Revista Española de Derecho Europeo
90 | Abril – Junio 2024
pp. 89-114
Madrid, 2024
DOI:10.37417/REDE/num90_2024_2231

ISSN: 1579-6302
Recibido: 27/02/2024 | Aceptado: 04/04/2024

LAS OBLIGACIONES DE REGISTRO DOCUMENTAL E INFORMACIÓN SOBRE HOSPEDAJE Y ALQUILER DE VEHÍCULOS A MOTOR EN ESPAÑA A LA LUZ DE LA NORMATIVA EUROPEA SOBRE PROTECCIÓN DE DATOS

THE OBLIGATIONS OF DOCUMENTARY REGISTRATION AND INFORMATION ON LODGING AND RENTAL OF MOTOR VEHICLES IN SPAIN IN THE LIGHT OF THE EUROPEAN REGULATIONS ON DATA PROTECTION

Alejandro Corral Sastre*

RESUMEN: Se analiza en el presente trabajo la adecuación a la legislación europea sobre protección de datos del Real Decreto 933/2021, de 26 de octubre, por el que se establecen las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor. Estas obligaciones impuestas a los prestadores de estos servicios en virtud de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, se basan en una imprecisa y difusa razón de seguridad pública que no justifica el tratamiento masivo y sistemático de toda la información sin discriminación alguna. Sobre todo, cuando lo que se pretende evitar son las formas de delincuencia más graves, esto es, terrorismo y delincuencia organizada. La más reciente jurisprudencia del Tribunal de Justicia de la Unión Europea exige

* Profesor Ayudante Doctor de Derecho Administrativo en la Universidad Complutense de Madrid. Correo-e: *acorra06@ucm.es*, ORCID ID: 0000-0002-5109-8920

Este trabajo de investigación se realiza en el marco del Proyecto de Investigación: "Identidad Digital, Derechos Fundamentales y Neuroderechos", financiado por el Ministerio de Ciencia e Innovación, [PID2020-120373RB-I00], del que es investigador principal el profesor Dr. José Luis Piñar Mañas, y en el que participo como investigador.

el cumplimiento estricto de los principios de minimización y proporcionalidad en el tratamiento de datos con fines policiales que no cumple la citada norma reglamentaria

PALABRAS CLAVE: Alojamiento, Alquiler de vehículos, Protección de datos, Seguridad pública.

ABSTRACT: This paper analyses the compliance with European legislation on data protection of Royal Decree 933/2021, of 26 October, which establishes the documentary registration and information obligations of natural or legal persons who provide accommodation and motor vehicle rental services. These obligations imposed on the providers of these services by virtue of Organic Law 4/2015, of 30 March, on the protection of public safety, are based on a vague and diffuse public safety reason that does not justify the massive and systematic processing of all information without any discrimination whatsoever. Especially when the aim is to prevent the most serious forms of crime, i.e. terrorism and organised crime. The most recent case law of the Court of Justice of the European Union requires strict compliance with the principles of minimisation and proportionality in the processing of data for law enforcement purposes, which the aforementioned regulation does not comply with.

KEYWORDS: Accommodation, Vehicle rental, Data protection, Public security.

INTRODUCCIÓN

A través del presente trabajo se quiere analizar la conformidad a Derecho Europeo de una norma española, el Real Decreto 933/2021, de 26 de octubre, por el que se establecen las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor.

El régimen jurídico sobre la protección del derecho fundamental a la protección de datos ha sufrido una importante reforma en los últimos años. En concreto, con la aprobación del Reglamento (UE) 2016/679 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 adelante, RGPD) y con 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 (Directiva 2016/680).

También debemos mencionar, en esta línea de reforma del marco jurídico en materia de protección de datos, 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 (Directiva PNR-UE).

Se ha tratado, por un lado, de establecer un estándar muy alto de protección de este derecho fundamental, a través del RGPD, en el que se imponen estrictas obligaciones a los responsables y encargados de tratamiento a la vez que se reconocen cada vez más amplios derechos a los titulares de los datos.

Pero, por otro lado, la Unión Europea, siendo consciente del riesgo que representa el terrorismo y las formas de delincuencia organizada grave[1], ha

[1] Hago referencia aquí a una interesante reflexión de M. Fuertes, (2022), *Metamorfosis del Estado. Maremoto digital y ciberseguridad*, Marcial Pons, sobre la cada vez mayor fragilidad de los Estados frente a determinados ataques, pág.12, "La fortaleza casi inexpugnable que exhibía en otras épocas el poder resulta ahora burlada. Los altos muros de esa alcazaba o fortaleza, las sólidas vigas de las que presumía la morada del Leviatán parecen de cartón piedra ante la facilidad con que se traspasan por unos espectros, esas corrientes eléctricas que impulsan una numeración que se convierte en datos, protocolos y programas que mueven tanta información". La profesora Fuertes se refiere aquí a la fragilidad del Estado frente a los ciberataques, pero lo cierto es que esa vulnerabilidad hay que trasladarla a los ataques terroristas y la ciberdelincuencia, frente a los que es Estado ha respondido, precisamente, con aumento en la recopilación de información a través de cada vez más sofisticados instrumentos (videovigilancia, PNR, datos biométricos, etc.)

creado un sistema normativo en el que las obligaciones impuestas a los responsables y encargados de tratamiento, cuando estos son autoridades públicas, quedan relativizadas. Al igual que los derechos de los titulares de los datos, que se ven, de alguna manera, mermados cuando el tratamiento de datos se hace con la finalidad de perseguir, detectar o enjuiciar infracciones penales[2].

No obstante, y esto es lo que se pretende analizar en el presente trabajo, el régimen previsto en estas Directivas, la 2016/680 y la 2016/681, tiene una finalidad muy concreta y específica, y la flexibilidad que supone respecto al régimen general debe interpretarse de manera muy restrictiva.

Así, se analizará la adaptación-incorporación al ordenamiento español de la normativa europea sobre la materia que se ha llevado a cabo a través de distintas normas: la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales; y 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.

Y haré hincapié en el Real Decreto 933/2021, de 26 de octubre, cuyo sistema de obligación de registro documental y de información, tan cuestionable, no tiene parangón en el resto de Europa, y si a la luz de la reciente sentencia

---

[2] Sobre las limitaciones a privacidad en aras de la seguridad, véase, L. A. Ballesteros Moffa (2020), *Las fronteras de la privacidad: el conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica*, Comares, pág., 80, "El régimen común de privacidad, en efecto, alberga una notable "letra pequeña" que rebaja el poder de exclusión al tratamiento por parte del titular de la información personal. Limitaciones que forman parte del mismo régimen de licitud del tratamiento, sin necesidad de acudir al catálogo de posibles excepciones y que, desde la perspectiva del régimen general, no solo habilitan tratamientos con fines de seguridad, sino también la transmisión de los datos personales para tratamientos ulteriores para tales fines, a partir incluso de tratamientos distintos, por cuanto la transmisión forma parte de las operaciones de tratamiento. Algo que, como se verá, tiene una especial incidencia para los responsables de tratamientos en el ámbito de las comunicaciones electrónicas. Sin perjuicio de que, a efectos de los deberes de información, acceso, notificación de cualquier rectificación, supresión o limitación del tratamiento y registro de las actividades del tratamiento [arts. 13.1.e), 14.1.e), 15.1c), 19 y 30.1.d) RGPD, y concordantes de la Directiva de policía (UE) 2016/680], no se consideren destinatarios «las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento» [art. 4.9) RGPD]. En el mismo sentido, H. S. Ayllón Santiago y C. M. Fernández González (2021), *Tratamiento de datos de carácter personal en el ámbito policial*, Reus, pág. 108. "Su ejercicio se (sic.) similar, pero no todos los derechos que asisten a los interesados bajo el ámbito de aplicación del RGPD son aplicables a las actuaciones en el marco de la Directiva con fines policiales".

del Tribunal de Justicia de la Unión Europea de 21 de junio de 2022, puede considerarse conforme al Derecho de la Unión. Adelanto, sin ánimo de destripar el final, que esta norma española por la que se imponen obligaciones de registro documental e información a las empresas de hospedaje y alquiler de vehículos tiene un difícil encaje en todo este sistema normativo europeo.

La interpretación realizada por el Tribunal de Justicia de la Unión para mantener la validez y vigencia de la Directiva 2016/681, apelando a principios como el de mantenimiento de la validez de las disposiciones e interpretación conforme a la Carta de Derechos Fundamentales, no puede ser suficiente, según estimo, para mantener la validez del Real Decreto 933/2021, de 26 de octubre, que debería ser derogado o modificado de manera inmediata, para no seguir vulnerando, entre otros, el derecho fundamental a la protección de datos reconocido el artículo 8 de la Carta. Como trataré de desarrollar en los próximos epígrafes, el Real Decreto 933/2021, de 26 de octubre, es contrario al Derecho de la Unión Europea.

La justificación ofrecida por el Gobierno que aprueba la norma, es decir, la necesidad de mantener la seguridad a la que se refiere el artículo 17 de la Constitución Española (precepto que, por cierto, también se refiere a la libertad), así como la incidencia para la seguridad ciudadana que puedan tener algunas actividades como las de hospedaje o alquiler de vehículos sin conductor (en los términos señalados por el artículo 25 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana), no justifican, en mi opinión, una regulación tan invasiva de derechos[3].

[3] Mucho menos si tenemos en cuenta la opacidad que ha caracterizado tradicionalmente a la policía española respecto al uso de información e instrumentos tecnológicos para el tratamiento de datos personales. Véase, en este sentido L. Cotino Hueso (2023), "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, 64, pág. 4, "Con estas tecnologías, ahora en milisegundos se capta la imagen de una persona, se genera una plantilla y se compara, por ejemplo, con las plantillas de personas buscadas. O se pueden generar automatizadamente grandes cantidades de datos procesados que pueden ser utilizados para múltiples finalidades. Estos datos son especialmente utilizados con finalidades de seguridad pública. En España solo se puede intuir que así sucede dada la total opacidad en la materia. Y es que cuando se ha ejercido el derecho de acceso a la información pública al respecto a autoridades policiales sobre el uso de estos sistemas, las respuestas han sido por lo general muy insatisfactorias. Por lo general se alegan cuestiones de seguridad para no dar ninguna información (art. 14 Ley 19/2013). Es más, incluso se acude a que el uso de tecnologías policiales es desde 1985 materia clasificada. Ello no solo lleva a la opacidad, sino que además conlleva que estas tecnologías ni siquiera queden bajo el ámbito de aplicación de la Ley Orgánica 7/2021 (art. 2. 3º d). Es decir, ni siquiera sería aplicable la reciente ley que específicamente regula los tratamientos de datos en materia criminal y de seguridad. Nadie cuestiona que lo normal en el ámbito policial y criminal será la excepción de la transparencia y acceso a la información (Considerando 26 Directiva (UE) 2016/680

Termino la introducción con una breve reflexión sobre el tiempo que nos ha tocado vivir. Es necesario hacer frente a los riesgos derivados del terrorismo y de la delincuencia grave. Esto implica desarrollar medidas e implantar instrumentos que nos ayuden a prevenir, detectar e impedir que se cometan esos delitos. Y llegado el caso, enjuiciar los mismos. Pero no todo vale. La esfera irreductible de derechos fundamentales y libertades públicas debe mantenerse intacta. Y esto no significa quedar desprotegidos frente a estas amenazas. Se trata de alcanzar un "difícil pero necesario equilibrio"[4], una adecuada ponderación entre derechos fundamentales.

1. RAZONES HISTÓRICAS DE LA OBLIGACIÓN DE REGISTRO DOCUMENTAL E INFORMACIÓN SOBRE HOSPEDAJE

Ya se ha indicado en el epígrafe anterior que este sistema previsto en el Real Decreto 933/2021, de 26 de octubre, es muy cuestionable. Algunos Estados de la Unión Europea tienen sistemas para informar sobre los familiares de los ciudadanos europeos que vayan a residir por menos de tres meses en el territorio, en aplicación de la Directiva 2004/38/CE del Parlamento Europeo y del Consejo de 29 de abril de 2004 relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros. Pero, en mi opinión, no son tan invasivos como el español.

Esta circunstancia llama la atención, por lo que es necesario, según entiendo, detenerse brevemente en analizar los orígenes y motivos que justifican su aparición, así como la evolución posterior a lo largo de los años hasta llegar al momento actual.

El origen de esta obligación parece remontarse a Decreto 1513/1959, de 18 de agosto, en relación con los documentos que deben llevar los establecimientos de hostelería referentes a la entrada de viajeros[5]. Por el contexto histórico y social de la norma, se puede deducir claramente cuáles son los motivos que llevan al Estado a realizar esta actividad. La vertiente de con-

---

[4] J. L. Piñar Mañas (2009), "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio", Documento de trabajo 147/2009, *Fundación Alternativas*, pág. 7, "Al analizar estos retos ha de partirse de una premisa común a todos ellos: no existe en absoluto una contradicción entre tales derechos o situaciones (libertad de expresión, transparencia, seguridad...) y la protección de datos. Más bien al contrario: solo respetando el derecho fundamental de todos a la protección de datos personales se conseguirá un marco adecuado de respeto a la libertad de expresión y al derecho de acceso a la información; un correcto desarrollo del mercado y una eficaz lucha contra el terrorismo".

[5] C. Martín Fernández (2023), "Las obligaciones de registro documental en los ámbitos del hospedaje y del alquiler de vehículos para garantizar la seguridad ciudadana", en H. Gonsálbez Pequeño, y A. M. Bueno Armijo, *Desregulación y regulación de la economía colaborativa en la actividad turística y las actividades con incidencia turística*, Thomson Reuters Aranzadi.

trol de la información en el ámbito turístico, en un momento del régimen franquista en el que comenzaba a mirarse al exterior, genera suspicacias que querían atajarse mediante el absoluto control policial de todas y cada una de las personas que entraban en España y se alojaban en algunos de los establecimientos turísticos señalados en la norma.

Bien es cierto que el Preámbulo de la norma refería exclusivamente motivos fiscales para justificar este control[6]. Pero en el fondo subyace, estimo, la fiscalización de toda la información posible que pudiera evitar que la pretendida apertura internacional derivase también en algo similar a nivel interno, es decir, una flexibilización de la vigilancia política interna[7]. En esta línea, resulta muy clarificador la unión de los Ministerios de Información y Turismo en uno solo, que no pretendía precisamente, según los autores, otorgar más importancia al turismo, sino controlar la información que se generaba desde este[8].

Esta finalidad de control político del Decreto de 1959 queda patente con la posterior ampliación de las obligaciones de registro documental a otros establecimientos de alojamiento como campings, apartamentos, bungalow y otros similares que se hace a través del Decreto 393/1974, de 7 de febrero. De la misma manera, se extienden estas obligaciones a las personas físicas o jurídicas dedicadas al alquiler de automóviles de turismo con o sin conductor. Esta ampliación de las obligaciones de registro documental responde a un contexto político y social muy concreto. El año anterior, en 1973, se había producido el atentado terrorista que acabo con la vida del entonces presidente del Gobierno, Luis Carrero Blanco. Para el atentado, los terroristas habían alquilado un bajo en la Calle Claudio Coello de Madrid desde donde excavaron un túnel hasta el dentro de la calle donde detonaron el explosivo al paso del vehículo que transportaba a Carrero[9].

---

[6] El Preámbulo del Decreto 1513/1959, de 18 de agosto, en relación con los documentos que deben llevar los establecimientos de hostelería referentes a la entrada de viajeros, establece lo siguiente: "Es un hecho comprobado que la multiplicidad de disposiciones sobre una misma materia dificulta su voluntario cumplimiento y la acción estatal que pretende servir"

[7] J., Muñoz Soro, (2014), "Política de información y contrainformación en el franquismo (1951-1973): «El Ministerio de Información es tan importante como el de la Guerra»", *Revista de Estudios Políticos*, pág. 238, "El desgajamiento de la información, así como su vinculación al turismo, ha sido interpretado como una maniobra destinada a poner bajo control directo de Franco y Carrero Blanco un área estratégica en la fase de consolidación internacional del régimen con vistas a la normalización de su imagen exterior"

[8] A., Moreno Garrido (2007), *Historia del turismo en España en el siglo xx*, Síntesis., pág. 195, conviene, por tanto, desterrar la idea de que, al hilo del progresivo aumento de visitantes, el Régimen quisiese corroborar la mayor importancia institucional del mismo elevando su categoría. Nada más lejos de la realidad". En el mismo sentido, F. Bayón Mariné, y L. Fernández Fuster, (1999), "Los orígenes", en la obra colectiva F. Bayón Mariné, (Dir.), *50 años del turismo español. Un análisis histórico y estructural*, Ramón Areces.

[9] C. Martín Fernández, (2023), *op. cit*., pág. 545.

Este atentado hizo crecer en el Gobierno la necesidad de incrementar el control sobre los establecimientos de alojamiento y el arrendamiento de vehículos. Un control encaminado, esencialmente, a supervisar si las personas que utilizaban estos servicios suponían una amenaza para el régimen.

Pues de aquellos barros vienen estos lodos. Es decir, esta obligación de las empresas de alojamiento turístico y de alquiler de vehículos tiene su origen en la necesidad del régimen franquista de controlar los posibles elementos subversivos. Y hoy se mantienen estas obligaciones, santificadas por la necesidad de salvaguardar la vida, la integridad física y la seguridad de los ciudadanos frente los ataques terroristas y las amenazas del crimen organizado, sobre todo teniendo en cuenta su marcado carácter transnacional[10].

2. JUSTIFICACIÓN DEL TRATAMIENTO DE LA INFORMACIÓN SOBRE LOS CONSUMIDORES DE SERVICIOS DE ALOJAMIENTO TURÍSTICO Y ARRENDAMIENTO DE VEHÍCULOS

Ante esta circunstancia, cabe plantearse la siguiente pregunta: ¿Está justificado el control sistemático y general de la identidad de todas aquellas personas que utilizan los servicios de alojamiento turístico o el arrendamiento de vehículos para evitar atentados terroristas o la amenaza del crimen organizado?

La respuesta del legislador español ha sido claramente afirmativa. Y para ello ha establecido la obligación legal de registro documental para determinadas personas físicas o jurídicas que se dedican a determinadas actividades consideradas "de riesgo" en el artículo 25 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (en adelante, LOPSC).

Pero desde el punto de vista doctrinal y jurisprudencial, lo cierto es que genera importantes dudas que, en los próximos epígrafes, trataré de desentrañar. El motivo que históricamente se ha utilizado para llevar a cabo estos tratamientos de información tan invasivos plantea hoy algunos problemas que deben ser analizados.

---

[10] El párrafo cuarto del Preámbulo del Real Decreto 933/2021, de 26 de octubre, por el que se establecen las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor, establece lo siguiente: "En el momento actual, los mayores ataques a la seguridad ciudadana vienen protagonizados tanto por la actividad terrorista como por el crimen organizado, en los dos supuestos con un marcado carácter transnacional. En ambos casos cobran especial relevancia en el modus operandi de los delincuentes la logística del alojamiento y la adquisición o uso de vehículos a motor, cuya contratación se realiza hoy en día por infinidad de vías, incluida la telemática, que proporciona una mayor privacidad en esas transacciones.

2.1. Marco jurídico general de la protección de datos. Especial referencia a la seguridad

La creación de bases de datos en nuestro país, lo que supone un tratamiento de datos personales de personas físicas, está sometido a unas reglas concretas contenidas en el Reglamento (UE) 2016/679 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 (a partir de ahora, RGPD). En esta norma europea, que supuso una auténtica revolución en la materia[11], pues cambió los paradigmas sobre la protección de este derecho fundamental, se contienen los principios básicos que deben regir en todo tratamiento de datos personales. Se resumen, según lo dispuesto en el artículo 5 del RGPD en licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación de plazo de conservación, integridad, confidencialidad y responsabilidad proactiva.

Este RGPD fue adaptado al ordenamiento jurídico español a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Adaptación, que no transposición, pues la norma europea, por sí sola, es directamente aplicable[12] sin más trámite desde su entrada en vigor a los 20 días de su publicación en el Diario Oficial de la Unión Europa, pese a su posterior dilatada *vacatio legis* de dos años[13].

Este es el régimen general en la materia. Se aplica a aquellos responsables o encargados de tratamiento, tanto del sector público como privado. Pero, como es sabido, existe un régimen especial para aquellos tratamientos realizados por autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, en cuyo caso resulta de aplicación la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, Directiva 2016/680), y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[14], que transpone, esta vez sí, la Directiva citada.

---

[11] Sobre las implicaciones que supuso el Reglamento General del Protección de Datos en nuestro país, véase J. L. Piñar Mañas (2016), *El Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos*, Reus.

[12] Señala el artículo 99 del propio RGPD que: "El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro".

[13] Fue publicado en el Diario Oficial de la Unión Europea el 4 de mayo de 2016, entró en vigor a los 20 días de su publicación, es decir, el 25 de mayo de 2016, pero no se empezó a aplicar hasta 2 años después, esto es, el 25 de mayo de 2018. Así lo dispone el artículo 99 del propio RGPD.

[14] La falta de transposición en plazo de la Directiva 2016/680, supuso una condena al Reino de España por parte de Comisión Europea que se podría haber evitado con una tramitación parlamentaria adecuada, tal y como expone I. Navarro Mejía,

En el caso de la norma que estamos analizando, el Real Decreto 933/2021, hay que tener en cuenta que, mientras que las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales se regirán por lo dispuesto en la Directiva 2016/680 y la Ley Orgánica 7/2021, de 26 de mayo, los sujetos privados obligados por la norma a recopilar los datos de los usuarios de los servicios indicados deben tener en cuenta lo dispuesto en el RGPD y la LOPDyGDD.

Por su parte, también es necesario mencionar 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, transpuesta a nuestro ordenamiento por 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. Esta norma, la Directiva 2016/681, ha sido sobre la que ha recaído la Sentencia del Tribunal de Justicia de la Unión Europea de 21 de junio de 2022 que, pese a que no la ha anulado, ha forzado una determinada interpretación de sus preceptos.

Cabe indicar, desde este momento, que no existe ninguna norma europea que obligue a los Estados miembros a recopilar información sobre actividades de hospedaje o alquiler de vehículos, por lo que es una obligación impuesta por el derecho nacional justificada, como hemos visto, en una difusa razón de seguridad pública que habrá de ser examinada. Y eso es lo que aquí me propongo, a la luz de la Sentencia del Tribunal de Justicia de la Unión Europea de 21 de junio de 2022, en el asunto C-817/19, *Ligue des droits humains*, en el que se viene a indicar, de manera resumida, que "En ausencia de amenaza terrorista real y actual o previsible a la que deba hacer frente un Estado miembro, el Derecho de la Unión se opone a una legislación nacional

---

(2021), "La falta de transposición de una directiva europea en materia reservada a ley orgánica: Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea de 25 de febrero de 2021. Asunto C-658/19", *Revista de las Cortes Generales*, (111), "En suma, este plazo de transposición no se cumplió, cuando este caso, dadas la naturaleza y la fecha de aprobación de la Directiva 2016/680, podría haber llevado a plantear de otra forma, desde su inicio, el procedimiento para cumplir esa transposición. Finalmente sí se aprobaría la norma correspondiente: la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Con su comunicación se pudo poner fin al pago de la multa coercitiva diaria impuesta por el TJUE. Así pues, la tramitación parlamentaria, que incluyó además la aprobación de enmiendas por el Senado y su consiguiente remisión al Congreso, duró poco más de tres meses, desde la presentación del texto hasta su aprobación. Existen por tanto sobradas razones para considerar la participación parlamentaria no como un obstáculo, sino como un apoyo para la transposición en plazo de directivas que, como la Directiva 2016/680, exigen la intervención de las Cortes Generales: por todo ello conviene separar los casos que requieren esta intervención de los que corresponden por definición al Gobierno".

que prevé la transferencia y el tratamiento de los datos PNR de los vuelos interiores de la UE y de los transportes realizados por otros medios en el interior de la Unión".

Esta interpretación es la que, en mi opinión, hace que se tambaleé la conformidad a Derecho de la Unión de una norma que exige, sin más concreción, la recopilación de todos los datos de los usuarios de servicios de alojamiento y alquiler de vehículos, por una razón de seguridad pública que, repito, es muy imprecisa.

3. ANÁLISIS DEL REAL DECRETO 933/2021, DE 26 DE OCTUBRE, A LA LUZ DE LOS PRINCIPIOS GENERALES CONTENIDOS EN EL RGPD

3.1. Licitud del tratamiento efectuado por personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor

Una de las primeras cuestiones que se ha de plantear respecto al tratamiento de los datos de los consumidores por parte de aquellas personas físicas o jurídicas que se dedican a ofrecer estos servicios en el mercado es, precisamente, su justificación o, si se quiere, el cumplimiento del principio de licitud (artículo 5.1.a) del RGPD).

Ello implica conocer la base jurídica que legitima el tratamiento de datos personales en este supuesto concreto. Y la encontramos en el artículo 6.1.c) del RGPD, es decir, que el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable. La Ley en la que se apoya el Real Decreto 933/2021, de 26 de octubre, para legitimar el tratamiento es la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC), en cuyo artículo 25 se establecen obligaciones de registro documental a todas las personas físicas o jurídicas que ejerzan actividades relevantes para la seguridad ciudadana, entre las que se indican, en concreto, las de hospedaje y alquiler de vehículos a motor.

Pero se debe analizar, igualmente, la manera en que la LOPSC legítima ese tratamiento, y para ello se debe acudir a lo establecido en los apartados 2 y 3 del mismo artículo 6 del RGPD, pues define como debe quedar configurada la obligación legal que sirva de base legítima para dicho tratamiento, exigiendo que la finalidad del tratamiento quede determinada en dicha base jurídica. De la misma manera: "Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación

de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido".

De esta manera, y de acuerdo con lo previsto en la LOPSC[15], parece claro que la finalidad que justificaría la imposición de esta obligación de comunicar los datos personales de los usuarios de los servicios de alojamiento y alquiler de vehículos a motor sería la preservación de la seguridad ciudadana y la prevención, detección y en su caso persecución de conductas delictivas.

Por tanto, como indica el Informe 2018-0103 de la Agencia Española de Protección de Datos, el tratamiento de datos de usuarios de servicios de establecimientos de alojamiento y vehículos a motor previsto en el Real Decreto 933/2021, de 26 de octubre, tiene base legítima conforme a lo previsto en el RGPD[16].

3.2. Sobre el principio de "minimización" de datos personales

Para comprobar la conformidad a Derecho de un tratamiento de datos personales debemos analizar no solo la legitimidad, sino el cumplimiento de otros principios recogidos en el artículo 5 del RGPD.

Analizo ahora el cumplimiento del principio de minimización, es decir, según lo establecido en el punto c) del mencionado artículo 5, se trata de que los datos tratados sean "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

En esta línea, el Real Decreto 933/2021, de 26 de octubre, distingue entre los "datos a facilitar en el ejercicio de la actividad de hospedaje" (Anexo I), y los "datos a aportar en el ejercicio de la actividad de alquiler de vehículos" (Anexo II). En relación con los primeros, además, debemos distinguir entre los "datos a facilitar en el supuesto de ejercicio profesional de la actividad" (apartado A), respecto a los "datos a facilitar en el supuesto de ejercicio no profesional" (apartado B). Esta última distinción se debe a que, según el apartado 4 del artículo 5 de la norma jurídica, "los sujetos obligados que desarrollen actividades de hospedaje de manera no profesional quedan excep-

---

[15] El apartado 2 del artículo 1 de la LOPSC establece que:

2. Esta Ley tiene por objeto la regulación de un conjunto plural y diversificado de actuaciones de distinta naturaleza orientadas a la tutela de la seguridad ciudadana, mediante la protección de personas y bienes y el mantenimiento de la tranquilidad de los ciudadanos.

[16] Agencia Española de Protección de Datos, Informe 2018-0103, pág. 6, De este modo, puede considerarse que los tratamientos de datos impuestos por el Proyecto sometido a informe a quienes ejercen actividades de hospedaje y alquiler de vehículos de motor se encontrarían amparados por lo dispuesto en el artículo 6.1 c) del Reglamento general de protección de datos.

tuados de las obligaciones de registro documental y conservación de datos previstos en este artículo, y solo estarán sujetos a las obligaciones de comunicación previstas en el artículo siguiente", es decir, se relajan las obligaciones de aquellas personas que se dediquen a la actividad de alojamiento de manera no profesional. Se está pensando, esencialmente, en personas físicas que explotan un inmueble como vivienda de uso turístico.

En cuanto a los datos que deben recogerse, son, según entiendo, excesivos. Nos vamos a centrar en los datos de los viajeros o los arrendatarios de vehículos a motor y conductores de estos (también los de, en su caso, el segundo conductor). Así, en el caso de los usuarios de servicios de alojamiento (Anexo I. A. 3) [17], puede tener sentido recopilar datos referidos a filiación, fecha de nacimiento, nacionalidad y correo electrónico, para cumplir una excesivamente genérica, en mi opinión, finalidad de seguridad pública. Lo que no creo que sea necesario, y atenta contra el principio de minimización, es la recolección de otros datos como: sexo, documento de identidad, número, tipo de documento, lugar de residencia completo (incluido domicilio), teléfonos fijo y móvil, número de viajeros y relación de parentesco entre ellos.

En el caso de caso del arrendamiento de vehículos a motor es, si se me permite la expresión, todavía peor. Aquí hay que distinguir entre los datos del arrendatario (Anexo II. 2)[18], datos del conductor principal (Anexo II. 3) y datos del segundo conductor, en su caso (Anexo II. 4), que son los mismos que los del primer conductor. Puede resultar necesario, en estos supuestos, comprobar que el conductor tenga el título habilitante necesario para conducir el vehículo que se está alquilando, pero no se justifica, en mi opinión, la necesidad de trata y comunicar a las fuerzas y cuerpos de seguridad otra información como la dirección completa del lugar de residencia, su teléfono móvil, fecha de nacimiento, etcétera.

---

[17] El Anexo I. A. 3, referido a los datos de los viajeros, indica que deben recogerse los siguientes datos: a) Nombre, b) Primer apellido, c) Segundo apellido, d) Sexo, e) Numero de documento de identidad, f) Número de soporte del documento, g) Tipo de documento (DNI, pasaporte, TIE), h) Nacionalidad, i) Fecha de nacimiento, j) Lugar de residencia habitual (Dirección completa, Localidad y País), k) Teléfono fijo, l) Teléfono móvil, m) Correo electrónico, n) Número de viajeros, o) Relación de parentesco entre los viajeros (en el caso de que alguno sea menor de edad).

[18] Respecto a los arrendatarios de vehículos a motor se exige: a) Nombre, b) Primer apellido, c) Segundo apellido, d) Sexo, e) Numero de documento de identidad, f) Tipo de documento (DNI, pasaporte, TIE), g) Nacionalidad, h) Fecha de nacimiento, i) Lugar de residencia habitual (Dirección completa, Localidad y País), j) Teléfono fijo, k) Teléfono móvil, l) Correo electrónico. También se exigen como datos del conductor principal (y del segundo si lo hubiera), lo siguientes: a) Nombre, b) Primer apellido, c) Segundo apellido, d) Sexo, e) Numero de documento de identidad, f) Tipo de documento (DNI, pasaporte, TIE), g) Nacionalidad, h) Fecha de nacimiento, i) Lugar de residencia permanente. – Dirección completa, – Localidad, – País, j) Teléfono fijo, k) Teléfono móvil, l) Correo electrónico, m) Carnet de conducir. – Tipo, – Validez, – Número, – Número de soporte.

3.3. Incremento de la información solicitada por el Real Decreto 933/2021, de 26 de octubre, respecto de la normativa anterior

En cualquier caso, es necesario indicar que los datos exigidos por el Real Decreto 933/2021, de 26 de octubre, han sido incrementados respecto a los que exigía la normativa anterior, es decir, la Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos[19]. Esta norma, por cierto, se mantiene vigente en tanto en cuanto no sea desarrollada por el Gobierno en los términos establecidos en la Disposición Derogatoria Única, apartado 2, del Real Decreto, y siempre y cuando no contravenga sus disposiciones.

Lo mismo ha ocurrido con los datos sobre la actividad de alquiler de vehículos a motor. La información que había que comunicar según la Orden de 2 de noviembre de 1989 por la que se regulan las modalidades de elaboración de libros-registro y otros documentos de control, obligatorios para determinados establecimientos, en relación con la Orden de 16 de septiembre de 1974 sobre control gubernativo de automóviles de alquiler, con o sin conductor, en desarrollo del artículo del Decreto 393/1974, de 7 de febrero, era sustancialmente menor a la que ahora exige el Real Decreto 933/2021, de 26 de octubre.

Es necesario plantearse, ante estas circunstancias, si realmente los datos solicitados según el nuevo Real Decreto del 2021 son los realmente precisos para el fin específico del tratamiento. Entiendo, personalmente, que no, pues ¿Para que se ha de solicitar el número de teléfono o el lugar completo de residencia en relación con una persona que, en principio, no ha cometido ningún delito? Si esa persona es investigada por la posible comisión de un delito su información será tratada conforme a lo establecido en la Directiva 2016/680 y la LO 7/2021, de 26 de mayo. Pero cualquier otro tratamiento previo, preventivo si se quiere, me parece excesivo y vulnera, por consiguiente, el principio de minimización analizado.

3.4. La jurisprudencia del Tribunal de Justicia de la Unión Europea sobre el principio de minimización

Para analizar el principio de minimización de datos, no obstante, conviene tener presente la jurisprudencia del Tribunal de Justicia de la Unión Europea con relación a la nulidad de la Directiva 2006/24/EC del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de da-

[19] La Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos, en cuyo Anexo solo exigía: Núm. de documento de identidad, Tipo de documento Fecha expedición del documento, Primer apellido, Segundo apellido, Nombre, Sexo, Fecha de nacimiento, País de nacionalidad, Fecha de entrada.

tos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas[20], que vino a declarar contrario al ordenamiento europeo el tratamiento masivo e indiscriminado de datos de tráfico en comunicaciones electrónicas al considerarse el mismo una intromisión en los derechos fundamentales a la intimidad y a la protección de datos personales consagrados en los artículos 7 y 8 de la Carta de Derechos Fundamentales.

A la AEPD le planteó serias dudas el cumplimiento de principio de minimización de datos a la vista del incremento de la información que exigía el Real Decreto 933/2021, de 26 de octubre, pues no se justificaba en ningún lugar la necesidad del aumento de los datos requeridos. Así lo puso de manifiesto en su Informe que elaboró el Gabinete Jurídico de la Agencia (N/REF: 175906/2018), en su Punto III:

> "En relación con el principio de minimización de datos debe tenerse en cuenta la doctrina sentada por el Tribunal de Justicia de la Unión Europea a partir de las sentencias de 8 de abril de 2014 (asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd)* y 21 de diciembre de 2016 (asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB),* en que se viene a declarar contrario al derecho de la Unión el tratamiento masivo e indiscriminado de datos de tráfico en comunicaciones electrónicas al considerarse el mismo una intromisión en los derechos fundamentales a la intimidad y a la protección de datos personales, consagrados en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.
> […]
> Como se ha indicado, el Proyecto sometido a informe se limita a señalar que procede la ampliación del tratamiento a los datos que se detallan en los Anexos por cuanto, en relación con el Anexo I, los datos "se consideran de interés desde el punto de vista de la seguridad". Asimismo, en cuanto a los incluidos en el Anexo II, que el tratamiento de los datos se justifica "por el elevado interés de todos ellos desde el punto de vista de la seguridad"[21].

A la AEPD no le pareció adecuada la justificación ofrecida por el Gobierno para incrementar la información requerida. A mí, personalmente, tampoco. No se puede esgrimir una razón tan genérica para aumentar los datos tratados.

Ante esta situación, la AEPD consideró necesario someter el Proyecto de Real Decreto a una evaluación de impacto en la protección de datos[22], en los

---

[20] Me refiero, en concreto, a la sentencia del Tribunal de Justicia de la Unión Europea de fecha 8 de abril de 2014 en los asuntos acumulados C-293/12 y C-594/12. El Tribunal analiza, al hilo de dos cuestiones prejudiciales planteadas por la *High Court* irlandesa y el *Verfassungsgerichtshof* austriaco, la validez de la Directiva 2006/24/CE, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y la vulneración, posteriormente declarada, de los artículos 7, 8 y 11 de la Carta de Derechos Fundamentales de la Unión Europea

[21] Agencia Española de Protección de Datos, (2018), N/Ref: 175906/2018, pág. 8.

[22] Ibidem, pág. 9, La AEPD se refiere a la necesidad de incorporar una evaluación de impacto en materia de protección de impacto en el informe ya citado más arriba, en los siguientes términos:

términos previstos en el artículo 35.1 del RGPD y el artículo 27 de la Directiva 680/2016, que ha sido transpuesto a nuestro ordenamiento a través del artículo 35 de la Ley Orgánica 7/2021, de 26 de mayo.

Este instrumento de la evaluación de impacto en la protección de datos implica, "como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas".

Lo que se trata, precisamente, es de evaluar los posibles riesgos para reducir las posibilidades de su concreción. En la práctica, las evaluaciones de impacto son un mecanismo idóneo para analizar si las cosas se están haciendo de conformidad con la legislación de protección de datos y si se cumplen los correspondientes principios.

No consta la realización de esta evaluación, por lo que la norma, que afecta de lleno al derecho fundamental a la protección de datos y genera altísimos riesgos en la materia, no ha sido analizada desde esta perspectiva. En la Memoria de Análisis de Impacto Normativo publicada en el Portal de Transparencia de la Administración General del Estado, se hace una somera referencia a la cuestión para indicar, únicamente, que se cumple la normativa sobre protección de datos (ni siquiera se hace referencia a qué normativa)

3.5. Sobre la obligación de someter la normativa a evaluación de impacto y la posible nulidad del Real Decreto 933/2021, de 26 de mayo

Si la evaluación de impacto en materia de protección de datos es obligatoria en los términos previstos en el artículo 35 de la Ley Orgánica 7/2021, de 26 de mayo, por la que se incorpora el artículo 27 de la Directiva 680/2016, el

---

"A juicio de esta Agencia, sin prejuzgar con ello si la enumeración efectuada por los Anexos I y II resulta conforme al principio de minimización citado, sería necesario que en la tramitación del Proyecto se llevase a cabo una adecuada evaluación de impacto en la protección de datos de la recogida y comunicación que se describen a fin de determinar si se da o no pleno cumplimiento a tal principio y si el tratamiento y comunicación de todos los datos mencionados puede considerarse limitada a lo mínimo necesario para atender las finalidades descritas en la Ley Orgánica 4/2015 y la Exposición de motivos del Proyecto, basándose en la información disponible por el propio Departamento proponente que justifique la necesidad de la recogida de los datos mencionados para la adecuada preservación de la seguridad ciudadana, dado que la mera referencia al "interés" de la información puede considerase suficiente para acreditar el cumplimiento del principio de minimización de datos".

Gobierno debería haber sometido el proyecto de Real Decreto a esta evaluación tal y como recomendó la AEPD en su informe.

Dicha evaluación tendría que haberse incorporado en el procedimiento de elaboración de la norma reglamentaria. Bien es cierto que no se encuentra entre los apartados de la Memoria de Análisis de Impacto Normativo según lo dispuesto en el artículo 26.3 de la Ley 50/1997, de 27 de noviembre, del Gobierno. Pero a la vista del contenido de la norma y como afecta al derecho fundamental a la protección de datos, la evaluación de impacto debe considerarse un informe preceptivo de acuerdo con lo previsto en el apartado 5 del artículo 26 de la citada Ley del Gobierno.

Fijadas estas premisas, la conclusión necesaria es que el Real Decreto 933/2021, de 26 de mayo, es nulo de pleno derecho[23] por no haber incluido en su procedimiento de elaboración la preceptiva evaluación de impacto en materia de protección de datos. Y ello en base a lo previsto en el artículo 47.2 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), pues supone una vulneración de una norma superior, en concreto, la Ley Orgánica 7/2021, de 26 de mayo que transpone la Directiva 2016/680, que se aplican, como es el caso, a los supuestos en que el responsable de tratamiento es una autoridad competente para la investigación, detección o enjuiciamiento de infracciones penales[24].

---

[23] Sin profundizar demasiado en la cuestión, cabe traer a colación, si quiera tangencialmente, la polémica doctrinal en torno a si cualquier vulneración sustancial o formal de los reglamentos debe llevar a la necesaria nulidad (tesis unitaria defendida por E. García de Enterría y T. R., Fernández, en su Curso de Derecho Administrativo defendida sin fisuras hasta la 18ª edición de 2017, que incluye ciertos matices) o se admiten otras formas más matizadas de sanción, como últimamente defienden F. López Ramón (2018), "La calificación de los vicios de los reglamentos", *Revista de Administración Pública*, 205, o L. Martín Rebollo, (2019), De nuevo sobre la invalidez en el derecho público, con particular referencia a la invalidez de los reglamentos. (Una reflexión abierta y algunas propuestas). *Revista de Administración Pública*, 210, por citar solo algunos ejemplos. Para un análisis detallado de la jurisprudencia en materia de nulidad de pleno derecho de disposiciones administrativas de carácter general por motivos formales, véase C. Tolosa Tribiño (2019), "La invalidez de los reglamentos. En particular, el efecto invalidante de los vicios de procedimiento", *Revista de Administración Pública*, 210.

[24] No puedo entrar a analizar otras posibles causas de nulidad, pero, podrían existir tal y como acredita V. Horcajuelo Rivera (2020), "Análisis del proyecto de real decreto por el que se imponen obligaciones de registro documental e información a las plataformas digitales de viviendas turísticas y de alquiler de vehículos que no presten el servicio subyacente", en M. Á. Recuerda Girela (2020), *Anuario de Derecho Administrativo 2020*, Aranzadi, pág., 418. "El Proyecto de Real Decreto solicita que las plataformas digitales de hospedaje y de alquiler de vehículos con conductor, presten o no presten el servicio subyacente y, por tanto, también las plataformas que sean PSSI neutros, reporten información constante de todas las reservas que se realicen a través de ellas. Es una obligación de registro y reporte continuada de todos los datos y no de aquellos que sean ilícitos o que se sospeche por la autoridad que sean ilícitos.

4. ESPECIAL REFERENCIA AL PRINCIPIO DE PROPORCIONALIDAD Y LA SENTENCIA DEL TRIBUNAL DE JUSTICIA E LA UNIÓN EUROPEA DE 21 DE JUNIO DE 2022

4.1. Origen del recurso

Sin perjuicio de lo que ya se ha concluido en el apartado anterior sobre la nulidad del Real Decreto 933/2021, de 26 de octubre, por no incluir la necesaria evaluación de impacto en materia de protección de datos y vulneración del principio de minimización, voy a analizar a continuación el contenido de la norma a la luz de la STJUE en el asunto C-817/19, *Ligue des droits humains*.

La *Ligue des droits humains* (LDH) es una asociación sin ánimo de lucro que en junio de 2017 interpuso ante el Tribunal Constitucional de Bélgica un recurso de anulación contra la Ley de 25 de diciembre de 2016, que transpone al Derecho belga la Directiva PNR[25], la Directiva API[26] y la Directiva 2010/65[27].

Según la LDH, esta ley vulnera el derecho al respeto de la vida privada y a la protección de los datos personales, garantizado tanto por el Derecho belga como por el Derecho de la Unión. Se pone en tela de juicio, por una parte, la enorme amplitud de los datos PNR y, por otra parte, el carácter general de la recogida, la transferencia y el tratamiento de estos datos.

En octubre de 2019, el Tribunal Constitucional belga planteó al Tribunal de Justicia diez cuestiones prejudiciales relativas, en particular, a la validez de la Directiva PNR y a la compatibilidad de la Ley de 25 de diciembre de 2016 con el Derecho de la Unión.

Por tanto, parece difícil que una obligación de este tipo tenga encaje en los supuestos contemplados en el artículo 15.2 de la Directiva de Comercio Electrónico. Dicho de otra forma, si el Proyecto de Real Decreto llegara aprobarse con un texto como el actual, que incluye a las plataformas que no prestan el servicio subyacente, podría ser una norma que vulnerara la Directiva de Comercio Electrónico".

[25] 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.

[26] 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.

[27] Directiva 2010/65/UE del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, sobre las formalidades informativas exigibles a los buques a su llegada o salida de los puertos de los Estados miembros y por la que se deroga la Directiva 2002/6/CE

4.2. Principales conclusiones de la sentencia sobre el cumplimiento del principio de proporcionalidad

Es necesario indicar, en primer lugar, que, aunque la sentencia se refiere a la validez de la Directiva PNR a la que ya nos hemos referido más arriba, las conclusiones a las que llega el TJUE afectan, como es lógico, a otras normas europeas y su adaptación a los ordenamientos internos.

En este sentido, lo que pretendemos a continuación es analizar las principales conclusiones de la sentencia y someter al Real Decreto 933/2021, de 26 de octubre (previamente habilitado por la LOPSC), al juicio correspondiente para comprobar si supera los requisitos fijados en la resolución judicial. A la vista de ello se podrá determinar si la norma reglamentaria nacional es contraria, o no, a Derecho de la Unión Europea.

La sentencia del TJUE establece que Directiva PNR conlleva injerencias de una gravedad importante en los derechos garantizados por los artículos 7 y 8 de la Carta, ya que tiene por objeto la implantación de un régimen de vigilancia continuo, no selectivo y sistemático que incluye la evaluación automatizada de datos de carácter personal de todas las personas que utilizan servicios de transporte aéreo (apartado 111)[28]. El Tribunal de Justicia recuerda que la posibilidad de que los Estados miembros justifiquen tal injerencia debe apreciarse ponderando su gravedad y comprobando que la importancia del objetivo de interés general perseguido se corresponde con esta gravedad.

En esta línea de argumentación, recuerda el Alto Tribunal que las potestades y facultades previstas en esta Directiva deben ser siempre interpretadas de manera restrictiva y que la recogida, transferencia, tratamiento y conservación de los datos (en este caso los PNR) previstos por esta Directiva se deben limitar a lo estrictamente necesario (apartado 186 de la sentencia)[29] para luchar contra los delitos terroristas y los delitos graves.

Así, el tratamiento de la información a la que se refiere la Directiva debe referirse estrictamente a los delitos terroristas y exclusivamente a los delitos graves que presenten un vínculo objetivo, cuando menos indirecto, con el

---

[28] Apartado 111 de la sentencia del TJUE, que establece lo siguiente:
"Habida cuenta de todas las consideraciones anteriores, procede considerar que la Directiva PNR comporta injerencias de una gravedad cierta en los derechos garantizados por los artículos 7 y 8 de la Carta, ya que, en particular, tiene por objeto la implantación de un régimen de vigilancia continuo, no selectivo y sistemático, que incluye la evaluación automatizada de datos de carácter personal de todas las personas que utilizan los servicios de transporte aéreo".

[29] Apartado 186 de la sentencia: En este sentido, los considerandos 7 y 15 de la Directiva PNR indican que el tratamiento automatizado previsto en el artículo 6, apartado 3, letra a), de esta Directiva debe limitarse a lo estrictamente necesario para la lucha contra los delitos de terrorismo y la delincuencia grave, garantizando al mismo tiempo un alto nivel de protección de esos derechos fundamentales.

transporte aéreo de pasajeros. Por lo que respecta a estos últimos delitos, la aplicación de este sistema no puede extenderse a delitos que forman parte de la delincuencia común con arreglo a las particularidades del sistema penal nacional (apartado 152)[30].

En la medida en que la Directiva PNR prevé la posibilidad a los Estados miembros de extender su aplicación a todos o parte de los vuelos interiores de la Unión, debe quedar limitada a lo estrictamente necesario. Únicamente si un Estado miembro constata la existencia de circunstancias suficientemente concretas para considerar que se enfrenta a una amenaza terrorista que se revela real y actual o previsible, la aplicación de esta Directiva a todos los vuelos interiores de la Unión con origen o destino en este Estado miembro, por un período de tiempo limitado a lo estrictamente necesario, si bien prorrogable, no debe exceder los límites de lo estrictamente necesario (apartado 171)[31]. Cuando no exista tal amenaza terrorista, la aplicación de dicha Directiva no puede extenderse a la totalidad de los vuelos interiores de la Unión, sino que debe limitarse a los vuelos interiores de la Unión que cubran determinadas conexiones aéreas o que respondan a planes de viaje o que se refieran a determinados aeropuertos respecto de los que existen, según la apreciación del Estado miembro de que se trate, indicios que permitan justificar esa aplicación (apartados 173 y 174)[32]

---

[30] Apartado152 de la sentencia: "Por lo tanto, incumbe a los Estados miembros garantizar que la aplicación del sistema establecido por la Directiva PNR se limite de manera efectiva a la lucha contra los delitos graves y que este sistema no se extienda a delitos que forman parte de la delincuencia común".

[31] Este apartado 171 de la referida resolución establece que: "Así, en una situación en la que se compruebe, sobre la base de la evaluación llevada a cabo por un Estado miembro, que existen circunstancias suficientemente concretas para considerar que este último se enfrenta a una amenaza terrorista que resulta real y actual o previsible, no parece que el hecho de que un Estado miembro prevea, en virtud del artículo 2, apartado 1, de esta Directiva, la aplicación dela Directiva PNR a todos los vuelos interiores de la Unión con origen o destino en este Estado miembro, por un período de tiempo limitado, sobrepase los límites de lo estrictamente necesario. En efecto, la existencia de dicha amenaza puede, por sí sola, establecer esa relación entre, de una parte, la transferencia y el tratamiento de los datos de que se trate y, de otra parte, la lucha contra el terrorismo (véase, por analogía, la sentencia de 6 de octubre de 2020, *La Quadrature du Net* y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 137).

[32] 173. En cambio, de no haber una amenaza terrorista real y actual o previsible a la que tenga que enfrentarse el Estado miembro de que se trate, no cabe considerar que la aplicación sin distinciones por parte de dicho Estado del sistema establecido por la Directiva PNR no solo a los vuelos exteriores de la Unión, sino también a todos los vuelos interiores de la Unión, se limite a lo estrictamente necesario.

174. En semejante situación, la aplicación del sistema establecido por la Directiva PNR a ciertos vuelos interiores de la Unión debe limitarse a la transferencia y al tratamiento de los datos PNR de los vuelos que cubran determinadas conexiones aéreas, que respondan a determinados planes de viaje o que conciernan a determinados aeropuertos respecto de los que existen indicios que permitan justificar esa aplicación. Corresponde al Estado miembro de que se trate, en tal situación, seleccionar

En resumen, los tratamientos previstos en normas como la Directiva PNR que suponen una injerencia grave en los derechos fundamentales de los ciudadanos por su carácter de vigilancia continua, no selectiva y sistemática, están justificados en la medida en que lo que se persigue es evitar delitos terroristas o delincuencia organizada grave. Es necesario, por tanto, una previa ponderación de los intereses en conflicto. El principio de proporcionalidad impide que esa injerencia tan intensa en el derecho fundamental a la protección de datos se realice para la prevención de la delincuencia común. Por tanto, la recopilación y utilización de esos datos solo estará justificada cuando sea estrictamente necesario, esto es, existan indicios, aunque sean indirectos, que permitan justificar la aplicación.

4.3. Aplicación de estos principios al sistema nacional derivado del artículo 25 de la LOPSC y el RD 933/2021

En este sentido, cabe señalar que la LOPSC, desarrollada en este sentido por el Real Decreto 933/2021, establece igualmente una vigilancia continua, no selectiva y automática de todas las personas que utilizan servicios de alojamiento turístico o alquilan vehículos a motor. Y ello está justificado en una finalidad general de seguridad pública, no para la persecución de las formas más graves de delincuencia como el terrorismo o la delincuencia organizada, sino también para la delincuencia común, lo que, en mi opinión, aplicando el principio de proporcionalidad al que se refiere la sentencia, tal y como esta lo interpreta, no supera el examen.

Es decir, la recopilación y tratamiento indiscriminado de toda la información de personas que utilizan servicios de alojamiento turístico o alquilan vehículos a motor no es proporcional y, por tanto, supone una vulneración del derecho fundamental a la protección de datos.

La aplicación de ese sistema cuando existan fundadas sospechas, aunque sea a través de indicios indirectos, de que se puedan cometer atentados terroristas o para evitar otras formas graves de delincuencia, como la organizada, sí estaría justificado y, por consiguiente, sería proporcional, sin que el derecho fundamental a la protección de datos sea vulnerado.

---

los vuelos interiores de la Unión en función de los resultados de la apreciación que debe efectuar con arreglo a los requisitos expuestos en los apartados 163 a 169 de la presente sentencia y volver a examinar periódicamente dicha situación en función de la evolución de las circunstancias que justificaron su selección, para garantizar que la aplicación del sistema instaurado por esa Directiva a los vuelos interiores de la Unión siga limitándose a lo estrictamente necesario.

5. BREVE REFERENCIA AL PLAZO DE CONSERVACIÓN DE LOS DATOS

5.1. Plazo de conservación previsto en la Directiva PNR según la sentencia del TJUE de 21 de junio de 2022

Respecto al plazo de conservación de los datos recopilados, la sentencia del TJUE establece que no se puede admitir una legislación nacional que prevea una duración general de conservación de estos datos de cinco años, aplicables a todos los pasajeros sin distinción. Así, el apartado 262 de la sentencia, establece:

> "…debe interpretarse en el sentido de que se opone a una normativa nacional que prevé una duración general de conservación de los datos PNR de cinco años, aplicable a todos los pasajeros aéreos sin distinción, incluidos aquellos respecto de los cuales ni la evaluación previa prevista en el artículo 6, apartado 2, letra a), de la Directiva PNR, ni las eventuales verificaciones realizadas durante el período de seis meses previsto en el artículo 12, apartado 2, de la referida Directiva, ni ninguna otra circunstancia han revelado la existencia de elementos objetivos que puedan demostrar la existencia de un riesgo en materia de delitos de terrorismo o de delitos graves que presenten un vínculo objetivo, cuando menos indirecto, con el transporte aéreo de pasajeros".

No se considera acorde a Derecho de la Unión, por vulneración del derecho fundamental a la protección de datos, la conservación sin más, sin ningún otro análisis o evaluación previa, de los datos de todos los ciudadanos, sin que existan elementos objetivos que permitan establecer algún tipo de conexión con la posibilidad de cometer atentados terroristas u otros delitos especialmente graves.

5.2. Plazo de conservación previsto en el Real Decreto 933/2021, de 26 de octubre

Según lo previsto en el artículo 5.3 de este Real Decreto, los datos del registro informático deberán conservarse durante un plazo de tres años a contar desde la finalización del servicio o prestación contratada.

Esta previsión, en mi opinión, tampoco cumple con la interpretación que hace el TJUE en su sentencia sobre la Directiva PNR. Y es que, como acabamos de ver, no es acorde a Derecho de la Unión establecer un plazo general de conservación sin más, es decir, sin realizar ningún tipo de justificación, análisis o evaluación previa que sirva de fundamento.

Cabe preguntarse, en este sentido, ¿Por qué tres años, y no dos, o cinco? ¿Se ha de conservar durante el mismo tiempo los datos de un delincuente condenado por delito grave que los de un ciudadano que no cometido delito alguno?

El Real Decreto 933/2021, de 26 de octubre, no hace esfuerzo alguno por justificar ese plazo de conservación ni por delimitar aquella información que, por la existencia de elementos objetivos, permita un plazo mayor de conservación, si se estima oportuno.

Esto vulnera el derecho fundamental a la protección de datos y, por tanto, debe ser derogado o declarado nulo mediante sentencia.

6. EL ALTO ESTÁNDAR GARANTISTA EXIGIDO POR EL TRIBUNAL CONSTITUCIONAL FEDERAL ALEMÁN PARA EL TRATAMIENTO DE DATOS POR AUTORIDADES POLICIALES

No puedo dejar pasar la ocasión sin referirme, si quisiera sucintamente, a la reciente sentencia del Tribunal Constitucional de Alemania de 16 de febrero de 2023 (1 BvR 1547/19, 1 BvR 2634/20) de la primera cámara del Tribunal Constitucional Federal (TCF), por la que se anulan dos leyes: la ley de Hesse sobre seguridad y orden público (HSOG), versión del 25 de junio de 2018 y la Sección 49 de la Ley de Procesamiento de Datos de la Policía de Hamburgo (PolDVG) en versión de 12 de diciembre de 2019[33].

Llama la atención como en dos países en los que se aplica el mismo marco jurídico sobre protección de datos, se llega a conclusiones tan diferentes sobre lo que pueden o no hacer las autoridades policiales. Bien en es cierto que el Real Decreto 933/2021, de 26 de octubre, no ha sido impugnado y, por tanto, el Tribunal Supremo no ha tenido ocasión de pronunciarse sobre su legalidad. Y sería injusto decir que los más altos tribunales españoles no son garantistas con el derecho fundamental a la protección de datos. Basta referirse a la sentencia 290/2000, 17/2013 o 76/2019, de 22 de mayo, todas de nuestro Tribunal Constitucional. Y lo mismo ha de decirse del Tribunal Supremo.

Pero lo cierto es que, más allá de las protestas de los profesionales de la hostelería y del alquiler de vehículos por las cargas administrativas y costes económicos que supone, no ha habido una atención seria por parte de la sociedad civil sobre lo que la recopilación de esos datos por parte de la policía puede suponer. Sobre todo, si se utilizan instrumentos de reconocimiento biométrico o inteligencia artificial.

Y es que, como digo, el Tribunal Constitucional Federal declara la inconstitucionalidad de las leyes mencionadas en tanto en cuanto no respetan los derechos fundamentales de los ciudadanos. Y fija unos patrones de referencia muy rigurosos sobre lo que los *Lander* pueden o no hacer en materia de tratamiento de la información, aunque sea para proteger la seguridad pública.

---

[33] Un análisis de estas resoluciones puede encontrase en L. Cotino Hueso (2023), "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial", *op. cit*.

Las comparaciones pueden resultar, a veces, muy antipáticas. Pero en la medida en que nos ayudan a mejorar, pienso, no deben dejar de hacerse. Sobre todo, cuando están en juego la garantía y la calidad de nuestros derechos fundamentales.

CONCLUSIÓN

En ocasiones, la inercia de otros tiempos hace que se mantengan determinadas obligaciones que, en el contexto jurídico actual, chirrían con estrépito. Es lo que ocurre, por ejemplo, con el Real Decreto 933/2021, de 26 de octubre, por el que se establecen las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor que, pese a su reciente aprobación, no viene sino a reproducir comportamientos de un Estado que ya están completamente superados.

El derecho fundamental a la protección de datos, reconocido en el derecho originario europeo, está en constante evolución y exige a los Estados miembros estar a la altura de las circunstancias. Bien es cierto que no es un derecho absoluto y, en ocasiones, se moldea ante derechos o intereses dignos, igualmente, de la más alta protección. Por ejemplo, la seguridad pública. En estos casos, los Estados deben delimitar, con precisión quirúrgica, hasta donde llega su poder frente al ciudadano para evitar daños mayores.

Así lo ha reconocido el TJUE a lo largo de una ya consolidada jurisprudencia que se ha ido desarrollando a lo largo de los últimos años. No vale cualquier cosa, nos viene a decir el más alto Tribunal europeo. Está bien que, a veces, un derecho fundamental como el de protección de datos pueda ceder para evitar atentados terroristas o graves formas de delincuencia organizada. Pero solo en esos supuestos. Lo que no está justificado es el uso del poder estatal, con sus potentes y devastadores instrumentos, para evitar cualquier forma de delito o, incluso, como se ha demostrado en los últimos años, con finalidades más espurias.

Este derecho fundamental, el de protección de datos, merece un esfuerzo por parte del Estado para justificar su invasión. Esto es, precisamente, lo que no hace el Reino de España en el Real Decreto 933/2021, de 26 de octubre, pues permite tratamientos masivos de datos personales, con tecnologías de la información, con una justificación absolutamente genérica: la seguridad pública. No supera esta norma las más básicas pruebas sobre minimización o proporcionalidad en el tratamiento de datos, y el Estado ni siquiera ha hecho un esfuerzo por intentarlo. Ni una evaluación de impacto si quiera, como le exige la normativa y le recordó, en su momento, la AEPD a través de un informe. Y tanta información, y recopilada de manera sistemática, y sin distinción sobre los posibles antecedentes penales del titular de los datos. En definitiva, y en mi opinión, un despropósito en un contexto tan garantista con

el derecho fundamental a la protección de datos, en el que la Unión Europea se ha erigido como modelo internacional.

Mantener la vigencia de este Real Decreto que, según entiendo, vulnera el derecho fundamental reconocido en el artículo 8 de la CDFUE. Atenta, frontalmente, contra el Derecho de la Unión, por lo que el Gobierno debería derogarlo o modificarlo, sustituyéndolo por uno más acorde a la jurisprudencia mencionada.

Se debe recordar, para finalizar, que en la medida que el derecho fundamental a la protección de datos personales está reconocido en el artículo 8 del CDFUE, y la Unión tiene competencia para el desarrollo legislativo del mismo (artículo 16 del TFUE), tal y como ha hecho con las normas más arriba mencionadas, el control de constitucionalidad de las normas nacionales en relación al derecho fundamental referido corresponde al TJUE, quien interpretará y definirá los límites del derecho y la validez de las normas a través de su jurisprudencia.

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018), N/REF: 175906/2018,

AYLLÓN SANTIAGO, H. S., y FERNÁNDEZ GONZÁLEZ, C. M., (2021), *Tratamiento de datos de carácter personal en el ámbito policial*, Reus.

BALLESTEROS MOFFA, L. A. (2020), *Las fronteras de la privacidad: el conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica*, Comares

BAYÓN MARINÉ, F., (Dir.), (1999), 50 años del turismo español. Un análisis histórico y estructural, Ramón Areces

CATALINA BENAVENTE, Mª. A., (2022), *El uso de los datos PNR en el proceso penal*, Aranzadi.

COTINO HUESO, L., (2023), "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, 64

FUERTES, M., (2022), *Metamorfosis del Estado. Maremoto digital y ciberseguridad*, Marcial Pons

GOSÁLBEZ PEQUEÑO, H. y BUENO ARMIJO, A. M., (2023) *Desregulación y regulación de la economía colaborativa en la actividad turística y las actividades con incidencia turística*, Thomson Reuters Aranzadi.

LÓPEZ RAMÓN, F (2018), "La calificación de los vicios de los reglamentos", Revista de Administración Pública, 205

MARTÍN REBOLLO, L., (2019), De nuevo sobre la invalidez en el derecho público, con particular referencia a la invalidez de los reglamentos. (Una reflexión abierta y algunas propuestas). *Revista de Administración Pública*, 210

MORENO GARRIDO, A. (2007), *Historia del turismo en España en el siglo xx*, Síntesis.

NAVARRO MEJÍA, I., (2021), "La falta de transposición de una directiva europea en materia reservada a ley orgánica: Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea de 25 de febrero de 2021. Asunto C-658/19", *Revista de las Cortes Generales,* (111)

PIÑAR MAÑAS, J. L. (2016), *El Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos*, Reus.

PIÑAR MAÑAS, J. L., (2009), "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio", Documento de trabajo 147/2009, *Fundación Alternativas*

QUINTANA JIMÉNEZ, A., (2019), "El control policial en los alojamientos de uso turístico y su incidencia en la seguridad", *Revista Internacional de Derecho del Turismo. RIDETUR*, 3.

RECUERDA GIRELA, M. Á., *Anuario de Derecho Administrativo 2020*, Aranzadi.

TOLOSA TRIBIÑO, C. (2019), "La invalidez de los reglamentos. En particular, el efecto invalidante de los vicios de procedimiento", *Revista de Administración Pública,* 210