Ley Orgánica 1/2020, de 16 de septiembre, de datos de Registro de Nombres de Pasajeros para la prevención, detección y enjuiciamiento de delitos de terrorismo y delitos graves «BOE» núm. 248, de 17 de septiembre 2020 [*BOE*-A-2020-10776]

Recepción de regulaciones en materia de datos personales

El 16 de septiembre fue publicada en el *BOE* la Ley Orgánica 1/2020 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.

Si bien el Anteproyecto tuvo aprobación del Consejo de Ministros en diciembre de 2018, la entrada en vigor en el día 17 de noviembre de 2020 dio término a un proceso que llevó un lustro y en el que tomaron parte los exministros de Interior del Partido Popular Jorge Fernández Díaz y Juan Ignacio Zoido.

Su interesante preámbulo señala, así, que, siendo la protección de la vida y de la seguridad de los ciudadanos el objetivo principal del espacio europeo de libertad y justicia, el Consejo de la Unión Europea ha adoptado una variedad de medidas a través del Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano [*DOUE* C 115, de 4-V-2010] de 4 de mayo de 2010, entre las que se encuentra el impulso para que la Comisión presentara una propuesta sobre la utilización de datos del Registro de Nombres de los Pasajeros («Passenger Name Record», en adelante PNR) para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves.

De esta forma, se creó un marco jurídico regional a fin de que la prevención prioritaria de estos tuviera lugar dentro de los límites señalados por la protección de datos de carácter personal, en lo que respecta a su tratamiento por las autoridades competentes. Seguidamente, tuvo lugar la adopción de 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 [*DOUE* L 119, de 4-V-2016], la cual insta a los Estados miembros a la introducción de disposiciones legales en sus ordenamientos para que los datos PNR de los vuelos exteriores de la Unión Europea sean transferidos a una Unidad de Información sobre Pasajeros (en adelante, UIP) que se cree en cada Estado.

Siguiendo esto último, podemos decir que la presente crónica comentará el resultado de cinco años de labores legislativas para la adopción de la citada Directiva; la cual quedó de esta forma incorporada al ordenamiento jurídico español.

Ars Iuris Salmanticensis,
vol. 9, Junio 2021, 356-359
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

1. BREVE RESUMEN DE SUS DISPOSICIONES

El primer capítulo de esta Ley Orgánica comienza con la descripción de su *objeto*: por un lado, regular la transferencia de los datos del Registro de Nombres de los Pasajeros por parte de las compañías aéreas y otras entidades obligadas; por el otro, 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. También es dable mencionar la designación de la Unidad de Información sobre Pasajeros española y, por último, el régimen sancionador. Los fines para los que pueden ser utilizados tales datos se limitan a la prevención, detección y enjuiciamiento de delitos de terrorismo y delitos graves, y su ámbito de aplicación contempla, en principio, todos los vuelos internacionales que tengan origen, destino o tránsito en España, tanto de carácter comercial como privados (art. 2).

Con relación a los sujetos obligados, el art. 3 diferencia a las compañías aéreas de las entidades de gestión de reservas de vuelos. El art. 4, por su parte, describe qué se entenderá por delitos de terrorismo y delitos graves.

Los datos a ser enviados a la UIP son especificados de entre los recopilados por parte de los sujetos obligados para sus propios fines comerciales en el transcurso normal de su actividad. Deberá también enviarse cierta información sobre los datos de la tripulación contenidos en el sistema de información de pasajeros (sistema API). En el caso de los vuelos privados, la ley dispone que deberán enviarse datos tanto de los pasajeros como los de la tripulación.

El capítulo II regula la UIP, incardinada con la estructura del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (art. 6). Entre sus funciones están la recepción, el tratamiento y el análisis de los datos PNR y los intercambios entre estos con las autoridades competentes tanto nacionales como de otros Estados miembros, terceros países y Europol.

Es interesante la regulación específica de la figura del «responsable de protección de datos», quien deberá garantizar la rigurosa observancia de la legislación vigente en materia de protección de datos de carácter personal durante el proceso descripto (art. 8).

Los propósitos para los que la UIP realizará el tratamiento de los datos PNR deben sujetarse a una metodología definida, la cual incluye la evaluación de las personas a bordo de la aeronave a fin de identificar a aquellas que pudieran tener relación con delitos de terrorismo o delitos graves; la revisión individual de los resultados de dicha evaluación previa automatizada; la respuesta a las peticiones de las autoridades competentes y el establecimiento de criterios predeterminados a utilizar en esas evaluaciones. Para ello, la UIP cotejará los datos PNR con las bases de datos disponibles y pertinentes a los efectos de los fines expuestos *ut supra*.

Las autoridades competentes para solicitar o recibir datos PNR o el resultado de dicho tratamiento por parte de la UIP son, asimismo: 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 pueden hacerlo las Comunidades

Ars Iuris Salmanticensis,
vol. 9, Junio 2021, 356-359
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

Autónomas que hayan asumido competencias para la protección de personas y bienes para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo policial propio (art. 14). Cabe destacar la exigencia de motivación suficiente y con suficiente base a cada petición de las autoridades competentes. De la misma, puede decirse, sobreviene la también subrayable prohibición absoluta de peticiones masivas y no fundamentadas (art. 14.2).

Finalmente, el art. 15 enumera una serie de disposiciones en materia de protección de datos entre las que se destacan la obligación de registro de las operaciones de recogida, consulta, transferencia y supresión de datos, así como la obligación de comunicar al interesado y a la autoridad nacional de control cualquier violación de los datos personales que dé lugar a un elevado riesgo para la protección de los mismos o afecte negativamente la intimidad del interesado. Esto es muy importante en la medida en la que los arts. 16 y 18 de la presente ley contemplan la posibilidad de envío de datos PNR o del resultado de su tratamiento tanto a otros Estados miembros como a terceros países. Los límites legales para tales procedimientos incluyen la adecuación a los fines de la norma y, una vez más, la exigencia de motivación.

En protección al derecho a la intimidad de los sujetos afectados y en especial de su protección de datos de carácter personal, se contempla la conservación de los mismos por el período de cinco años después de su transmisión. Asimismo, luego de seis meses de recepción, se ordenará un «enmascaramiento» de dichos datos; a los que solo se podrá acceder previa aprobación de la Autoridad Judicial o (y aquí esta garantía se debilita) de la Secretaría del Estado de Seguridad. Cumplido el primer plazo, los datos serán suprimidos definitivamente (art. 19).

Finalmente, el capítulo III regula el régimen sancionador; aplicándose el régimen general previsto en la LO 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Así, se definen los sujetos responsables, se clasifican las infracciones en muy graves, graves y leves (arts. 25 a 28) y se determinan las sanciones de acuerdo a la infracción de que se trate (arts. 29 a 21). Es interesante que, para las mismas, se tengan en cuenta, entre otras circunstancias, la repercusión en la «seguridad pública» [art. 29.a)], «la gravedad» o el «beneficio económico obtenido» [29.b) y c)]. Finalmente, se determinan las normas procedimentales.

2. VALORACIÓN CRÍTICA

Por lo expuesto, puede decirse que la Ley Orgánica comentada cumple con las exigencias de la Directiva (UE) tanto en el sentido de crear un sistema uniforme para el tratamiento de los datos PNR definiendo su contenido, los fines a los que se limita su recogida y su utilización y transmisión, como en el de establecer la obligatoriedad de la adopción de medidas que faciliten el cumplimiento por los operadores de sus deberes, incluida la imposición de sanciones efectivas, proporcionadas y disuasorias ante eventuales incumplimientos.

Ars Iuris Salmanticensis,
vol. 9, Junio 2021, 356-359
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

Es dable señalar, asimismo, que la norma obedece a una tendencia propia de las sociedades postindustriales y a las tensiones que RIVERO ORTEGA definió en 2015 como la clásica dialéctica entre libertad y seguridad (*vid.* RIVERO ORTEGA, Ricardo. 2015: «La nueva Ley Orgánica de Seguridad Ciudadana: ¿Estado de prevención o Derecho administrativo del enemigo?». *Ars Iuris Salmanticensis*, junio 2015, 25: 11-16).

Así, para una parte de la doctrina, una nueva configuración surgida de la *Sociedad del Riesgo* hace necesarias intervenciones cautelares tanto a través de un Estado vigilante preventivo como de un conjunto de medidas policiales y punitivas en clave de seguridad desde el Derecho administrativo hasta el Derecho penal. Por esto, a diferencia de lo sucedido con la LO 2/2015 de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo, este sector afirma a su vez que, con respecto a tal delito, los esfuerzos deben centrarse en la prevención antes que en su sanción.

En este caso podemos verificar que se efectúan tales intervenciones en forma de obligaciones como la de poner a disposición de las autoridades una cantidad enorme de información; información que incluso es almacenada por un período de cinco años. Asimismo, una agravante de las sanciones viene a ser la repercusión en la *seguridad pública*. ¿Estamos, entonces, ante una ley que responde a lo que el autor citado denomina *Derecho administrativo del enemigo*? Una respuesta posible es que debe también prestarse atención a los límites mencionados: por un lado, la prohibición de peticiones masivas y, por el otro, dos exigencias: la de la aprobación de la Autoridad Judicial para el acceso a la información recopilada y la de motivación suficiente (la cual, según el artículo citado, no debiera trivializarse).

La seguridad del Estado es algo que indudablemente debe ser abordado con políticas preventivas. No obstante, lejos está de poder considerarse como la única prioridad. Es por esto que quizá el aspecto más interesante de esta Ley Orgánica es que nos permite identificar, en un marco regional y local, las posiciones más destacables de la citada *dialéctica*.

Víctor-Hugo GARCÍA
Abogado (UBA)/Becario de la Agencia Sueca de Cooperación al Desarrollo (Styrelsen för Internationellt Utvecklingssamarbete)
Stockholms Universitet
VictorHugo.DP@usal.es

Ars Iuris Salmanticensis,
vol. 9, Junio 2021, 356-359
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND