# El derecho aéreo entre lo público y lo privado

## Aeropuertos, acceso al mercado, drones y responsabilidad

Mª Jesús Guerrero Lebrón
Juan Ignacio Peinado Gracia
(Directores)

Isabel Contreras de la Rosa
(Coordinadora)

El derecho aéreo entre lo público y lo privado: aeropuertos, acceso al mercado, drones y responsabilidad.
Mª Jesús Guerrero Lebrón, Juan Ignacio Peinado Gracia (Directores) ; Isabel Contreras de la Rosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2017. ISBN 978-84-7993-331-9. Enlace: http://hdl.handle.net/10334/3824

# REGISTRO DE PASAJEROS AÉREOS EN LA UE. REFORMAS NORMATIVAS

**Trinidad Vázquez Ruano**
*Profesora Contratada Doctora (Acred. T.U.)*
*Derecho mercantil*
*Universidad de Jaén*

**Alessia Buggea**
*Derecho mercantil*
*Universidad de Jaén*

**Resumen.**
Los datos de carácter personal de los pasajeros es un tema que ha presentado en la práctica del transporte aéreo cierta polémica, en particular respecto de la transferencia internacional de dicha información, la cual se justifica en razones de seguridad pública y defensa. Esencialmente, en lo que respecta a la lucha contra los actos terroristas y la delincuencia armada. El objeto del presente trabajo se centra en el análisis de los cambios legislativos en materia de protección de datos de carácter personal producidos en el marco del ordenamiento europeo. Nos referimos, en concreto, a 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[1]; así como, a la Directiva 2016/680 sobre la protección de las personas físicas en cuanto 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[2]; y a la Directiva 2016/681, sobre registro de datos de pasajeros aéreos (PNR o Pas-

1. Reglamento (UE) 2016/679, del Parlamento europeo y del Consejo, de 27 de abril, 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 (DOUE L 119, de 4 de mayo. Reglamento general de protección de datos).
2. Directiva 2016/680, del Parlamento europeo y del Consejo, de 27 de abril, 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

senger Name Record) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, tendente a facilitar una mayor seguridad.

**Palabras clave.**

Tutela del pasajero aéreo, datos de carácter personal, tratamiento y registro de datos, seguridad nacional.

**Sumario.**



## 1. La protección de los datos personales de los pasajeros aéreos

### 1.1. Referencias normativas básicas

La rápida evolución de las tecnologías de la información y de la comunicación, al igual que la globalización ha hecho prever nuevos desafíos en materia de protección de datos de carácter personal. En la actualidad, la recogida, el tratamiento e intercambio de información personal ha alcanzado niveles significativos y el uso de instrumentos tecnológicos y telemáticos como las cámaras digitalizadas, la localización de terminales telefónicos móviles y las diversas herramientas de comunicación, entre las que se encuentran las redes sociales, se ha generalizado.

de sanciones penales, y a la libre circulación de dichos datos (DOUE L 119, de 4 de mayo) y por la que se deroga la Decisión Marco 2008/977/JAI. Antecedente directo de este texto normativo es la Posición (UE) 5/2016 del Consejo de 8 de abril de 2016, con vistas a la adopción de una Directiva del Parlamento Europeo y del Consejo 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 (2016/C 158/01).

En el momento en que la difusión del uso de la red de redes, Internet, estaba en su apogeo entró en vigor un marco normativo sobre la protección de los datos personales en el ámbito comunitario. Nos referimos, a la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[3]. Dicho texto ha sido referencia europea en lo que concierne a la tutela de los datos de carácter personal de los sujetos, si bien su contenido sufrió algunas modificaciones posteriores[4]. La nota de relevancia de esta primera norma en la materia fue la creación de un marco regulador destinado a establecer un equilibrio entre la tutela de la vida privada de las personas y la libre circulación de los datos personales dentro de la UE, razón que llevó a determinar restricciones en cuanto a la recogida y utilización de los datos personales y la imposición a los Estados miembros de que concretasen el organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de la información personal.

La norma indicada define el dato de carácter personal como *cualquier información concerniente a personas físicas identificadas o identificables*[5]. Por lo que, no sólo se trata de las informaciones que habitualmente identifican a los sujetos, sino también de aquellas otras que, si bien en un principio no lo hacen de forma directa, si es posible que a posteriori o en relación con otros datos permitan hacerles identificables. En igual sentido, el tratamiento de datos de carácter personal es un concepto amplio que abarca cualquier actuación o proceso técnico que, con independencia de que se realice de manera automatizada o no[6], hace posible que

3. Directiva 95/46/CE, del Parlamento europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOUE L 281, de 23 de noviembre).

4. Tal es el caso de la reforma impuesta por la aprobación del Reglamento (CE) 1882/2003, del Parlamento Europeo y del Consejo, de 29 de septiembre, sobre la adaptación a la Decisión 1999/468/CE del Consejo de las disposiciones relativas a los comités que asisten a la Comisión en el ejercicio de sus competencias de ejecución previstas en los actos sujetos al procedimiento establecido en el artículo 251 del Tratado CE (DOUE L 284 de 31 de octubre).

5. Art. 2 a) de la Directiva 95/46/CE.

6. Arts. 2 b) de la Directiva 95/46/CE.

la información que ostenta la categoría de personal pueda recopilarse, grabarse y conservarse e, incluso, que se modifique, bloquee o cancele. Incluyéndose, asimismo, los supuestos en los que dicha información es objeto de cesión a terceros. No cabe duda que las informaciones solicitadas por las compañías aéreas a los pasajeros ostentan la categoría de datos de carácter personal en los términos de la norma. La recopilación del nombre y apellidos de los pasajeros, la fecha de nacimiento, el número de identificación fiscal, la dirección postal o el número de teléfono móvil o fijo son datos que permiten identificar de manera directa al sujeto al cual pertenecen. Siendo la compañía aérea que recoge esta información la encargada de su tratamiento.

No obstante lo anterior, el intercambio de información a través de servicios públicos de comunicaciones electrónicas como la red Internet y los terminales de telefonía móvil y fija, hicieron necesario un nuevo texto normativo para asegurar el derecho de los usuarios a la protección de la intimidad y la confidencialidad de sus comunicaciones, lo que llevó al legislador comunitario a aprobar la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas[7]. El objetivo esencial de esta norma que complementa a la anterior es garantizar la seguridad en el tratamiento de los datos de carácter personal, la notificación de las posibles vulneraciones y la confidencialidad de las comunicaciones intercambiadas. En este sentido, no sólo se prohíben las comunicaciones no solicitadas en las que el usuario no hubiera manifestado su conformidad al respecto, sino además se exige a los proveedores de servicios de comunicaciones que garanticen que sólo las personas autorizadas tienen acceso a los datos personales, que los protejan ante pérdidas o alteraciones accidentales y otros tratamientos ilícitos; así como, que apliquen una política de seguridad sobre el tratamiento de los datos de carácter personal. Por su parte, corresponde a los Estados miembros asegurar la confidencialidad de las comunicaciones realizadas a través de las redes públicas, lo que significa que se han de prohibir las escuchas, interceptaciones, almacenamientos o que se sometan a cualquier tipo de vigilancia o interrupción sin el consentimiento

7. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DOUE L 201, de 31 de julio, Directiva sobre la privacidad y las comunicaciones electrónicas).

de los usuarios, salvo si la persona está autorizada legalmente a hacerlo y, a su vez, respeta unos requisitos específicos; y que se asegure que únicamente es posible el almacenamiento de información o el acceso a la ya almacenada en el equipo personal del abonado si recibe la información clara y completa y tiene la posibilidad de manifestar su rechazo u oposición. Pese a lo indicado sobre los extremos necesarios, la norma no impide que las disposiciones nacionales restrinjan estas facultades si ello resulta necesario y es proporcional para proteger intereses públicos específicos, como es el caso de las investigaciones de actividades delictivas o la tutela de la seguridad nacional, la defensa o la seguridad pública.

Sin embargo, los últimos atentados y ataques terroristas sufridos a nivel internacional y comunitario han hecho replantear la tutela de la información de carácter personal en el marco de la UE, esencialmente a fin de alcanzar el equilibrio entre la salvaguarda de la intimidad de las personas y la adecuación de los cambios a la realidad del momento. En la medida en que se precisa la obtención y tratamiento de la información personal a efectos de seguridad y defensa de los intereses generales[8]. Ello ha hecho que se aprueben nuevos textos normativos que son el objeto de estudio en el presente trabajo y de cuyo análisis nos ocupamos seguidamente. Hacemos referencia al 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, y a las Directivas 2016/680 sobre la protección de las personas físicas en cuanto al tratamiento de los datos personales para usos judiciales y/o policiales y 2016/681 en lo que afecta al registro de los datos de pasajeros aéreos (PNR). La nueva regulación aprobada en el seno de la UE establece los principios de necesario cumplimiento en materia de protección de la información de carácter personal y, además, incluye previsiones específicas en cuanto al intercambio de datos transfronterizos dentro de la UE y los estándares mínimos a observar en relación con el tratamiento de los mismos en cada país.

8. Para ampliar la información, *vid.* AA.VV. (2015), *Hacia un nuevo derecho europeo de protección de datos: Towards a new european data protection regime,* (Coord. RALLO LOMBARTE, A./ GARCÍA MAHAMUT, R.), Valencia; y AA.VV. (2015), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, (Dir. COLOMER HERNÁNDEZ, I. Coord. OUBIÑA BARBOLLA, S.), Pamplona.

### 1.2. El necesario registro de los datos personales de los pasajeros (*Passenger Name Record*. PNR)

Los ataques sufridos en Estados Unidos en el 2001 hicieron incrementar las exigencias de control de los datos de los pasajeros y tripulantes de los transportes aéreos que afectan a dicho territorio y que se fundan en la prevención y lucha contra el terrorismo, hecho que también influyó en el ámbito comunitario[9]. Así, la UE sintió la necesidad de crear un régimen de protección de la seguridad y garantía pública. Esto es, de promover una política de armonización tendente a limitar el terrorismo, en particular, a través de la creación de un registro de datos personales de cada viajero (*Passenger Name Record*) y prever la intervención y colaboración de las autoridades de los Estados miembros en la comprobación sistemática de esos datos e informaciones.

No obstante dicha exigencia, la pretensión de la Euro-cámara no fue clara a este respecto, en cuanto que se plantearon ciertas cuestiones y aspectos controvertidos, básicamente en lo que hace a la protección de la intimidad de los datos de los pasajeros que las compañías aéreas almacenan y del riesgo que supone que dicha información supere los simples datos biográficos de los mismos (datos API o *Advance Passenger Information*[10]). Por cuanto, las instituciones norteamericanas tratan de acceder directamente a una serie de datos personales e informaciones sobre los pasajeros y tripulantes, así como disponer de ellos durante cierto tiempo en el que, además, se los pueden ceder a las aduanas y a

9. Nos referimos a la obligación impuesta por parte de las autoridades a las compañías aéreas de ofrecer al *Department of Homeland Security* acceso electrónico a ciertos datos de los pasajeros. *Vid.* VÁZQUEZ RUANO, T. (2014), "Transferencia internacional de datos personales en el transporte aéreo. La Custom Border Protetion en el sistema USA", *Rivista Diritto dei Trasporti*, número especial, 1, págs.115-131.

10. Art. 18 y Anexo I de la Directiva 2016/681. Ello puede suponer una infracción a lo dispuesto en los arts. 7, 8.1 y 21 de la Carta de Derechos Fundamentales de la UE y en el art. 16 del Tratado de Funcionamiento de la UE. Hay diversas categorías de datos y que implican una mayor invasión de la esfera personal de la persona, así el art. 9 del Reglamento general en materia de protección de datos alude al tratamiento de datos personales especialmente sensibles o "categorías especiales de datos", como lo son: los datos vinculados al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la salud, la vida sexual, la afiliación sindical, de naturaleza genética o biométrica. El tratamiento de estos datos sólo será posible cuando esté autorizado por el derecho de la UE o un Estado miembro, sea preciso para proteger los intereses vitales del afectado, o el propio interesado los haya hecho públicos de forma manifiesta.

diversas autoridades gubernamentales. De hecho, la Comisión europea se ha mostrado reacia en este sentido porque implica un refuerzo de la posición de la UE sobre la protección de los datos personales en el marco de sus políticas y, al mismo tiempo, la determinación de un sistema armonizado al respecto resulta complejo[11]. En esta línea argumental, ya se manifestó la Directiva 2004/82/CE, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas[12]. Por dicha regulación se ha exigido a los transportistas aéreos, previa petición de las autoridades encargadas del control de las personas en las fronteras exteriores, comunicar los datos de los pasajeros (API) que se dirijan a un paso fronterizo de la UE. La información que ha de facilitarse hace referencia a los siguientes datos biográficos: el número y clase del documento de viaje utilizado, la nacionalidad, el nombre y la fecha de nacimiento del pasajero, el paso fronterizo utilizado para acceder a la UE, las horas de salida y llegada del transporte y el número total de personas transportadas. Aunque, se precisa que dichos datos sean eliminados a las veinticuatro horas después de su envío, en cuanto los pasajeros hayan entrado en el territorio de los Estados miembros. Por su parte, corresponde a la entidad transportista borrar los datos personales veinticuatro horas después de la llegada del medio de transporte al destino. A pesar de ello, hay que señalar que los datos oficiales API son datos referidos únicamente al

11. La transferencia internacional de datos de carácter personal entre la UE y los EE.UU. se halla marcada jurídicamente por la Decisión 2000/520/CE de la Comisión, de 26 de julio sobre la adecuación de la protección conferida por los Principios de Puerto Seguro (*Safe Harbor*) para la protección de la vida privada y las correspondientes preguntas más frecuentes (*Frequently Asked Questions –FAQs-*), publicadas por el Departamento de Comercio de Estados Unidos de América (DOUE L 215, de 25 agosto). *Vid.* VÁZQUEZ RUANO, *op.cit.,* págs.120-129. Sin embargo, el TJUE en su Sentencia de 6 de octubre de 2015 (Asunto C 362/14. ECLI:EU:C:2015:650) ha anulado dicha Decisión. En consecuencia, se permite a las Agencias nacionales de Protección de Datos de la UE la posibilidad de examinar si la entidad o lugar al que se destinan los datos de carácter personal, es fiable. Entendiendo por "nivel de protección adecuado" que el tercer país garantice efectivamente un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al de la UE.

12. 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 (DOUE L 261 de 6 de agosto), adoptada tras los atentados de Madrid y complementaria al art. 26 del Acuerdo de Schengen de 14 de junio de 1985, perfeccionado por la Directiva 2001/51/CE del Consejo, de 28 de junio de 2001 (DOUE L 87 de 10 de julio) que se aplica en caso de denegada entrada por un Estado miembro a los nacionales de terceros países.

pasajero y que figuran en la parte de lectura óptica del pasaporte, permitiendo la identificación de terroristas y delincuentes conocidos mediante la utilización de sistemas de alerta; mientras que la información de los datos PNR está conformada por un conjunto más amplio de elementos. Ya que pertenecen a una base de datos del sistema de reservas de la línea aérea que cuenta con información del pasaje y del pasajero y también con otros datos del viaje y su organización que ofrece el propio afectado.

Junto a estas previsiones normativas, se aprobaron diversos textos en materia de protección de los intereses de los titulares de los datos de carácter personal en el marco comunitario[13], pero adelantamos que ninguno de ellos consiguió garantizar un sistema estable en la materia objeto de nuestro estudio. En 2007, la Comisión propuso la adopción de la Decisión marco del Consejo 2007/0237 (CNS), sobre utilización de datos del registro de nombres de los pasajeros con fines represivos[14], la cual pretendía establecer una armonización de las disposiciones de los Estados miembros sobre el deber de las compañías aéreas de transmitir, como mínimo, los datos PNR a las autoridades competentes cuando realizasen vuelos hacia o desde el territorio de un Estado de la UE, lo cual estaba justificado en la prevención de atentados terroristas y la delincuencia organizada.

La entrada en vigor en 2009 del Tratado de Lisboa introdujo nuevas condiciones respecto de las garantías y tratamiento de los datos personales e hizo necesaria su sustitución, la cual se llevó a término con una nueva Propuesta de

13. Las ya mencionadas Directiva 95/46/CE relativa a la protección de datos, la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 , 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 por la que se modifica la Directiva 2002/58/CE (DOUE L 105, de 13 de abril. Esta norma fue anulada por el TJUE por constituir una injerencia de especial gravedad en la vida privada y la protección de datos) y el Reglamento (CE) 45/2001 del Parlamento y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOUE L 8, de 12 de enero). Así como, la Decisión Marco del Consejo, de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DOUE L 350, de 30 de diciembre).

14. Propuesta de decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) con fines represivos [SEC(2007) 1422. SEC(2007) 1453]. Bruselas 6 de noviembre de 2007 (COM(2007) 654 final).

Directiva que la Comisión presentó en 2011[15], sobre la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves. En este nuevo texto, se sigue la argumentación del anterior respecto de los datos PNR, aunque se puso de manifiesto el carácter comercial de la información que se registra sobre los pasajeros aéreos. Ha de tenerse en cuenta que los datos del registro de nombres de los pasajeros son facilitados por los propios titulares de manera directa, pero los recopilan y tratan las empresas que realizan el transporte aéreo y se utilizan en relación con los servicios que las mismas les ofrecen (sistemas de adquisición de billetes, realización de la reserva y la facturación del transporte). Por tanto, resulta preciso garantizar la adecuada protección de los derechos fundamentales y, en concreto, el derecho a la intimidad de los pasajeros aéreos, a pesar de que la finalidad que justifica su recopilación y tratamiento esté basada en razones de limitación del terrorismo y la delincuencia organizada. Así, se exige que los datos PNR se utilicen únicamente con una finalidad coercitiva y de seguridad, no siendo posible que con ellos se elaboren perfiles de los sujetos al margen de ese fin, se incumplan los períodos de conservación de los datos y se vulneren los principios de necesidad y proporcionalidad en el tratamiento de los mismos.

Las deficiencias del conjunto normativo existente y las cuestiones controvertidas que se plantearon desde su presentación, dieron paso a la Propuesta de Directiva sobre PNR europeo en abril de 2013, la cual fue rechazada por el Comité de libertades civiles del Parlamento Europeo en base a dos razones esenciales: la necesidad y proporcionalidad del sistema planteado sobre la recopilación de los datos de los pasajeros[16]. De un lado, por la desproporcionada cantidad de

15. Propuesta de Directiva del Parlamento Europeo y del Consejo 2011/0023, de 2 de febrero de 2011, relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves (Bruselas, 2 de febrero de 2011. COM(2011) 32 final. 2011/0023 (COD) C7-0039/11). Disponible en el recurso electrónico: <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2011)0032_/com_com(2011)0032_es.pdf>.

16. Resolución del Parlamento Europeo de 23 de abril de 2013. Resulta de interés la consulta de la declaración de los miembros del Consejo Europeo tras la reunión de los Jefes de Estado y Gobierno, Bruselas, de 12 de febrero de 2015, en relación con las propuestas PNR de la UE (disponible en el recurso electrónico: <http://www.consilium.europa.eu/es/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/> y el Informe sobre la aplicación de las medidas del Coordinador de la lucha

información que la Comisión se proponía incluir en la base de datos sobre los pasajeros aéreos. Y, de otro, por el período de tiempo establecido durante el que esos datos se podían almacenar y tratar. Finalmente, ha sido cinco años después de la primera versión de Propuesta de Directiva del Parlamento Europeo y del Consejo, cuando se ha aprobado la nueva normativa en la materia y que es objeto de nuestro análisis. La Comisión Europea no ha querido sino que los Estados miembros cuenten con un conjunto homogéneo de normas y principios para acometer la lucha contra el terrorismo, los atentados, el contrabando de drogas, el tráfico de seres humanos y, a su vez, que se garantice el respeto de la privacidad y el cumplimiento de los derechos de los pasajeros del transporte aéreo. De este modo, parece haberse conseguido un equilibrio entre la protección de la privacidad de los sujetos y la seguridad en la marco de la UE.

## 2. Aspectos esenciales de la reforma normativa en materia de protección de datos personales en la UE

La inseguridad y desconfianza social que ha surgido tras los últimos ataques terroristas en el ámbito comunitario ha hecho necesaria una reforma legislativa en materia de protección de datos de carácter personal para lograr un adecuado equilibrio entre la salvaguarda de la intimidad de los ciudadanos y la correcta adecuación de los cambios a la realidad del momento. Las novedades legislativas comunitarias prescriben diferentes niveles de obligatoriedad y diversos ámbitos sancionadores para cada tipología de destinatario. Teniendo en cuenta, al mismo tiempo, la continua evolución e implementación de las tecnologías de la información y la comunicación. Por tanto, se trata de una importante novedad normativa que afecta a los Estados miembros de la UE y que repercute en el ámbito telemático y de las nuevas tecnologías. Este último, precisa de un fortalecimiento de la seguridad y garantía sobre la adecuada digitalización y sistematización de la información relativa a cada persona física en particular.

antiterrorismo de la UE (disponible en el recurso electrónico: <http://data.consilium.europa.eu/doc/document/ST-9422-2015-REV-1/es/pdf>.

El derecho aéreo entre lo público y lo privado: aeropuertos, acceso al mercado, drones y responsabilidad.
Mª Jesús Guerrero Lebrón, Juan Ignacio Peinado Gracia (Directores) ; Isabel Contreras de la Rosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2017. ISBN 978-84-7993-331-9. Enlace: http://hdl.handle.net/10334/3824

La reforma normativa europea que nos ocupa en este trabajo presenta unos principios cuyo objetivo esencial es la utilización lícita, leal y trasparente de los datos de cada persona garantizando la armonización de las disposiciones en la materia. Se trata de una importante modificación legislativa que ha sido posible mediante el alcance de un compromiso europeo que ha permitido conseguir un equilibrio entre la exigencia de reforzar la seguridad y proteger los datos personales en una era digital, y en razón de la precisa necesidad de salvaguardar la seguridad pública ante actos delictivos. Siendo en este contexto en el que se sitúan las iniciativas legislativas sobre el tratamiento de los datos personales indicadas con anterioridad y que a continuación abordamos con mayor detenimiento.

### 2.1. 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) Referencia al ámbito de aplicación*

El Reglamento (UE) 679/2016 entró en vigor el 25 de mayo 2016 y será operativo en vía directa en los países miembros de la UE a partir del 25 de mayo de 2018. La norma deja un bienio de temporalidad para las adecuaciones necesarias a las propias políticas de tratamiento de datos de carácter personal, puesto que son numerosas las novedades introducidas en cuanto a las obligaciones organizativas, documentales, técnicas y de personal que los titulares del tratamiento, públicos y privados, tendrán que implementar. La finalidad esencial del Reglamento comunitario general sobre protección de datos es asegurar una aplicación coherente y homogénea de las normas de tutela y la libre circulación de los datos personales en toda la UE. Es decir, la pretensión de su contenido no es otra que determinar una disciplina sobre la protección de los datos personales uniforme en el ámbito comunitario, así como incrementar y establecer un coherente nivel de garantía de la referida información personal y suprimir los obstáculos en materia de circulación de estos datos en el panorama europeo.

El contenido normativo previsto se aplica desde la perspectiva material tanto a lo relativo al tratamiento efectuado en el ámbito digital, como al llevado a cabo

mediante medios análogos[17]. Por su parte, la nueva disciplina abarca territorialmente el tratamiento de los datos de las personas físicas efectuados por responsables o titulares del tratamiento establecidos en el seno de la UE y siendo independiente que el mismo se realice o no en dicho ámbito; y también a los tratamientos que, si bien se llevan a cabo por titulares pertenecientes a países externos a la UE, los sujetos que los ejercen se encuentran residiendo en territorio europeo[18].

Al respecto, es necesario aclarar que en lo que afecta a la primera categoría de sujetos, es decir a los titulares o responsables establecidos en el marco comunitario, resulta fundamental la definición de establecimiento. En este sentido, se trata de un concepto no vinculado a particulares requisitos formales, sino que es estrictamente conexo al lugar del efectivo desarrollo de la actividad, siendo suficiente la subsistencia de un establecimiento. Más compleja es, sin embargo, la interpretación relativa a la segunda categoría, en cuanto a los responsables que no siendo comunitarios se hallan en territorio de la UE, en cuyo caso la aplicación de la norma va a depender de que las actividades de tratamiento de información personal estén relacionadas con *la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago;* o con *el control de su comportamiento, en la medida en que este tenga lugar en la Unión.* Sobre ello, se especifica que para determinar si hay una oferta de bienes o servicios conviene verificar, en concreto, si el titular tiene intención de ofrecer bienes y servicios en la UE y es irrelevante a tal fin la existencia o no de pago de una contraprestación. En lo que hace a las actividades electrónicas se precisa, además, que la mera accesibilidad a la página web, a un correo electrónico u otras coordenadas de contrato o el uso de un idioma habitualmente utilizado, son elementos insuficientes para comprobar la intencionalidad referida. No obstante, factores como el uso de un idioma o de la unidad de moneda de un Estado miembro, la posibilidad de ordenar bienes o servicios en el idioma de un Estado miembro, la mención de clientes que se encuentran en la UE, pueden subrayar la intención de ofrecer bienes y servicios a los interesados. En definitiva, se trata de una determinación genérica que amplía notablemente el ámbito de aplicación de la norma.

17. Art. 2.1º del Reglamento (UE) 679/2016.

18. Art. 3 del Reglamento (UE) 679/2016.

En lo que respecta a las particulares tipologías de tratamiento excluidas del ámbito de aplicación de este texto normativo, se encuentran las siguientes. En primer lugar, los datos relativos a personas fallecidas y, por otro lado, los datos tratados de forma anónima que no permiten la identificación del sujeto interesado. Por ende, los principios en materia de protección de datos no deben aplicarse a la información anónima, en cuanto que no guarda relación con una persona física identificada o identificable. Como aspecto novedoso y relevante, la norma denomina *seudonimización* o datos personales seudonimizados a los que se complementan con otra información adicional y, de este modo, pueden hacer a la persona identificable. Esto es, que permiten determinar la identidad del interesado (persona física) por su relación con otra información. Tal es el caso de datos como: el nombre, un número de identificación, datos de localización, un identificador en línea o elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de la misma.

*b) Nuevos principios y facultades del interesado*

El Reglamento general de protección de datos supone un refuerzo del derecho fundamental a la tutela de los datos personales de los sujetos que afianza el control que éstos pueden ejercer sobre la información que les pertenece. A este respecto, los principios fundamentales que caracterizan el lícito tratamiento de los datos de carácter personal en el ámbito comunitario engloban desde la legalidad del mismo, hasta la transparencia, pero con algunas notas novedosas[19].

La observancia del principio de legalidad del tratamiento implica que se considere lícito aquél en el que la información del interesado se trate cuando éste hubiera expresado su consentimiento de modo libre, específico, informado e inequívoco. Condicionantes que permiten afirmar que el consentimiento se ha ofrecido válidamente y a través de un acto afirmativo que sea reflejo de la manifestación de la voluntad del interesado[20]. Por tanto, no está permitido recabar

19. Arts. 5 a 11 del Reglamento (UE) 679/2016.

20. Al respecto, DAVARA RODRÍGUEZ, M. A. (2006), *Manual de Derecho Informático*, Pamplona, págs. 67-70; SERRANO PÉREZ, M. Mª. (2003), *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, págs. 433-460.

información personal que no se haga de manera leal o que se realice a través de mecanismos que sean contrarios a Derecho. Si bien, se impone además que el responsable del tratamiento pruebe la manifestación de la voluntad del titular de la información personal. Esta última apreciación hace referencia al principio de responsabilidad, lo que significa que compete al responsable del tratamiento la aplicación de las medidas adecuadas para que pueda confirmar la prestación del consentimiento por parte del interesado de manera correcta, salvo que el tratamiento sea necesario para la ejecución de un contrato, el cumplimiento de obligaciones legales, la realización por parte de su titular de una actuación de interés público o en el ejercicio de poderes públicos conferidos al responsable, y la persecución de un interés legítimo en donde no prevalezcan los derechos y libertades del sujeto interesado.

Por su parte, el principio de transparencia trae como consecuencia que el responsable del tratamiento informe de los extremos necesarios al interesado y que, en todo caso, ha de hacerse en *forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño.* La información que ha de facilitarse al interesado se centra en los siguientes extremos: la identidad del responsable del tratamiento y su finalidad y, en igual sentido, sobre los datos necesarios para que el tratamiento sea leal y transparente[21]. Así, se ha de informar acerca de los riesgos, normativa, salvaguardias y los derechos relativos al tratamiento de los datos personales. En consonancia con ello, se exige la necesidad de que la información o datos que se recopilen sean los mínimos en cuanto al fin que justifique dicho tratamiento y que la finalidad esté debidamente determinada, sea explícita y legítima, presupuestos que cabe entender como límites a la finalidad del tratamiento en beneficio del interesado. Ello exige, al mismo tiempo, que los datos sean exactos y estén actualizados y que se conserven únicamente durante el período necesario para alcanzar los fines del tratamiento y que no se destinen al cumplimiento de un objetivo distinto al previsto inicialmente, si el titular no lo ha autorizado con anterioridad. Por su parte, corresponde al responsable del tratamiento garantizar la

21. Sobre la materia véanse, entre otros: ALONSO MARTÍNEZ, C. (2002), *Protección de datos de carácter personal. El consentimiento en entidades financieras*, Madrid, págs. 130-131; DAVARA RODRÍGUEZ, *op.cit.,* pág. 86.

integridad y confidencialidad de la información objeto del mismo y la necesidad de que demuestre que ha cumplido con las exigencias indicadas. Debiendo informar al afectado en los casos en los que los datos personales han sido pirateados[22].

El interesado -que es titular de los datos que son objeto de tratamiento- tiene reconocidos en la norma comunitaria una serie de derechos[23]. En primer término, se mantiene la previsión de los ya conocidos como derechos *ARCO*. A saber: el derecho de acceso a los datos personales de su titularidad e informaciones particulares; el derecho de rectificación de las informaciones erróneas o inexactas sobre el mismo[24]; la posibilidad de su cancelación y el derecho de oposición que permite al interesado oponerse en cualquier momento al tratamiento de los datos personales[25]. No obstante, el ejercicio de esta última facultad no impide que el responsable pueda continuar con el tratamiento de la información, si acredita que existen motivos legítimos imperiosos para que el tratamiento prevalezca sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

A pesar de que el Reglamento mantiene las previsiones anteriores, reconoce dos novedades importantes en cuanto a la protección del afectado por el tratamiento de los datos de carácter personal. Nos referimos al denominado *derecho al olvido* que ha de entenderse como la efectiva facultad de suprimir los datos personales[26]; y al *derecho a la portabilidad de los datos* o el traslado de los datos

22. Arts. 13, 14, 24 del Reglamento (UE) 679/2016.

23. Arts. 12 a 21 del Reglamento (UE) 679/2016. En relación con los *derechos ARCO*: FREIXAS GUTIÉRREZ, G. (2001), *La protección de los datos de carácter personal en el derecho español*, Barcelona, págs. 60-62; SERRANO PÉREZ, *op.cit.,* págs. 78-80.

24. Art. 33 del Reglamento (UE) 679/2016.

25. Apartado 1º del art. 21 del Reglamento (UE) 679/2016.

26. Art. 17 del Reglamento (UE) 679/2016. Al respecto, consúltese la Sentencia del Tribunal de Justicia, (Gran Sala), de 13 de mayo de 2014, "*Google v. Spain*", Asunto C-131/12 (disponible en el recurso electrónico: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES>). Sobre la materia es de interés el artículo de LÓPEZ CALVO, J. (2016), "Sobre la aparente discrepancia entre las Salas de lo Contencioso y Civil del TS sobre derecho al olvido. Un problema de diferente visión sobre la congruencia entre pretensiones de las partes y fallo. Google Spain, al menos, como establecimiento de Google Inc.", *Sepin*. En esta materia, también interesa destacar los trabajos de: LÓPEZ PORTAS, Mª. B. (2015), "La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE",

personales a otro proveedor de servicios[27]. En lo que respecta a la previsión particular del derecho al olvido o de supresión se trata de la facultad del interesado *a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias…*", las cuales están relacionadas en el texto de la norma. De la definición reproducida se puede deducir la posibilidad de su ejercicio en diversos planteamientos: si el tratamiento de la información está subordinado a la prestación del consentimiento, la revocación del mismo constituye el requisito necesario a efectos de su cancelación; cuando los datos sean recogidos para finalidades o tipologías de tratamiento, la cancelación se podrá efectuar si los datos ya no son necesarios para perseguir los fines por los cuales fueron recogidos; cuando el afectado hubiera manifestado su oposición; en los supuestos en los que el tratamiento se haya llevado a cabo de manera ilícita; y la supresión basada en la observancia de una obligación legal. En cualquiera de estas posibilidades, compete al titular del tratamiento de los datos la obligación de cancelarlos de sus archivos y también de comunicárselo a terceros y a los diversos titulares. No obstante, queda al margen el caso en el que el tratamiento sea necesario tanto para ejercer el derecho a la libertad de expresión e información; como en cuanto al cumplimiento de una obligación legal que requiera dicho tratamiento, o que así se exija para el cumplimiento de una actuación realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; además, de por razones de interés público en el ámbito de la salud pública; o con fines de archivo público, investigación científica o histórica o fines estadísticos; y, cuando corresponda, para la formulación, el ejercicio o la defensa de reclamaciones.

La *portabilidad de datos* o el derecho a trasladar los datos a otro proveedor de servicios supone la facultad del interesado a obtener los datos personales tratados por el titular de manera gratuita, salvo en los casos en los que el tratamiento sea necesario para cumplimiento de una misión realizada en virtud del interés público o en el ejercicio de poderes públicos conferidos al responsable. La

Revista de derecho político, núm. 93, págs. 143-175; MURILLO DE LA CUEVA, P. L. (2007), "Perspectivas del derecho a la autodeterminación informativa", IDP: revista de Internet, derecho y política, núm. 5.

27. Art. 20 del Reglamento (UE) 679/2016.

facilitación de la información personal ha de hacerse en un formato estructurado, que sea de uso común y permita su lectura mecánica. Esencialmente porque la finalidad de obtener dicha información personal va a ser la de su entrega o comunicación a otro responsable del tratamiento. La excepción a la gratuidad se establece cuando el interesado solicite más copias de los datos objeto de tratamiento, pues en ese supuesto el titular podrá pedir el reembolso de los gastos administrativos que ello le ha generado.

Junto a lo mencionado, la protección de los datos personales implica que se asegure un límite de plazo de su conservación, por lo que será el responsable el que determine los plazos para su supresión o revisión periódica. En cuanto a la facultad de limitación del tratamiento se ejerce por parte del interesado en la medida en que cuestione la exactitud de los datos personales; en los casos en los que el tratamiento sea ilícito y el interesado se oponga a la cancelación de los datos, pidiendo la limitación de su utilización; cuando los datos ya no sean necesarios para la finalidad del tratamiento, pero sí precisos para su titular; y cuando el interesado se haya opuesto al tratamiento, mientras se confirma que los motivos legítimos del responsable prevalecen sobre los del afectado[28].

Además del respeto de los referidos principios, la norma impone una serie de obligaciones de necesario cumplimiento al titular del tratamiento de los datos personales[29], de entre las que destacamos la de adoptar y actualizar las medidas técnicas y organizativas que sean precisas para asegurar dicha información y que se plasmarán en el documento de seguridad elaborado a tal fin. Así, la adopción de estas medidas implica que los datos personales recopilados en los ficheros no se modifiquen, extravíen o, en su caso, se acceda a ellos o se traten por terceras personas que no estuvieran autorizadas. En definitiva, compete a la compañía aérea la adopción de las medidas de naturaleza técnica y organizativa que sean necesarias para garantizar la seguridad de los datos proporcionados por los pasajeros. En este supuesto, en cuanto que es un tratamiento de datos personales de carácter básico, dichas medidas serán las que se refieren a ese mismo nivel en relación con las funciones y deberes que ha de cumplir el personal del responsable del tratamiento; así

28. Arts. 13, 14, 24 del Reglamento (UE) 679/2016.

29. Arts. 24 a 43 del Reglamento (UE) 679/2016.

como, el registro de las incidencias que se hubieran observado y las medidas aplicadas para solventarlas, el control de acceso a la información y la gestión de los soportes que la contengan y, por último, la realización de copias de seguridad.

### 2.2. Previsiones jurídicas contenidas en la Directiva 2016/680 en cuanto al tratamiento de datos personales por autoridades competentes en materia de comisión de hechos delictivos

La Directiva 2016/680, relativa a la protección de las personas físicas en materia de tratamiento de datos personales por las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, está interconectada con la aprobación del texto del Reglamento referido con anterioridad. El contenido normativo que nos ocupa guarda relación, por tanto, con el Reglamento general de protección de datos, en cuanto que rige de modo particular el tratamiento de los datos de las personas en relación con la comisión de hechos delictivos a nivel europeo y se aplica al intercambio de datos transfronterizos dentro de la UE. Razón por la que su fundamento es redefinir una disciplina europea sobre la protección de los datos de carácter personal de manera uniforme en todos los países miembros de la UE, en particular respecto a la transmisión de datos para cuestiones judiciales y policiales. Quedando fuera de su ámbito de aplicación las actividades de seguridad nacional.

El objeto de la Directiva fundamentalmente se centra en la disciplina del tratamiento de los datos de carácter personal de los usuarios por parte de las autoridades competentes para la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos en el seno de la UE y, en su caso, en la posible trasmisión de los mismos al extranjero[30]. Pues, como es sabido, las autoridades propias de los Estados miembros están afiladas y colaboran con la Organización Internacional

30. La presente Directiva, ya en vigor, tiene que ser ejecutada por los ordenamientos de los Estados miembros dentro de mayo 2018 (art. 1 de la Directiva). Sin embargo, se prevén excepciones específicas (art. 63 de la Directiva) que permiten aplazar tal fecha a mayo de 2023 o de 2026.

de Policía Criminal intercambiándose datos e informaciones de los sujetos[31]. Esta Organización se ocupa de recopilar, almacenar y difundir información para ayudar a las autoridades competentes a prevenir y combatir la delincuencia internacional. Por ello, es preciso el refuerzo de su cooperación y que se lleve a cabo un intercambio eficaz de datos personales, protegiendo los derechos y libertades fundamentales en relación con el tratamiento de los mismos. Así, el motivo de la aprobación de esta nueva norma reside en la necesidad de establecer nuevas garantías en materia de transmisión de datos que hasta el momento se ha caracterizado por ser inseguro si atendemos a la desproporcionada cantidad de medios telemáticos utilizados tanto por personas físicas, como por empresas privadas o autoridades públicas para el intercambio de información personal. Sin embargo, dicha tecnología permite la implicación de las autoridades de policía y de las judiciales en la lucha contra el terrorismo internacional y, más concretamente, contra la criminalidad. Haciéndose necesario el equilibrio entre ambos intereses contrapuestos, a fin de que la recopilación y tratamiento de los datos de carácter personal se haga con la debida garantía.

En este sentido, la norma comunitaria recoge no sólo los derechos de los interesados que son los titulares de los datos e informaciones que se tratan, sino también el elenco de obligaciones que necesariamente han de respetar y observar los responsables y encargados del tratamiento de los datos, las medidas de seguridad aplicables en cada caso o la creación por parte de cada Estado miembro de una autoridad independiente y autónoma de control que, al mismo tiempo, colabore con la del resto de Estados miembros en el intercambio de información. Los principios fundamentales que han de observarse en el tratamiento y trasferencia de datos se concretan en los siguientes[32]: el tratamiento lícito y leal de la información de carácter personal, en el sentido de que sea necesario para el desempeño de una función de interés público realizada por una autoridad competente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales

31. Organización Internacional de Policía Criminal. *Vid.* AA.VV. (2015), *La transmisión…op.cit.,* y SUBIJANA ZUNZUNEGUI, J. I. (1997), "Policía judicial y derecho a la intimidad en el seno de la investigación criminal", *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, núm. Extra 10, págs. 121-160.

32. Arts. 4 y 5 de la Directiva 680/2016.

o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, y los intereses vitales del afectado; que la finalidad de la recopilación de la misma sea determinada, explícita y legítima; que los datos recabados sean adecuados, pertinentes, no excesivos y exactos en relación con los fines objeto del tratamiento; el principio de conservación de los datos únicamente durante el tiempo necesario para cumplir la finalidad que lo justifica; y que en el tratamiento se garantice un nivel de seguridad adecuado que tengan en cuenta la naturaleza, el alcance, el contexto y los fines del mismo y el riesgo que puede comportar para los derechos y libertades de los interesados y, de manera específica, de las personas vulnerables. Añadiéndose la exigencia de que el titular del tratamiento sea responsable y demuestre que ha cumplido dichos presupuestos, previsión que responde a los postulados contenidos en el Reglamento general. Junto a estos principios básicos, la norma establece la necesidad de que se fijen unos plazos que resulten apropiados para la supresión de los datos personales recopilados o para una revisión de su conservación.

Además, interesa destacar la novedosa distinción que hace la norma no sólo de las diversas categorías de interesados que son titulares de los datos de carácter personal objeto de tratamiento, sino también de las del propio tratamiento[33]. En el primer caso, y siempre que sea posible, se deberá diferenciar claramente entre los datos personales objeto de tratamiento, según afecten a los diversos grupos de personas y sin que ello limite la aplicación del derecho a la presunción de inocencia. Nos referimos, de un lado, a las personas sobre las que existen motivos fundados que hacen presumir que han cometido una infracción penal o, en su caso, pueden cometer; de otro, los sujetos que ya tienen una condena por la comisión de una infracción penal; por otro lado, los que resultan ser o pueden ser víctimas; y por último, los terceros afectados (tal es el caso de testigos). En lo que afecta a las categorías de tratamiento conviene diferenciar los datos personales basados en hechos y los basados en apreciaciones personales, en los que se prevén disposiciones de control sobre su calidad y se incluyen la protección de intereses vitales del interesado y las obligaciones de las autoridades competentes de informar al destinatario con respecto a sus condiciones. Es decir, la observancia del principio de

33. Arts. 6 y 7 de la Directiva 680/2016.

calidad de los datos personales objeto de tratamiento y, en las transmisiones que se hagan de los mismos, ha de indicarse la información precisa para que el Estado que los recibe valore que son exactos, completos y fiables[34]. En consecuencia, se determina el deber de especificar con claridad qué información está basada de manera exclusiva en apreciaciones personales de los investigadores involucrados.

A lo anterior se añade el reconocimiento de los derechos del interesado y su forma de ejercicio: información necesaria y adicional que se debe poner a su disposición y el derecho de acceso, rectificación o supresión de los datos personales que le conciernen, incluyendo las limitaciones que puedan establecer los Estados miembros. Y la facultad de los interesados a presentar reclamaciones si consideran que el tratamiento de sus datos infringe las disposiciones normativas. Así, quién hubiera sufrido daños y perjuicios materiales o inmateriales consecuencia de un tratamiento ilícito tiene derecho a recibir una indemnización del responsable del mismo o de la autoridad competente.

En consonancia con lo expuesto, la norma determina un elenco de obligaciones de necesario cumplimiento por parte de responsable del tratamiento de los datos de carácter personal[35]. De forma sucinta, cabe hacer alusión a la necesidad de facilitar al interesado la información y cualquier comunicación en relación con el tratamiento de la información que le concierne y de manera concisa, inteligible y de fácil acceso, empleando un lenguaje claro y sencillo, al igual que del ejercicio de los derechos que se le reconocen[36]. Asimismo, corresponde al responsable del tratamiento no sólo garantizar su seguridad[37], sino también establecer las medidas técnicas y organizativas adecuadas, en razón de la naturaleza, el ámbito, el contexto y los fines del mismo, y de los riesgos y gravedad para los derechos y libertades de los interesados[38]. Cabe indicar que el riesgo se concretará haciendo una evaluación objetiva, en cuyo caso un alto riesgo es un especial riesgo de perjuicio

34. Apartados 4º y 5º del art. 7 de la Directiva 680/2016.

35. Arts. 12 a 31 de la Directiva 680/2016.

36. Arts. 12 a 14 de la Directiva 680/2016.

37. Art. 29 de la Directiva 680/2016.

38. Arts. 19, 27 y 31 de la Directiva 680/2016 y véase también el 20 en cuanto a la tutela de los datos desde el diseño y por defecto.

para los derechos y libertades de los interesados. En el caso de que se empleen las nuevas tecnologías y ello suponga que sea probable que el tratamiento implique un alto riesgo, el responsable previamente tiene que hacer una evaluación del impacto de las operaciones de tratamiento. No obstante, si existiesen vulneraciones de la seguridad de los datos personales que son objeto del tratamiento, el responsable debe comunicárselo, sin dilación indebida, a la autoridad de control correspondiente[39] y al sujeto afectado. Téngase en cuenta, asimismo, que en todo caso compete al responsable demostrar que el tratamiento que hace de los datos personales se adecua a la normativa aplicable. A tal fin, el responsable del tratamiento tiene que conservar un registro de las categorías de actividades de tratamiento de datos que haya realizado bajo su responsabilidad[40] y cuyo objetivo no es otro que poder acreditar que dicho tratamiento se ha llevado a cabo de modo legal, el autocontrol, la garantía de la integridad y la seguridad de los datos y en el ámbito de los procesos penales.

Por último, es preciso destacar los principios que han de tenerse en cuenta respecto de la trasferencia que las autoridades competentes hagan de la información de carácter personal a otro país o a una organización internacional, en razón del cumplimiento de los objetivos de la norma comunitaria. La finalidad de establecer unos principios necesarios en cuanto a la trasferencia es asegurar que no se interfiera en el nivel de protección de las personas físicas[41]. Por tanto, la exigencia es que se obtenga la correspondiente autorización específica, salvo que el receptor de los datos personales garantice un nivel de protección adecuado. A menos que se trate de uno de los siguientes supuestos y que son excepciones a esta regla general; que la cesión trate de proteger los intereses vitales del interesado o de otro sujeto; que sea para salvaguardar intereses legítimos del interesado y así lo disponga el Derecho del Estado miembro que transfiere los datos; que se pretenda prevenir una amenaza grave e inmediata para la seguridad pública; y en concretos casos individuales.

39. A más tardar 72 horas después de que haya tenido constancia, en caso contrario deberá motivar la dilación en su notificación.

40. Arts. 24 y 25 de la Directiva 680/2016.

41. Arts. 35 a 39 de la Directiva 680/2016. Así como, arts. 45 y 47 del Reglamento (UE) 679/2016.

El contenido de la Directiva que nos ocupa se complementa con el de la Directiva 2016/681, concerniente a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, que disciplina la trasferencia por las compañías aéreas a los Estados miembros de datos PNR de pasajeros de vuelos internacionales, además del tratamiento de tales datos por las autoridades competentes, y de cuyas previsiones nos referimos a continuación.

## 3. La directiva 2016/681, relativa al registro de nombres de pasajeros (PNR)

### 3.1. Aspectos relevantes de la regulación

La Directiva 2016/681 es una de las medidas de la UE contra el terrorismo tras los atentados sucedidos en el ámbito comunitario (París y Bruselas). De modo que, mediante el registro de los datos de los pasajeros, es posible detectar los movimientos y actuaciones de los que los hubieron cometido o, en su caso, resulten sospechosos. Si bien, la justificación de la aprobación de este nuevo texto normativo no reside sólo en hacer frente a los ataques del terrorismo y en individualizar a los terroristas y su trazabilidad, sino también en reprimir crímenes organizados como el tráfico de seres humanos, la explotación sexual de los niños, el tráfico de drogas y la comisión de otras actuaciones delictivas diversas[42]. La Directiva 2016/681 tiene por objeto regular la comunicación de los datos privados de los pasajeros aéreos recogidos en un registro de información (PNR) que las compañías aéreas transfieren a los Estados miembros para vuelos exteriores a dicho ámbito y cuya utilización es proporcional a los fines perseguidos en la misma, entre los que se delimitan la prevención, detección, investigación y enjuiciamiento de delitos terroristas y otros delitos de gravedad; así como, la colaboración de las

42. Anexo II de la Directiva 2016/681. Véase CATALINA BENAVENTE, Mª. A. (2016), "La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos por en la lucha contra el terrorismo y la delincuencia grave (1)", Diario La Ley, núm. 8801, *passim.*

autoridades en materia de protección de datos personales para reforzar el control de los vuelos provenientes de terceros países hacía la UE[43].

La utilización de una base de datos para supervisar a los ciudadanos de la UE que concluyen transportes aéreos con destino fuera del territorio comunitario y que contiene datos e informaciones relevantes, no ha sido una materia exenta de polémica en la práctica. Pues no sólo se almacena la información que la policía y las autoridades poseen de los ciudadanos europeos que viajan, sino también otros datos como las formas de pago empleadas y diversa información que permite elaborar el perfil del pasajero[44]. Así, los datos PNR se catalogan como la información facilitada por el pasajero y recogida por las compañías aéreas cuya finalidad es realizar la reserva y el proceso de facturación. Es decir, los requisitos del viaje de los pasajeros sobre la fecha e itinerario del mismo, los datos del billete y asiento, los de contacto, información sobre el pago y otros datos en relación con el equipaje. Si bien, conviene señalar que algunas compañías aéreas recogen los datos API como parte de los PNR. Ello ha hecho, como se ha indicado, que se genere un debate en el seno europeo basado en la contradicción que se plantea con el principio de libre circulación de Schengen[45], el cual no contempla controles sistemáticos de los ciudadanos de los países de la UE que viajan de un Estado miembro a otro. Fundamentalmente, por cuanto los datos no se recogen por categorías, sino que son perfilados con la pretensión de constatar si hay comportamientos anómalos y esto se puede considerar tanto un problema de protección de la información de carácter personal y, más bien, de legitimidad constitucional de la norma respecto al contenido de los Tratados de la UE. Así, la jurisprudencia del Tribunal de Justicia de la UE se ha opuesto a los sistema de conservación de datos personales

43. Art. 11 de la Directiva 2016/681.

44. Art. 12 de Directiva 2016/681. En cuanto a los datos sensibles tendrán que ser borrados transcurridos 30 días y se convertirán en anónimos y serán guardados por las Unidades de información sobre pasajeros por un periodo suplementario de 5 años.

45. Se alude a la supresión de los controles en las fronteras interiores para las personas y al posible acceso al espacio europeo mediante la mera exhibición de pasaporte o documento que acredite la identidad del sujeto. Se trata de medidas contenidas en el Acuerdo de Schengen, de 14 de junio de 1985, y en el Convenio de aplicación del Acuerdo de Schengen, firmado el 19 de junio de 1990 que entró en vigor el 26 de marzo de 1995.

que resulte contraria a los principios de protección de los mismos en la medida en que se extienda a *cualquier persona*, es decir a sujetos sobre los que no existe una mínima sospecha delictiva[46].

El nuevo texto de la norma define los datos PNR con el siguiente tenor: *relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades.* En ningún caso, el registro de datos PNR debe basarse en el origen racial o étnico, religión o convicciones, opiniones políticas o de cualquier otro tipo, la pertenencia a un sindicato, la salud, vida u orientación sexual. En sentido opuesto, únicamente contendrán información sobre las reservas e itinerarios del viaje y que permita a las autoridades competentes identificar a los pasajeros aéreos que representen una amenaza para la seguridad de los países de que se trate.

Por consiguiente, la Directiva pretende disciplinar la garantía de la seguridad, la tutela de la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes, por resultar necesario que los Estados miembros impongan la obligación de transferir dichos datos que recojan las compañías aéreas que realizan vuelos exteriores al territorio de la UE, incluidos los datos API[47]. La

46. En este sentido, interesa consultar la STJUE de 8 de abril de 2014, Asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros*, que anuló la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 sobre conservación de datos en materia penal (disponible en el recurso electrónico: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf>); la STJUE (de 6 de octubre de 2015, Asunto C-362/14, *Maximillian Schrems/Data Protection Commissioner*, que cuestionó la legitimidad de la protección de datos personales transferidos por la entidad *Facebook* de Irlanda a los EE. UU. (disponible en el recurso electrónico: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf>; y la Sentencia del Tribunal Europeo de Derechos Humanos, de 12 de enero de 2016, Asunto 61496/08, *Barbulescu vs. Rumanía*, que autorizó a un empleador a supervisar los correos electrónicos de uno de sus trabajadores.

47. El art. 8 de la Directiva 2016/681 determina que en el supuesto de que las compañías aéreas hayan recopilado los datos de información anticipada sobre los pasajeros, pero no los conserven con iguales medios técnicos que los datos PNR, se han de adoptar las medidas necesarias para garantizar que las compañías aéreas envíen también esos datos a la UIP del Estado miembro.

finalidad que justifica el tratamiento de los datos PNR, como se ha indicado, se limita a la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves. Y, en todo caso, se atenderá a las garantías necesarias para asegurar la legalidad del tratamiento de dicha información y su trasferencia, lo que supone necesariamente que los afectados pueden ejercer los derechos relativos al tratamiento de sus datos personales (derecho de acceso, rectificación, supresión y restricción, así como el derecho de indemnización, cuando corresponda). Por tanto, la norma prevé una lista taxativa o *numerus clausus* de los datos del registro de nombres de los pasajeros que pueden ser recopilados por las compañías aéreas y de los delitos que se consideran graves, cuya prevención puede llevarse a cabo con su tratamiento[48].

En definitiva, la Directiva comunitaria que analizamos ofrece unas garantías en materia de protección de datos y que resultan proporcionales a los riesgos en los que se pueden incurrir en el entorno actual. En este sentido, una de las principales razones para tener un registro de pasajeros aéreos es la necesidad de contar con disposiciones comunes y de protección para los ciudadanos sobre un sistema de registro de información común y que aglutine a los que existen en cada Estado miembro. Por su parte, la observancia del principio de proporcionalidad trae como consecuencia que la actual regulación atienda a las finalidades por las que los datos PNR podrán ser tratados en un contexto de actividades de contraste, de intercambio de tales datos entre los Estados miembros y entre éstos y terceros países, de conservación, de protocolos y formatos de datos comunes para la trasferencia por parte de las compañías aéreas y de salvaguarda de la vida privada de los sujetos.

### 3.2. La Unidad de información sobre pasajeros (UIP) y la trasmisión de datos PNR

La Directiva europea, como se ha adelantado, se aplica a vuelos exteriores al marco territorial de la UE, con lo que las compañías aéreas están obligadas a facilitar a las autoridades de los Estados miembros los datos PNR de vuelos con llegada o salida fuera de la UE. Por su parte, los Estados miembros podrán recoger

48. Anexo I de la Directiva 2016/681. *Vid.* CATALINA BENAVENTE, *op.cit.*

datos PNR en relación con vuelos interiores seleccionados cuando hubieran decidido extender los efectos de la norma comunitaria a su ámbito interno[49] (por ejemplo, los vuelos desde un Estado miembro a otro u otros Estados miembros), siendo precisa la previa petición por escrito a la Comisión. En relación con ello, la norma comunitaria impone a los Estados miembros la necesidad de establecer una *Unidad de información sobre pasajeros* (UIP) propia[50], la cual tiene por finalidad la recopilación de los datos PNR. Siendo la competente para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo y delitos graves. Las Unidades de información sobre pasajeros son las responsables de la recogida, conservación y tratamiento de datos PNR, además de su trasferencia a las autoridades competentes y de su intercambio con las Unidades de información sobre pasajeros de otros Estados miembros y con entidades de carácter internacional, como la Europol[51]. Los Estados miembros pueden, además, decidir si recabar y tratar datos PNR provenientes de otros operadores económicos, distintos de las compañías aéreas, como las agencias de viajes u operadores turísticos, que igualmente ofrecen servicios de reserva de vuelos.

La información referida se conservará por un periodo temporal de cinco años contados desde su trasmisión a la UIP, si bien pasados seis meses desde que fueron trasferidos, se convertirán en anónimos mediante un mecanismo que permite ocultar algunos elementos. Es decir, se despersonalizan los datos PNR mediante el encubrimiento de los elementos que hacen factible la identificación directa de los pasajeros que son los titulares de los mismos. Nos referimos, en particular, a datos como: el nombre, la dirección y otros de contacto[52]. Para garantizar la protección de datos, la UIP ha de nombrar a un responsable de su protección que será el encargado de supervisar el tratamiento de la información y aplicar las garantías que corresponda. Por su parte, los Estados miembros tienen el deber de prohibir el

49. Art. 2 de la Directiva 2016/681.

50. Arts. 8 y 9 de la Directiva 2016/681. Dentro de un Estado miembro puede disponer de distintas sucursales y los mismos también podrán establecer conjuntamente una UIP para intercambiar información (CATALINA BENAVENTE, *op.cit.*).

51. Consúltese el art. 10 de la Directiva 2016/681, en relación con las condiciones de acceso de Europol a los datos PNR.

52. Art. 12 de la Directiva 2016/681.

tratamiento de datos PNR que revelen información sensible como el origen racial o étnico, las opiniones políticas, la religión o las convicciones filosóficas, la pertenencia a sindicatos, el estado de salud, la vida o la orientación sexual del interesado.

En cuanto a la trasmisión y el almacenamiento de los datos PNR, la Comisión Europea respalda las directrices emanadas de la Organización de Aviación Civil Internacional, señalando que las mismas se constituyen en la base de los formatos admitidos para la transmisión de los datos PNR. La práctica de la aviación internacional plantea dos formas básicas de cesión: el método *push* o de transmisión por el que las compañías aéreas envían a la autoridad competente los datos sin permitirle el acceso a la base de datos; y el método *pull* o de extracción, en cuyo caso la autoridad solicitante puede acceder al sistema de reservas de la aerolínea y recabar una copia de la información. Siendo, por tanto, el primero de los métodos el que garantiza en mayor medida la tutela de la información personal y el que ha de ser obligatorio para las compañías aéreas[53]. De este modo, las transmisiones de datos PNR por parte de las compañías aéreas a las UIP se efectuarán mediante medios electrónicos que ofrezcan garantías suficientes en relación con las medidas de seguridad técnicas y organizativas que rigen el tratamiento de los datos que se va a llevar a cabo[54]. En caso de fallo técnico, los datos PNR podrán ser transmitidos por otro medio adecuado, siempre que se mantenga el mismo nivel de seguridad y que se cumpla de manera íntegra el derecho de la UE en materia de protección de datos. En todo caso, se requiere que los datos PNR sean transmitidos en un formato admitido que garantice su legibilidad por las partes interesadas. Si bien, la referida trasferencia de los datos se admitirá caso por caso y de manera exclusiva en razón de la prevención, detección, investigación y enjuiciamiento de delitos terroristas y otros delitos de gravedad.

La temporalidad en que dicha obligación ha de cumplirse está limitada, a saber: entre las 24 a 48 horas antes de la hora de salida del vuelo que esté programada, e inmediatamente después del cierre del vuelo o, lo que es lo mismo, cuando los pasajeros hayan embarcado y no sea posible que lo hagan otros, ni que se desembarque. Esta norma general, no es aplicable cuando el acceso a los datos

53. Cdo. 16 de la Directiva 2016/681.

54. Art. 16 de la Directiva 2016/681.

PNR sea preciso para atender una amenaza concreta y real relacionada con delitos de terrorismo o delitos graves. En relación con ello, además, se permite la cesión de datos del registro de nombres de pasajeros a terceros países y del resultado del tratamiento[55], cuando se cumplan ciertas exigencias normativas. Cuales son: *que sean esenciales para responder a una amenaza específica y real relacionada con delitos de terrorismo o delitos graves de un Estado miembro o de un tercer país, y el consentimiento previo no pueda obtenerse a su debido tiempo*. El país de que se trate ha de contar con un nivel adecuado de protección, lo cual es comprobable por la firma o suscripción de acuerdos bilaterales de transferencias de ese tipo de datos.

## 4. Conclusiones

Las compañías aéreas han de proteger y tutelar la información y los datos de carácter personal de los pasajeros que contratan sus servicios en la medida en que es una información que permite identificar o, en su caso, hacer identificable a la persona física que es titular de los mismos. Sin embargo, esta apreciación se contrapone con la necesidad de velar por la seguridad y defensa en el ámbito internacional, ya que ello requiere que los datos de los pasajeros se faciliten a entidades de terceros países.

El tratamiento de datos de carácter personal que realizan las compañías aéreas es lícito en cuanto que está justificado en el cumplimiento de la actividad que les compete. Si bien, ello no les exime de respetar y atender los presupuestos normativos previstos en materia de protección de la información de carácter personal a fin de garantizar el correcto tratamiento de los datos de los pasajeros. Las compañías aéreas son, en este sentido, responsables del tratamiento de los datos de los usuarios y deben adoptar las medidas técnicas y organizativas apropiadas para evitar pérdidas, alteraciones o accesos por parte de terceros no autorizados a la información personal de los pasajeros.

La reforma legislativa en materia de protección de datos personales en el ámbito normativo de la UE ha determinado un avance importante para los

55. Art. 11 de la Directiva 2016/681.

ciudadanos y la tutela de sus derechos. Los nuevos textos suponen una modificación del panorama normativo anterior, aunque conservando los principios básicos en la materia, y concretando nuevas exigencias que han sido fundamentales. En este sentido, conviene reseñar la adecuación de las normas sobre protección de datos a los cambios operados por la implementación de las nuevas tecnologías. Así, el Reglamento general sobre protección de datos personales refuerza los derechos de las personas físicas para la tutela de los mismos, integrando la disciplina preexistente, e introduciendo nuevas facultades (derecho al olvido y el derecho a la portabilidad). En otros casos, sin embargo, se delimitan algunos de los extremos vigentes con anterioridad estableciendo modalidades para su ejercicio y diversas obligaciones a los que son titulares.

En definitiva, la nueva normativa asegura una disciplina uniforme en la materia que, al mismo tiempo, es reflejo de una mayor exactitud y trasparencia en el acceso a los datos personales, y amplía la seguridad y confianza de los sujetos. En particular, en cuanto al tratamiento de los datos personales para usos judiciales y/o policiales y el registro de los datos de los pasajeros aéreos (PNR). La nueva regulación aprobada en el marco comunitario no sólo establece los principios que han de observarse en materia de protección de datos de carácter personal; sino que, además, incluye previsiones específicas sobre el intercambio de datos transfronterizos dentro de la UE y los estándares mínimos que el tratamiento de los mismos ha de respetar en cada país. Siendo un reto de indudable trascendencia práctica, como se irá comprobando de manera paulatina.

## 5. Bibliografía

AA.VV. (2015), *Hacia un nuevo derecho europeo de protección de datos: Towards a new european data protection regime,* (Coord. RALLO LOMBARTE, A./ GARCÍA MAHAMUT, R.), Valencia.

AA.VV. (2015), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, (Dir. COLOMER HERNÁNDEZ, I. Coord. OUBIÑA BARBOLLA, S.), Pamplona.

ALONSO MARTÍNEZ, C. (2002), *Protección de datos de carácter personal. El consentimiento en entidades financieras*, Madrid.

CATALINA BENAVENTE, Mª. A. (2016), "La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos por en la lucha contra el terrorismo y la delincuencia grave (1)", *Diario La Ley*, núm. 8801.

DAVARA RODRÍGUEZ, M. A. (2006), *Manual de Derecho Informático*, Pamplona.

FREIXAS GUTIÉRREZ, G. (2001), *La protección de los datos de carácter personal en el derecho español*, Barcelona.

LÓPEZ CALVO, J. (2016), "Sobre la aparente discrepancia entre las Salas de lo Contencioso y Civil del TS sobre derecho al olvido. Un problema de diferente visión sobre la congruencia entre pretensiones de las partes y fallo. Google Spain, al menos, como establecimiento de Google Inc.", *Sepin*.

LÓPEZ PORTAS, Mª. B. (2015), "La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE", *Revista de derecho político*, núm. 93, (págs. 143-175).

MURILLO DE LA CUEVA, P. L. (2007), "Perspectivas del derecho a la autodeterminación informativa", *IDP: revista de Internet, derecho y política*, núm. 5.

SERRANO PÉREZ, M. Mª. (2003), *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid.

SUBIJANA ZUNZUNEGUI, J. I. (1997), "Policía judicial y derecho a la intimidad en el seno de la investigación criminal", *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, núm. Extra 10, (págs. 121-160).

VÁZQUEZ RUANO, T. (2014), "Transferencia internacional de datos personales en el transporte aéreo. La Custom Border Protetion en el sistema USA", *Rivista Diritto dei Trasporti*, número especial, 1, (págs.115-131).