LOS DERECHOS FUNDAMENTALES EN SOCIEDADES MULTICULTURALES Y PROTECCIÓN DE DATOS PERSONALES EN LA UNION EUROPEA: EL CAMINO DE IDA Y VUELTA DE LOS DATOS PNR.*

FUNDAMENTAL RIGHTS IN MULTICULTURAL SOCIETIES AND PROTECTION OF PERSONAL DATA IN THE EUROPEAN UNION: THE ROAD OF IDA AND RETURN OF PNR DATA *

Alvaro A. Sánchez Bravo.[1]

Resumen: los datos Pnr constituyen un elemento imprescindible para el control del trafico de pasajeros. no obstante, plantean problemas en lo referente a la violación de la intimdad y otros derechos de los ciudadanos. Su regulación y marco jurídico ha supuesto en numerosas ocasiones enfrentamientos con estados ajenos ala Unión Europea, especialmente Estados Unidos, en aras de la preservación de la seguridad nacional y la lucha contra el terrorismo. La reforma del Marco Europeo de Protección de Datos, ha incorporado a la normativa europea una Directiva específica sobre Datos PNR.

Palavras chave: Datos personales - Union Europea - Directiva.

Summary: Pnr data is an essential element for the control of passenger traffic. however, they pose problems in relation to the violation of privacy and other rights of citizens. Its regulation and legal framework has often involved clashes with states outside the European Union, especially the United States, in the interests of preserving national security and combating terrorism. The reform of the European Data Protection Framework has incorporated into European legislation a specific Directive on PNR Data.

Key words: Personal data - European Union - Directive.

[1] Doctor en Derecho. Profesor de la Facultad de Derecho de la Universidad de Sevilla. Presidente de la Asociación Andaluza de Derecho, Medio Ambiente y Desarrollo Sostenible. Expert European Research Council Executive Agency. European Comission. Académico Correspondiente Academia SulRioGrandense de Direito do Trabalho. Coeditor Revista Internacional de Direito Ambiental (RIDA).

Introducción

La protección de las personas físicas en lo tocante al tratamiento de datos personales constituye un derecho fundamental, recogido en la Carta de los Derechos Fundamentales de la Unión Europea (art. 8.1)[2] y en el Tratado de Funcionamiento de la Unión Europea (art. 16.)[3], estableciéndose que toda persona tiene derecho a la protección de los datos personales que le conciernen.

La sociedad globalizada[4] exige, cada vez más, un acopio, utilización y transmisión de datos personales que abarca las actividades más cotidianas, y las decisiones globales más relevantes. En el ámbito de la Unión europea, las normas y principios relativos a la protección de datos personales deben, independientemente de la nacionalidad o residencia de sus titulares, respetar sus libertades y derechos fundamentales; contribuyendo igualmente a la consecución de un espacio europeo de libertad, seguridad y justicia[5].

Ahora bien, esa globalización también a ha llegado a las actividades delictivas, al terrorismo y a otras formas de barbarie que intentan destruir o menoscabar la pacífica convivencia, como cimiento de sociedades democráticas y libres.

El terror "viaja" o al menos lo intenta, por todo el planeta, por lo que se hizo necesario el establecimiento de unos mecanismos de control y vigilancia y de intercambio de información que permitan detectar, prevenir y contrarrestar los efectos delos atentados criminales. Ahora bien, esto no puede hacerse de cualquier forma, a cualquier preciso, pues con el pretexto de defender la democracia, podemos

---

* Texto del trabajo presentado como conclusión de los Estudios de PosDoctorado en el Programa de Pós-Graduação em Direito – Mestrado e Doutorado. Universidade Regional Integrada do Alto Uruguai e das Missões. URI-San, bajo la supervisión del Prof. Dr. Joao Martin Bertaso.

[2] ARTÍCULO 8.- Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

[3] Artículo 16 (antiguo artículo 286 TCE)

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

[4] SANCHEZ BRAVO, A., Internet y la sociedad europea de la información: implicaciones para los ciudadanos, Publicaciones de la Universidad de Sevilla, 2001.

[5] 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. DO L 119.04.05.2016. Considerando (2).

convertirla en un estado totalitario, sometiendo a los ciudadanos a un control sistemático de sus datos personales y actividades vinculadas.

Los desgraciados acontecimientos del 11 de septiembre de 2001, en New York, llevaron a Estados Unidos a adoptar una serie de medidas legislativas y policiales tendentes a blindar su territorio frente a eventuales nuevos ataques terroristas. La promulgación de la PatriotAct y la creación de la Oficina Nacional de Seguridad son solo algunos ejemplos relevantes de estas iniciativas.

Paralelamente, en aplicación de la Ley de Seguridad en los Transportes la Administración estadounidense obligó unilateralmente, bajo la amenaza de fuertes sanciones e incluso la pérdida de los derechos de aterrizaje, a las compañías aéreas que operan vuelos con destino a su territorio a transferirle los datos personales sobre pasajeros y los miembros de las tripulaciones de los vuelos con destino procedentes de este país. En concreto las compañías aéreas debían suministrar al Servicio de Aduanas y Protección de Fronteras (abreviatura en inglés, CBP) un acceso electrónico a los datos de los pasajeros que figuran en el *registro de los nombres de los pasajeros* (abreviatura en inglés, ***PNR***) para los vuelos que tienen destino, origen o que hacen escala en Estados Unidos6.

Esta imposición suponía en el ámbito comunitario europeo la necesidad de considerar si el cumplimiento de las exigencias estadounidenses por parte de las compañías aéreas supone una subversión de las exigencias y garantías que para la protección de datos establece la Directiva 95/46/CE7. En concreto su artículo 25, establece que para la transferencia a terceros países, éstos deberán garantizar un "nivel de protección adecuado". Y es precisamente la determinación de ese nivel el que desató la polémica entre las instituciones comunitarias y la zozobra en los ciudadanos.

No obstante, la problemática terrorista soportada por Estados Unidos, se ha expandido en los últimos años al territorio europeo, que ha soportado, y soporta execrables atentados que desde diversas ideologías radicales, fundamentalmente de base islamista, intentan colocar en jaque nuestra modelo civilizatorio, nuestra democracia, y en definitiva, nuestros derechos humanos.

Ello, como veremos ha llevado con extraordinaria celeridad, a la adopción de la normativa necesaria para un correcto uso de los datos PNR, que sea coherente con la normativa europea de protección de datos, recientemente modificada.

Es por ello que resulta interesante mostrar cual fue el *iter* legislativo, y, sobre todo, constatar como cuando los hechos nos son más próximos se aceleran las soluciones, aún a riesgo de conculcar los derechos de los ciudadanos.

---

[6] Grupo del artículo 29 sobre protección de datos. Dictamen 4/2003 relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de los pasajeros, 13 de junio de 2003, 11070/03/ES WP 78.

[7] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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. Sobre su contenido, vid., SANCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea*, Publicaciones de la Universidad de Sevilla, 1998; e *Internet y la sociedad europea de la información: implicaciones para los ciudadanos*, Publicaciones de la Universidad de Sevilla, 2001

1. Acuerdo de la Comisión Europea de 2004

Tras las medidas aprobadas por el Gobierno USA de acceso a las listas de los pasajeros, las compañías aéreas europeas, con el respaldo de la Comisión, plantearon serias objeciones a su aplicación en cuanto podía vulnera la normativa comunitaria de protección de datos. No obstante, pese a unos iniciales aplazamientos, las autoridades estadounidenses, y concretamente el CBP, comunicó que a partir del día 5 de marzo de 2003 comenzaría a imponer sanciones.

Ante tal situación, la Comisión inició una serie de negociaciones con el Departamento estadounidense de Seguridad Interior (DHS) en un intento de garantizar que los datos del PNR gocen de una protección adecuada, en línea con la normativa europea de protección de datos.

En diciembre de 2003, la Comisión declaró haber llegado a un acuerdo con Estados Unidos, y manifestó su disposición para elaborar una Decisión que estableciese que el Servicio de Aduanas y protección de Fronteras de Estados Unidos (abreviatura en inglés, CBP) garantizaba un nivel de protección adecuado.

Dicha Decisión fue adoptada por la Comisión el 14 de mayo de 2004[8], incorporando como anexo los Compromisos del CBP.

La Decisión establece dos consideraciones respecto a su ámbito material de aplicación;

El CBP ofrece, conforme al apartado 2 del art. 25 de la Directiva 95/469, un nivel de protección adecuado de los datos de PNR que se transfieren desde la Comunidad relativos a vuelos con destino u origen en Estados Unidos.

Los compromisos de la Decisión no empecen el cumplimiento de otras condiciones o restricciones que puedan imponerse en aplicación de la Directiva 95/46.

Pero quizás lo más relevante sea considerar el contenido de los Compromisos del CBP. Dichos compromisos suponían, a juicio de la Comisión, una importante mejora de la situación, que se concreta en:

Las autoridades estadounidenses recogerían y conservarían menos datos. Se acordó una lista de 34 categorías de datos (los PNR de algunas compañías aéreas contienen más de 60 campos) y en la mayoría de los registros individuales sólo se cumplimentará un número limitado de estos campos.

Los datos sensibles, como las preferencias alimentarias o las necesidades especiales de los pasajeros, que pueden revelar su raza, religión o estado de salud, no se transferirían o, si se transfirieran, serían filtrados y eliminados por el CBP.

Los datos del PNR se utilizarían exclusivamente para prevenir y combatir el terrorismo y los delitos conexos, y otros delitos graves, incluida la delincuencia organizada, que tengan carácter transnacional, lo que supone una mayor precisión de las finalidades anteriormente previstas por Estados Unidos.

3C(2004) 1914. 2004/535/CE. DOUE L 235/11. 06.07.2004.

[9] Art. 25.2 Directiva 95/46: " *El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad vigentes en dichos países*".

Los datos del PNR no se compartirían «en masa»; se intentaba responder así a las preocupaciones relativas a la utilización de estos datos en planes de vigilancia generalizada que se están preparando en Estados Unidos. El CBP compartiría los datos del PNR de forma limitada, caso por caso, y únicamente para las finalidades acordadas; cuando los datos procedentes de la UE se transfieran conforme a estas condiciones estrictas a las autoridades policiales de países distintos de Estados Unidos, se comunicará este hecho sistemáticamente a una autoridad de la UE designada al efecto.

La mayoría de los datos PNR se suprimirían al cabo de tres años y medio (frente a los cincuenta años que proponía en un principio Estados Unidos). Los ficheros a los que se haya accedido se conservarán en un fichero de datos suprimidos durante ocho años suplementarios con fines de auditoría (frente al plazo indefinido que se pretendía en un principio).

Las autoridades de protección de datos de la UE tendrían la posibilidad de examinar con el Director responsable de la protección de la intimidad (ChiefPrivacyOfficer) del DHS los casos de los pasajeros cuyas denuncias, por ejemplo, por presuntos abusos en la utilización de los datos que les conciernen o por no rectificación de datos imprecisos no haya resuelto de forma satisfactoria el DHS10.

El Acuerdo elaborado por la Comisión fue aprobado por el Consejo de la Unión en su Decisión de 17 de mayo de 200411, facultando al Presidente del Consejo para que designe la/s persona/s que firmarán el Acuerdo en nombre de la Comunidad Europea.

2. Las objeciones del grupo del Art. 29 sobre Protección de Datos

El Grupo del art. 29[12], emitió un primer Dictamen sobre estas cuestiones en octubre de 200213, y un segundo dictamen en junio de 200314, donde ponía de manifiesto serias objeciones a los Acuerdos que entonces se negociaban y que ponían en cuestión el régimen protector que respecto a los datos personales se había conseguido en la Unión. En concreto, se cuestionaba la finalidad de las transferencias, la adecuación al principio de proporcionalidad de los datos a transferir, el tratamiento de los datos sensibles, el momento de las transferencias y el período de conservación de los datos, la opción por un sistema de transferencia "push" 15 el control estricto de la posterior cesión de datos a terceros, las garantías y

[10] IP/04/650.
[11] DO L 183/83, 20.05.2004.
[12] Grupo creado en virtud del art. 29 de la Directiva 95/46/CE. Se trata de un organismo de la Unión, de naturaleza consultiva e independiente, para la protección de datos y el derecho a la intimidad. Según el art. 30 tendrá, de entre sus cometidos: "*b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros*."
[13] Dictamen 6/2002, de 24 de octubre, WP 66. http://europa.eu.int/comm/internal_market/privacy/workingroup_fr.htm
[14] Dictamen 4/2003, de 13 de junio, WP 78.
[15] Según el propio Grupo del art. 29, "*el único mecanismo de transferencia de datos cuya aplicación no suscita problemas importantes es el sistema* ***push****, según el cual las compañías aéreas seleccionan y transfieren los datos a las autoridades estadounidenses, en oposición al sistema* ***pull****, en el que las autoridades estadounidenses disponen de acceso directo en línea a las bases de datos de las compañías aéreas y de los sistemas de reserva*." Dictamen 4/2003, cit., p. 6.

los derechos de los interesados, el mecanismo de aplicación y de resolución de los litigios, y el nivel de los compromisos.

Posteriormente en su Dictamen de enero de 200416 , tras haber recibido de la Comisión la versión actualizada de los Acuerdos con Estados Unidos, y constatar la mejora en los Acuerdos, concluye de manera contundente que no puede estimarse que se haya alcanzado un nivel adecuado de protección de los datos. A mayor abundamiento, indica que cualquier decisión al respecto debe cumplirse como exigencias indispensables:

- Calidad de los datos:

la finalidad de la transferencia de datos debe ser únicamente la lucha contra los actos de terrorismo y determinados delitos conexos que habrá que definir; la lista de los datos que deben transferirse debe ser proporcionada y no excesiva; el cotejo de datos con los de personas sospechosas debe atenerse a normas de elevada calidad que garanticen la certeza de los resultados; los períodos de conservación de los datos deben ser cortos y proporcionados;los datos de los pasajeros no deben utilizarse para implantar y/o probar el sistema CAPPS II17, o sistemas similares.

– Los datos sensibles no deben transmitirse.

– Derechos de los interesados:

deben facilitarse a los pasajeros información clara, actual y comprensible; debe garantizarse sin discriminación un derecho de acceso y rectificación; deben preverse disposiciones suficientes que garanticen a los pasajeros el acceso a un mecanismo de recurso verdaderamente independiente.

– Nivel de compromiso de las autoridades estadounidenses:

los compromisos asumidos por las autoridades estadounidenses deben ser plenamente vinculantes para Estados Unidos; procede clarificar el ámbito de aplicación, la base jurídica y el valor de un posible «acuerdo internacional ligero».

– Las transferencias posteriores de datos del PNR a otras administraciones o autoridades extranjeras deben limitarse estrictamente.

– Método de transferencia: conviene establecer un método de transferencia «push», es decir, que los datos sean seleccionados y transferidos por las compañías aéreas a las autoridades estadounidenses.

Tras la aprobación del Acuerdo por la Comisión y el Consejo, el Grupo volvió a posicionarse, en su Dictamen de junio de 200418 , claramente en contra del contenido del Acuerdo, señalando que la "Comisión no ha tenido en cuenta, más que parcialmente las exigencias mínimas formuladas por el Grupo", y exhortando a que,

[16]Dictamen 2/2004, de 29 de enero de 2004, WP 87.

[17] El sistema CAPPS II ha sido desarrollado por la Oficina de Seguridad Nacional de los Estados Unidos; organismo creado por la Administración Bush tras los atentados del 11-S. El CAPPS I (*ComputerAssistedPassenger Pre-Screening*. Preinspección de Pasajeros asistida por Ordenador) se basaba exclusivamente en el registro de direcciones de los pasajeros, historial de viajes, antecedentes criminales y otras informaciones no determinadas. El CAPPs II introduce un mayor número de variables, además de un acceso a bases de datos comerciales relativos a datos financieros, historiales médicos, seguros y datos de empadronamiento , entre otros. A cada pasajero se le asigna un código de seguridad durante su registro en una compañía aérea: verde, para los que supongan un riesgo mínimo, amarillo para los de un riesgo mayor (situación de alerta) y rojo para los considerados como altamente peligrosos. En función de cada calificación el pasajero es objeto o no de ulteriores revisiones "en profundidad". Cfr. http://www.cem.itesm.mx/dacs/publicaciones/logos/anteriores/n37/fgutierr.html

[18] Dictamen 6/2004, de 22 de junio, WP 95.

como mal menor, se adopten una serie de medidas urgentes para "evitar al máximo los ataques a los derechos de los pasajeros"19 .

Posteriormente, en su Dictamen de septiembre de 2004 20 , ha elaborado una serie de orientaciones acerca de las informaciones que deben suministrarse a los pasajeros, donde de manera simple y didáctica se pasa revista a todas las cuestiones que pueden surgir respecto a la recepción por el CBP de los datos PNR de los pasajeros de vuelos entre la Unión Europea y Estados Unidos.

3. La firme posición del Parlamento Europeo

El Parlamento Europeo, una vez tuvo conocimiento de las negociaciones de la Comisión, y a la vista de la propuesta de Decisión, se posicionó abiertamente en contra del mismo, tanto por cuestiones de forma, como en lo atinente al fondo de los acuerdos que en ese momento se pretendían adoptar. Tal es así que en su Resolución de marzo de 200421 , señala: "*6. Pide a la Comisión que bloquee: a) el sistema "pull" a partir del 1 de julio de 2004, y que desde esa fecha aplique el sistema "push" con los 19 puntos propuestos el 13 de junio de 2003 por el Grupo a que se refiere el artículo 29 de la Directiva 95/46/CE; b) las iniciativas para crear una gestión europea centralizada de los datos de PNR, tal como contempla la Comunicación COM (03) 826 y ha confirmado recientemente el comisario competente a la comisión parlamentaria, en la medida en que, en las actuales circunstancias, esas iniciativas violan los principios de proporcionalidad y subsidiariedad;*

7. Entretanto, se reserva el derecho a recurrir al Tribunal de Justicia en el caso de que la Comisión Europea adoptara el proyecto de Decisión; asimismo, recuerda a la Comisión el principio de cooperación leal entre las Instituciones, en aplicación del artículo 10 del Tratado, al tiempo que la insta a no adoptar durante el período de elecciones una decisión cuyo contenido corresponda al de la propuesta examinada en la presente Resolución;

8. Se reserva el derecho de recurrir al Tribunal de Justicia para verificar la legalidad del acuerdo internacional previsto y, en particular, su compatibilidad con la protección de un derecho fundamental;

9. Considera de vital importancia que los resultados de las negociaciones no sirvan de modelo para la actividad posterior de la Unión Europa con miras al desarrollo de sus propios medios de lucha contra la delincuencia, así como en

---

[19] Estas medidas urgentes se concretarían en: 1) las compañías aéreas deberán modificar tan rápido como sea posible el sistema de transferencia de datos y pasar del sistema "global" al sistema "concreto"; 2) los pasajeros deben ser correctamente informados de la transferencia de los datos; 3) el acuerdo no obliga ni autoriza a las compañías aéreas a recoger otros datos que los registrados y conservados con fines comerciales; 4) deben ponerse en marcha las reuniones periódicas de control del cumplimiento de los Acuerdos, establecidas para verificar el correcto cumplimiento de la protección de datos; y 5) convocatoria de una reunión con las compañías aéreas.

[20] Dictamen 8/2004, de 30 de septiembre, WP 97.

[21] P5_TA-PROV (2004)0245. Protección de datos personales de los pasajeros aéreos. Resolución del Parlamento Europeo sobre el proyecto de Decisión de la Comisión por la que se determina el nivel de protección adecuado de los datos personales incluidos en los registros de nombres de pasajeros aéreos (PNR) transferidos a la Oficina de Aduanas y Protección de Fronteras de los Estados Unidos (2004/2011(INI))

materia de almacenamiento de datos y protección de la confidencialidad de los mismos;

10. Insta a la Comisión a que retire el proyecto de Decisión".

El desarrollo de los acontecimientos evidenció como la Comisión y el Consejo hicieron caso omiso a las prevenciones apuntadas por el Parlamento Europeo.

En mayo, el propio Parlamento declaró la no pertinencia de la tramitación por vía de urgencia del Acuerdo sobre transferencia de datos, tal y como había solicitado el Consejo. Además el Parlamento acordó solicitar un dictamen al Tribunal de Justicia sobre la viabilidad de la propuesta, optando por posponer el voto final y reenviando el informe a la Comisión parlamentaria a la espera del dictamen del Alto tribunal comunitario sobre si el acuerdo es compatible o no con la normativa comunitaria22.

No obstante esta solicitud de dictamen judicial, la Comisión y el Consejo aprobaron, como ya hemos referido, sendas Decisiones dando validez al Acuerdo.

Ante esta actitud la Comisión de Asuntos jurídicos de la Eurocamara pidió, en su reunión del 16 de junio, al Presidente del Parlamento que denunciase la Decisión de la Comisión y el Consejo. El entonces presidente, Pat Cox, tras unos iniciales "titubeos" planteó ante el Tribunal de Justicia de la Unión Europea un recurso de anulacanulación. Su conveniencia la expresa de manera muy elocuente: "Esta decisión ha sido tomada tras una larga consulta y refleja la preocupación de una inmensa mayoría del Parlamento Europeo, en cuanto a la necesidad de defender los derechos y libertades fundamentales de los ciudadanos europeos".

4. Sentencia del TJCE de 30 de Mayo de 2006

La sentencia del Tribunal de Justicia Europeo de 30 de mayo de 2006[23] anuló la Decisión de la Comisión sobre el carácter adecuado de la protección y la Decisión del Consejo por la que se concluye un acuerdo en materia de registros de los nombres de los pasajeros (PNR) La sentencia obligaba a las instituciones de la Comunidad a denunciar el Acuerdo con los Estados Unidos en materia de transferencia de datos de pasajeros el 30 de septiembre de 2006, a más tardar. Por esta razón, toda transferencia de datos de pasajeros a las autoridades de los Estados Unidos no tendría fundamente jurídico en el Derecho europeo tras la denuncia de dicho Acuerdo. Como señalo el Grupo de Trabajo del art. 2924, era posible que

[22] Cfr. http://www.noticias.info/Archivo/2004/200405/20040505/20040505_23258.shtm

[23]SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)de 30 de mayo de 2006. «Protección de las personas físicas en lo que respecta al tratamiento de datospersonales – Transporte aéreo – Decisión 2004/496/CE – Acuerdo entre laComunidad Europea y los Estados Unidos de América – Registros de nombres delos pasajeros que se transfieren al Servicio de aduanas y protección de fronteras delos Estados Unidos de América – Directiva 95/46/CE – Artículo 25 – Estadosterceros – Decisión 2004/535/CE – Nivel de protección adecuado»En los asuntos acumulados C-317/04 y C-318/04.
https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/28._Sentencia_de_30_de_mayo_de_2006._Asuntos_C-317-04_y_C-318-04_Parlamento_Europeo_v_Consejo_de_la_Uni-oo-n_Europea.pdf

[24] DICTAMEN 5/2006 DEL GRUPO DE TRABAJO EN RELACIÓN CON LA PROTECCIÓN DE LAS PERSONAS POR LO QUE SE REFIERE AL TRATAMIENTO DE DATOS PERSONALES sobre la sentencia del Tribunal de Justicia Europeo de 30 de mayo de 2006 en los asuntos acumulados C-317/04 y

fuera necesario introducir medidas a nivel de la legislación nacional, como, por ejemplo, la total suspensión de las transferencias de datos a las autoridades de los Estados Unidos.

Los argumentos son contundentes:

"Sobre la Decisión sobre el carácter adecuado de la protección

En primer lugar, el Tribunal de Justicia examina si la Comisión podía válidamente adoptar la Decisión sobre el carácter adecuado de la protección sobre la base de la Directiva 95/46/CE. A este respecto, recuerda que el artículo 3, apartado 2, de la Directiva excluye de su ámbito de aplicación el tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario y, en cualquier caso, el tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.

Se desprende de la Decisión sobre el carácter adecuado de la protección que la exigencia de que se transfieran los datos se basa en la normativa estadounidense relativa a la intensificación de la seguridad, que la Comunidad apoya plenamente a Estados Unidos en su lucha contra el terrorismo y que los datos de los PNR deben utilizarse únicamente para los fines de prevención y lucha contra el terrorismo y delitos conexos y otros delitos graves, incluida la delincuencia organizada. En consecuencia, la transferencia de los datos de los PNR al CBP constituye un tratamiento que tiene por objeto la seguridad pública y las actividades del Estado en materia penal.

Si bien es correcto considerar que los datos de los PNR son inicialmente recogidos por las compañías aéreas en el marco de una actividad comprendida en el ámbito de aplicación del Derecho comunitario, a saber, la venta de un billete de avión que da derecho a una prestación de servicios, sin embargo, el tratamiento de datos contemplado en la Decisión sobre el carácter adecuado de la protección tiene una naturaleza bien distinta. En efecto, el tratamiento de datos a que se refiere esta Decisión no es necesario para la realización de una prestación de servicios, sino que se considera necesario para salvaguardar la seguridad pública y para fines represivos.

El hecho de que los datos de los PNR sean recogidos por operadores privados con fines mercantiles y de que sean éstos quienes organizan su transferencia a un Estado tercero no se opone a que dicha transferencia se considere un tratamiento de datos excluido del ámbito de aplicación de la Directiva. En efecto, esta transferencia se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública.

El Tribunal de Justicia concluye que la Decisión sobre el carácter adecuado de la protección no está comprendida en el ámbito de aplicación de la Directiva dado que se refiere a un tratamiento de datos personales que está excluido de ésta. Por consiguiente, anula dicha Decisión. No es necesario examinar los demás motivos invocados por el Parlamento.

Sobre la Decisión del Consejo

El Tribunal de Justicia señala que el artículo 95 CE en relación con el artículo 25 de la Directiva no puede constituir la base de la competencia de la

---

C-318/04 sobre la transmisión de los registros de nombres de pasajeros a los Estados Unidos. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp122_es.pdf

Comunidad para celebrar el Acuerdo controvertido con Estados Unidos. En efecto, este Acuerdo se refiere a la misma transferencia de datos que la Decisión sobre el carácter adecuado de la protección y, por tanto, a tratamientos de datos que están excluidos del ámbito de aplicación de la Directiva. Por consiguiente, el Tribunal anula la Decisión del Consejo por la que se aprueba la celebración del Acuerdo y no considera necesario examinar los demás motivos invocados por el Parlamento"[25]

Los efectos de la Sentencia no se hicieron esperar, y la presión del gobierno norteamericano tampoco, que continuó en la idea de exigir los datos PNR, si bien intentando adaptarlo a las nuevas exigencias jurisprudenciales de la Unión Europea.

El 27 de junio de 2006, el Consejo decidió autorizar a la Presidencia, asistida por la Comisión, a entablar negociaciones para un Acuerdo con los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional (Department of HomelandSecurity) de los Estados Unidos26 .

El 11 de octubre de 2006, el Departamento de Seguridad del Territorio Nacional de los Estados Unidos envió una nota dirigida a la Presidencia del Consejo y a la Comisión relativa a la interpretación de determinadas disposiciones de los Compromisos publicados el 11 de mayo de 2004 por el DHS en relación con la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas27.

La respuesta por parte de las instituciones comunitarias, fue la siguiente: "A la vez que tomamos conocimiento del contenido de su nota, deseamos reiterar la importancia que la Unión Europea y los Estados miembros conceden al respeto de los derechos fundamentales, en especial a la protección de los datos personales.

El hecho de que el DHS se comprometa a seguir aplicando los Compromisos permite a la Unión Europea considerar que, a efectos de la aplicación del Acuerdo, el DHS garantiza un nivel adecuado de la protección de datos".

Con base en dichas negociaciones, el 16 de octubre en Luxemburgo y el 19 de octubre, ambos de 2006, se firma el Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos.

Hasta la fecha la Unión europea sólo ha celebrado acuerdos similares a los descritos anteriormente, también con Canadá y Australia, y limitados al transporte aéreo.En junio de 2015 el Consejo adoptó una Decisión por la que se autoriza la apertura de negociaciones con vistas a un acuerdo con México.

---

[25]Prensa e Información. COMUNICADO DE PRENSA N° 46/06. 30 de mayo de 2006. Sentencia del Tribunal de Justicia en los asuntos acumulados C-317/04 y C-318/04. CJE/06/46.

[26] DECISIÓN 2006/729/PESC/JAI DEL CONSEJO de 16 de octubre de 2006 relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DOUE C 298/27, 27.10.2006.

[27]Nota del Departamento de Seguridad del Territorio Nacional (DHS) de los Estados Unidos de América a la Presidencia del Consejo y a la Comisión relativa a la interpretación de determinadas disposiciones de los compromisos publicados el 11 de mayo de 2004 por el DHS en relación con la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas (2006/C259/01), DOUE C 259/1, 21.10.2006.

De esta manera, las únicas disposiciones vigentes en materia de transferencia de datos por las compañías aéreas a las autoridades de la UE, eran las contenidas en la Directiva 2004/82/CE del Consejo[28], según la cual las compañías aéreas tienen la obligación de comunicar a las autoridades competentes de los Estados miembros los datos de información anticipada sobre pasajeros (AdvancePassengerInformation, (API).

Los datos API, son datos esencialmente biográficos, que incluyen el número y tipo de documento de viaje utilizado, la nacionalidad, el nombre y apellidos completos, la fecha de nacimiento, el puesto fronterizo de entrada, el código de transporte, los horarios de salida y llegada del transporte, el número total de pasajeros transportados y el lugar de embarque inicial.

No obstante, la transferencia y tratamiento de los datos PNR se considera una aplicación mucho más eficaz en la lucha contra el terrorismo internacional, ya que contienen más elementos y se dispone de ellos antes que de los datos API, lo que permitirá una mayor anticipación[29].

5. Marco Jurídico datos Pnr nn la Unión Europea: Directiva (UE) 2016/681

No obstante el acuerdo con Estados Unidos, la Comisión Europea continuó trabajando en el marco regulatorio de los datos PNR, y, en concreto, en lo relativo a la utilización de esta categoría de datos con fines policiales[30], que no llegó a aprobarse debido a la entrada en vigor del Tratado de Lisboa[31] en 2009, dado que no se ajustaba a los nuevos requisitos exigidos en los Tratados.

Dentro de lo que se dio en llamar el "nuevo" marco europeo de protección de datos, se ha aprobado recientemente, junto al Reglamento0 general de protección de datos[32], y la Directiva de protección de datos en asuntos criminales[33], la *Directiva relativa a la utilización de los datos PNR*[34].

---

[28]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, DO L 261. 06.08.2004.

[29]https://es.wikipedia.org/wiki/Sistema_PNR_europeo

[30]Propuesta de Decisión marco 2007/0237 (CNS) del Consejo, de 6 de noviembre de 2007, sobre la utilización de datos del registro de nombres de los pasajeros (PassengerName Record-PNR) con fines represivos.

[31]TRATADO DE LISBOA POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA Y EL TRATADO CONSTITUTIVO DE LA COMUNIDAD EUROPEA (2007/C 306/01). DOUE C 306. 17.12.2007.

[32]Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DO L 119.04.05.2016.

[33]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. DO L 119.04.05.2016.

[34]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,

Sus objetivos, como indica, su Considerando (5), son garantizar la seguridad, proteger 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.

Como señaló el propio Consejo europeo, la necesidad del uso de los datos PNR deriva de que "las actividades terroristas y de delincuencia organizada a menudo conllevan desplazamientos internacionales. En respuesta a la supresión de los controles en las fronteras interiores en virtud del Convenio de Schengen, la UE prevé el intercambio de datos personales entre autoridades policiales. El sistema PNR va encaminado a complementar los instrumentos que ya existen para hacer frente a la delincuencia transfronteriza. El tratamiento de datos PNR permitiría a las autoridades policiales descubrir a las personas no sospechosas de realizar actividades delictivas o terroristas antes de que un análisis específico de los datos mostrara que podrían serlo.

Además, la mayoría de los Estados miembros ya utilizan los datos PNR a disposición de la policía u otras autoridades en virtud de la legislación nacional. Un sistema de PNR de la UE permitiría también armonizar las disposiciones legales de los Estados miembros, evitando así la inseguridad jurídica y las deficiencias de seguridad, salvaguardando al mismo tiempo la protección de datos".[35].

La finalidad de la recogida y uso de los datos PNR, viene determinada por la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo[36] y delitos graves (entendiéndose por tales, conforme al apartado 9) del art. 3 de la Directiva, "*los delitos incluidos en el anexo II que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no*

---

investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. DO L 119.04.05.2016.

[35]http://www.consilium.europa.eu/es/policies/fight-against-terrorism/passenger-name-record/

[36]DECISIÓN MARCO DEL CONSEJO, de 13 de junio de 2002, sobre la lucha contra el terrorismo. (2002/475/JAI). DOCE L 164. 22.06.2002. Conforme a su art. 1, deben considerare "*delitos de terrorismo los actos intencionados a que se refieren las letras a) a i) tipificados como delitos según los respectivos Derechos nacionales que, por su naturaleza o su contexto, puedan lesionar gravemente a un país o a una organización internacional cuando su autor los cometa con el fin de:*

— intimidar gravemente a una población,

— obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo,

— o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional;

a) atentados contra la vida de una persona que puedan tener resultado de muerte;

b) atentados graves contra la integridad física de una persona;

c) secuestro o toma de rehenes;

d) destrucciones masivas en instalaciones gubernamentales o públicas, sistemas de transporte, infraestructuras, incluidos los sistemas informáticos, plataformas fijas emplazadas en la plataforma continental, lugares públicos o propiedades privadas, que puedan poner en peligro vidas humanas o producir un gran perjuicio económico;

e) apoderamiento ilícito de aeronaves y de buques o de otros medios de transporte colectivo o de mercancías;

f) fabricación, tenencia, adquisición, transporte, suministro o utilización de armas de fuego, explosivos, armas nucleares, biológicas y químicas e investigación y desarrollo de armas biológicas y químicas;

g) liberación de sustancias peligrosas, o provocación de incendios, inundaciones o explosiones cuyo efecto sea poner en peligro vidas humanas;

h) perturbación o interrupción del suministro de agua, electricidad u otro recurso natural fundamental cuyo efecto sea poner en peligro vidas humanas;

i) amenaza de ejercer cualesquiera de las conductas enumeradas en las letras a) a h)".

inferior a tres años con arreglo al derecho nacional de un Estado miembro")[37]. El tratamiento de datos personales debe ser proporcional a los objetivos específicos de seguridad que se pretenden alcanzar con la Directiva (Considerando (11).

Pero ¿que son los PNR, y cual su extensión? De nuevo, la Directiva en su art. 3, apartado5) establece que por «registro de nombres de los pasajeros» o «PNR»: una relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades".

La lista de los datos PNR, conforme al Considerando 15) debe elaborarse teniendo en cuenta las necesidades de información de las autoridades públicas para el cumplimiento de los fines determinados anteriormente, debiendo contener la información detallada sobre las reservas e itinerarios de viajes que permita a las autoridades competentes identificar a los pasajeros por vía aérea que representan una amenaza para la seguridad interior. El Anexo I, bajo la denominación de "*Datos del registro de nombres de los pasajeros recopilados por las compañías aéreas*" establece como categorías de datos: 1. Localizador de registro PNR 2. Fecha de reserva/emisión del billete 3. Fecha(s) fechas de viaje prevista(s) 4. Nombre(s) y apellido(s) 5. Dirección y datos de contacto (número de teléfono, dirección de correo electrónico) 6. Todos los datos de pago, incluida la dirección de facturación 7. Itinerario completo del viaje para el PNR específico 8. Información sobre viajeros

[37] ANEXO II
Lista de los delitos a que se refiere el artículo 3, punto 9
1. pertenencia a una organización delictiva
2. trata de seres humanos
3. explotación sexual de niños y pornografía infantil
4. tráfico ilícito de estupefacientes y sustancias psicotrópicas
5. tráfico ilícito de armas, municiones y explosivos
6. corrupción
7. fraude, incluido el que afecte a los intereses financieros de la Unión
8. blanqueo del producto del delito y falsificación de moneda, con inclusión del euro
9. delitos informáticos/ciberdelincuencia
10. delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y
variedades vegetales protegidas
11. ayuda a la entrada y residencia ilegales
12. homicidio voluntario, agresión con lesiones graves
13. tráfico ilícito de órganos y tejidos humanos
14. secuestro, detención ilegal y toma de rehenes
15. robo organizado y a mano armada
16. tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte
17. falsificación y violación de derechos de propiedad intelectual o industrial de mercancías
18. falsificación de documentos administrativos y tráfico de documentos administrativos falsos
19. tráfico ilícito de sustancias hormonales y otros factores de crecimiento
20. tráfico ilícito de materiales radiactivos o sustancias nucleares
21. violación
22. delitos incluidos en la jurisdicción de la Corte Penal Internacional
23. secuestro de aeronaves y buques
24. sabotaje
25. tráfico de vehículos robados
26. espionaje industrial.

asiduos 9. Agencia de viajes/operador de viajes 10. Situación de vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva 11. Información PNR escindida/dividida 12. Observaciones generales (incluida toda la información disponible sobre menores de 18 años no acompañados, como nombre y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada) 13. Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos (*Automatic Ticket FareQuote*) 14. Datos del asiento, incluido el número 15. Información sobre códigos compartidos 16. Toda la información relativa al equipaje 17. Número de viajeros y otros nombres de viajeros que figuran en el PNR 18. Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API) (incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada) 19. Todo el historial de cambios de los datos PNR indicados en los números 1 a 18.

Como se observa, un detallado y problemático elenco de datos que podrán ser objeto de tratamiento, estableciendo la obligación de la transferencia de datos PNR de las compañías aéreas a las autoridades nacionales (art. 8), así como el tratamiento que estas efectúen de esos datos. Con arreglo a la nueva Directiva, las compañías aéreas tendrán que facilitar los datos PNR de los vuelos que entren en la UE o salgan de esta. También permitirá, aunque no será obligatorio, que los Estados miembros recopilen los datos PNR correspondientes a determinados vuelos interiores de la UE.

Ahora bien, dichas listas no podrán basarse (Considerando (15), ni consecuentemente tratarse datos, estando expresamente prohibido (art.13. 4), cuando revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona.

Cada Estado miembro deberá crear la denominada «Unidad Información sobre los Pasajeros» (UIP), que recibirá los datos PNR de las compañías aéreas, tal y como establece el art. 4. Sus funciones se desglosan en dos: a) recoger los datos PNR, almacenar, procesar y transferir los datos o el resultado de su tratamiento a las autoridades competentes (conforme al art. 7, cada Estado elaborará la lista de autoridades competentes, que lo serán siempre en función de su capacidad para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo); b) intercambiar los datos y/o los resultados de tratamiento con las UIP de otros Estados (art. 9) y con Europol (art. 10). Igualmente, conforme al art. 11, se autoriza la transferencia de datos a terceros países, que solo podrá producirse en circunstancias muy particulares y deberá estudiarse caso por caso.

Importante en esta materia es la obligación, establecida en el art. 5, de que de todas las UIP tendrán que designar un responsable de la protección de datos personales que, junto a la labor de control del tratamiento de datos y efectivación de garantías, constituirá también el punto único de contacto en el que los interesados podrán ejercer sus derechos en todo lo relativo al tratamiento de sus datos PNR.

En el marco de estas actividades, conforme al art. 6, los datos PNR pueden utilizarse de distintos modos:

- para la evaluación previa a la llegada o a la salida de los pasajeros en comparación con criterios de riesgo predeterminados o para identificar a determinadas personas;
- como contribución a la definición de estos criterios de riesgo;
- con vistas a investigaciones o enjuiciamientos determinados.

En lo tocante a la conservación y despersonalización de los datos (art. 12), éstos se conservarán inicialmente durante seis meses, después de lo cual se enmascararán y conservarán durante otros cuatro años y medio, con un estricto procedimiento de acceso a la totalidad de los datos.

El art. 13 contiene las previsiones relativas a la protección de los datos de carácter personal, que pueden agruparse:

prohíbe la recogida y el uso de datos sensibles

los Estados miembros deberán asegurarse de que los pasajeros reciban una información precisa, de fácil acceso, y comprensión sobre la recogida de datos PNR y sus derechos.

el tratamiento automatizado de los datos PNR no podrá ser la única base para tomar decisiones que tengan consecuencias jurídicas adversas o que afecten gravemente a una persona.

Cuando existan indicios de una posible violación de los datos personales que suponga un elevado riesgo para la protección de estos o afecten negativamente a la intimidad del interesado, se debe comunicar, sin demora injustificada, al interesado y a la autoridad supervisora nacional.

La Directiva establece, igualmente, la obligación de desarrollar protocolos técnicos comunes, que hagan interoperables las transferencias de datos por medios electrónicos, y que ofrezcan, conforme al art. 16, garantías suficientes en relación con las medidas de seguridad técnicas y las medidas organizativas que rigen el tratamiento de datos a llevar a cabo. No obstante, pude producirse algún fallo técnico. En este supuesto, se autoriza la transmisión de datos por otro procedimiento adecuado, siempre que se conserve el mismo nivel de seguridad y se cumpla estrictamente lo relativo a la protección de datos personales.

La Directiva opta por el sistema de transmisión de datos, frente al de extracción, y así las compañías aéreas "transmitirán" los datos PNR a la autoridad solicitante, manteniendo aquellas el control de los datos suministrados, lo que proporciona un mayor nivel de protección de datos. Este sistema será obligatorio para todas las compañías aéreas (Considerando (16).

Reflexiones Finales

El resurgimiento de los nacionalismos exacerbados y violentos, de las teologías de la guerra y la aniquilación, de las tribus y grupos de la caverna ha colocado al planeta al borde de una hecatombe, donde los sufridos ciudadanos, como casi siempre, seremos los primeros en pagar.

Pero la constatación de esta realidad no nos debe llevar, como se está comprobando en la realidad, a un control planetario de nuestras actividades, de nuestra vida. No podemos caer en la inversión del sagrado principio de la presunción de inocencia, por el peligroso y antidemocrático de la "presunción de culpabilidad",

donde se nos exige, en el mejor de los casos, que entreguemos nuestra intimidad, para que no se sabe muy bien quien, sin control, decida si somos o no ciudadanos honorables; o tan simplemente, ciudadanos.

Estamos asistiendo a la consolidación de un nuevo paradigma harto peligroso para los derechos de los ciudadanos y las libertades públicas. Este no es otro que el de la "seguridad a toda costa". Frente a los esfuerzos por mantener y agrandar el ámbito de las libertades en las sociedades democráticas, la seguridad es el valor-guía que lo modula y delimita todo.

No es asumible, en estas coordenadas, que el Estado pretenda, amparado en lo indeterminado de la seguridad, protegerse de sus propios ciudadanos, pues, desposeído de la base social y legitimadora que lo sustenta, sus acciones carecen de sentido, deviniendo pura arbitrariedad. La seguridad es fácilmente obtenible en Estados totalitarios que ven a sus ciudadanos como potenciales delincuentes frente a los cuales todo, o casi todo, vale, pues lo relevante y prioritario es mantener la estructura de poder al precio que sea menester.

Hay que luchar contra la violencia y el terrorismo, pero de manera ejemplificante. Con determinación, pero sin intrusiones innecesarias; con normas contundentes, pero que respeten las libertades y derechos de los ciudadanos.

Referências

UNION EUROPEA. 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. DO L 119.04.05.2016. Considerando (2).

UNION EUROPEA. **Grupo del artículo 29 sobre protección de datos. Dictamen 4/2003** relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de los pasajeros, 13 de junio de 2003, 11070/03/ES WP 78.

UNION EUROPEA. **Directiva 95/46/CE** del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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.

SANCHEZ BRAVO, A., **Internet y la sociedad europea de la información**: implicaciones para los ciudadanos, Publicaciones de la Universidad de Sevilla, 2001.

SANCHEZ BRAVO, A. La protección del derecho a la libertad informática en la Unión Europea, Publicaciones de la Universidad de Sevilla, 1998;

Convidado