

Transferencias internacionales de datos personales entre Europa y USA

Emilio Aced Fález

La regulación de las transferencias de datos personales a terceros países que no proporcionan un nivel de protección adecuado es un elemento capital del régimen de protección de datos establecido por la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos¹ (“la Directiva”), plasmado en los artículos 25² y 26³ de la misma. En el primero de ellos

¹ Diario Oficial n° L 281 de 23/11/1995

² “Artículo 25. Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apdo. 4

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión”.

³ “Artículo 26. Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

- a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o
- b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
- c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
- d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
- e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
- f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al

se establecen los principios generales por los que éstas se han de regir y en el segundo las excepciones a dicho régimen general.

En primer lugar hay que mencionar que la Directiva no considera transferencias internacionales aquellas que se dan entre los países del Espacio Económico Europeo (EEE), formado por los Estados miembros de la Unión Europea (UE) además de Islandia, Liechtenstein y Noruega ya que no tienen la consideración de “terceros estados” desde el punto de vista del Derecho comunitario. Además, todos los pertenecientes al EEE tienen la obligación de transponer a su Derecho nacional las previsiones de la Directiva y, por ende, constituyen un ámbito geográfico armonizado en el que se establece un régimen de protección equivalente.

Analizando ya el régimen de la Directiva, el elemento sustantivo más importante es la prohibición de transferir datos a un país tercero que no garantice un nivel de protección adecuado, expresado en el apartado 1 del artículo 25.

Si analizamos este apartado encontraremos un elemento de capital importancia: la necesidad de que, independientemente de que los datos personales vayan a ser transferidos a un país tercero para su tratamiento, dicha transferencia no dispensa, en modo alguno, del cumplimiento del resto de las obligaciones que la Directiva impone para los tratamientos de datos personales en los Estados miembros. Estas obligaciones incluyen los principios de información al interesado, los de calidad de datos, la necesidad de legitimación de los tratamientos en base a los criterios del artículo 7 o la garantía de los derechos de acceso, rectificación, cancelación y oposición. Por poner ejemplos concretos, esto significa, ciñéndonos al caso español, que si se desea transferir datos a un país tercero con la finalidad de que en el mismo se produzca un tratamiento por encargo del responsable establecido en España, con independencia de los mecanismos que se utilicen para la legitimación de la transferencia (país de destino adecuado, garantías contractuales, etc.) deberán cumplirse las obligaciones que establece el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), respecto de la obligatoriedad de regular dicho tratamiento mediante un contrato que incluya una serie de requisitos imprescindibles. De la misma manera, si la transferencia constituye una cesión o comunicación de datos, para poder realizarla deberá de estarse en presencia de alguno de los supuestos legitimadores presentes en el artículo 11 de la LOPD.

ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaron su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión”.

A continuación, el artículo 26.1 establece una serie de excepciones a la regla general permitiendo la transferencia a países no adecuados en determinadas circunstancias y, a su vez, el apartado segundo de este mismo artículo deja en manos de los Estados miembros la posibilidad de proceder a autorizar transferencias a países no adecuados, incluso aunque no se invoque alguna de las excepciones del apartado 1, siempre y cuando se obtengan garantías que, a juicio de la autoridad competente del Estado miembro en cuestión⁴, resulten suficientes. Estamos, pues, en presencia de un sistema de tres niveles que implican un grado de dificultad creciente para poder transferir datos personales: adecuación del país de destino, posible aplicación de una de las excepciones previstas o autorización si se obtienen garantías suficientes.

Hasta ahora, hemos estudiado las posibilidades que la Directiva otorga a los Estados miembros para regular el movimiento internacional de datos personales, o lo que es lo mismo, no nos hemos apartado de las competencias que se ejercen en el ámbito nacional sin intervención de las instituciones comunitarias. Pero también existen posibilidades de intervención de la Comisión Europea, ya que la Directiva le atribuye, fundamentalmente, dos tipos de competencias: declarar que un país tercero reúne las condiciones necesarias para ser considerado adecuado y decidir que un conjunto de cláusulas contractuales tipo ofrecen las garantías suficientes para poder ser utilizadas para la transferencia de datos personales a países no adecuados. En cualquiera de estos supuestos, una vez la Comisión ha aprobado estas decisiones, los Estados miembros están obligados a tomar las medidas legales necesarias para adaptarse a dichas Decisiones.

La Comisión Europea ha ejercido estas competencias en diversas ocasiones. Por lo que respecta a la primera de ellas, existen decisiones de la Comisión declarando la adecuación de Suiza, Hungría, el sistema de Puerto Seguro para los Estados Unidos de América y Canadá⁵. Asimismo, existen dos decisiones declarando dos conjuntos de cláusulas contractuales tipo como oferentes de garantías suficientes para su utilización en la transferencia de datos personales a países no adecuados⁶. En este segundo caso, las decisiones de la Comisión no impiden que los Estados miembros puedan autorizar transferencias en base a otras cláusulas que, a su juicio, ofrezcan garantías suficientes, sino, exclusivamente, que ningún Estado miembro podrá denegar una autorización de transferencia que utilice las cláusulas tipo aprobadas por la Comisión, por lo que su objetivo fundamental es proporcionar una herramienta útil para aquellas compañías que realicen transferencias desde varios Estados de la UE y que, desde la aprobación de las cláusulas tipo, podrán usar un mismo modelo de contrato para solicitar la autorización en todos los Estados miembros.

Las decisiones de adecuación respecto de terceros países aprobadas hasta la fecha por la Comisión tienen un serie de elementos comunes. En primer lugar, dando

⁴ La autoridad que decide sobre la existencia de garantías suficientes difiere de un Estado miembro a otro. Por ejemplo, en España es la Agencia de Protección de Datos, en los Países Bajos, el Ministerio de Justicia previo informe de la autoridad de control de protección de datos, en el Reino Unido, es el propio responsable del tratamiento que realiza la transferencia el que decide si las garantías son adecuadas o no.

⁵ Decisiones 2000/518/CE, 2000/519/CE y 2000/520/CE (Diario Oficial nº L 215 25/8/2000) y 2002/2/CE (Diario Oficial nº L 2 4/1/2002) respectivamente.

⁶ Decisión 2001/497/CE (Diario Oficial nº L 181 4/7/2001) y Decisión 2002/16/CE (Diario Oficial nº L 6 10/1/2002)

estricto cumplimiento a la condición que examinábamos al principio de este documento, las decisiones establecen, taxativamente, que la aplicación de las mismas sólo afecta a las transferencias de datos personales al tercer país desde la UE y, en ningún caso, al resto de condiciones y obligaciones establecidas en el Derecho nacional de cada Estado miembro.

Además, sin perjuicio de las competencias que les asignen las Leyes nacionales, se otorga a las Autoridades de Control de los Estados miembros la posibilidad de bloquear una transferencia determinada cuando la autoridad de supervisión del país tercero ha resuelto que la entidad ha vulnerado las condiciones de la Decisión o si existen grandes probabilidades de que se estén vulnerando las normas de protección de datos y la autoridad de supervisión del país tercero no ha tomado ni tomará las medidas necesarias para resolver el caso, la continuación de la transferencia podría crear riesgo inminente de grave perjuicio a los afectados y, además, la autoridad de control del Estado miembro ha hecho esfuerzos razonables para notificárselo a la entidad y proporcionarle la oportunidad de alegar.

Asimismo, existe la posibilidad de que la Comisión suspenda una Decisión si la Autoridad del tercer país responsable del cumplimiento de las normas de protección de datos no está ejerciendo su función

Una vez analizado el marco general de las transferencias internacionales de datos personales en la Directiva, pasaremos a ocuparnos del caso concreto de EE.UU. Para comenzar, debemos preguntarnos porqué existe un problema entre EE.UU. y la UE. El problema se deriva de la existencia de dos entendimientos distintos de lo que la privacidad es y significa y de los mecanismos que deben utilizarse para su salvaguardia.

Para la UE, la protección de datos personales es un derecho fundamental de los ciudadanos. Así lo reconocen explícitamente algunas constituciones de los Estados miembros (la española, entre ellas) y, de modo definitivo, la Carta de los Derechos Fundamentales de la Unión Europea⁷, solemnemente proclamada en Niza, por los Jefes de Estado y de Gobierno de la UE, el siete de diciembre del año dos mil. Además, tanto la UE mediante diversas directivas como sus Estados miembros al transponer las mismas, han aprobado normas jurídicas de obligado cumplimiento y de carácter general en las que se establecen los principios y los derechos que los ciudadanos tienen respecto al tratamiento de sus datos personales. Finalmente, en todos los Estados miembros existen autoridades de control independientes encargadas de la supervisión del cumplimiento de la legislación en esta materia.

Por su parte, en EE.UU. la protección de datos se considera un elemento disponible por parte de los ciudadanos, regulado parcialmente en una multitud de

⁷ “Artículo 8. Protección de datos de carácter personal.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente”.

El texto completo de la Carta se puede consultar en <http://ue.eu.int/df/docs/es/CharteES.pdf>

normas específicas y sectoriales⁸ sin conexión entre ellas, poniéndose casi todo el énfasis en la autorregulación y sin que exista una autoridad o autoridades de control encargadas de garantizar eficazmente el cumplimiento de las reglas y la aplicación de unos estándares universalmente aceptados. Por ello, esta situación hacía inviable la posibilidad de una declaración de adecuación de los EE.UU. por parte de la Comisión Europea.

No obstante, según se iba acercando el plazo efectivo de entrada en vigor de la Directiva (octubre de 1998), se iba extendiendo la inquietud entre las grandes multinacionales estadounidenses que operan en Europa respecto de la posibilidad de que las autoridades de control europeas, en virtud de las restricciones presentes en la Directiva, pudieran proceder a un bloqueo de las transferencias de datos personales entre la UE y los EE.UU. Si tenemos en cuenta que ambos son los socios comerciales más importantes para la otra parte, las consecuencias de un tal bloqueo hubieran sido incalculables.

Por ello, las autoridades del Departamento de Comercio de los EE.UU. y la Comisión Europea comenzaron unas negociaciones tendentes a buscar un acuerdo que pudiera solventar estas dificultades y, eventualmente, permitir la aprobación de una Decisión de adecuación por la Comisión.

Después de casi dos años de negociaciones que dieron lugar, además de a diversos borradores, a encendidos debates y a varios pronunciamientos por parte de las autoridades de control europeas en el marco del Grupo de Trabajo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, establecido en el artículo 29 de la Directiva y por ello más conocido como Grupo de Trabajo del Artículo 29 (GT29), finalmente, la Comisión aceptó que los Principios de Puerto Seguro, junto con las Preguntas más Frecuentes (en adelante “Puerto Seguro”), publicados por el Departamento de Comercio de los EE.UU. ofrecían un nivel de protección adecuado para la transferencia de datos personales desde Europa a dicho país.

Puerto Seguro es una Decisión de adecuación de carácter sectorial a la que pueden acogerse, exclusivamente, compañías establecidas en los EE.UU., por lo que no se puede extender su aplicación, como en algún momento se ha pretendido (e incluso se sigue pretendiendo) a compañías filiales de empresas americanas establecidas fuera de este país.

Para que una empresa estadounidense pueda disfrutar de los beneficios de Puerto Seguro debe satisfacer un conjunto de condiciones mínimas. Como decíamos, debe ser una compañía establecida en EE.UU., sujeta a la jurisdicción de la Comisión Federal de Comercio (FTC) o al Departamento de Transportes de los EE.UU. (únicas entidades reconocidas hasta el momento por la Comisión Europea) y haber manifestado de forma inequívoca y pública su compromiso de cumplir las condiciones establecidas en Puerto Seguro. Estas condiciones se consideran cumplidas desde el momento en que notifique

⁸ Según el Commissioner Swindle, de la Federal Trade Commission de los EE.UU., en los últimos años y hasta junio de 2002, se habían examinado más de cien proyectos relativos a la privacidad en el Congreso de los EE.UU. (Conferencia Internacional de Autoridades de Protección de Datos, Cardiff, 2002).

su adhesión a Puerto Seguro al Departamento de Comercio. El Departamento de Comercio mantendrá una lista a disposición del público de las entidades adheridas

Los elementos de Puerto Seguro que figuran en la Decisión 2000/520/CE son los Principios (Anexo 1), las Preguntas más frecuentes - FAQs (Anexo II), un Estudio de aplicación en el que se detallan las competencias estatales y federales en materia de prácticas desleales y fraudulentas y protección de la vida privada (Anexo III), un Memorando sobre daños y perjuicios por violación de las reglas de protección de la intimidad, autorizaciones explícitas y fusiones y absorciones según el Derecho estadounidense (Anexo IV), una Carta de la FTC en la que se examinan las competencias sus competencias para la supervisión de Puerto Seguro, basada en la capacidad de perseguir las prácticas comerciales desleales y fraudulentas ya que, al fundarse Puerto Seguro en una auto certificación en la que las compañías manifiestan su voluntad de respetar sus principios, el incumplimiento de dicho compromiso podría considerarse un práctica desleal o fraudulenta y, además, la FTC adquiere el compromiso de dar prioridad a la tramitación de reclamaciones por violaciones de Puerto Seguro (Anexo V), una Carta del Dpto. de Transporte de características similares a la FTC pero en su ámbito de competencias (Anexo VI) y la relación de organismos competentes para supervisar la aplicación de Puerto Seguro, compuesta por la FTC y el Departamento de Transportes como antes se mencionó (Anexo VII).

No es el objeto de este documento hacer un análisis exhaustivo de los componentes del sistema de Puerto Seguro antes referidos. Baste, pues, mencionar que el marco en el que se desarrollaron las negociaciones fueron las Directrices sobre la Protección de la Vida Privada y los Flujos Transfronterizos de Datos (1980) de la OCDE⁹, ya que son el único instrumento internacional sobre protección de datos personales reconocido por los EE.UU. y del que también son signatarios los Estados miembros de la UE.

Los principios de Puerto Seguro son siete: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación que, en términos de la Directiva harían referencia al derecho de información, consentimiento, comunicación a terceros, seguridad, calidad de datos, derecho de acceso y recursos, responsabilidad y sanciones, aunque con un contenido bastante más limitado. Estos principios, muy generales, se completan con un conjunto de Preguntas más Frecuentes (FAQs) que intentan aclarar y precisar el alcance de los mismos y dar solución a algunas dudas interpretativas que pudieran surgir en su aplicación.

Las FAQs son quince y hacen referencia a datos especialmente protegidos, excepciones relativas al ejercicio del periodismo, responsabilidad subsidiaria de los proveedores de servicios de Internet o telecomunicaciones, excepciones a los principios de notificación, opción y acceso para los bancos de inversiones y sociedades de auditoría, la función de las autoridades de protección de datos europeas, condiciones y compromisos adquiridos a través de la auto certificación, verificación del cumplimiento de Puerto Seguro, alcance del derecho de acceso, condiciones especiales referentes a los

⁹ Se pueden consultar en <http://www1.oecd.org/publications/e-book/9302012E.PDF>

datos de Recursos Humanos transferidos desde la UE, regulación contractual de los tratamientos por cuenta de terceros, resolución de litigios y ejecución, precisiones sobre el derecho de opción, transferencia de información sobre viajes, transferencia de datos relativos a productos médicos y farmacéuticos y, finalmente, sobre la información extraída de registros públicos e información de dominio público.

En sus dictámenes respecto de los sucesivos borradores de Puerto Seguro que fueron sometidos a su consideración, las autoridades europeas de protección de datos se mostraron muy críticas con diversos aspectos de los mismos. Finalmente, tras haber conseguido incluir algunas de sus consideraciones en el texto definitivo de Puerto Seguro, en su último dictamen, el GT29 manifestó sus últimas reservas al acuerdo.

El GT29 seguía mostrando su preocupación por la excesiva complejidad de la solución de Puerto Seguro, en el que además, las formulaciones de los principios son, en muchos casos, diluidas a través de las excepciones y restricciones que aparecen posteriormente reflejadas en las FAQs.

Otro aspecto fundamental de su análisis era la falta de verificación del cumplimiento de los requisitos de las entidades que certifican su adhesión a Puerto Seguro. En efecto, el sistema se basa, exclusivamente, en una declaración unilateral de las compañías respecto de que cumplen los requisitos de Puerto Seguro y, posteriormente, el control de dicho cumplimiento se encomienda a una auditoría que se puede llevar a cabo por personal interno de la entidad. Es decir, estamos ante un esquema de auto certificación, autorregulación y auto evaluación en el que pueden no existir nunca controles externos respecto de las actividades y prácticas de protección de datos de las compañías adheridas a Puerto Seguro. Este hecho cobra aun mayor gravedad si cabe a la vista de los últimos acontecimientos ocurridos en EE.UU. y que han dañado muy gravemente la confianza en los autocontroles de las empresas, incluso si son llevados a cabo por auditores externos y, además, en un entorno como el financiero en el que existía una larga tradición, una regulación explícita y unas normas de buena práctica asentadas a través de décadas de ejercicio.

Como ya se ha mencionado, el GT29 también expresa su preocupación por el extenso régimen de excepciones presentes en las FAQs que desvirtúan lo establecido en los Principios y, especialmente, las referentes al derecho de acceso. En este sentido, ni siquiera se garantiza que, tras ejercer el derecho de acceso, se reciban los datos de “forma fácilmente inteligible”, estando dicho derecho reconocido en el Principio de Participación Individual de las Directrices OCDE que, como antes se dijo, constituyeron el marco jurídico de referencia en las negociaciones. Además, sólo se prevé la rectificación o supresión de la información inexacta y ni siquiera se explicita la obligación de cancelar los datos cuando se obtenga sin consentimiento del afectado o de manera incompatible con lo establecido en Puerto Seguro.

En relación con el principio de opción se señala la indefinición sobre los datos especialmente protegidos, ya que la fórmula utilizada en la última frase del mismo “*En cualquier caso, una entidad debe tratar como delicada toda información recibida de un tercero cuando dicho tercero la identifique y la trate como información delicada*”,

introduce un factor de ambigüedad que puede resultar en una desprotección del afectado. El GT29 siempre sugirió el empleo de la locución “Además” en lugar de “En cualquier caso”, lo que eliminaría cualquier posibilidad de interpretación errónea.

Respecto de las transferencias ulteriores, se critica el hecho de que se permita remitir datos personales a terceros que no participan en el sistema mediante la mera firma de un compromiso por escrito para que el tercero ofrezca el mismo nivel de protección que el requerido por Puerto Seguro, máxime cuando esta mera formalidad exime de toda responsabilidad a la empresa que transfiere los datos. El GT29 afirma que esta aproximación no es coherente con el sistema y que, en estos casos, debería de requerirse el consentimiento del afectado.

Uno de los puntos que suscitó mayor polémica durante toda la negociación fue el de las garantías respecto al efectivo cumplimiento de los principios por parte de las empresas adheridas al sistema. Puerto Seguro prevé una compleja mecánica de tramitación de reclamaciones y recursos en varios niveles y con distintas posibilidades, de difícil comprensión por parte del afectado al que, además, no se le ofrece suficiente apoyo y asistencia ni se le proporcionan vías adecuadas de recurso individual para defender sus intereses cuando se siente perjudicado pues, en todo caso, ha de depender de terceros para la defensa de los mismos.

Además del GT29, también el Parlamento Europeo en su Resolución sobre el proyecto de decisión de la Comisión relativa a la adecuación de la protección garantizada por los principios estadounidenses de puerto seguro y preguntas más frecuentes relacionadas publicadas por el Departamento de Comercio de los EE.UU. (C5-0280/2000 - 2000/2144(COS))¹⁰ se mostró muy crítico con el acuerdo y estableció que, sólo si se cumplían una serie de condiciones, podría considerarse que Puerto Seguro ofrecía una protección adecuada. Dichas condiciones eran las siguientes:

- reconocimiento de un derecho individual de recurso ante un organismo público independiente, competente para examinar los recursos relativos a presuntas violaciones de los principios,
- obligación de las empresas que se hayan adherido a compensar los daños, morales o patrimoniales, sufridos por las personas interesadas en caso de violación de los principios y compromiso de las mismas de borrar los datos personales obtenidos o tratados de forma ilícita,
- posibilidad de identificar fácilmente las modalidades para borrar los datos y obtener compensación por los daños;
- establecimiento de una primera verificación por parte de la Comisión del funcionamiento correcto del sistema en un plazo de seis meses a partir de su entrada en vigor, y envío de un informe sobre los resultados de la verificación y sobre los problemas detectados al Grupo de Trabajo previsto en el artículo 29, al

¹⁰ Se puede consultar en http://www.europarl.eu.int/home/default_es.htm

Comité previsto en el artículo 31 de la Directiva, así como a la comisión competente del Parlamento Europeo;

Como se ve, las condiciones del Parlamento Europeo seguían muy de cerca las preocupaciones expresadas por el GT29 en sus dictámenes y ponían de manifiesto las importantes lagunas presentes en el acuerdo de Puerto Seguro.

Por último, vamos a examinar los últimos acontecimientos en relación con Puerto Seguro. Recientemente, y para satisfacer una de las condiciones del Parlamento Europeo, la Comisión Europea ha procedido a realizar una primera evaluación de la puesta en marcha de Puerto Seguro, cuyas conclusiones principales, reflejadas en un informe remitido al GT29, merece la pena señalar. En primer lugar se hace constar que todos los elementos de Puerto Seguro están en vigor y funcionando. También se señala que no se tienen noticias de que existan quejas de ciudadanos sin resolver pero al mismo tiempo no se proporciona ninguna información respecto de las quejas presentadas, los motivos de las mismas, los mecanismos de resolución empleados o el grado de satisfacción de los afectados con los resultados obtenidos.

Quizás el aspecto más relevante puesto de manifiesto en el informe son las deficiencias en el grado de transparencia de las entidades adheridas al sistema, ya que existe un porcentaje significativo de las mismas que no han hecho pública su política de privacidad o lo misma presente serias deficiencias respecto del estándar marcado por Puerto Seguro. Este hecho es de gran relevancia puesto que, como hemos tenido ocasión de ver anteriormente, las posibilidades de intervención de los organismos supervisores americanos (FTC y Departamento de Transportes) se basan en que se hayan llevado a cabo prácticas comerciales desleales o ilícitas y el hecho que puede llevar a la aplicación de medidas por contravenciones de este precepto es el incumplimiento de las condiciones sobre protección de datos que las compañías públicamente han garantizado a los ciudadanos de los que reciben datos personales.

Como último punto, el informe destaca que las entidades arbitrales previstas por Puerto Seguro (Alternative Dispute Resolution Bodies o ADRs en sus siglas en inglés) no se han adherido a Puerto Seguro lo que debilita el sistema de cumplimiento o aplicación. Por su parte, los ADRs han justificado posteriormente esta falta de adhesión a Puerto Seguro por el hecho de que, al ser organizaciones sin ánimo de lucro, no están sometidas a la jurisdicción de la FTC, lo que las impide auto certificarse. No obstante, este hecho no debe ser óbice para que públicamente declaren su conformidad con los Principios de Puerto Seguro y adecuen sus tratamientos de datos personales a los mismos.

Adicionalmente, en los últimos meses están teniendo lugar una serie de intentos por parte de las autoridades americanas para conseguir una decisión de adecuación para su sector financiero –excluido de Puerto Seguro– en base a los nuevos desarrollos legislativos realizados por parte estadounidense en este sector y, fundamentalmente, por la reforma llevada a cabo de la Fair Credit Reporting Act (FCRA) y la entrada en vigor de la Graham-Leach-Bliley Act (GLBA), que regula la comunicación de información sobre las personas que obtienen productos o servicios de las entidades financieras.

Aunque ni la Comisión Europea ni las autoridades de control de la UE se han pronunciado todavía, los primeros análisis de dichas normas parecen arrojar serias dudas de que las mismas pudieran aducirse como instrumentos que pudieran garantizar un nivel de protección adecuado. No obstante, una línea argumental que se va abriendo paso es que sí, a juicio de las autoridades estadounidenses, las referidas leyes proporcionan un nivel de adecuación equivalente a Puerto Seguro, las entidades financieras no deberían de tener ningún problema en auto certificarse en Puerto Seguro y, de esa manera, comenzar a disfrutar de las ventajas del mismo instantáneamente.

Para finalizar este trabajo, no puedo dejar de referirme a una paradoja que puso de manifiesto el Profesor Stefano Rodotà, Presidente del GT29, en su intervención en la Conferencia Internacional de Autoridades de Protección de Datos celebrada en Cardiff en septiembre de 2002. Decía el Profesor que habiendo nacido en EE.UU. tanto el concepto del derecho a la privacidad como el de Autoridad de Control Independiente no acababa de entender como el cocktail formado por ambos resultaba tan difícil de digerir al otro lado del Atlántico. Pues bien, a mi juicio, de la adecuada resolución de esta ecuación con dos incógnitas, dependerá la buena marcha futura de la protección de datos en EE.UU. y por ende, de las relaciones entre los mismos y la UE.