajeros española podrá trasladar a Europol las demandas de información relacionadas con datos PNR que estime oportuno, así como las procedentes de las autoridades competentes”.



La citada disposición no trae causa de ningún precepto de la Directiva PNR, no quedando claro su significado, toda vez que las funciones de EUROPOL desde el punto de vista de la aplicación de la citada Directiva quedan limitadas a las establecidas en los apartados 1 y 2 del artículo 10 y se refieren a la posibilidad de solicitud de datos por parte de EUROPOL a las UIP de los Estados Miembros, sin que se establezca un procedimiento de remisión, obligatoria o voluntaria a EUROPOL ni de las solicitudes efectuadas por un Estado a la UIP de otro ni, aún en menor medida, las solicitudes de transmisión realizadas por las autoridades competentes del propio Estado miembro de la UIP.

De este modo, parece que el precepto se referiría a un supuesto en que la UIP aprecia la relevancia de la solicitud de información a efectos de la aplicación de la normativa de funcionamiento de EUROPOL o para el cumplimiento de los fines propios de EUROPOL. Sin embargo, ninguna de estas clarificaciones se lleva a cabo por el artículo 11 del Anteproyecto.

Por todo ello sería preciso que se clarificase el párrafo segundo del artículo 11 del Anteproyecto especificando las finalidades que justificarían esta transmisión de información relativa a las solicitudes, que podría llevarse a cabo cuando fuera necesario para el cumplimiento de las funciones de EUROPOL previstas en el artículo 4 del Reglamento 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016.

XII

El artículo 14 del Anteproyecto incorpora al derecho español las normas de protección de datos previstas en el artículo 13 de la Directiva PNR, reproduciendo en gran medida lo dispuesto en la Directiva.

Como primera cuestión a tomar en consideración, debe recordarse lo indicado en el apartado VIII de este informe tanto en lo referente a la referencia expresa de esta Agencia como autoridad de control como en la inclusión de un nuevo artículo (provisionalmente el 14 bis) referido a las funciones de la Agencia.

Dicho lo anterior, la única cuestión que debe analizarse en relación con el artículo 14 es la referente al régimen normativo que será de aplicación supletoria a las disposiciones del Anteproyecto. A estos efectos, como ya se indicó, y dentro del nuevo marco europeo en materia de protección de datos de carácter personal, debe diferenciarse entre el régimen aplicable a los sujetos obligados, sometidos al Reglamento 2016/679, y el que será de aplicación a la UIP y a las autoridades competentes, sometidas dentro de este nuevo marco a la Directiva 2016/680 en cuanto a los tratamientos llevados a cabo para la prevención, detección, investigación y enjuiciamiento de infracciones penales.



El problema se plantea por el hecho de que mientras el Reglamento 2016/679 será de aplicación directa en nuestro país en el momento en que sea de plena aplicación conforme a su artículo 99.2, es decir, el 25 de mayo de 2018, la Directiva exigirá una norma de trasposición a nuestro derecho, siendo así que en el presente momento no existe Anteproyecto alguno de trasposición de la Directiva 2016/680 al derecho interno.

Al propio tiempo, debe recordarse que se encuentra actualmente en tramitación en las Cortes generales el Proyecto de Ley Orgánica de Protección de Datos de carácter personal, que tiene por objeto no la adaptación del Reglamento 2016/679 al derecho interno, dado que dicha norma es de aplicación directa, sino la adaptación del derecho interno al propio Reglamento.

Atendida la situación actual en que, como se ha indicado, no se ha iniciado la tramitación de disposición alguna de trasposición al derecho interno de la Directiva 2016/680, la disposición transitoria cuarta del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal establece que “Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva”.

Todo lo que ha venido indicándose afecta particularmente al apartado 1 del artículo 14 ahora analizado, que establece el régimen supletorio del Anteproyecto, estableciendo lo siguiente:

“Todos los tratamientos de datos de carácter personal que realicen en aplicación de esta ley la Unidad de Información sobre Pasajeros y las autoridades competentes referidas en el artículo 9 se regirán supletoriamente por la legislación que trasponga la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016.



No obstante, los tratamientos de datos de carácter personal realizados por los sujetos obligados referidos en el artículo 4 se registrarán, sin perjuicio de las obligaciones previstas en esta ley, por el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y por la legislación que lo adapta a nuestro ordenamiento jurídico.”

A nuestro juicio este apartado ha de ser objeto de una profunda modificación a fin de ajustar su régimen al que podría estar vigente en el momento en que entrase en vigor el Anteproyecto de Ley Orgánica sometida a informe en que, probablemente y dado el estado de tramitación de las normas a las que se ha hecho referencia, es posible que se encontrase en vigor la Ley Orgánica que adapta el derecho español al Reglamento 2016/679, pero probablemente no se haya aprobado aún la norma de trasposición de la Directiva 2016/680, lo que supondrá la aplicación, al menos transitoriamente, de las disposiciones actualmente vigentes en materia de protección de datos.

Por ello, si bien es posible establecer una regla clara de supletoriedad para los tratamientos llevados a cabo por los sujetos obligados deberá establecerse una previsión más general para los efectuados por la UIP y las autoridades competentes.

Al propio tiempo, carece de sentido el uso de la expresión “no obstante” al comienzo del párrafo referido a los sujetos obligados, dado que no se trata del establecimiento de una excepción al régimen de los sometidos a la Directiva 2016/680, sino de la aplicación a dichos sujetos de un régimen enteramente distinto.

Por todo ello se considera que, siguiendo la estructura de la propia Directiva PNR el apartado 1 del artículo 14 debería configurarse como precepto separado, referido al régimen supletorio de la Ley Orgánica y desdoblarse en dos, proponiéndose la siguiente redacción para los mismos:

“Artículo 14 ter. Derecho aplicable.

1. Los tratamientos de datos de carácter personal que lleven a cabo en aplicación de esta ley la Unidad de Información sobre Pasajeros y las autoridades competentes referidas en el artículo 9 se registrarán por la presente Ley Orgánica y supletoriamente por las normas que regulen en derecho español el tratamiento de datos por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.



2. Sin perjuicio de las obligaciones establecidas en esta Ley Orgánica, los tratamientos de datos de carácter personal realizados por los sujetos obligados referidos en el artículo 4 se registrarán **por lo dispuesto en** el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y por la legislación que **adapta el** ordenamiento jurídico **español a dicho Reglamento.**”

XIII

Resta por último hacer referencia al régimen sancionador regulado en el Capítulo III del Anteproyecto sometido a informe en desarrollo del artículo 14 de la Directiva PNR.

En relación con este punto, debe tenerse en cuenta que el citado precepto prevé que “Los Estados miembros establecerán el régimen de sanciones aplicables a los incumplimientos de las disposiciones nacionales adoptadas en aplicación de la presente Directiva y adoptarán toda medida necesaria para garantizar la aplicación de estas”, añadiendo que “En particular, los Estados miembros establecerán sanciones, incluidas las pecuniarias, contra las compañías aéreas que no transmitan datos con arreglo a lo establecido en el artículo 8, o no lo hagan en el formato exigido”. En todo caso “Dichas sanciones deberán ser efectivas, proporcionadas y disuasorias.

Los artículos 18 a 20 tipifican las posibles infracciones por los sujetos obligados de las disposiciones del Anteproyecto, incorporando algunas conductas que simultáneamente implicarán una infracción de las disposiciones generales de protección de datos que les son de aplicación conjuntamente con las establecidas en el texto sometido a informe.

Así, el artículo 19 tipifica como graves las infracciones consistentes en “la transmisión de datos inexactos” (apartado e) o “La falta de diligencia en el mantenimiento de los sistemas electrónicos seguros de transmisión de los datos PNR y de acceso a los mismos, o la no disponibilidad de medios alternativos seguros de transmisión o acceso al principal” (apartado g).

Igualmente, será infracción leve conforme al artículo 20 a) “El incumplimiento de la obligación de informar a los pasajeros y a los miembros de la tripulación de que sus datos serán tratados y enviados a la Unidad de Información sobre Pasajeros”.



Al propio tiempo, el artículo 16 establece un régimen aplicable a los supuestos en que unos mismos hechos puedan “ser calificados con arreglo a dos o más preceptos de esta u otra ley”, estableciendo como primer criterio de aplicación el principio de especialidad, lo que supondría en la práctica la aplicación en todo caso de la norma sometida a informe.

Pues bien, frente al citado criterio, debe recordarse que el Reglamento 2016/679 establece un régimen sancionador claramente más disuasorio que el establecido en el Anteproyecto sometido a informe, por cuanto las infracciones tipificadas en los artículos 19 e) y 20 a) podrán ser sancionadas con multa “de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía”, conforme al artículo 83.5 del Reglamento, y la tipificada en el artículo 19 g) podrá serlo, en caso de falta de adopción de las correspondientes medidas técnicas y organizativas para garantizar la integridad, confidencialidad y disponibilidad de la información con multa “de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía”.

Además, en muchos supuestos, las tres vulneraciones mencionadas pueden encontrarse subsumidas en las correspondientes conductas infractoras del Reglamento por falta de garantía de la exactitud de los datos, falta de implantación de medidas de seguridad o incumplimiento de la obligación de información al interesado.

Sin embargo, el artículo 21 del Anteproyecto establece para las infracciones graves una multa de 20.001 a 60.000 euros y para las leves, entre las que, como se ha indicado se encontraría la vulneración de uno de los derechos esenciales establecidos en la normativa de protección de datos, cual es el derecho del afectado a ser informado del tratamiento, de 3.000 a 20.000 euros.

Como se ha indicado, sin embargo, del primero de los criterios mencionados en el artículo 16.1 del Anteproyecto se desprendería que el régimen sancionador aplicable no sería el correspondiente a la sanción más grave, sino el establecido en la norma especial; es decir, la ahora informada.

Esta circunstancia se agrava si además se tiene en cuenta que el artículo 23 establece una competencia para la imposición de sanciones que no corresponderá a esta Agencia Española de Protección de Datos, sino a los correspondientes órganos del Ministerio del Interior.



Con todo ello se genera una situación completamente anómala en la que, por una parte, órganos distintos de esta Agencia conocerán de las infracciones de la normativa de protección de datos y por otra impondrán sanciones cuyos límites cuantitativos son enormemente distintos de los propios de la legislación de protección de datos.

Todo ello genera, como se dijo, una situación completamente anómala en la que determinados responsables del tratamiento quedarían excluidos de la competencia de esta Agencia y sujetos a un régimen sancionados mucho más benévolo en atención a la aplicación del principio de especialidad al que se refiere el artículo 16.1 a) del Anteproyecto, lo que mal se compadece con la adecuada garantía de los derechos fundamentales por parte de esas compañías beneficiadas como consecuencia de esta regulación especial, además de generar una situación discriminatoria en perjuicio de quienes, precisamente, no están sujetos a las obligaciones adicionales establecidas en el Anteproyecto..

De este modo **resulta en todo punto necesario que se modifique el régimen sancionador del Anteproyecto en los siguientes términos:**

- **Se supriman el inciso “así como la transmisión de datos inexactos” del apartado e) del artículo 19, así como el apartado a) del artículo 20 en su integridad.**
- **Se modifique el apartado g) del artículo 19 a fin de limitar su alcance a los sistemas de transmisión de datos y en ningún caso a las medidas de seguridad implantadas por los sujetos obligados, estableciendo una salvedad expresa a la posible existencia de una vulneración de la legislación general de protección de datos aplicable a dichos sujetos obligados.**
- **En todo caso se suprima el criterio de especialidad referido en el artículo 16.1 a) o se especifique en dicho artículo que las reglas mencionadas en el mismo no afectarán en ningún caso a la aplicación de las normas sancionadoras que procedan con arreglo a la normativa de protección de datos de carácter personal.**

Solo en caso de aceptarse las tres observaciones mencionadas será posible para esta Agencia Española de Protección de Datos manifestar su conformidad con el régimen de competencias establecido en el artículo 23 del Anteproyecto sometido a informe.



Por otra parte, el artículo 28.1 del Anteproyecto dispone que “Las autoridades y órganos de las distintas administraciones públicas competentes para imponer sanciones de acuerdo con esta ley podrán acceder a los datos relativos a los sujetos infractores que estén directamente relacionados con la investigación de los hechos constitutivos de infracción, sin necesidad de consentimiento previo del titular de los datos, con las garantías de seguridad, integridad y disponibilidad, de conformidad con lo establecido en la normativa reguladora de protección de datos de carácter personal”

A juicio de esta Agencia, y a fin de que la redacción del precepto resulte más acorde con lo establecido en la normativa de protección de datos se propone modificar la redacción de este precepto en los siguientes términos:

“Las autoridades y órganos de las distintas administraciones públicas competentes para imponer **las sanciones previstas en** esta ley podrán acceder **en el ejercicio de dichas competencias** a los datos relativos a los sujetos infractores que estén directamente relacionados con la investigación de los hechos constitutivos de infracción, con las **debidas** garantías de seguridad, integridad y disponibilidad. **El acceso y el tratamiento posterior de los datos se realizarán en todo caso** de conformidad con lo establecido en la normativa reguladora de protección de datos de carácter personal.”

Finalmente, **debe tenerse en cuenta que corresponderá a esta Agencia Española de Protección de Datos el ejercicio de sus potestades en relación con las posibles infracciones de las disposiciones de protección de datos que pudieran cometerse tanto por la UIP como por las autoridades competentes en el tratamiento de los datos de carácter personal a los que se refiere el Anteproyecto sometido a informe, lo que debería constar en el mismo.**