La intimidad de la Unión Europea y la seguridad de los Estados Unidos: la tensión entre la ley europea de protección de datos y los esfuerzos por parte de los Estados Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros delitos

Carter Manny*

SUMARIO: INTRODUCCIÓN.—EL MARCO LEGAL PARA LA PROTECCIÓN DE LA INTIMIDAD EN LA UNIÓN EUROPEA Y EN LOS ESTADOS UNIDOS: *La protección de la intimidad en Europa. La protección de la*

* Profesor adjunto de Derecho Mercantil en la Universidad del Sur de Maine, Portland (Maine) 04104-9300 EE.UU.; correo electrónico: manny@usm.main.edu; tel.: +1 207 780 4129, fax: +1 207 780 4662. Se han presentado versiones de este trabajo en un Congreso sobre relaciones comerciales entre la Unión Europea y los Estados Unidos patrocinado por la Oxford Round Table en la Universidad de Oxford (Oxford), Reino Unido, el 2 de agosto de 2004, y en la reunión anual de la Academia de Estudios Jurídicos del Comercio en Ottawa, Canadá, el 20 de agosto de 2004.

INTRODUCCIÓN

Existen diferencias importantes entre Europa y los Estados Unidos con respecto al uso del ordenamiento jurídico en aras de proteger la intimidad. Los Estados miembros de la Unión Europea disfrutan de un sistema armonizado de leyes para la protección integral de los datos, administrado por las agencias gubernamentales de cada país. Estas leyes reflejan la visión de que la intimidad es un derecho humano fundamental que disfruta de la protección obligada de los gobiernos. Dicha protección se aplica tanto al uso de los datos dentro de Europa como a las transferencias internacionales con destino a países fuera de la Unión Europea.

En los Estados Unidos, sin embargo, el régimen jurídico no contiene el mismo compromiso con la protección de la intimidad. Al contrario, existe un cajón de sastre de disposiciones regionales y estatales, constitucionales, estatutarias y reglamentarias, la mayoría de las cuales se refieren a un espectro limitado de actividades comerciales. En muchos casos, ya sea debido a la falta de derechos legales, ya sea debido a la naturaleza de las mismas disposiciones legales, el régimen estadounidense confía en que el particular tomará medidas para proteger su información personal. A fines del siglo XX había en los Estados Unidos relativamente poca preocupación pública por el uso gubernamental de información personal, y mucho más recelo respecto al uso comercial de los datos. Por consiguiente, la protección de la intimidad se consideraba una cuestión más bien de protección al consumidor, y no tanto de protección de derechos humanos.

Los atentados terroristas en los Estados Unidos el día 11 de septiembre de 2001 cambiaron esto. La seguridad se convirtió de repente en una preocupación primordial. Había personas en el gobierno que creían que la tecnología informática en general, y las prácticas de extracción de datos en particular, podrían ayudar a detectar la actividad terrorista y a mejorar la seguridad pública general, la seguridad de fronteras y la seguridad del transporte aéreo. Entre los proyectos interiores de los Estados Unidos está el Proyecto del Departamento de Defensa denominado *Total Information Aware-*

ness (Conocimiento Total de Información), cuyo nombre se cambió por el de *Terrorism Information Awareness* (Conocimiento de Información sobre el Terrorismo), y que examinaría las bases de datos comerciales y del gobierno en busca de indicios de posible actividad terrorista. Con respecto a la seguridad de fronteras, en la actualidad se están exigiendo ciertos datos biométricos de las personas que solicitan visado; esto consiste en tomar la fotografía digital y escanear los dedos de los visitantes extranjeros, y los mismos datos se obtendrán, en la frontera, de los visitantes que provienen de la mayoría de los países cuyos ciudadanos no precisan de visado para entrar en los Estados Unidos. Con respecto a la aviación nacional, existen el sistema CAPPS (cuyas siglas en inglés significan «Sistema Informatizado de Preselección de Pasajeros»), que se utiliza en la actualidad, y un sistema propuesto denominado CAPPS II. Ambos utilizan una combinación de análisis por ordenador de la información sobre reservas de pasajeros y otros factores para intentar evitar el embarque de gente peligrosa.

Con respecto a los vuelos internacionales, existen sistemas adicionales para la recogida y el análisis de los datos de los pasajeros. La Ley de Seguridad de la Aviación y del Transporte[1], aprobada por el Congreso de los Estados Unidos en el mes de noviembre de 2001, requiere que el gobierno estadounidense tenga acceso a los datos que poseen las aerolíneas sobre los pasajeros de vuelos entrantes con origen fuera de los Estados Unidos. Esta Ley ha suscitado inquietudes en relación con la protección de la intimidad por parte de Europa, que tiene un sistema integral de protección de datos, porque las bases de datos sobre pasajeros aéreos incluyen con frecuencia aspectos como información sobre tarjetas de crédito, el historial de viaje de la persona, reservas de hotel y otras informaciones sin vínculo directo al vuelo en sí, que pueden proporcionar muchos detalles sobre la vida privada del pasajero. Por otro lado, de acuerdo con el sistema europeo de protección de datos, la transferencia de datos personales fuera de la Unión Europea es ilegal en casos donde la Comisión Europea no está convencida de que el país de destino proporcione una protección «adecuada» a la intimidad, o donde ninguna de las excepciones limitadas previstas sea de aplicación. Dado que ninguna excepción de acuerdo con la ley europea parecía cubrir tales transferencias, y dado que el régimen jurídico estadounidense generalmente no satisface las normas europeas de protección adecuada a la intimidad, las líneas aéreas tuvieron que verse con la difícil elección entre proporcionar los datos al gobierno estadounidense y así infringir la ley europea, o negarse y enfrentarse a la posibilidad de perder los derechos de aterrizar en los Estados Unidos.

Este trabajo examina la tensión entre la ley europea de protección de datos y la necesidad por parte de los Estados Unidos de promover la seguridad dentro del contexto de la disputa sobre la transferencia de los datos de pasaje-

[1] Véase *Aviation and Transportation Security Act,* Pub. L. 107-71 § 115 (2001), codificada en 49 U.S.C. § 44909(c).

ros aéreos. Examina las negociaciones entre la Comisión Europea y el Departamento de Seguridad Nacional de los Estados Unidos, que llegaron a un arreglo provisional en el año 2004. Asimismo, considera la tensión dentro de Europa entre grupos de cargos públicos, algunos de los cuales resaltan la necesidad de proteger la intimidad como un derecho fundamental, y otros que perciben una mayor necesidad de transigir en un acuerdo político más pragmático con uno de sus principales socios de comercio y aliados. Esta tensión llevó al Parlamento Europeo a impugnar acciones de la Comisión Europea y del Consejo de Ministros ante el Tribunal Europeo de Justicia, por exceder su autoridad al pactar el arreglo. Antes de examinar los detalles de la controversia entre la Unión Europea y los Estados Unidos, es conveniente contrastar los marcos que ostentan ambos sistemas para la protección de la intimidad.

EL MARCO LEGAL PARA LA PROTECCIÓN DE LA INTIMIDAD EN LA UNIÓN EUROPEA Y EN LOS ESTADOS UNIDOS

La protección de la intimidad en Europa

Desde el final de la Segunda Guerra Mundial ha habido muchas declaraciones multilaterales sobre la importancia de la intimidad como derecho humano. Éstas incluyen la Declaración Universal de los Derechos Humanos de las Naciones Unidas (1948)[2], el Convenio de Derechos Humanos del Consejo de Europa (1950)[3], las Directrices de la OCDE sobre la Protección de la Intimidad y los Flujos Transfronterizos de Datos Personales (1980)[4] y el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (1981)[5], siendo este último también conocido como el Convenio 108. En 1995, la Unión Europea adoptó la Directiva sobre Protección de Datos[6] para armonizar las leyes nacionales sobre protección de datos. La intimidad se reconoce como derecho humano también en la Carta de Derechos Fundamentales de la Unión Europea (2000)[7] y en el Proyecto de la Constitución para la Unión Europea (2003)[8].

---

[2] Véase *The Universal Declaration of Human Rights,* artículo 12, reeditada en Marc ROTENBERG, *The Privacy Law Sourcebook 2003*, 316.

[3] Véase *Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms,* artículo 8, reeditado en Marc ROTENBERG, *The Privacy Law Sourcebook 2003*, 322.

[4] Véase *OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* OECD Doc. (D 58 final) (1 de octubre de 1980) [en adelante, «las directrices de la OCDE»].

[5] Véase *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,* Eur. T.S. No. 108 (28 de enero de 1981).

[6] Directiva 95/46/CE, 1995 O.J. (L281) 31 [en adelante, «la Directiva sobre Protección de Datos»].

[7] Véase *Charter of Fundamental Rights of the European Union,* artículo 8, reeditada en Marc ROTENBERG, *The Privacy Law Sourcebook 2003,* 436.

[8] Véase *Proyecto de Tratado por el que se instituye una Constitución para Europa,* artículo 50, 2003 O.J. (C169) 1.

El marco jurídico general de la legislación europea sobre la intimidad se expone en la Directiva sobre Protección de Datos, que establece un sistema administrado por las autoridades en materia de protección de datos, y que se aplica a todas las bases de datos, tanto gubernamentales como particulares, que contienen información personal. La Directiva impone una limitación, en el sentido de que los datos recogidos con fines determinados no deben utilizarse para otros fines[9]. Asimismo, contiene el principio de la proporcionalidad: los datos deben ser adecuados, pertinentes y no excesivos en relación al fin para el cual se han recogido[10]. Los datos deben ser exactos y actualizados[11], y no deben conservarse durante más tiempo que el necesario para los fines para los que fueron recogidos[12]. Existen límites sobre la recogida o el tratamiento de datos sensibles, que se definen como datos personales que traten del origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a sindicatos, la salud o la vida sexual. Los datos sensibles se pueden tratar, por ejemplo, para fines de empleo o sanidad, o en general con el consentimiento del interesado[13]. La Directiva sobre Protección de Datos exige que se comuniquen al individuo los fines para los cuales los datos serán tratados, los destinatarios de la transferencia de datos y el derecho de acceder a la información y rectificar los errores que existan[14]. Los interesados tienen el derecho de tomar acción judicial privada por perjuicios en caso de infracción de la ley, además del derecho al recurso administrativo[15].

La Directiva sobre Protección de Datos es una de las fuentes variadas de legislación europea sobre la intimidad. Se encuentran algunas protecciones para la intimidad en otras leyes sectoriales. Semejante disposición rigiendo la información de carácter personal se encuentra en el Reglamento de Sistemas Informatizados de Reserva, que afirma que los datos personales del consumidor sólo se pondrán a la disposición de otras personas no implicadas en la transacción en caso de que el consumidor preste su consentimiento[16].

La protección de la intimidad en los Estados Unidos

La ley federal estadounidense posee estatutos distintos para el sector público y para el privado. La Ley federal sobre la Intimidad[17] es de aplicación

---

[9] *Directiva sobre Protección de Datos, supra,* nota 6, artículo 6(1)(b).
[10] *Id.,* artículo 6(1)(c).
[11] *Id.,* artículo 6(1)(d).
[12] *Id.,* artículo 6(1)(e).
[13] *Id.,* artículo 8.
[14] *Id.*, artículos 10 y 12.
[15] *Id.,* artículos 22 y 23.
[16] Reglamento (CEE) n.º 2299/89 del Consejo, por el que se establece un código de conducta para los sistemas informatizados de reserva, 1989 O.J. (L220) 1 [en adelante, «el Reglamento de Sistemas Informatizados de Reserva»].
[17] 5 U.S.C. § 552a (2000).

solamente a datos que obran en poder del gobierno federal. Sus disposiciones tienen muchos aspectos en común con el sistema europeo. Existe una restricción en cuanto a los fines, que dispone que la información recogida para un fin no debe utilizarse para otro fin sin el consentimiento del interesado. Existe un principio de calidad de datos, que exige que la información sea exacta, pertinente y oportuna. Existe un derecho de acceso y rectificación. Los datos no deben revelarse sin el consentimiento del interesado, a menos que sea de aplicación una de varias excepciones; entre ellas, en la ejecución del ordenamiento jurídico, en órdenes emitidas por un órgano jurisdiccional y por circunstancias apremiantes con relación a la sanidad o la seguridad del interesado. No obstante, dado que la Ley sobre la Intimidad no confiere derechos a extranjeros no-residentes, no serviría de ayuda a la mayoría de los europeos que puedan sentir inquietud al saber que datos suyos, en calidad de pasajeros, estén en manos del gobierno estadounidense. Sin embargo, los europeos pueden presentar una solicitud al Servicio de Aduanas y Protección de Fronteras, de acuerdo con la Ley federal de Libertad de Información[18], y así enterarse de la naturaleza de los datos de pasajero que se poseen a nombre del interesado.

Los estatutos federales sobre la intimidad en el sector privado están dirigidos a industrias o actividades específicas. Entre éstas están la industria de los informes de crédito[19], las organizaciones sanitarias[20], las empresas de servicios financieros[21], la industria de televisión por cable[22], las entidades educativas[23] y las empresas de alquiler de vídeo[24]. La legislación sobre la intimidad no atañe a los sistemas de reserva de las aerolíneas. No obstante, la violación de una política sobre la intimidad, adoptada de modo voluntario por una empresa, puede ser objeto de ejecución de acuerdo con las disposiciones sobre prácticas mercantiles injustas, conforme al apartado 5 de la Ley de la Comisión Federal de Comercio[25], para la mayoría de las empresas, y mediante el apartado 411(a) de la Ley federal de Aviación de 1958[26], para las aerolíneas.

---

[18] 5 U.S.C. § 552 (2000). La Ley de Libertad de Información contiene excepciones, algunas de las cuales restringen la publicidad de información retenida para ciertos fines con respecto a la ejecución del ordenamiento jurídico. 5 U.S.C. § 552a(b)(7). No se exige publicidad, por ejemplo, cuando «podría razonablemente esperarse que [dicha publicidad] interfiera con actuaciones ejecutivas», o cuando podría revelar técnicas para investigaciones o acciones judiciales si cabe dentro de la sospecha razonable que las mismas corren el riesgo de burlar la ley. 5 U.S.C. § 552a(b)(7)(A) y (E).

[19] *Fair Credit Reporting Act,* 15 U.S.C. §§ 1681-1681t.

[20] *Privacy of Individually Identifiable Health Information,* 45 C.F.R. §§ 164.102-164.534, 164.104 (2002) (conocido como «el Reglamento sobre Intimidad de la Ley de Responsabilidad y Portabilidad del Seguro Médico»).

[21] *Gramm-Leach-Bliley Act,* 15 U.S.C. §§ 6801-6810.

[22] *Cable Communications Policy Act,* 47 U.S.C. § 551(a).

[23] *Family Educational Rights and Privacy Act,* 20 U.S.C. § 1232g.

[24] *Video Privacy Protection Act,* 18 U.S.C. § 2710(e).

[25] 15 U.S.C. § 45(a)(1) (2000).

[26] 49 U.S.C. § 41712(a) (2000).

LOS ESFUERZOS ESTADOUNIDENSES A FAVOR DE LA SEGURIDAD, CON RELACIÓN A LA TECNOLOGÍA INFORMÁTICA

Extracción de datos y la información nacional estadounidense

El Proyecto propuesto denominado Conocimiento de Información sobre el Terrorismo (antes Conocimiento Total de Información), ejecutado por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) del Departamento de Defensa estadounidense, tenía como su objetivo la extracción de información desde bases de datos comerciales y otras bases de datos en los Estados Unidos para detectar la actividad terrorista. El pueblo estadounidense tuvo conocimiento del Proyecto por primera vez en otoño del año 2002, cuando dirigía la Agencia el antiguo almirante John Poindexter, quien fue involucrado en el escándalo «Irán-Contra» durante el gobierno de Reagan. Debido a la polémica acerca del Proyecto, dimitió Poindexter en agosto de 2003[27] y el Congreso acordó restringir la financiación del Proyecto Conocimiento Total de Información al mes siguiente[28]. El programa, sin embargo, puede continuarse, utilizando contratistas privados, además de empleados de la DARPA, como una «cuenta de bolsa negra», es decir, sin necesidad de aprobación ni de supervisión por parte del Congreso estadounidense[29].

La práctica del gobierno de extraer información de bases de datos comerciales para detectar actividades terroristas se contempló en un informe del mes de febrero de 2004, emitido por la Comisión Consultiva de Tecnología e Intimidad (TAPAC), nombrada por el Secretario de Defensa, Donald Rumsfeld. En un artículo publicado en el *Wall Street Journal* el día 3 de junio de 2004, el Presidente de la Comisión, Newton Minow, expuso un resumen de las conclusiones de la misma, diciendo que la extracción de datos es una práctica esencial si los Estados Unidos han de defenderse, mas es igualmente esencial que se limite la extracción de datos a búsquedas dirigidas meticulosamente hacia un objetivo específico y que se cumplan las normas legales existentes[30]. Minow avisó de los peligros de la extracción de datos sin supervisión rigorosa y sin garantías; dentro de dicha extracción, se podría examinar a fondo información sobre personas que no han hecho nada para merecer sospechas. Tal programa tendría un efecto espeluznante sobre la libertad. Él mismo observó que los riesgos se aumentan en cuanto la extracción de datos está expuesta a problemas de índole técnica, entre ellos el uso

---

[27] Véase, *e.g.,* «Poindexter Resigns But Defends Program», *Washington Post*, 13 de agosto de 2003, en A02.

[28] Véase, *e.g.,* «Congress Defunds Controversial "Total Information" Program», disponible en *http://www.commondreams.org/cgi-bin/print.cgi?file = /headlines03/0926-02.htm* (visitado por última vez el 11 de julio de 2004).

[29] Véase «Total Information Awareness Alive and Well in Arlington County», disponible en *http:// prison planet.Com/ articles/june2004/060704 tia.htm* (visitado por última vez el 11 de julio de 2004).

[30] Véase Newton MINOW, «Seven Clicks Away», *Wall St. J.,* 3 de junio de 2004, A14.

de información errónea o incompleta, lo cual incrementaría mucho la probabilidad de producir falsas alarmas. También advirtió de que las técnicas y los datos reunidos para combatir el terrorismo podrían utilizarse para otros fines. Muchas de sus inquietudes son compartidas por cargos públicos de Europa.

La extracción de datos y la selección de pasajeros aéreos en los Estados Unidos

El Sistema Informatizado de Preselección de Pasajeros (CAPPS) se adoptó en 1998 como respuesta a las actividades de la Comisión de Seguridad de Aviación, que existió en los Estados Unidos desde 1996 a 1997 y fue presidida por el Vicepresidente Gore. La Comisión se formó después de que se estrellara el vuelo 800 de la TWA a la altura de Long Island (Nueva York), en el verano de 1996[31]. El sistema CAPPS original consistía en la aplicación de un algoritmo secreto de selección a los datos de reserva del pasajero, en el momento en que el pasajero realiza la facturación para un vuelo. Después del 11 de septiembre de 2001, también se agregaron al sistema una lista de nombres para «exclusión aérea» y una lista de nombres para «vigilancia», para identificar a personas que, según las conclusiones del gobierno estadounidense, no hay que permitir embarcar a menos que las autoridades policiales federales (normalmente el FBI) den su permiso para cada caso de forma individual[32].

El sistema de selección propuesto como sustituto, CAPPS II, analizaría datos provenientes de bases de datos comerciales y del gobierno, además de información proveniente del sistema de reservas aéreas. CAPPS II exigiría que las líneas aéreas obtengan información adicional de los pasajeros en el momento de la reserva, información que no se exige actualmente y que comprendería la fecha de nacimiento, la dirección y el número de teléfono de casa del pasajero. Después de comprobar la identidad del pasajero, el sistema realizaría una valoración de riesgos para detectar si el viajero supone una amenaza terrorista o es un fugitivo nombrado en una orden estatal o federal de busca y captura por un delito de violencia. Las tres categorías de riesgo de pasajeros son: 1) ningún riesgo; 2) riesgo desconocido o elevado, y 3) riesgo alto. Los resultados de la valoración del riesgo del pasajero se imprimen entonces en un mensaje encifrado en la tarjeta de embarque, para indicar el nivel correspondiente de preselección. En su día, el sistema podría transmitir la valoración de riesgo de cada pasajero por medios electrónicos al punto de control de seguridad[33].

CAPPS II ha sido polémico, no sólo porque emplea bases de datos co-

---

[31] Véase, *e.g.*, Richard A. CLARKE, *Against All Enemies: Inside America's War on Terror,* 123.

[32] Véase Edward HASBROUCK, «Total Travel Information Awareness», disponible en *http://www.Hasbrouck.org/articles/travelprivacy.html* (visitado por última vez el 11 de julio de 2004).

[33] Véase la Administración Estadounidense de Seguridad en el Transporte, «CAPPS II at a Glance», disponible en *http://www.tsa.gov/public/display?theme=5&content=0900051980088d91& print=yes* (visitado por última vez el 18 de marzo de 2004).

merciales, sino porque en numerosos casos las líneas aéreas han entregado datos de pasajeros a agencias gubernamentales y a contratistas del gobierno para que se realicen pruebas de la tecnología de preselección propuesta. Northwest Airlines fue la primera en entregar datos para pruebas en 2001[34]. Entre otras, están JetBlue[35], American Airlines[36], Delta, Continental, America West y Frontier Airlines[37]. CAPPS II también ha recibido críticas desde dentro del gobierno federal. Un informe del mes de febrero de 2004, emitido por la Oficina de Contabilidad General de los Estados Unidos, ha señalado muchos problemas con la puesta en práctica de CAPPS II; entre otros, retrasos en la obtención de datos de pasajeros para realizar pruebas, la precisión de los datos, la manera de evitar accesos no autorizados al sistema, la intimidad, la cooperación internacional necesaria para obtener datos de pasajeros, la posible expansión del programa más allá de su fin original, y la posibilidad de evadir el sistema utilizando una identidad robada y viajando bajo el nombre de otra persona[38].

Pruebas para el propuesto Programa estadounidense de Viajeros Inscritos

En un esfuerzo por aligerar la verificación de pasajeros en aeropuertos, la Administración de Seguridad en el Transporte (TSA) comenzó en el verano del año 2004 a realizar pruebas con un mecanismo denominado «Programa de Viajeros Inscritos» en cinco aeropuertos estadounidenses: Boston, Washington, Houston, Minneapolis y Los Ángeles. La TSA recogerá información de los solicitantes, determinará la identidad de los mismos, realizará un control de historial y emitirá una ficha de identificación a los que cumplan los requisitos[39]. A los viajeros aceptados se les toman las huellas dactilares y se les escanea el iris. Mientras no dispare ninguna alarma de seguridad, el viajero inscrito evita pasar por una «verificación secundaria». Al llegar al aeropuerto, cada viajero inscrito se somete a un escaneo del dedo índice de las dos manos. Si las huellas no confirman la identidad del pasajero, se le somete a un escaneo del iris[40].

---

[34] Véase «NWA Defends Customer Data Disclosure to NASA Research Center After 9/11 Attacks», 3 *Privacy & Security L. Rep.* (BNA) 278 (2004).

[35] Véase «JetBlue Faces Class Action, DOT Scrutiny over Customer Data Sent to DOD Contractor», 2 *Privacy & Security L. Rep.* (BNA) 1089 (2003).

[36] Véase «American Airlines Approved Disclosure of Passenger Records for Aviation Security», 3 *Privacy & Security L. Rep.* (BNA) 459 (2004).

[37] Véase «Passenger Data Given to TSA Contractors for CAPPS II Project, Top TSA Official Says», 3 *Privacy & Security L. Rep.* (BNA) 751 (2004).

[38] Véase la Oficina Estadounidense de Contabilidad General, «Aviation Security: Computer Assisted Passenger Prescreening System Faces Significant Implementation Challenges», disponible en *http://www.epic.Org/privacy/airtravel/gao-capps-rpt.pdf* (visitado por última vez el 7 de marzo de 2004).

[39] Véase *Notice of Intent to Request Approval from the Office of Management and Budget for Three New Collections of Information/Registered Traveler Pilot Program; Satisfaction and Effectiveness Measurement Data Collection Instruments*, 69 Fed. Reg. 12, 865 (aviso) (2004).

[40] Véase «TSA Launches Registered Traveler Pilot Program at Minneapolis Airport», 3 *Privacy & Security L. Rep.* (BNA) 811 (2004).

Los datos biométricos y la seguridad fronteriza de los Estados Unidos

También se están utilizando datos biométricos para promocionar la seguridad de la frontera estadounidense. En la primera fase del programa U.S.-VISIT, que entró en vigor en enero de 2004, a las personas que solicitan un visado para entrar en los Estados Unidos es necesario realizarlas un escaneo del dedo índice de las dos manos y sacar una fotografía digital en el momento de entregar la solicitud. Los datos entran en una base de datos del Departamento de Estado. En la frontera estadounidense, la zona del visado que puede ser leído por una máquina se escanea, para permitir al agente de frontera acceder al archivo sobre el visitante en la base de datos del Departamento de Estado. Entonces se confirma la identidad del visitante, comparando nuevos escaneos de dedo y una fotografía digital tomada en la frontera con los escaneos de dedo y la foto de la base de datos. El nombre del visitante se compara entonces con una lista de nombres de terroristas y criminales buscados. Durante sus primeros dos meses, el programa U.S.-VISIT identificó a 60 criminales en la frontera estadounidense, de entre los dos millones de visitantes tratados[41]. A partir de septiembre de 2004, a los visitantes provenientes de 27 países cuyos ciudadanos no están obligados a obtener visado —entre ellos, la mayoría de Europa Occidental— se les realizará un escaneo de dedos y una foto digital al entrar en los Estados Unidos[42].

El ordenamiento jurídico estadounidense está exigiendo que se incluyan identificadores biométricos en los visados y en los pasaportes de los países para los cuales no se exige visado[43]. El plazo original de ejecución, que acababa en octubre de 2004, se ha extendido hasta octubre de 2005, en parte debido a la necesidad que tienen los países de cumplir con las normas técnicas que impone la Organización Internacional de Aviación Civil para los pasaportes biométricos, adoptadas en mayo de 2004, y que prevén que se utilice un microchip para almacenar una fotografía digital y otros datos. Además, el Departamento de Seguridad Nacional necesitaba un tiempo adicional para instalar los equipos y el *software* para leer los documentos[44].

La Unión Europea está contemplando la posibilidad de exigir que los pasaportes emitidos a los ciudadanos de la Unión contengan identificadores biométricos. En el mes de junio de 2004, el Consejo de Ministros de Justicia y Asuntos Interiores acordó que los Estados miembros deberían incluir una

---

[41] Véase Department of Homeland Security Testifies on U.S.-VISIT Program, disponible en *http://www.useu.be/Terrorism/USResponse/Mar0404* (visitado por última vez el 7 de marzo de 2004) (testimonio de Asa Hutchinson, Subsecretario para la Seguridad de la Frontera y del Transporte, del Departamento Estadounidense de Seguridad Nacional, ante la Comisión sobre la Reforma del Gobierno, de la Cámara de Representantes de los Estados Unidos, 4 de marzo de 2004).

[42] Véase «Administration Announces Plans to Begin Fingerprinting Visitors from Allied Countries», 3 *Privacy & Security L. Rep.* (BNA) 428 (2004).

[43] Véase *Enhanced Border Security and Visa Entry Reform Act of 2002,* Pub. L. 107-173, § 303, codificada en 8 U.S.C. § 1732.

[44] Véase *Id.* Véase también «Biometric Passport Delay Signed into Law; To Fill Gap, Visitors Face US-VISIT System», 3 *Privacy & Security L. Rep.* (BNA) 950 (2004).

fotografía digital en el pasaporte biométrico y que debería existir la opción de incluir huellas digitales[45]. Los Ministros fueron motivados tanto por la necesidad de cumplir con los nuevos requisitos estadounidenses como por el deseo de responder a una solicitud hecha por los jefes de gobierno de los Estados miembros después de los atentados en trenes que tuvieron lugar en marzo del año 2004 en Madrid. Algunos eurodiputados opinaban que el Consejo debería haber esperado a recibir la contribución del Parlamento, ya que algunas propuestas pueden referirse a tecnología defectuosa. También criticaron a los Estados Unidos por no adoptar pasaportes biométricos para ciudadanos estadounidenses[46].

LA SEGURIDAD DE LOS ESTADOS UNIDOS: EL DEBATE SOBRE LOS DATOS DE PASAJEROS AÉREOS

También se está aplicando la tecnología de la información a los pasajeros que pretenden entrar en los Estados Unidos por aire. El gobierno estadounidense tiene interés en dos categorías de datos, en cuanto a los pasajeros que llegan en vuelos internacionales. La primera categoría, denominada información de Registro del Nombre del Pasajero (*Passenger Name Record,* o PNR), consiste en los datos que contiene la base de datos del sistema de reservas de la línea aérea. Aunque es posible que el registro de cada pasajero contenga hasta 60 campos o categorías de información, en la mayoría de los casos, de 10 a 15 campos, aproximadamente, contendrán datos[47]. La información PNR en el sistema de reservas puede incluir no sólo el nombre del pasajero, su dirección postal, su dirección de correo electrónico y su número de tarjeta de crédito, sino un amplio espectro de otros datos de viaje; entre otros, las reservas de hotel y de alquiler de coche, las preferencias alimenticias e información sobre las discapacidades que tenga el pasajero[48]. También puede haber información sobre viajes anteriores, que puede incluir vuelos tomados, el historial de casos de no presentarse para reservas aéreas anteriores y los números de las tarjetas de crédito utilizadas en el pasado para pagar viajes. El Derecho estadounidense define la información de registro del nombre del pasajero en términos amplios para incluir cualquier información contenida

---

[45] Véase «EU Ministers Agree on Biometric Passport; Danish Member of Parliament Blasts Deal», 3 *Privacy & Security L. Rep.* (BNA) 687 (2004).

[46] *Id.*

[47] Véase, *e.g., Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach,* COM(2003)826 final.

[48] Para una explicación detallada de los datos de registro del nombre del pasajero, véase, *e.g.,* Edward HASBROUCK, «What's in a Passenger Name Record (PNR)?», disponible en *http://www.hasbrouck.org/articles/PNR.html* (visitado por última vez el 5 de julio de 2004). La mayoría de las líneas aéreas no controla a su propia base de datos, sino que utiliza uno de los cuatro grandes Sistemas Informatizados de Reservas que funcionan a nivel mundial: Sabre, Galileo/Apollo, Amadeus y Worldspan. De los cuatro, Amadeus es el único situado en Europa. Los demás se sitúan en los Estados Unidos. Sólo Amadeus está controlado por líneas aéreas. Los demás pertenecen a titulares independientes. *Id.*

en un sistema de reservas aéreas que exponga la identidad y los planes de viaje del pasajero[49].

La segunda categoría de datos de pasajero, conocida generalmente como Información Anticipada de Pasajeros (*Advance Passenger Information,* o API), es más restringida que los datos PNR y consiste en el nombre de la persona, su fecha de nacimiento, su nacionalidad, su género, el país emisor del pasaporte o visado y el número de cada documento. Asimismo, los datos API incluyen el número de vuelo del pasajero, el aeropuerto de salida y el de llegada.

Promulgada dos meses después de los atentados terroristas del 11 de septiembre de 2001, la Ley de Seguridad de la Aviación y del Transporte exige que las líneas aéreas operadoras de vuelos internacionales con destino en los Estados Unidos pongan información del registro del nombre del pasajero a disposición del Servicio de Aduanas y Protección de Fronteras (*Bureau of Customs and Border Protection,* o CBP) a demanda de este último[50]. No existe limitación sobre la anticipación con que se puede presentar una petición de información; por lo tanto, pueden ser días o incluso semanas antes del vuelo. Debido a que los datos PNR de un pasajero pueden ser extensos, el efecto que tiene el estatuto es el de habilitar al Servicio de Aduanas y Protección de Fronteras para acceder a una cantidad significativa de información de carácter personal que no está relacionada de forma directa con el vuelo que está a punto de tomar el pasajero. La transferencia en potencia de un espectro tan amplio de información de carácter personal resulta problemática a la luz del principio europeo de proporcionalidad, que prohíbe la recogida excesiva de datos.

El estatuto también exige que la línea aérea recoja y transmita datos anticipados de pasajeros (API) en el momento de la salida de un vuelo. La Ley de Seguridad de la Aviación y del Transporte[51] y la Ley de Mejora de Seguridad Fronteriza y Reforma de Entrada por Visado de 2002[52] exigen la transferencia de una lista de pasajeros y tripulación para cada vuelo extranjero que entra en los Estados Unidos. La información de la lista se ha definido de manera que incluye, de cada persona, el nombre, fecha de nacimiento, país de ciudadanía, género, información de pasaporte e información de visado[53]. Se

---

[49] Véase *Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States,* 67 Fed. Reg. 42710 (regla provisional) (2002), codificada en 19 C.F.R. § 122.49b(b) (2004).

[50] Véase *Aviation and Transportation Security Act,* Pub. L. 107-71 § 115 (2001), codificada en 49 U.S.C. § 44909(c)(3). El estatuto emplea la frase «Servicio de Aduanas», denominación del antecesor del actual Servicio de Aduanas y Protección de Fronteras.

[51] Véase *Aviation and Transportation Security Act,* Pub. L. 107-71 § 115 (2001), codificada en 49 U.S.C. § 44909(c)(2).

[52] Véase *Enhanced Border Security and Visa Entry Reform Act of 2002,* Pub. L. 107-173 § 402(a) (2002), codificada en 8 U.S.C. § 1221(a). El estatuto exige, asimismo, que se proporcione una lista de los pasajeros que se han presentado para la salida del vuelo. 8 U.S.C. § 1221(b).

[53] Véase *Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States,* 66 Fed. Reg. 67482 (regla provisional) (2001), codificada en 19 C.F.R. § 122.49a(b)(2) (2004). Véase también 8 U.S.C. § 1221(c).

trata de información del mismo tipo que la que estaría a disposición del oficial de la CBP en el aeropuerto de destino al decidir si admitir la entrada de la persona a los Estados Unidos. Según la Ley de Seguridad de la Aviación y del Transporte, la información de la lista debe transmitirse por medios electrónicos a la CBP dentro del máximo de quince minutos después de la salida del avión desde el aeropuerto extranjero[54]. Así, la información de la lista suele proporcionar al Servicio de Aduanas y Protección de Fronteras un aviso previo de varias horas sobre la identidad de la gente que desembarcará en el aeropuerto estadounidense, y no constituye más intrusión que la que ocurrirá cuando la persona se enfrente al oficial de la CBP en la sala de llegadas del aeropuerto. Debido a que la transferencia de información de la lista de pasajeros no ha resultado especialmente polémica, este trabajo se concentrará solamente en la categoría más amplia de los datos del registro del nombre del pasajero.

Alternativas para la transferencia legítima de los datos de los pasajeros desde Europa a los Estados Unidos

De las varias alternativas dispuestas en la Directiva sobre Protección de Datos para la transferencia legítima de los datos de los pasajeros al Servicio de Aduanas y Protección de Fronteras, existen solamente dos opciones realistas. La primera sería que la línea aérea obtenga de cada pasajero el «consentimiento de forma inequívoca» para la transferencia. La otra sería que el gobierno de los Estados Unidos prestase suficientes garantías para que la Comisión Europea pueda concluir que habría una protección «adecuada» de la intimidad. El gobierno de los Estados Unidos y la Comisión Europea han tenido experiencia previa en articular un sistema para alcanzar la segunda alternativa. En julio de 2000, el Departamento estadounidense de Comercio y la Comisión llegaron al Acuerdo de Puerto Seguro, en el cual empresas estadounidenses, otorgando una serie de compromisos voluntarios en materia de la intimidad, se han convertido en candidatas para recibir datos personales desde Europa. La Comisión determinó que existía una protección adecuada para la intimidad de los datos transferidos a los participantes en el Acuerdo localizados en los Estados Unidos[55].

Los demás casos donde sería posible construir una base legal para transferencias, o no están disponibles o resultan extremadamente onerosos. El primer caso trataría de la posibilidad de hacer una excepción sobre la base de la seguridad nacional. Aunque los Estados miembros pueden, por razones de

---

[54] *Id.* La salida del aeropuerto extranjero se define como el momento en que las ruedas se declaran retraídas después del despegue. *Id.* Sin embargo, según la Ley de Mejora de Seguridad Fronteriza y Reforma de Entrada por Visado de 2002, sólo hay que suministrar la lista antes de la llegada de la aeronave u otra nave al puerto estadounidense. 8 U.S.C. § 1221(a).

[55] Véase *Issuance of Safe Harbor Principles and Transmission to European Commission,* 65 Fed. Reg. 45,666 (2000).

seguridad nacional, limitar ciertos derechos del interesado al aviso y al acceso, estas limitaciones no constituyen la base de una transferencia de datos fuera de la Unión Europea[56]. Por otro lado, es la seguridad de un Estado miembro, no la de otro país, la que constituiría el motivo de tales limitaciones[57]. Una segunda posibilidad sería que la transferencia fuera necesaria por «un interés público importante»[58], pero ésta probablemente no sea factible porque el interés público tendría que tener su raíz en el sitio donde está situado el pasajero, no en los intereses del país de destino[59]. Una tercera posibilidad sería que se pudieran efectuar transferencias con la aprobación del gobierno de cada Estado miembro[60], pero ésta exigiría un proceso oneroso de hasta veinticinco aprobaciones distintas a nivel nacional, cada una de las cuales tendría que incluir una determinación de la suficiencia de las garantías de intimidad prestadas por el gobierno de los Estados Unidos. Una cuarta posibilidad sería que se pudieran efectuar transferencias de acuerdo con cláusulas contractuales tipo aprobadas por la Comisión Europea[61], pero dichas cláusulas no son apropiadas porque están diseñadas para transferencias internacionales entre empresas, no entre una empresa y un gobierno.

También podría permitirse la transferencia de datos de pasajeros si se obtuviera de cada pasajero el «consentimiento de forma inequívoca». Este procedimiento presentaría a cada pasajero la elección, potencialmente coercitiva, entre consentir una transferencia de todos los datos que quiera el Servicio estadounidense de Aduanas y Protección de Fronteras, sin límite de uso, o abandonar sus planes de viajar a los Estados Unidos por avión. El sentido del «consentimiento» en estas circunstancias contradice el criterio que mantiene que el consentimiento, para poder ser válido, tiene que «prestarse libremente»[62]. El Comisario de Mercado Interior, Frits Bolkestein, ha explicado que la Comisión Europea rechazó la idea de depender completamente de esta alternativa, que habría proporcionado ninguna protección para la intimidad de los ciudadanos europeos, y en su lugar eligió abrir negociaciones con los Estados Unidos en un intento de lograr una solución para toda la Unión, obteniendo compromisos del gobierno de los Estados Unidos en el sentido

---

[56] *Directiva sobre Protección de Datos*, *supra,* nota 6, artículo 13(1).

[57] Véase, *e.g.,* María Verónica PÉREZ ASINARI e Yves POULLET, «Public Security Versus Data Privacy, the Airline Passenger Data Disclosure Case», 20 *Computer L. & Security* 98, 105 (2004) [en adelante, PÉREZ ASINARI y POULLET]

[58] *Directiva sobre Protección de Datos*, *supra,* nota 6, artículo 26(1)(4).

[59] El Grupo de Trabajo del artículo 29, compuesto por los comisarios europeos de protección de datos, apunta también que la excepción por motivos de «interés público» no debería reconocerse en conexión con una «decisión unilateral, tomada por un tercer país por motivos que tan sólo obedecen a sus propios intereses públicos». «Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States 6», disponible en *http://europa.eu.int/comm./internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf* (visitado por última vez el 21 de junio de 2004).

[60] *Directiva sobre Protección de Datos*, *supra,* nota 6, artículo 26(2).

[61] *Directiva sobre Protección de Datos*, *supra,* nota 6, artículo 26(4).

[62] Véase, *e.g.,* «Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States 6», disponible en *http://europa.eu.int/comm./internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf* (visitado por última vez el 21 de junio de 2004); PÉREZ ASINARI y POULLET, *supra,* nota xx, 105.

de proteger suficientemente los intereses de intimidad de los pasajeros, para que se pueda justificar una determinación de adecuación según la Directiva sobre Protección de Datos[63].

NEGOCIACIÓN, ACUERDO E IMPUGNACIÓN PARLAMENTARIA

La Declaración Conjunta de febrero de 2003 y sus repercusiones

Poco antes de que las transferencias de datos PNR desde Europa hacia los Estados Unidos fueran a empezar, la Comisión Europea y el Servicio de Aduanas de los Estados Unidos (que entró a formar parte del Departamento de Seguridad Nacional) llegaron a un arreglo provisional concebido para reconciliar los requisitos estadounidenses de acceso a los datos de los pasajeros con la legislación europea sobre la protección de datos. En el mes de febrero de 2003, las partes emitieron una declaración conjunta (la Declaración Conjunta sobre Información de Registro del Nombre del Pasajero) que puso de manifiesto que la estrategia de la Comisión era intentar obtener suficientes garantías de intimidad para poder emitir una determinación de «adecuación» según el apartado 6 del artículo 25 de la Directiva sobre Protección de Datos[64]. La Declaración Conjunta contenía un considerando de entendimientos mutuos, en el sentido de que los datos se utilizarían solamente para combatir el terrorismo y otras ofensas criminales graves, que habría que desarrollar medidas protectoras para los datos sensibles, y que a los interesados se les proporcionaría acceso a sus propios datos según lo dispuesto en la Ley estadounidense de Libertad de Información. También exponía objetivos para un arreglo bilateral futuro, entre la Unión Europea y los Estados Unidos, sobre los datos de los pasajeros aéreos, con suficientes limitaciones sobre los fines para los cuales se pueden utilizar los datos, sobre las transferencias sucesivas y sobre el almacenamiento, con protección contra el acceso no autorizado, y con vías de recurso para los pasajeros, entre ellas la posibilidad de revisión y rectificación de datos. Por otro lado, el Servicio de Aduanas de los Estados Unidos aseguró que sólo revisaría los datos PNR de las personas que estuvieran viajando hacia, desde o a través de los Estados Unidos, que sólo utilizaría los datos para detectar posibles terroristas y otras amenazas contra la seguridad nacional y la seguridad pública, y que tomaría medidas para proteger los datos para que no se revelasen en casos inapropiados. El

---

[63] Véase «Speech by Frits Bolkestein, Internal Market Commissioner, to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market on December 16, 2003, Speech/03/613», disponible en *http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action* (visitado por última vez el 30 de enero de 2004).

[64] Véase «European Commission/US Customs Talks on PNR Transmission, Brussels, 17/18 February Joint Statement», disponible en *http://www.statewatch.org/news/2003/feb/11usdata2.htm* (visitado por última vez el 9 de julio de 2004) [en adelante, *la Declaración Conjunta sobre PNR*].

Servicio de Aduanas asimismo afirmó que, para mayor comodidad de las líneas aéreas y para ahorrarles cambios técnicos costosos, utilizaría un sistema para acceder a los sistemas de reservas de éstas, en vez de exigir que ellas transmitieran la información. El empleo de un sistema que accede a una base de datos de reservas aéreas se denomina *pull system* (sistema de extracción). Un sistema a través del cual la línea aérea inicia la transferencia de datos del pasajero al gobierno de los Estados Unidos se denomina *push system* (sistema de transmisión). Por último, el Servicio de Aduanas aceptó la opinión de la Comisión Europea en el sentido de que era necesario, a largo plazo, llegar a un acuerdo multilateral sobre la cuestión de compartir los datos de los pasajeros aéreos, forjado en el seno de la Organización Internacional de Aviación Civil.

Muchos en Europa no recibieron con agrado la Declaración Conjunta sobre PNR. El presidente del Grupo de Trabajo del artículo 29 señaló problemas a la luz de la legislación sobre protección de datos, y sugirió intentar convencer a los Estados Unidos para que se extendiese la fecha tope del 5 de marzo de 2003 para el comienzo de las transferencias de los datos de los pasajeros. En una carta al presidente de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento Europeo, el presidente del Grupo de Trabajo, Stefano Rodotà, expuso brevemente la necesidad de clarificar cómo la Declaración Conjunta sobre PNR proporcionaría una base legal para las transferencias de datos, sobre todo con respecto a los temas identificados por el Grupo de Trabajo en su informe del mes de octubre de 2002 sobre los datos de los pasajeros aéreos[65], y que las transferencias podrían llevar a que los pasajeros interpongan demandas, ya sea en los sistemas jurisdiccionales nacionales o ante las autoridades de protección de datos[66]. Más adelante, en aquel mismo mes, el presidente Rodotà se dirigió a una audiencia parlamentaria, donde apuntó que las autoridades nacionales de protección de datos podrían ser objeto de acciones legales en su propio país si no impugnaban la Declaración Conjunta. Expresó la opinión de que el gobierno estadounidense estaba obligando a otros países a respetar sus leyes y que la única manera de resolver el conflicto legal sería a través de un acuerdo multilateral[67].

El Parlamento también estuvo insatisfecho con la Declaración Conjunta sobre PNR. Criticó la acción de la Comisión, adoptando una resolución que cuestionaba la validez legal de la Declaración, hacía una llamada para que se suspendiera y recomendaba que el Presidente del Parlamento inter-

---

[65] Véase «Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States», disponible en *http://europa.eu.int/comm/internal_market/privacy/docs/pdocs/2002/ wp66_en.pdf* (visitado por última vez el 21 de junio de 2004).

[66] Véase «Letter from Stefano Rodota, Chairman of the Article 29 Working Party, to Jorge Salvador Hernandez Mollar, Chairman of the European Parliament's Committee on Citizens' Freedoms, Rights and Justice (LIBE)», del 3 de marzo de 2003, disponible en *http:/www.statewatch.org/news/2003/mar/art29ch.pdf* (visitado por última vez el 9 de julio de 2004).

[67] Véase «EU Privacy Official Calls U.S. Request for Airline Passenger Data "Unlawful"», 2 *Privacy & Security L. Rep.* (BNA) 318 (2003).

pusiera recurso en contra ante el Tribunal Europeo de Justicia[68]. Una voz crítica rechazó la estrategia de la Comisión en el sentido de negociar con los Estados Unidos para obtener garantías suficientes de intimidad para alcanzar la «adecuación» y, en su lugar, abogó porque se basara toda transferencia de datos de pasajeros en un sistema de consentimiento, en el cual se rogaría a cada pasajero que proporcionara la información en un impreso en el momento de formalizar su vuelo a los Estados Unidos[69]. Como ya se ha mencionado, aunque se puede defender que dicha práctica cumple con la legislación europea sobre protección de datos, también se podría ver como una medida coercitiva y sería onerosa en cuanto a su administración y costosa para las líneas aéreas.

Mientras, la Comisión respondió a la crítica resaltando el aspecto pragmático de la Declaración Conjunta sobre PNR. Una oficial de la Comisión hizo hincapié en que se estaba velando por la comodidad del pasajero, porque se evitarían largas esperas a la llegada. Añadió que este tipo de datos siempre se ha obtenido al llegar un pasajero a los Estados Unidos, pero que ahora los datos no se recogerían de manera aleatoria, sino sistemática[70].

El Dictamen de junio de 2003 del Grupo de Trabajo del artículo 29

En junio de 2003, el Grupo de Trabajo del artículo 29 emitió un Dictamen sobre el estado de las negociaciones entre la Comisión Europea y el gobierno de los Estados Unidos respecto a los datos de pasajeros[71]. El Grupo de Trabajo reconoció que era probable que cualquier acuerdo fuese determinado por criterios de tintes pragmáticos cuando escribió: «en última instancia habrá que atender a consideraciones de carácter político»[72]. Aunque se inclinaba por un arreglo multilateral como la mejor solución a largo plazo, el grupo de comisarios de protección de datos proporcionó sugerencias en cuanto al contenido de un acuerdo bilateral con los Estados Unidos. Según el parecer del Grupo de Trabajo, antes de emitir una determinación de adecuación, la Comisión debería tener una idea más clara de las prácticas estadounidenses dictadas por el sistema propuesto CAPPS II, la recogida por los

---

[68] Véase *European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights,* P5_TA(2003)0097, B5-0187/2003. Véase también «European Parliament Demands Suspension of Deal on Data on Transatlantic Travelers», 2 *Privacy & Security L. Rep.* (BNA) 256 (2003); «Massive Majority in European Parliament against deal with US on access to passenger data», disponible en *http://www.statewatch/org/news/2003/mar/12epvote.htm* (visitado por última vez el 27 de junio de 2004).

[69] Véase «Transfer of Transatlantic Passenger Data to U.S. Fought by European Parliamentarians», 2 *Privacy & Security L. Rep.* (BNA) 557 (2003) (citando comentarios de Marco Capato, miembro del Partido Radical de Italia).

[70] Véase «EU Privacy Official Calls U.S. Request for Airline Passenger Data "Unlawful"», 2 *Privacy & Security L. Rep.* (BNA) 318 (2003) (citando comentarios de Sue Binns, de la Comisión Europea).

[71] Véase «Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data», disponible en *http://europa.eu.int/comm./internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf* (consultado por última vez el 21 de junio de 2004).

[72] *Id.* en 10.

Estados Unidos de datos biométricos (de los solicitantes de visados, de los pasaportes y en la frontera) y el programa propuesto de Conocimiento de Información sobre el Terrorismo. El Grupo de Trabajo también se empeñaba en que los compromisos dados por los Estados Unidos fueran vinculantes, en que éstos se publicasen en el Registro Federal y en que cualquier arreglo bilateral entre la Comisión Europea y los Estados Unidos no durase más de tres años.

El grupo de comisarios de protección de datos estaba muy preocupado por limitar los fines para los cuales los datos se emplearían y se opuso a la posición estadounidense de que los datos pudieran utilizarse para combatir otras ofensas criminales graves además del terrorismo. Asimismo, el Grupo de Trabajo quería que la cantidad de datos PNR se limitase a 19 en vez de 38 campos de datos, para así cumplir con el principio de proporcionalidad: que los datos recogidos fuesen adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos. Entre los datos individuales que el Grupo de Trabajo encontró oponibles estaban la dirección postal del pasajero, su número de teléfono y dirección de correo electrónico, y los campos «abiertos» que permiten que la línea aérea o agente de viajes incluya información y comentarios diversos.

Los métodos utilizados para transferir datos, la práctica de compartir entre agencias y el calendario de plazos también revestían importancia para los comisarios de protección de datos. Estaban a favor del empleo de un sistema de transferencia del tipo *push*, en el cual las líneas aéreas iniciarían las transferencias de datos, en vez de un sistema de extracción del tipo *pull*, que permitiera al gobierno estadounidense acceder a los sistemas de reserva. Un sistema de transferencia contribuiría a limitar las clases de datos transferidos a las permitidas por el principio de proporcionalidad. El Grupo de Trabajo resaltó que los Estados Unidos tenían que especificar las instituciones que podrían recibir los datos de los pasajeros. Los comisarios de protección de datos querían restringir el calendario de acceso y el período de retención de datos. Opinaban que la transferencia inicial no debería ocurrir más de cuarenta y ocho horas antes de la salida del vuelo, con un máximo de una actualización de datos, y que los datos de los pasajeros no deberían retenerse después de un período de «algunas semanas o incluso meses»[73].

El Grupo de Trabajo también estaba preocupado por los derechos de los pasajeros. A los pasajeros «se debería informar... con claridad y precisión» de sus derechos; entre ellos, el derecho de acceso, el de rectificación y el de reparación[74]. Además, el Grupo de Trabajo quería que cada pasajero tuviera acceso no sólo a los datos transferidos, sino a datos de nueva creación; por ejemplo, el perfil de riesgo o lista de exclusión que podría generarse con los datos transferidos desde Europa. Los comisarios de protección de datos comentaron la necesidad de añadir un derecho del pasajero a rectificación y la

[73] *Id.* en 8.
[74] *Id.*

agregación de una disposición significativa con respecto a la ejecución forzosa.

La línea pragmática de la Comisión

Mientras tanto, los líderes de la Comisión intentaban llegar a un arreglo viable. En una carta de fecha 12 de junio de 2003 al Secretario del Departamento de Seguridad Nacional, Tom Ridge, el Comisario de Mercado Interior, Frits Bolkestein, expresó con franqueza la necesidad de encontrar una solución práctica al conflicto entre los diferentes regímenes legales de protección de la intimidad en Europa y en los Estados Unidos[75]. «Nos exponemos a una confrontación transatlántica de gran crispación sin salida evidente. Es mejor evitar tales confrontaciones. Donde se trata de los esfuerzos por combatir el terrorismo, es incluso más importante que mostremos un frente sólido, pero que lo hagamos de una manera que no reste fuerza a los mismos valores que estamos defendiendo»[76]. El Comisario identificó otras áreas de desacuerdo importante. Primero, los fines para los cuales los Estados Unidos pueden utilizar los datos deberían limitarse al terrorismo y otros delitos graves según lo necesario para combatir el terrorismo. Segundo, los Estados Unidos deberían eliminar los datos sensibles (por ejemplo, los que revelen el estado de salud, las creencias religiosas, etc.) hasta que las líneas aéreas adopten un sistema de transferencia del tipo *push system* con filtros. Tercero, los Estados Unidos deberían proporcionar un mecanismo eficaz e independiente de reparación donde los pasajeros puedan presentar sus recursos por agravios.

Varios meses más tarde, en un discurso dado el día 9 de septiembre de 2003 a la Comisión LIBE del Parlamento Europeo, el Comisario Bolkestein informó de que uno de los obstáculos al acuerdo se había eliminado al aceptar el Secretario Ridge, en una carta del 7 de agosto, el uso de filtros por parte de los Estados Unidos para eliminar los datos sensibles[77]. Sin embargo, las dos partes siguieron sin acordar el tipo de limitación que se podría lograr con respecto al objetivo de los datos, los tipos de datos que se podrían recoger, el tiempo durante el cual se podrían retener y los mecanismos de reparación que se podrían ofrecer a los pasajeros europeos. Informó de que los Estados Unidos querían utilizar los datos para perseguir ofensas criminales graves, además del terrorismo; querían recoger datos en 39 campos del registro del pasajero y querían retener los datos durante hasta seis o siete años.

El señor Bolkestein dijo ante la Comisión Parlamentaria que él veía tres

---

[75] Véase «Letter from Frits Bolkestein, Internal Market Commissioner, to Tom Ridge, U.S. Secretary of the Department of Homeland Security», del 12 de junio de 2003, disponible en *http://www.statewatch.org/news/2003/sep/Bolkestein-12JUN2003.html* (visitado por última vez el 27 de junio de 2004).

[76] *Id.*

[77] Véase «Meeting of Parliament's LIBE Committee, 9 September 2003, Speaking notes for Mr Bolkestein on U.S./EU talks on PNR», disponible en *http://www.statewatch.Org/news/2003/sep/Bolkestein-libe-9-09-03.pdf* (visitado por última vez el 27 de junio de 2004).

posibles líneas de acción. Primero, seguir negociando con los Estados Unidos para intentar lograr una protección adecuada para la intimidad de los datos de los pasajeros. Segundo, los Estados miembros podrían hacer cumplir la legislación europea y bloquear las transferencias de datos. Tercero, la Comisión Europea podría hacer cumplir el artículo 6 del Reglamento de Sistemas Informatizados de Reserva, que prohíbe la transferencia de datos sin el consentimiento del pasajero, con tal de que la Comisión obtuviera suficientes pruebas de infracciones. Advirtió que acciones ejecutivas europeas en el caso de las últimas dos alternativas probablemente llevarían a la realización de inspecciones secundarias al llegar los pasajeros europeos a los Estados Unidos, con los consiguientes retrasos importantes, y podrían llevar a los Estados Unidos a suspender los derechos de aterrizaje o multar a las aerolíneas europeas. En comparación, la mejor alternativa era negociar un acuerdo bilateral con los Estados Unidos. Describió un acuerdo que hiciera de puente entre los dos regímenes y que asegurara «el más alto nivel de protección que se pueda alcanzar para los datos de los ciudadanos de la Unión Europea». Añadió que «la Comisión estaría dispuesta a andar por este camino sólo con el apoyo claro del Parlamento y del Consejo»[78], una posición que fue modificada en el año 2004, a pesar de la oposición de la mayoría parlamentaria.

Intentos parlamentarios de influir sobre las negociaciones

En septiembre de 2003, el Parlamento solicitó que se fijara una fecha tope de fin de año para llegar a un acuerdo entre la Unión Europea y los Estado Unidos[79], y al mes siguiente pidió que la Comisión Europea comenzara a ejecutar el Reglamento de Sistemas Informatizados de Reserva[80]. El Parlamento también pidió que la Comisión determinara qué datos podrían transferirse, y bajo qué condiciones, siempre que no hubiera discriminación contra pasajeros no estadounidenses. Asimismo, expresó el criterio de que los datos no fueran conservados después de que el pasajero abandonase territorio estadounidense, que a los pasajeros se les proporcionara una información completa y precisa antes de la compra del billete y que otorgaran su consentimiento informado a la transferencia de datos a los Estados Unidos, y que los pasajeros tuvieran a su disposición un procedimiento rápido y eficaz de recursos. El Parlamento pidió el bloqueo del acceso a los datos de los pasajeros por parte de los Estados Unidos si las transferencias no cumplían estos requisitos o si de otra manera vulneraban la Directiva sobre Protección de Datos o el Reglamento de Sistemas Informatizados de Reserva[81].

---

[78] *Id.*

[79] Véase «U.S., EU Set End of Year Deadline to Resolve Airline Passenger Data Issues», 2 *Privacy & Security L. Rep.* (BNA) 1097 (2003).

[80] Véase *European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA,* P5_TA(2003)0429, B5-0411/2003.

[81] *Id.*

El arreglo al que se llegó en diciembre de 2003

El día 16 de diciembre, la Comisión emitió un informe dirigido al Consejo y al Parlamento anunciando el acuerdo al que había llegado con los Estados Unidos[82]. El acuerdo consistía en un enfoque múltiple de varios componentes. El primero iba a ser una determinación de adecuación emitida por la Comisión según lo dispuesto en el apartado 6 del artículo 25 de la Directiva sobre Protección de Datos, en combinación con un acuerdo bilateral entre el Consejo y el Departamento de Seguridad Nacional conforme al primer párrafo del apartado 3 del artículo 300 del Tratado de la Comunidad Europea. Esto se completaría con un aviso a los pasajeros antes de la compra de billetes, con respecto a los usos a los que se dedicarían los datos PNR en la base de datos de la línea aérea, para que los pasajeros pudieran tomar una decisión fundamentada sobre su viaje a los Estados Unidos. La solución, asimismo, incluyó un consenso en el sentido de que el uso por los Estados Unidos de un sistema de extracción para acceder a los datos de los pasajeros sería sustituido por un sistema de transmisión provisto de filtros, en el cual las líneas aéreas podrían controlar la transmisión de datos a los Estados Unidos. La Comisión expresó su apoyo al desarrollo de una posición europea sobre el empleo de los datos PNR de los pasajeros que llegan a Europa para fines de seguridad de aviación y de fronteras. Por último, la Comisión declaró que iría trabajando para la creación de un marco multilateral para las transferencias de los datos PNR para la seguridad de la aviación y de las fronteras bajo los auspicios de la Organización Internacional de Aviación Civil, a través de una propuesta que la Comisión elevaría en su día al Consejo.

El informe también cubrió las condiciones ofrecidas por el Departamento de Seguridad Nacional (DHS), que la Comisión había aceptado. Con respecto al tema de la proporcionalidad, la Comisión aceptó la posición del DHS en el sentido de que habría acceso a datos en 34 campos; entre ellos, la dirección postal, la dirección de correo electrónico, el número de teléfono e información sobre la tarjeta de crédito. Las líneas aéreas no estarían obligadas a recoger datos en ningún campo de los 34 que estuviera vacío. Esto fue significativo, porque los datos PNR de la mayoría de los pasajeros contienen de 10 a 15 elementos. Con respecto a una limitación de fines, los Estados Unidos accedieron a que los datos podrían utilizarse para perseguir el terrorismo y los delitos que tienen o pueden tener vínculos con el terrorismo. Los Estados Unidos cumplieron con su compromiso anterior de separar y eliminar todos los datos sensibles. Con respecto a la ejecución, la Comisión no tuvo éxito en conseguir un compromiso de los Estados Unidos de adherirse a un sistema de resolución de disputas donde figurase un órgano independiente. En su lugar, las quejas que no pudieran ser resueltas por el personal del DHS se elevarían por vía interna al Oficial Jefe de Protección de la Intimi-

[82] *Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach,* COM(2003)826 final.

dad del Departamento. La solución global entre la Unión Europea y los Estados Unidos sobre los datos de los pasajeros fue provisional, y se contemplaba una duración de tres años y medio, con una revisión conjunta anual a realizar por la Comisión y el DHS. Los datos no se conservarían más allá del período de tres años y medio. También hubo un compromiso en el sentido de que los datos PNR de Europa no se incluirían en el propuesto sistema estadounidense de preselección de pasajeros aéreos, CAPPS II.

El Comisario Frits Bolkestein habló ante el Parlamento Europeo el día de la emisión del informe[83]. Resaltó la naturaleza política de la solución, repitiendo una frase del Dictamen del Grupo de Trabajo del mes de junio anterior, en el sentido de que «en última instancia habrá que atender a consideraciones de carácter político»[84]. Recordó al Parlamento que la Comisión había rechazado la propuesta de exigir que las líneas aéreas obtuvieran el consentimiento de los pasajeros a las transferencias de los datos PNR y, en su lugar, había mantenido negociaciones que acabaron con la obtención de concesiones hechas por los Estados Unidos. Resaltó que las negociaciones habían llevado a una reducción de los fines para los cuales los Estados Unidos podrían utilizar los datos, abarcando ahora «el terrorismo y delitos conexos» y «otros delitos graves, incluida la delincuencia organizada, que tengan un carácter transnacional». Pero la «consideración de carácter político» que servía de base y que había sido elegida por la Comisión era una consideración pragmática de que el riesgo del terrorismo justificaba alguna erosión de los principios de protección de la intimidad, y que «la Unión Europea no puede negar a su aliado en la lucha contra el terrorismo una solución que los Estados Miembros estarían en libertad de articular por sí mismos. Los Estados Miembros de la Unión Europea pueden hacer excepciones según lo dispuesto en el Artículo 13 de la Directiva»[85].

El documento de las promesas de protección de la intimidad, denominado «los Compromisos» por el Servicio estadounidense de Aduanas y Protección de Fronteras (CBP), que formó la base de la solución acordada con la Comisión, se emitió en enero de 2004[86]. Proporcionó más detalles que el informe de la Comisión del mes anterior. La restricción de fines se amplió para incluir la fuga en caso de orden de arresto y en caso de deten-

---

[83] «Speech by Frits Bolkestein, Internal Market Commissioner, to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market on December 16, 2003, Speech/03/613», disponible en *http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action* (visitado por última vez el 30 de enero de 2004).

[84] Véase «Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data», disponible en *http://europa.eu.int/comm./internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf* (visitado por última vez el 21 de junio de 2004).

[85] «Speech by Frits Bolkestein, Internal Market Commissioner, to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market on December 16, 2003, Speech/03/613», disponible en *http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action* (visitado por última vez el 30 de enero de 2004).

[86] Véase «Draft Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection, January 14, 2004», disponible en *http://www.statewatch.Org/news/2004/jan/EUUSAG2.pdf* (visitado por última vez el 4 de febrero de 2004).

ción por «terrorismo y delitos conexos» y «otros delitos graves, incluida la delincuencia organizada, que tengan un carácter transnacional». El método de transferencia sería un sistema de extracción, pero sólo hasta que las líneas aéreas desarrollaran un sistema de transmisión. Con respecto a la duración del acceso a los sistemas de reservas aéreas, el CBP manifestó que extraería datos hasta setenta y dos horas antes de la salida y realizaría controles posteriores un máximo de tres veces. Cuando se introduzca un sistema de «transmisión», éste tendrá que mandar los datos a los Estados Unidos setenta y dos horas antes de la salida del vuelo, repitiendo la transmisión cuando haya cambios después del envío inicial. Si el CBP obtiene información anticipada sobre una persona «que presenta(n) un peligro concreto» y que probablemente viaje en un vuelo dado, puede extraer información sobre aquella persona con una antelación de más de setenta y dos horas antes de la salida del vuelo. El documento hace mención de que los derechos de los pasajeros a acceder a sus datos en manos del CBP serán según lo dispuesto en la Ley de Libertad de Información[87], y que los compromisos del CBP para proteger la intimidad de los datos PNR europeos no confieren derechos privados de acción algunos. La versión de enero de los Compromisos asumidos por el Servicio estadounidense de Aduanas y Protección de Fronteras se parecía en gran medida a la de los que formaron parte del acuerdo final del mes de mayo de 2004[88].

Aunque el informe de diciembre de la Comisión al Consejo y al Parlamento mencionó que la solución no autorizaría el uso de los datos de los pasajeros europeos para el funcionamiento del sistema propuesto de preselección de pasajeros CAPPS II, está claro que la Comisión ha dado su consentimiento al uso de dichos datos para las pruebas de CAPPS II, y que se ha comprometido a participar en más negociaciones para llegar a un acuerdo sobre el uso en el sistema propuesto de preselección[89]. El documento emitido por el Servicio de Aduanas y Protección de Fronteras en enero puso de manifiesto que la Comisión está de acuerdo en que los datos de los pasajeros europeos pueden utilizarse para probar el sistema CAPPS II. Seis meses más tarde, sin embargo, la propuesta de CAPPS II casi se extinguió debido a inquietudes en materia de seguridad, según una declaración hecha

---

[87] 5 U.S.C. § 552

[88] Véase Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), 11 de mayo de 2004, adjuntos como Anexo a «Commission Decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection», disponible en *http://europa.eu.int./comm./internal_market/privacy/docs/adequacy/pnr/c-2004-1914_en.pdf* (visitado por última vez el 10 de junio de 2004). Uno de los pocos cambios entre los Compromisos de enero y los de mayo es que el último documento declara que los datos PNR no pueden utilizarse para operaciones excepto en una situación de emergencia que exija la identificación positiva de un terrorista conocido o una persona con relaciones probadas con el terrorismo. *Id.*

[89] «Letter from Frits Bolkestein, Internal Market Commissioner, to Tom Ridge, U.S. Secretary of Homeland Security», del 18 de diciembre de 2003, disponible en *http://europa.eu.int/comm./internal_market/privacy/docs/adequacy/pnr/2003-12-18-letter-bolkestein_en.pdf* (visitado por última vez el 10 de junio de 2004).

en enero de 2004 por el Secretario del Departamento estadounidense de Seguridad Nacional, Tom Ridge[90].

La reacción al acuerdo por parte del Grupo de Trabajo

El Grupo de Trabajo del artículo 29 emitió un dictamen a finales de enero de 2004 que señaló que, aunque los compromisos más recientes del Servicio estadounidense de Aduanas y Protección de Fronteras contenían algunas mejoras, seguían sin proporcionar una protección adecuada de la intimidad de los datos de los pasajeros[91]. Muchos de los comentarios se parecían a los expresados anteriormente en el mes de junio. El Grupo de Trabajo estaba preocupado porque había una limitación insuficiente de los fines para los cuales se podrían emplear los datos, ya que podrían utilizarse para crímenes sin relación con el terrorismo, según la frase «otros delitos graves, incluida la delincuencia organizada, que tengan un carácter transnacional». Los comisarios de protección de datos seguían opinando que el espectro de datos era demasiado amplio, e insistían en la posición expresada en el Dictamen del Grupo de Trabajo de junio de 2003, que decía que, según el principio de la proporcionalidad, debería reducirse el número de elementos de datos de 34 a 19[92].

Los comisarios seguían recomendando que los datos se retuvieran durante un máximo de «semanas o meses», en vez de tres años y medio. Los datos sensibles deberían eliminarse antes de ponerse a disposición de los Estados Unidos, y debería haber restricciones adicionales sobre el empleo de los datos derivados de los datos PNR. Aunque el Grupo de Trabajo vio con buenos ojos que los Estados Unidos accedieran a utilizar un sistema de transmisión para las transferencias de datos, criticó la lentitud excesiva de dicho país en desarrollar la tecnología de extracción. Con respecto al calendario, los comisarios de protección de datos seguían recomendando que la primera transferencia no tuviera lugar con más de cuarenta y ocho horas de antelación a la salida del vuelo, con una sola actualización, en lugar del sistema expuesto en los Compromisos, que permitía que la primera transferencia se realizara con una antelación de hasta setenta y dos horas antes de la salida, y con hasta tres actualizaciones. El Grupo de Trabajo también protestó por la falta de restricciones sobre el número de agencias a las cuales el gobierno de los Estados Unidos podría transferir los datos[93].

Otra protesta tenía que ver con la falta de un mecanismo independiente

[90] Véase «DHS Announces Plans to "Redesign" Computerized Aviation Security Program», 3 *Privacy & Security L. Rep.* (BNA) 829 (2004).

[91] Véase «Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (CBP)», disponible en *http://europa.us.Int/comm./internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf* (visitado por última vez el 10 de junio de 2004).

[92] *Id.*

[93] *Id.*

para el recurso por parte de los pasajeros, sobre todo en vista de que, según se declaraba en los Compromisos, éstos no creaban ningún derecho privado de acción. El Grupo de Trabajo sugirió la creación de algo parecido al asesoramiento expuesto en FAQ 5 del Acuerdo de Puerto Seguro, sobre las organizaciones estadounidenses que asumían compromisos con respecto a la intimidad para poder habilitarse para recibir datos personales de Europa bajo la determinación, por parte de la Comisión, de adecuación según el Acuerdo de Puerto Seguro. FAQ 5 estableció un mecanismo para la resolución de disputas, consistente en una mesa informal de representantes de las autoridades europeas de protección de datos. Las organizaciones estadounidenses que participasen prometerían respetar los dictámenes emitidos por la mesa, incluidos los que dictaran el pago de una indemnización por parte de una organización a un pasajero por violación de un compromiso de protección de intimidad según el Acuerdo de Puerto Seguro. Si una organización estadounidense participante no respetara un dictamen de la mesa, podría ser, según las leyes de los Estados Unidos, responsable de una práctica comercial injusta o engañosa[94].

El Grupo de Trabajo protestó por el uso de los datos de los pasajeros europeos para probar el sistema CAPPS II. El Grupo también puso en duda si los Compromisos del Servicio de Aduanas y Protección de Fronteras serían jurídicamente vinculantes para el gobierno de los Estados Unidos. Además, el Grupo de Trabajo expresó su inquietud sobre la calidad de los datos estadounidenses, ya que algunas de las cancelaciones de vuelos desde Europa a los Estados Unidos a finales de diciembre por razones de seguridad se debían a errores en la correlación de los nombres de los pasajeros con los nombres de personas sospechosas de ser terroristas[95].

La Unión Europea y las propuestas de sistemas multilaterales de datos de pasajeros

Europa también ha contemplado propuestas para un sistema armonizado para la transferencia de datos de pasajeros. Un Estado miembro, el Reino Unido, ya tiene tal sistema para los pasajeros que llegan en vuelos internacionales, el Sistema de Información de Pasajeros Aéreos[96]. En 2003, el gobierno de España propuso una Directiva europea sobre la recogida de datos

---

[94] Véase *Frequently Asked Questions (FAQs) FAQ 5 - The Role of Data Protection Authorities,* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (2000).

[95] Véase, *e.g.,* «U.S. "Terror" List Still Lacking», *Wall St. J.,* 2 de enero de 2004, A4. (Informando de que las autoridades francesas han dicho que algunas cancelaciones de vuelos de Air France en diciembre de 2003 se debían a que algunos pasajeros tenían nombres parecidos a los que figuraban en una lista del FBI. Un pasajero cuyo nombre se parecía al del líder de un grupo terrorista tunecino resultó ser un niño de cinco años. Otros pasajeros señalados desde la lista estadounidense resultaron ser un agente de seguros galés y una señora china de edad avanzada que había regentado un restaurante de París.)

[96] Véase «EU Justice Ministers Agree to Require Collection of Inbound-Passengers' Data», 3 *Privacy & Security L.* (BNA) 393 (2004).

de pasajeros para los vuelos con destino a y dentro de Europa. Varios borradores sobre la información anticipada con respecto a los pasajeros se contemplaron en el 2003 y 2004[97], y resultaron en desacuerdos sobre los fines para los cuales se podrían utilizar dichos datos, los plazos de retención y las limitaciones sobre las transferencias. En marzo de 2004, los Ministros de Justicia de los Estados miembros efectuaron cambios en un borrador de Directiva, alargando el período de retención y permitiendo el uso de los datos en la lucha contra el terrorismo y contra la delincuencia organizada, asimismo, para fines de inmigración[98]. El Parlamento, sin embargo, no aprobó el documento y devolvió la propuesta a un comité[99].

No obstante, a finales de abril de 2004, el Consejo de Ministros adoptó una Directiva sobre los datos de los pasajeros aéreos sin contar con un dictamen del Parlamento Europeo[100]. La Directiva sobre Datos de Pasajeros Aéreos, que debe transponerse al ordenamiento jurídico nacional para septiembre de 2006, se aplica exclusivamente a los vuelos con origen fuera de la Unión Europea y permite que los datos se utilicen para la ejecución de la legalidad en general, además de para el control de fronteras y fines de inmigración, con sujeción a las disposiciones generales de la Directiva sobre Protección de Datos. Los datos que se recogen se limitan a la información anticipada sobre los pasajeros; entre ellos, el nombre del pasajero, su fecha de nacimiento, su nacionalidad, el número y tipo de documento de viaje que utiliza y la información sobre el vuelo. Los datos deben transferirse a más tardar al final del embarque, y la línea aérea debe borrarlos normalmente dentro de las veinticuatro horas siguientes a la llegada del vuelo. A la autoridad gubernamental que tiene los datos del pasajero se le exige borrar la información dentro de las veinticuatro horas siguientes a la transmisión, salvo donde se necesite más adelante para fines legítimos de control de frontera[101].

Tal y como han declarado la Comisión Europea y el Grupo de Trabajo del artículo 29, el tema de las transferencias internacionales de los datos de los pasajeros es un fenómeno global que, en última instancia, habrá que resolver a través de un acuerdo multilateral. La Unión Europea presentó una propuesta para un marco multilateral para los datos de Registro del Nombre del Pasajero en una reunión de la Organización Internacional de Aviación Civil en marzo y abril de 2004[102]. En la propuesta se sugirió la formulación

---

[97] Véase «Irish Presidency seeking to push through plan for the surveillance of travel», disponible en *http://www.statewatch.Org/news/2004/jan/21eu-pnr-compromise.htm* (visitado por última vez el 30 de enero de 2004).

[98] Véase «EU Justice Ministers Agree to Require Collection of Inbound-Passengers' Data», 3 *Privacy & Security L.* (BNA) 393 (2004).

[99] Véase «EU Parliament Blocks Justice Minister Move to Introduce Airline Passenger Data System», 3 *Privacy & Security L.* (BNA) 391 (2004).

[100] Directiva 2004/82/CE del Consejo, 2004 O.J. (L261) 24 [en adelante, la Directiva sobre Datos de Pasajeros Aéreos].

[101] *Id.*

[102] Véase «An International Framework for the Transfer of Passenger Name Record (PNR) Data», disponible en *http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp075_en.pdf* (visitado por última vez el 24 de junio de 2004).

de unas normas para el tratamiento de datos con respecto a la transparencia, una limitación en relación con los fines, unos límites de almacenamiento, unas restricciones sobre la transferencia sucesiva, los derechos de los pasajeros, las vías de recurso, unas normas en cuanto al tipo de acceso realizado por el gobierno (de «extracción» o de «transmisión»), el calendario de transferencia, los filtros, la seguridad de los datos y unas normas para la armonización de los campos de datos[103].

Los sistemas australiano y canadiense de datos de pasajeros

Australia y Canadá también tienen sistemas para la recogida de los datos de los pasajeros de vuelos internacionales con destino en territorio nacional, incluidos los vuelos que tienen su origen en Europa. En consecuencia, estos dos sistemas se enfrentan a la misma clase de cuestiones que el sistema estadounidense, con respecto a las transferencias internacionales de datos según la Directiva sobre Protección de Datos. Una diferencia importante, sin embargo, es que tanto Australia como Canadá tienen leyes amplias de protección de datos que, por lo general, son coherentes con el modelo europeo. El Grupo de Trabajo del artículo 29 ha emitido dictámenes sobre la adecuación de la protección proporcionada por los sistemas australiano y canadiense de datos de pasajeros con sujeción al apartado 6 del artículo 25 de la Directiva sobre Protección de Datos.

El Grupo de Trabajo ha llegado a la conclusión de que el sistema australiano de datos de pasajeros, que emplea información de Registro del Nombre del Pasajero, proporciona una protección adecuada a la intimidad de los datos provenientes de Europa[104]. Un factor importante es el hecho de que el sistema australiano de aduanas está sujeto a la Ley de Intimidad de 1988, que está basada en las Directrices de la OCDE. Muchos de los datos nunca llegan a los ojos de ningún funcionario. Los datos de más del 95% de los pasajeros de cualquier vuelo son eliminados por *software,* de manera que la gran mayoría de los datos PNR nunca llegan a ser visualizados ni descargados por Aduanas. La información PNR correspondiente al 5% restante de los pasajeros se analiza por un funcionario de Aduanas, pero en un caso típico las personas «interceptadas» en la frontera para más evaluación suman solamente entre el 0,05 y el 0,1% de los pasajeros. Las Aduanas de Australia almacenan los datos PNR de un pasajero sólo si se encuentra que dicha persona ha infringido la legislación de protección de fronteras. Se consideran solamente 18 elementos de datos PNR, salvo cuando la persona está dentro de ese 0,05 a 0,1% de los pasajeros que son «interceptados». Los datos sensi-

[103] *Id.*

[104] Véase «Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines», disponible en *http://europa.eu.int/internal_market/privacy/docs/wpdocs/2004/wp85_en.pdf* (visitado por última vez el 24 de junio de 2004).

bles se separan con filtros. Aduanas es el único organismo que utiliza los datos; no se transfieren salvo cuando se alega que el pasajero ha cometido un delito o cuando un órgano jurisdiccional ordena la transferencia de los datos PNR a este último. Los pasajeros tienen el derecho de acceso y el de rectificación, y pueden recurrir ante un órgano independiente, la Oficina del Comisionario Federal de Protección de la Vida Privada de Australia[105].

Aunque el Grupo de Trabajo albergaba algunas inquietudes sobre la adecuación de la protección proporcionada por el sistema canadiense de PNR, se reconoce que, como en el caso del sistema estadounidense, «en última instancia habrá que atender a consideraciones de carácter político» por parte de la Comisión[106]. Como los Estados Unidos, Canadá emplea un sistema de extracción, en el cual el gobierno tiene acceso a los sistemas de reservas. Puesto que Canadá permite que los datos sean utilizados para el fin amplio de la identificación de las personas que supongan un riesgo a la salud y a la seguridad del país, el Grupo de Trabajo consideró que dichos datos deben restringirse, para mayor coherencia con la limitación de fines. Los comisarios de protección de datos también estaban preocupados porque el sistema canadiense permitía la recogida de 38 campos de datos PNR, en vez de los 19 que, en la opinión del Grupo de Trabajo, cabían dentro del principio de proporcionalidad al contemplar el sistema estadounidense. Por otro lado, el grupo europeo estaba preocupado porque el período de seis años de retención de datos era demasiado largo, y porque había escasas restricciones con respecto a la transferencia de los datos a las instituciones gubernamentales, tanto dentro como fuera de Canadá. Aunque los derechos de acceso y rectificación estaban presentes para las personas dentro de Canadá, y se estaban extendiendo por vía administrativa a los ciudadanos europeos fuera de Canadá, el Grupo de Trabajo opinaba que hacía falta comprobar cómo funcionaría esto en la práctica[107].

Las reacciones belga y holandesa a las reclamaciones de pasajeros con respecto al sistema estadounidense

Las autoridades de protección de datos, tanto de Bélgica como de Holanda, han recibido quejas de que la transferencia de datos de Registro del Nombre del Pasajero desde Europa hasta los Estados Unidos violaba la ley de protección de datos. El caso belga fue presentado por un diputado del Parlamento Europeo, Marco Capato, miembro del Partido Radical de Italia, y la queja se basó en viajes desde Bélgica a los Estados Unidos. En una decisión emitida en diciembre de 2003, la Autoridad Belga de Protección de

[105] *Id.*

[106] Véase «Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and advanced Passenger Information from airlines», disponible en *http://europa.eu.int/internal_market/privacy/docs/wpdocs/2004/wp88_en.pdf* (visitado por última vez el 24 de junio de 2004).

[107] *Id.*

Datos juzgó que tres líneas aéreas estadounidenses, Continental, Delta y United, violaban la ley belga al transferir datos personales fuera de los Estados Unidos[108].

Sobre la base de una petición hecha por la Fundación *Bits of Freedom,* la Autoridad Holandesa de Protección de Datos investigó posibles transferencias de datos personales de ciudadanos holandeses por parte de Northwest Airlines a la Administración Nacional de Aeronáutica y del Espacio (NASA) de los Estados Unidos en 2001, como parte de un proyecto para desarrollar un método para detectar a potenciales terroristas. Debido a la presión ejercida sobre la industria aérea en 2001 después de los atentados del 11 de septiembre, y el cambio correspondiente en la política de Northwest respecto al uso de los datos de los pasajeros, la Autoridad Holandesa de Protección de Datos concluyó en una carta de abril de 2004 que la transferencia fue un acontecimiento puntual que no merecía más investigación[109].

La respuesta del Parlamento Europeo a las acciones de la Comisión y del Consejo

En varias votaciones celebradas en marzo y abril de 2004, el Parlamento expresó su oposición al acuerdo que la Comisión había establecido con los Estados Unidos y recomendó que el asunto fuese impugnado ante el Tribunal Europeo de Justicia. El día 9 de marzo, el Parlamento decidió, con una mayoría de 439 a favor y 39 en contra, respaldar un informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) que se oponía a la posición de la Comisión con respecto a las transferencias de los datos de los pasajeros[110]. El día 18 de marzo, la Comisión LIBE se pronunció, por una mayoría de 24 contra 7, a favor de un acuerdo que declaraba que las acciones de la Comisión con respecto a los pasajeros infringían la ley europea y que los temas en cuestión deberían someterse al Tribunal Europeo de Justicia[111]. El día 31 de marzo, el Parlamento se declaró en contra del acuerdo, por una mayoría de 229 contra 202[112], e hizo un llamamiento a la Comisión

---

[108] Véase «Belgian Privacy Committee Supports MEP's Complaint on Illegal Transfer of Personal Data to USA», disponible en *http://www.statewatch.org/news/2004/jan/17pnr.decision.htm* (visitado por última vez el 27 de junio de 2004). El señor Capato presentó su queja después de la decisión belga del 18 de diciembre de 2003. *Id.*

[109] Véase «Carta de Uldo van de Pol, vicepresidente de la Autoridad Holandesa de Protección de Datos, a Northwest Airlines», del 6 de abril de 2004, disponible en *http://www.cbpweb.Nl/downloads_uit/z2004-0310.pdf* (visitado por última vez el 24 de junio de 2004).

[110] Véase, *e.g.,* «U.S.-EU Atlantic Air Passenger Pact Violates Privacy Laws, Parliament Says», 3 *Privacy & Security L.* (BNA) 301 (2004).

[111] Véase, *e.g.,* «U.S.-EU Passenger-Data Pact Rejected by Civil Liberties Panel of EU Parliament», 3 *Privacy & Security L. Rep.* (BNA) 330 (2004).

[112] Véase, *e.g.,* «EU-US PNR (passenger name record) "Deal" to Go for a Second Vote in European Parliament», disponible en *http://www/statewatch.org/news/2004/apr/11eu-us-pnr-ep2.htm* (visitado por última vez el 26 de junio de 2004). Véase también «European Parliament resolution on the draft commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name records (PNRs) transferred to the US Bureau of Customs and Border Protection, P5_TA-Prov(2004)0245», disponible en *http://www.statewatch.org/news/2004/mar/ep-pnr-report.pdf* (visitado por última vez el 26 de junio de 2004).

para que adoptara un sistema alternativo propuesto por la Comisión LIBE que no incluiría 34, sino 19 campos de datos[113]. El día 6 de abril, la Comisión de Asuntos Jurídicos del Parlamento votó a favor de impugnar el acuerdo sobre pasajeros de la Comisión ante el Tribunal Europeo de Justicia[114], y el día 21 de abril el Parlamento acordó, por una mayoría de 276 votos contra 260, pedir el dictamen del Tribunal[115].

La adhesión de diez nuevos Estados miembros a la Unión Europea el día 1 de mayo de 2004 no redujo la oposición parlamentaria al acuerdo. El 4 de mayo el Parlamento ampliado acordó, por una mayoría de 343 votos contra 301, no recoger la petición del 30 de abril de los Ministros de los que eran entonces los quince Estados miembros de la Unión Europea pidiendo que el Parlamento reconsiderara su decisión del 21 de abril de impugnar el acuerdo sobre PNR ante el Tribunal[116].

A pesar de la resistencia continuada del Parlamento, la Comisión Europea realizó una determinación formal de adecuación el día 14 de mayo[117], después de la adopción de «Compromisos» por parte del Servicio de Aduanas y Protección de Fronteras del Departamento de Seguridad Nacional de los Estados Unidos, el día 11 de mayo[118]. El 17 de mayo, el Consejo de Ministros, por lo tanto, emitió su decisión de aprobar un acuerdo sobre datos de pasajeros entre la Unión Europea y los Estados Unidos[119]. El acuerdo propiamente dicho se firmó en Washington el 28 de mayo[120].

Aunque la aprobación por parte del Consejo del acuerdo sobre datos de pasajeros hizo obsoleta la reciente impugnación jurídica realizada por el Parlamento ante el Tribunal Europeo de Justicia, algunos diputados inmediatamente pidieron nueva acción para intentar convencer al Tribunal de que anulara la decisión de adecuación o el acuerdo internacional, o las dos cosas, con sujeción al artículo 230 del Tratado de la Comunidad Europea[121]. El 16

---

[113] Véase, *e.g.,* «European Parliament Votes to Cancel Agreement with U.S. over Passenger Data», 3 *Privacy & Security L. Rep.* (BNA) 391 (2004).

[114] Véase, *e.g.,* «European Parliamentary Committee Votes to Challenge Passenger Data Policy in Court», 3 *Privacy & Security L. Rep.* (BNA) 436 (2004).

[115] Véase, *e.g.,* «European Parliament Votes to Go to Court on EU-US PNR Deal», disponible en *http://www.statewatch.org/news/2004/apr/13ep-vote-pnr-court.htm.*

[116] Véase «European Parliament Upholds April Vote to Oppose EC-U.S. Passenger Data Deal», 3 *Privacy & Security L. Rep*. (BNA) 549 (2004).

[117] Véase *Decisión de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection),* 2004 O.J. (L235)11.

[118] Véase *Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data,* 69 Fed. Reg. 41543 (aviso) (2004).

[119] Véase *Decisión del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos,* 2004 O.J. (L183) 83.

[120] Véase, *e.g.,* «U.S., EU Officials Sign Agreement to Let DHS Collect Passenger Data», 3 *Privacy & Security L. Rep.* (BNA) 661 (2004).

[121] Véase, *e.g.,* «EC, EU Ministers Approve Plan for Transfer of Passenger Data to U.S.», 3 *Privacy & Security L. Rep*. (BNA) 601 (2004).

de junio, la Comisión de Asuntos Jurídicos del Parlamento aprobó un acuerdo pidiendo que el Tribunal anulara el acuerdo del Consejo sobre datos de pasajeros y la decisión de adecuación de la Comisión[122]. El día siguiente, una mayoría de los líderes de partidos en el Parlamento —un grupo conocido como «la Conferencia de Presidentes»— y la Comisión de Asuntos Jurídicos prestaron su apoyo a la acción judicial en contra de la Comisión[123]. A finales de junio, Pat Cox, el Presidente saliente del Parlamento, realizó el anuncio formal de la petición parlamentaria solicitando que el Tribunal anulara la Decisión del Consejo del 17 de mayo de suscribir el acuerdo sobre los datos de pasajeros[124]. Si el Parlamento tiene éxito en persuadir al Tribunal de que anule el acuerdo sobre los datos de pasajeros, tal decisión judicial probablemente supondría el comienzo de una nueva ronda de negociaciones entre la Comisión Europea y los Estados Unidos. Mientras tanto, es probable que la Comisión Europea pida con ahínco un acuerdo multilateral sobre los datos de pasajeros que sea compatible con las normas europeas de protección de datos dentro del marco que presentó la Unión Europea a la Organización Internacional de Aviación Civil[125].

CONCLUSIÓN

La polémica sobre los datos de pasajeros aéreos es representativa de la dificultad de reconciliar los principios europeos sobre la intimidad con el sistema estadounidense, que no sólo carece de una legislación integral sobre la intimidad, sino que tiende hacia el empleo de prácticas de extracción de datos como medio para contrarrestar el terrorismo. Las negociaciones entre la Unión Europea y los Estados Unidos sobre las transferencias de datos de pasajeros dieron como resultado un acuerdo que era, en gran medida, político, y que puso a prueba los principios europeos sobre la protección adecuada de la intimidad al buscar la Comisión Europea, con la participación del Consejo de Ministros, una forma pragmática de resolver la disputa. La reacción en Europa demostró que la tensión entre intimidad y seguridad existe no sólo al otro lado del Atlántico, sino dentro de la misma Europa, ya que los defensores de los principios de la intimidad en el Parlamento convencieron a una mayoría de sus co-diputados para montar una oposición legal a la solución, y

---

[122] Véase, *e.g.,* «EU Lawmakers Want Courts to Scrap EU-U.S. Passenger Data Exchange Accord», 3 *Privacy & Security L. Rep.* (BNA) 723 (2004).

[123] Véase, *e.g.,* «EU-US PNR Deal: European Parliament Discussing New Court Cases», disponible en *http://www.statewatch.org/news/2004/jun/10eu-us-pnr-ep.htm* (visitado por última vez el 22 de junio de 2004).

[124] Véase, *e.g.,* «European Parliament to Go to Court over Council and Commission Decisions on PNR Data Agreement with USA», disponible en *http://www.statewatch.org/news/2004/jun/21-ep-court-pnr.htm* (visitado por última vez el 26 de junio de 2004); «Euro Parliament Challenges EU-U.S. Deal Providing for Exchange of Passenger Data», 3 *Privacy & Security L. Rep.* (BNA) 793 (2004).

[125] Véase «An International Framework for the Transfer of Passenger Name Record (PNR) Data», disponible en *http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp075_en.pdf* (visitado por última vez el 24 de junio de 2004).

ya que los expertos en intimidad de las autoridades nacionales de protección de datos expresaron su crítica del acuerdo.

El diálogo público sobre el empleo de los datos de pasajeros podría sacar provecho de una información más completa sobre la eficacia de las prácticas de extracción de datos, sobre todo al determinar qué tipos de datos encajan dentro del principio europeo de la proporcionalidad como «adecuados, pertinentes y no excesivos». Por ejemplo, el Grupo de Trabajo ha decidido que la dirección, el número de teléfono y los datos de «viajero frecuente» de un pasajero se incluían en la lista de elementos de datos que eran excesivos para el fin de combatir el terrorismo. Sin embargo, Newton Minow, el Presidente de una Comisión Consultiva del gobierno sobre la protección de la intimidad en los Estados Unidos, ha escrito que información de esta índole, de haberse utilizado como una parte de un análisis dirigido de datos en el empleo de bases de datos gubernamentales y comerciales, podría haber revelado conexiones entre los 19 secuestradores de aviones del 11 de septiembre de 2001. Empezando con dos pasajeros que habían reservado vuelo y que ya eran sospechosos de terrorismo, y un tercero que ostentaba un visado caducado, se podrían haber rastreado los vínculos entre los demás 16 secuestradores, y de éstos a los tres primeros, a través de direcciones compartidas, números de teléfono compartidos y números de «viajero frecuente» compartidos[126]. Puesto que el empleo de esta clase de datos podría haber sido eficaz para la identificación de todos los 19 secuestradores antes de la salida de los vuelos el 11 de septiembre, quizás su recogida sea coherente con el principio de la proporcionalidad, sobre todo si se utilizan solamente como una parte de una búsqueda dirigida en bases de datos, realizada sobre la base de una sospecha razonable de conexiones con el terrorismo.

La Comisión Europea y otros reconocen que existe la necesidad urgente de desarrollar unas normas multilaterales que cumplan con los principios europeos de protección de datos y, a la vez, permitan medidas eficaces de seguridad. También existe la necesidad de un foro multilateral permanente sobre los datos de pasajeros, como el Grupo de Acción Financiera Internacional, que coordina los esfuerzos por combatir el blanqueo de dinero y el suministro de fondos para el terrorismo. En cuanto al desarrollo de unas normas internacionales para la transferencia de datos de pasajeros, el sistema australiano podría ser un buen modelo, porque pone el énfasis sobre la minimización de los datos y así reduce los riesgos a la intimidad. Puesto que el sistema australiano desecha de modo automático los datos de más del 95% de los pasajeros, que presentan poco riesgo según el juicio del sistema, puede también mejorar la eficacia, ya que reduce la cantidad de información que se somete a escrutinio en busca de actividad sospechosa.

---

[126] Véase Newton MINOW, «Seven Clicks Away», *Wall St. J.,* 3 de junio de 2004, A14. El señor Minow, Presidente de la Comisión Federal de Comunicaciones de los Estados Unidos en los años sesenta, también fue Presidente de la Comisión Consultiva de Tecnología e Intimidad del Departamento de Defensa de los Estados Unidos, que emitió un informe en marzo de 2004.

La tensión entre seguridad e intimidad ha existido durante siglos, así como la comprensión de que la libertad ha de ser preservada. Como observara Benjamin Franklin hace más de doscientos años: «Aquellos que pueden sacrificar la libertad esencial para obtener un poco de seguridad provisional no se merecen ni la libertad ni la seguridad»[127]. Y como observara, más recientemente, la Comisión de Tecnología y Defensa de la Intimidad del Departamento de Defensa de los Estados Unidos: «Bien podía haber añadido Franklin que los que cambian la libertad por la seguridad, con demasiada frecuencia no logran ni la una ni la otra»[128].

[127] Benjamin FRANKLIN, *Historical Review of Pennsylvania* (1759), reeditado en John BARTLETT, *Familiar Quotations* 310 (16.ª ed., 1992).

[128] «Safeguarding Privacy in the Fight Against Terrorism, Report of the Technology and Privacy Advisory Committee, xii», disponible en *http://www.epic.org/privacy/profilinf/tia/tapac_report.pdf* (visitado por última vez el 12 de julio de 2004).