Resolución adoptada por el Defensor del Pueblo (e.f.) el 14 de diciembre de 2020, con motivo de la solicitud de interposición de recurso de inconstitucionalidad contra la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves

(*Boletín Oficial del Estado,* núm. 248, de 17 de septiembre de 2020*)*

ANTECEDENTES

PRIMERO. Mediante escrito recibido en el Registro del Defensor del Pueblo el 5 de octubre de 2020 un ciudadano solicitó recurso de inconstitucionalidad frente a la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves (BOE de 17 de septiembre).

Considera el compareciente, en un breve escrito, que esta Ley Orgánica vulnera el artículo 18 de la Constitución (en lo que se refiere a la intimidad personal y a la protección de datos) por el «exceso, abuso, que supone que se acopian datos para los delitos enumerados en el capítulo (quiere decir artículo) 4; pues ninguno de ellos, con ser graves, deberían conllevar medidas tan extraordinarias como el control (sistemático) de los pasajeros de vuelos». Considera que el principio de «proporcionalidad» no se respeta en esta ley pues, junto a otros delitos, como los de terrorismo, se podría investigar con las medidas establecidas en esta ley otros que considera de «importancia relativa», como la corrupción.

También solicita la interposición de recurso de inconstitucionalidad contra la Orden 1262/2020, de 30 de septiembre, de la Consejería de Sanidad de la Comunidad de Madrid, por la que se adoptan medidas específicas de actuación por razón de salud pública para asegurar el cumplimiento de las obligaciones de aislamiento o cuarentena para la contención de la transmisión del covid-19 en la Comunidad de Madrid (*Boletín Oficial de la Comunidad de Madrid* número 238, de 1 de octubre).

Finalmente, se refiere a una norma de la Junta de Andalucía, que no identifica, relativa a los datos que deben incluirse en la historia clínica de los ciudadanos. Aporta un link de internet que es una breve información institucional de la Junta de Andalucía con el epígrafe «La historia digital de salud incorporará los hábitos de vida de los usuarios. Los profesionales de Atención Primaria podrán añadir información clave para la asistencia a los ciudadanos, como tabaquismo, consumo de alcohol o actividad física». También pide recurso de inconstitucionalidad contra la norma que daría soporte a esta incorporación a la historia digital de salud.

Sobre lo indicado en los dos últimos párrafos no procede pronunciamiento alguno en esta Resolución al no referirse a leyes o normas con rango de Ley, objeto propio del recurso de inconstitucionalidad.

SEGUNDO. La Ley Orgánica 1/2020 traspone a España 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.

Se pretendía —y ahora se implementa en España— que los Estados miembros de la Unión Europea transfiriesen los datos PNR de los vuelos exteriores de la Unión Europea a una Unidad de Información sobre Pasajeros a crear en cada Estado, sin perjuicio de que pueda también aplicarse a los vuelos interiores de la Unión, según el criterio de cada país. Asimismo, la Directiva exige la creación de un sistema uniforme en la Unión Europea para el tratamiento de los datos PNR.

Se trata de facilitar, en el ámbito de toda la Unión, la persecución del terrorismo y de otros delitos que se especifican.

El objeto de la Ley es regular, por un lado, la transferencia de los datos PNR por parte de las compañías aéreas y otras entidades obligadas; en segundo término, la recogida, el tratamiento y la protección de esos datos, su transmisión a las autoridades competentes y el intercambio de dichos datos con otros Estados miembros, Europol y terceros Estados; su vez, la designación de la Unidad de Información sobre Pasajeros española y, por último, el régimen sancionador.

Estos datos solo pueden ser utilizados para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves. Los datos se refieren a los pasajeros de los vuelos internacionales que tengan origen, destino o tránsito en España, tanto de carácter comercial como privados y, si existen indicios suficientes de una contrastada situación de riesgo, se podrán incluir excepcionalmente vuelos nacionales.

Los datos se aportan a la Unidad de Información sobre Pasajeros española (UIP), incardinada en la estructura del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado dependiente de la Secretaría de Estado de Seguridad, Unidad encargada de la recepción y tratamiento de los datos.

Se regula específicamente la figura del responsable de protección de datos, cuyo principal cometido será el de garantizar la rigurosa observancia de la legislación vigente en materia de protección de datos de carácter personal durante todo el proceso de recepción, tratamiento, transmisión, conservación y supresión de los datos PNR.

La transmisión de datos se llevará a cabo utilizando los formatos determinados y los protocolos definidos en la Decisión de Ejecución de la Comisión UE 2017/759, de 28 de abril de 2017, relativa a los protocolos comunes y los formatos de datos que deberán

utilizar las compañías aéreas para la transmisión de los datos PNR a las Unidades de Información sobre Pasajeros.

Los datos serán enviados en dos momentos distintos; el primero entre las 48 y las 24 horas anteriores a la salida programada del vuelo, y el segundo se producirá una vez cerrado el vuelo, es decir, en el momento a partir del cual nadie puede entrar en el avión ni abandonarlo. Si durante el vuelo se produce alguna modificación en el destino, también deberá ser transmitida.

Sin perjuicio de las obligaciones establecidas en esta ley orgánica, los tratamientos de datos de carácter personal realizados por los sujetos obligados se regirán por lo dispuesto en 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 la legislación interna que se dicte en uso de la habilitación contenida en aquel.

En relación con el tratamiento de los datos de carácter personal por parte de las autoridades competentes, estas estarán sujetas al deber de proporcionar o poner a disposición del interesado la información y facilitar el ejercicio de los derechos de estos contemplados en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la ley orgánica que la incorpore a nuestro ordenamiento interno.

Los propósitos del tratamiento de los datos serán evaluar a las personas a bordo de la aeronave a fin de identificar a aquellas que pudieran tener relación con delitos de terrorismo o delitos graves; revisar individualmente los resultados de dicha evaluación previa automatizada; responder peticiones de las autoridades competentes o de Europol y establecer criterios predeterminados a utilizar en esas evaluaciones.

Las autoridades que pueden solicitar o recibir datos PNR o el resultado del tratamiento de dichos datos por la UIP son las Direcciones Generales de la Policía y de la Guardia Civil, el Centro Nacional de Inteligencia, la Dirección Adjunta de Vigilancia Aduanera y el ministerio fiscal. También se contemplan como autoridades competentes las correspondientes de las comunidades autónomas que hayan asumido estatutariamente competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio. Los jueces y tribunales, en garantía del principio de independencia constitucional, se regirán en cuanto a las peticiones de dicha información y a la colaboración con la UIP por lo dispuesto en su legislación específica.

Las peticiones de las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas. Todo tratamiento que lleven a cabo estas autoridades competentes sobre los datos recibidos de la UIP, lo será para los fines propios de la lucha contra los delitos de terrorismo y los delitos graves.

España podrá enviar datos PNR o el resultado de su tratamiento a otros Estados miembros, de oficio o atendiendo una solicitud concreta. Las peticiones entre Estados han de ser motivadas y siempre orientadas al cumplimiento de los fines previstos en la Ley Orgánica 1/2020.

Se contempla la posibilidad de que una autoridad competente española pueda dirigirse directamente a la Unidad de Información sobre Pasajeros de otro Estado miembro para una solicitud de información, siempre que se den conjuntamente las circunstancias de urgencia e imposibilidad de comunicación con la UIP nacional. En todo caso se remitirá copia de la petición a la UIP española.

La transferencia de datos a Europol se llevará a cabo electrónicamente y de forma motivada, siempre que entre dentro del ámbito de sus competencias y sea necesaria para el ejercicio de sus funciones.

Se incluye el procedimiento de transmisión de datos a terceros países. En este intercambio se tendrá que observar lo establecido en la legislación que trasponga 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.

En garantía del derecho a la intimidad de los sujetos afectados y en especial de su derecho a la protección de datos de carácter personal, se contempla que los datos PNR facilitados a la UIP por los sujetos obligados serán conservados durante cinco años a contar desde su transmisión. Una vez transcurridos seis meses desde su recepción, los datos PNR que permitan la identificación directa del pasajero serán despersonalizados mediante enmascaramiento, y solo se permitirá el acceso a la totalidad de los mismos previa aprobación por la autoridad judicial o por la persona titular de la Secretaría de Estado de Seguridad.

Cumplido el plazo de los cinco años serán suprimidos definitivamente, sin perjuicio de su utilización por parte de las autoridades competentes que los hayan recibido y que los estén utilizando en el marco de un asunto concreto a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves.

Además de trasponer la Directiva, la Ley Orgánica 1/2020 introduce algunos aspectos adicionales pero conexos a aquélla: a) deberán enviarse los datos de la tripulación y de cualquier otra persona a bordo; b) prevé la aplicación del régimen jurídico previsto a los vuelos internacionales dentro de la UE y no solo de la UE a terceros países; c) prevé la posibilidad de aplicar el régimen jurídico previsto a los vuelos nacionales y a vuelos privados; d) incluye, como sujetos obligados, a las entidades de gestión de reserva de vuelos.

FUNDAMENTOS JURÍDICOS

PRIMERO. Después de los atentados del 11 de septiembre de 2001 en los Estados Unidos, resultaría anacrónico discutir la necesidad, para una lucha más eficaz contra el terrorismo, de que las autoridades puedan conocer qué personas han abordado un determinado vuelo. Tampoco se puede discutir que ello afecta a la intimidad y a los datos de las personas; de los pasajeros y las tripulaciones. El debate se centra ahora en las garantías que deben rodear ese conocimiento por las autoridades para que la limitación de la intimidad y el acceso a los datos sean respetuosos con el principio de proporcionalidad, que debe regir toda limitación de los derechos fundamentales.

SEGUNDO. La Ley Orgánica 1/2020 cumple una obligación de España como Estado miembro de la Unión Europea al trasponer la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Procede de un Anteproyecto de Ley del Gobierno, versión corregida de uno anterior que, como dice el Dictamen del Consejo de Estado de 13 de septiembre de 2018 es

> un texto totalmente renovado y mejorado con respecto a la versión inicial del Anteproyecto, habiendo tenido en consideración las amplias críticas y observaciones formuladas al texto inicial por las entidades informantes, en especial por el Consejo General del Poder Judicial, por el Consejo Fiscal y por la AEPD.

Como dice también este Dictamen

> desde hace más de 60 años los datos personales de los pasajeros han sido recogidos en registros llevados de forma manual y han sido utilizados por servicios de aduanas, por las autoridades policiales y por las propias compañías aéreas. Los avances tecnológicos han permitido que la recogida y tratamiento automatizado de estos datos se convierta en herramienta eficaz en la lucha contra el terrorismo y otras formas de delincuencia grave. Esto ha puesto de manifiesto la necesidad de crear un marco legal que permita compartir los datos PRN de forma efectiva, garantizando al mismo tiempo los derechos fundamentales y libertades afectados de los pasajeros.

TERCERO. Con respecto a los derechos fundamentales a la intimidad personal y, derivado de éste, a la protección de los datos personales (artículos 18.1 y 18.4 de la Constitución) el Tribunal Constitucional dice que

> el canon de control que debemos aplicar para enjuiciar la constitucionalidad [...] ha de ser integrado a partir, entre otras, de las normas de Derecho de la Unión Europea que protegen los correspondientes derechos fundamentales (STC 26/2014, de 13 de febrero).

La Unión Europea, consciente de la necesidad de luchar de manera efectiva contra el terrorismo y otros delitos graves, y de la necesidad también de acceder a datos personales para hacerlo, dictó a la vez, en 2016, un importante paquete normativo: la

Directiva 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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, RGPD) y 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.

En nuestra jurisprudencia constitucional, el derecho a la intimidad personal implica la existencia de un ámbito propio y reservado a la acción y conocimiento de los demás y confiere a la persona el poder jurídico de imponer el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, 206/2007, de 24 de septiembre, y 70/2009, de 23 de marzo).

El derecho a la protección de los datos personales es el reconocimiento de «un derecho a controlar el uso de los datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención». El derecho a la protección de datos personales incorpora un poder de disposición y control sobre los datos personales, que constituye parte del contenido del derecho fundamental a la protección de datos, y se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Por ello, la recogida y posterior tratamiento de los datos de carácter personal se ha de fundamentar en el consentimiento de su titular, facultad que solo cabe limitar en atención a derechos y bienes de relevancia constitucional, de modo que esa limitación esté justificada, sea proporcionada y, además, se establezca por ley (STC 292/2000, de 30 de noviembre).

Conforme al Tribunal Supremo, es legítima

> aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos (STS 159/2009, de 29 de junio).

CUARTO. El Defensor del Pueblo considera que la Ley Orgánica 1 /2020 se ajusta a la Constitución por las siguientes razones:

a) Es legítimo el acceso a datos de viaje por las autoridades siempre que se persiga un fin legítimo de orden superior, en este caso la lucha contra el terrorismo y otros delitos graves. En particular, ha de hacerse notar que, a diferencia de lo que sostiene el compareciente, la corrupción debe considerarse un delito grave que justifica el acceso a datos de viaje para ser mejor combatida.

b) La intromisión en la intimidad y el acceso a los datos personales no puede ser incondicionada, sino severamente limitada. En este sentido, se trata aquí de la trasposición de una Directiva de la Unión Europea, lo que ha constituido el marco de las posibilidades de actuación del Estado. Por otra parte, cuanto excede en la Ley Orgánica de lo indicado en la Directiva es complementario o permitido por aquella: a) deberán enviarse los datos de la tripulación y de cualquier otra persona a bordo; b) prevé la aplicación del régimen jurídico previsto a los vuelos internacionales dentro de la Unión Europea y no solo de la Unión Europea a terceros países; c) prevé la posibilidad de aplicar el régimen jurídico previsto a los vuelos nacionales y a vuelos privados; d) incluye, como sujetos obligados, a las entidades de gestión de reserva de vuelos. Todo ello mejora la lucha contra delitos graves sin apartarse del espíritu de la directiva y, en el caso de la aplicación a vuelos nacionales, exige el acuerdo *ad casum* del Consejo de Ministros.

c) El principio de proporcionalidad en la intromisión en derechos fundamentales queda salvado por previsiones como las siguientes:

- Los datos solo pueden ser utilizados para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y otros delitos graves.
- Los datos se aportan a una Unidad especializada del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado: Los propósitos del tratamiento de los datos serán evaluar a las personas a bordo de la aeronave a fin de identificar a aquellas que pudieran tener relación con delitos de terrorismo o delitos graves; revisar individualmente los resultados de dicha evaluación previa automatizada; responder peticiones de las autoridades competentes o de Europol y establecer criterios predeterminados a utilizar en esas evaluaciones.
- Se regula específicamente la figura del responsable de protección de datos para velar por los derechos de los ciudadanos durante todo el proceso de recepción, tratamiento, transmisión, conservación y supresión de los datos PNR.
- Está plenamente vigente para estos casos la legislación de protección de datos europea y española: los tratamientos de datos de carácter

personal realizados por los sujetos obligados se regirán por lo dispuesto en 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. En relación con el tratamiento de los datos de carácter personal por parte de las autoridades competentes, estas estarán sujetas al deber de proporcionar o poner a disposición del interesado la información y facilitar el ejercicio de los derechos de estos contemplados en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Se aplica también la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Las peticiones de las autoridades competentes (policiales, CNI, vigilancia aduanera, judicial y Ministerio Fiscal) serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas. Todo tratamiento que lleven a cabo estas autoridades competentes sobre los datos recibidos de la UIP, lo será para los fines propios de la lucha contra los delitos de terrorismo y los demás delitos graves.
- Hay una limitación temporal en la conservación de los datos, contemplándose dos momentos: a los seis meses de la obtención de los datos y a los cinco años.

  Una vez transcurridos seis meses desde su recepción, los datos PNR que permitan la identificación directa del pasajero serán despersonalizados mediante enmascaramiento, y solo se permitirá el acceso a la totalidad de los mismos previa aprobación por la autoridad judicial o por la persona titular de la Secretaria de Estado de Seguridad.

  Cumplido el plazo de cinco años serán suprimidos definitivamente, sin perjuicio de su utilización por parte de las autoridades competentes que los hayan recibido y que los estén utilizando en el marco de un asunto concreto a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves.

En conclusión, los fines de la recogida de los datos a que se refiere la Ley Orgánica 1/2020 y las garantías que la rodean sitúan esta Ley dentro del marco de la legislación europea, la Constitución española (artículo 18) y el conjunto de la legislación de protección de datos vigente en nuestro país.

Teniendo en cuenta las consideraciones anteriormente efectuadas, se adopta la siguiente:

RESOLUCIÓN

Previo el preceptivo informe de la Junta de Coordinación y Régimen Interior en su reunión del día 14 de diciembre de 2020, y con pleno respeto a cualquier otra opinión diferente, el Defensor del Pueblo (e.f.) resuelve en relación con la previsión contenida en el artículo 162.1.a) de la Constitución española y el artículo 32 de la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional, **no interponer** recurso de inconstitucionalidad contra la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves (BOE número 248, de 17 de septiembre).