DECISIÓN DE LA COMISIÓN

de 26 de julio de 2000

con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América

[notificada con el número C(2000) 2441]

(Texto pertinente a efectos del EEE)

(2000/520/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Vista 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 datos [1], y, en particular, el apartado 6 de su artículo 25,

Considerando lo siguiente:

(1) De conformidad con la Directiva 95/46/CE, los Estados miembros deben prever que la transferencia a un tercer país de datos personales únicamente pueda efectuarse cuando el tercer país de que se trate garantice un nivel de protección adecuado y cuando con anterioridad a la transferencia se respeten las disposiciones legales de los Estados miembros adoptadas con arreglo a las demás disposiciones de dicha Directiva.

(2) La Comisión puede determinar que un tercer país garantiza un nivel de protección adecuado. En tal caso, pueden transferirse datos personales desde los Estados miembros sin que sea necesaria ninguna garantía adicional.

(3) De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe evaluarse atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos, y con respecto a unas condiciones determinadas. El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, previsto en dicha Directiva [2] ha publicado orientaciones sobre la elaboración de dichas evaluaciones [3].

(4) Ante la existencia de enfoques diferentes de la protección de datos en los terceros países, tanto la evaluación del nivel de protección adecuado como la ejecución de cualquier decisión basada en el apartado 6 del artículo 25 de la Directiva 95/46/CE deben hacerse de forma que no resulte en una discriminación arbitraria o injustificada frente a o entre terceros países, si prevalecen en ellos condiciones similares, y no constituya una restricción comercial disimulada habida cuenta de los compromisos internacionales adquiridos por la Comunidad.

(5) El nivel adecuado de protección de la transferencia de datos desde la Comunidad a Estados Unidos de América, reconocido por la presente Decisión, debe alcanzarse si las entidades cumplen los principios de puerto seguro para la protección de la vida privada, con objeto de proteger los datos personales transferidos de un Estado miembro a Estados Unidos de América (en lo sucesivo denominados «los principios»), así las preguntas más frecuentes (en lo sucesivo denominadas «FAQ»), en las que se proporciona orientación para aplicar los principios, publicadas por el Gobierno de Estados Unidos de América con fecha 21 de julio de 2000. Además, las entidades deben dar a conocer públicamente sus políticas de protección de la vida privada y someterse a la jurisdicción de la Federal Trade Commission (Comisión Federal de Comercio, FTC) a tenor de lo dispuesto en el artículo 5 de la Federal Trade Commission Act, en la que se prohíben actos o prácticas desleales o fraudulentas en el comercio o en relación con él, o a la jurisdicción de otros organismos públicos que garanticen el cumplimiento efectivo de los Principios y su aplicación de conformidad con las FAQ.

(6) La presente Decisión no debe aplicarse ni a los sectores ni a los tratamientos de datos que no estén sujetos a la jurisdicción de los organismos estadounidenses enumerados en el anexo VII de la presente Decisión.

(7) Para garantizar que esta Decisión se aplique correctamente, es necesario que las entidades que suscriban los principios y las FAQ puedan ser reconocidas por los interesados (por ejemplo, las personas sobre las que existen datos, los exportadores de datos y las autoridades responsables de la protección de datos). Para ello, el Departamento de Comercio de Estados Unidos de América o su representante debe comprometerse a mantener

---

[1] DO L 281 de 23.11.1995, p. 31.

[2] La dirección en Internet del Grupo de trabajo es: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

[3] WP 12: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea, aprobado por el Grupo de trabajo el 24 de julio de 1998.

y poner a disposición del público una lista de las entidades que autocertifiquen su adhesión a los principios y su aplicación de conformidad con las FAQ y que estén sujetas a la jurisdicción de como mínimo uno de los organismos públicos enumerados en el anexo VII de la presente Decisión.

(8) Aunque se compruebe el nivel adecuado de la protección, por motivos de transparencia y para proteger la capacidad de las autoridades correspondientes de los Estados miembros de garantizar la protección de las personas en lo que respecta al tratamiento de sus datos personales, resulta necesario especificar en la presente Decisión las circunstancias excepcionales que pudieran justificar la suspensión de flujos específicos de información.

(9) El «puerto seguro» creado por los principios y las FAQ puede precisar ser objeto de revisión teniendo en cuenta la experiencia adquirida, las novedades relativas a la protección de la vida privada en circunstancias en que la tecnología hace cada vez más fácil la transferencia y tratamiento de datos personales, y los informes de aplicación elaborados por las autoridades correspondientes.

(10) El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, previsto en el artículo 29 de la Directiva 95/46/CE ha emitido dictámenes sobre el nivel de protección que proporcionan los principios en Estados Unidos de América, dictámenes que se han tenido en cuenta en la preparación de la presente Decisión ([4]).

(11) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité previsto en el artículo 31 de la Directiva 95/46/CE.

([4]) WP 15: Dictamen 1/99 relativo al nivel de protección de datos en Estados Unidos de América y a los debates en curso entre la Comisión Europea y el Gobierno de los Estados Unidos de América.
WP 19: Dictamen 2/99 relativo a la idoneidad de los principios internacionales de puerto de seguro que hizo públicos el Departamento estadounidense de Comercio el 19 de abril de 1999.
WP 21: Dictamen 4/99 relativo a las preguntas más frecuentes que hará públicas el Departamento de Comercio de Estados Unidos de América en relación con la propuesta de principios de puerte seguro.
WP 23: Documento de trabajo sobre el estado del debate entre la Comisión Europea y el Gobierno de Estados Unidos de América acerca de los principios internacionales de puerto seguro.
WP 27: Dictamen 7/99 relativo al nivel de protección de datos previsto por los principios de puerto seguro hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de Estados Unidos de América.
WP 31: Dictamen 3/2000 sobre el diálogo entre la Unión Europea y Estados Unidos de América acerca del Acuerdo de «puerto seguro».
WP 32: Dictamen 4/2000 sobre el nivel de protección que proporcionan los principios de puerto seguro.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

1. A los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, para todas las actividades cubiertas por la misma, se considerará que los principios de puerto seguro, (en lo sucesivo denominados «los principios»), que figuran en el anexo I de la presente Decisión, aplicados de conformidad con la orientación que proporcionan las preguntas más frecuentes (en lo sucesivo denominadas «FAQ») publicadas por el Departamento de Comercio de Estados Unidos de América con fecha 21 de julio de 2000, que figuran en el anexo II de la presente Decisión, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a entidades establecidas en Estados Unidos de América, habida cuenta de los siguientes documentos publicados por el Departamento de Comercio de Estados Unidos de América:

a) Estudio de aplicación, que figura en el anexo III;

b) Memorando sobre daños y perjuicios por violación de la vida privada y autorizaciones explícitas en la legislación estadounidense, que figura en el anexo IV;

c) Carta de la Comisión Federal de Comercio, que figura en el anexo V;

d) Carta del Departamento estadounidense de Transporte, que figura en el anexo VI.

2. En relación con cada transferencia de datos deberán cumplirse las condiciones siguientes:

a) la entidad receptora de los datos deberá haber manifestado de forma inequívoca y pública su compromiso de cumplir los principios aplicados de conformidad con las FAQ;

b) la entidad estará sujeta a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el anexo VII de la presente Decisión, que estará facultado para investigar las quejas que se presenten y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como reparaciones para los particulares, independientemente de su país de residencia o de su nacionalidad, en caso de incumplimiento de los principios y su aplicación de conformidad con las FAQ.

3. Se considerará que la entidad que autocertifica su adhesión a los principios y su aplicación de conformidad con las FAQ cumple las condiciones mencionadas en el apartado 2 a partir de la fecha en que notifique al Departamento de Comercio de Estados Unidos de América o a su representante el compromiso a que se refiere la letra a) del apartado 2, así como la identidad del organismo público a que se refiere la letra b) del apartado 2.

Artículo 2

La presente Decisión se refiere únicamente a la adecuación de la protección proporcionada en Estados Unidos de América con arreglo a los principios y su aplicación de conformidad con las FAQ a fin de ajustarse a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46/CE, y no afecta a la aplicación de las demás disposiciones de dicha Directiva pertenecientes al tratamiento de datos personales en los Estados miembros, y en particular a su artículo 4.

Artículo 3

1. Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios y su aplicación de conformidad con las FAQ, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos siguientes:

a) el organismo público de Estados Unidos de América contemplado en el anexo VII de la presente Decisión, o un mecanismo independiente de recurso, a efectos de la letra a) del principio de aplicación, que figura en el anexo I de la presente Decisión, ha resuelto que la entidad ha vulnerado los principios y su aplicación de conformidad con las FAQ; o

b) existen grandes probabilidades de que se estén vulnerando los principios; existen razones para creer que el mecanismo de aplicación correspondiente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad y proporcionarle la oportunidad de alegar.

La suspensión cesará en cuanto esté garantizado el cumplimiento de los principios y su aplicación de conformidad con las FAQ y las autoridades correspondientes de la Unión Europea hayan sido notificadas de ello.

2. Los Estados miembros informarán a la Comisión a la mayor brevedad de la adopción de medidas con arreglo al apartado 1.

3. Asimismo, los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no garantice dicho cumplimiento.

4. Si la información recogida con arreglo a los apartados 1 a 3 demuestra que un organismo responsable del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no está ejerciendo su función, la Comisión lo notificará al Departamento de Comercio de Estados Unidos de América y, si procede, presentará un proyecto de medidas con arreglo al procedimiento que establece el artículo 31 de la Directiva, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.

Artículo 4

1. La presente Decisión podrá adaptarse en cualquier momento de conformidad con la experiencia resultante de su aplicación o si el nivel de protección establecido por los principios y las FAQ es superado por los requisitos de la legislación estadounidense.

La Comisión analizará en todo caso, basándose en la información disponible, la aplicación de la presente Decisión tres años después de su [notificación] a los Estados miembros e informará de cualquier resultado pertinente al Comité previsto en el artículo 31 de la Directiva 95/46/CE, en particular de toda prueba que pueda afectar a la evaluación de que las disposiciones del artículo 1 de la presente Decisión proporcionan protección adecuada a efectos del artículo 25 de la Directiva 95/46/CE y de toda prueba de que la presente Decisión se está aplicando de forma discriminatoria.

2. La Comisión presentará, si procede, proyectos de medidas de conformidad con el procedimiento establecido en el artículo 31 de la Directiva 95/46/CE.

Artículo 5

Los Estados miembros adoptarán todas las medidas necesarias para cumplir la presente Decisión, a más tardar en un plazo de noventa días a partir de la fecha de su notificación a los Estados miembros.

Artículo 6

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 26 de julio de 2000.

Por la Comisión

Frederik BOLKESTEIN

Miembro de la Comisión

ANEXO I

PRINCIPIOS DE PUERTO SEGURO (PROTECCIÓN DE LA VIDA PRIVADA)

Publicados por el Departamento de Comercio de Estados Unidos de América el 21 de julio de 2000

El 25 de octubre de 1998 entró en vigor la legislación general sobre la protección de la vida privada en la Unión Europea, es decir, la Directiva relativa a la protección de datos (en adelante denominada «la Directiva»). En ella se dispone que sólo pueden transferirse datos personales a aquellos países no comunitarios que ofrezcan un nivel «adecuado» de protección de la vida privada. Aunque Estados Unidos de América y la Unión Europea comparten el objetivo de mejorar la protección de la vida privada de sus ciudadanos, los primeros siguen un enfoque diferente al de la Unión Europea. el planteamiento de Estados Unidos de América es sectorial y tiene como fundamento una mezcla de legislación, reglamentación, y autorregulación. Dadas las diferencias, muchas entidades estadounidenses han expresado su inquietud sobre las consecuencias del «nivel de adecuación» que exige la Unión Europea para las transferencias de datos personales desde la Unión Europea a Estados Unidos de América.

A fin de disipar la incertidumbre y sentar un marco más predecible para estas transferencias de datos, el Departamento Federal de Comercio publica el presente documento más las preguntas más frecuentes («los principios»), o FAQ, en su calidad de autoridad competente para estimular, fomentar y desarrollar el comercio internacional. Dichos principios se formularon en consulta con la industria y la opinión pública para facilitar el comercio y las transacciones entre Estados Unidos de América y la Unión Europea. Son de utilización exclusiva de las entidades estadounidenses que reciben datos personales de la Unión Europea, al efecto de reunir los requisitos de «puerto seguro» y obtener la correspondiente presunción de «adecuación». Puesto que los principios se concibieron exclusivamente para lograr este objetivo concreto, resultaría impropia su utilización con otros fines. Los principios no pueden utilizarse para sustituir a las disposiciones nacionales que transponen la Directiva y que se aplican al tratamiento de datos personales en los Estados miembros.

La decisión de adherirse a los requisitos de «puerto seguro» es totalmente voluntaria, pero éstos pueden cumplirse de distintas maneras. Las entidades que decidan adherirse a los principios deben aplicarlos para obtener y conservar las ventajas del puerto seguro y declararlo públicamente. Así, si una entidad se integra en un programa autorregulado de protección de la vida privada que siga los principios mencionados, reúne las condiciones de puerto seguro. También puede reunirlas elaborando sus propias medidas autorreguladoras de protección de la vida privada siempre que se adecuen a dichos principios. Cuando una entidad siga una política de autorregulación completa o parcial que cumpla los principios, la vulneración de dicha autorregulación podrá perseguirse en virtud del artículo 5 de la Federal Trade Commission Act (Ley de la Comisión federal de comercio), por la que se prohíben las practicas desleales o fraudulentas, o de otras leyes o normativas similares. (Véase en el anexo la lista de autoridades competentes estadounidenses reconocidas por la Unión Europea). Además, las entidades sujetas a disposiciones de naturaleza legal, reglamentaria, administrativa u otra (o a reglamentaciones), que protejan con eficacia el secreto de los datos personales, podrán acogerse también a los beneficios del puerto seguro. Los beneficios del puerto seguro surten efecto desde la fecha en que la entidad que desee acogerse a ellos notifique al Departamento Federal de Comercio (o a su representante) su adhesión a los principios, de conformidad con las orientaciones de la FAQ sobre autocertificación.

La adhesión a estos principios puede limitarse: a) cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explíticas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables. A fin de ser coherentes con el objetivo de mejorar la protección de la vida privada, las entidades deberán esforzarse en aplicar estos principios de manera completa y transparente, lo que incluye indicar en sus políticas de protección de la vida privada cuándo se aplicarán de manera regular las limitaciones a los principios permitidas por la anterior letra b). Por esta misma razón, cuando se permita la opción a tenor de los principios y/o de la legislación de Estados Unidos de América, se espera que las entidades opten por el mayor nivel de protección posible.

Las entidades pudieran desear por razones prácticas o de otro tipo aplicar los principios a todas sus operaciones de tratamiento de datos, pero sólo tendrán que hacerlo con las transferencias de datos una vez que se hayan adherido al «puerto seguro». A efectos de cumplimiento de los requisitos de puerto seguro, las entidades no están obligadas a aplicar dichos principios a la información conservada en sistemas de archivo procesados manualmente. Las entidades que

deseen disfrutar del puerto seguro para recibir información conservada en sistemas de archivo procesados manualmente procedente de la Unión Europea deberán aplicar los principios a toda información de este tipo transferida con posterioridad a su entrada en el puerto seguro. Si una entidad desea que los beneficios del puerto seguro se apliquen también a la información sobre recursos humanos transferida desde la Unión Europea para usarla en el contexto de una relación laboral, deberá indicarlo al Departamento de Comercio (o su representante) en la autocertificación y atenerse a los requisitos establecidos en las FAQ relativas a la autocertificación.

Asimismo, las entidades podrán aportar las garantías que exige el artículo 26 de la Directiva si incluyen los principios en aquellos convenios que celebren por escrito con quienes transfieran los datos desde la Unión Europea, siempre que la Comisión y los Estados miembros autoricen las demás cláusulas de este tipo de modelos de contratos.

La legislación estadounidense se aplicará a las cuestiones relativas a la interpretación y el cumplimiento de los principios de puerto seguro (incluidas las FAQ) y a las políticas de protección de la vida privada de las entidades adheridas al puerto seguro, excepto si éstas se han comprometido a cooperar con las autoridades europeas de protección de datos. Salvo que se indique otra cosa, serán aplicables todas las disposiciones de los principios de puerto seguro y las FAQ.

Se entiende por datos personales e información personal los datos referidos a una persona identificada o identificable que entren en el ámbito de la Directiva y sean recibidos desde la Unión Europea por entidades estadounidenses, cualquiera que sea la forma en que se registren.

NOTIFICACIÓN

Las entidades informarán a los particulares de los fines con los que cuales recogen y utilizan información sobre ellos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales se revelará la información; las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación. La notificación se hará en lenguaje claro y transparente la primera vez que se invite a los particulares a proporcionar a la entidad información personal o, posteriormente, tan pronto como sea posible, pero en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que la transfiere o la divulga por primera vez a un tercero ([1]).

OPCIÓN

Las entidades ofrecerán a los particulares la posibilidad de decidir (exclusión) si su información personal: a) puede divulgarse a un tercero ([1]) o bien b) puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o no haya sido autorizado posteriormente por el particular. Se deben proporcionar a los particulares mecanismos claros y transparentes, fácilmente disponibles y asequibles para ejercer su derecho de opción. Si se trata de información delicada, como datos sobre el estado de salud, el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afilicación sindical o la vida sexual de la persona, la opción de participar será afirmativa o explícita (aceptación) si la información va a revelarse a un tercero o a utilizarse para un fin distinto del que inicialmente motivó la recogida de información o de una manera distinta a la autorizada con posterioridad por éste al optar por la «aceptación». 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.

TRANSFERENCIA ULTERIOR

Para revelar información a terceros, las entidades deberán aplicar los principios de notificación y opción. Cuando una entidad desee transferir los datos a un tercero que actúe como agente, como se describe en la nota final, podrá hacerlo si previamente se asegura de que éste suscribe los principios, si es objeto de una resolución sobre su «adecuación» con arreglo a la Directiva u otra disposición o si firma con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios. Si la entidad cumple estos requisitos, no será responsable (a menos que la propia entidad acuerde lo contrario) del tratamiento realizado por el tercero a quien haya transferido este tipo de información y que vulnere las limitaciones o estipulaciones establecidas, a menos que la entidad sepa, o debiera saber, que el tercero realizaría dicho tratamiento y no haya adoptado medidas razonables para impedir o detener tal tratamiento.

([1]) La notificación o la opción no son necesarias cuando la información se revela a un tercero que ejecute un cometido, como agente, en nombre y bajo instrucciones de la entidad. No obstante, en este caso sí se aplica el principio de transferencia ulterior.

SEGURIDAD

Las entidades que creen, mantengan, utilicen o difundan información personal tomarán precauciones razonables para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, su modificación y su destrucción.

INTEGRIDAD DE LOS DATOS

De acuerdo con los principios, la información personal debe ser pertinente para los fines con los que se utiliza. Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el particular. En la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales.

ACCESO

Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona; o cuando puedan vulnerarse los derechos de otras personas.

APLICACIÓN

Una protección eficaz de la vida privada debe incluir mecanismos para garantizar la conformidad con los principios, una vía de recurso para las personas a que se refieran los datos y se vean afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora. Como mínimo, tales mecanismos deben incluir: a) una vía de recurso independiente, asequible e inmediatamente disponible para investigar y resolver con arreglo a los principios las denuncias y litigios de los particulares y otorgar daños y perjuicios donde determinen la legislación aplicable o las iniciativas del sector privado; b) procedimientos de seguimiento para comprobar que los certificados y declaraciones de las empresas sobre sus prácticas en materia de vida privada se ajustan a la verdad y que dichas prácticas se aplican en consecuencia; y c) obligación de subsanar los problemas derivados del incumplimiento de los principios para las entidades que se hayan adherido a ellos y las sanciones correspondientes contra ellas, que serán lo suficientemente rigurosas para garantizar su cumplimiento.

Anexo

Lista de organismos jurídicos de Estados Unidos de América reconocidos por la Unión Europea

La Unión Europea reconoce la competencia de los siguientes organismos públicos estadounidenses para investigar las quejas y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como preparaciones para los particulares en caso de incumplimiento de los principios aplicados de conformidad con las FAQ:

— la Comisión Federal de Comercio (Federal Trade Commission, FTC) con arreglo a la competencia que le confiere el artículo 5 de la Ley de la Comisión Federal de Comercio,

— el Departamento de Transporte con arreglo a la competencia que le confiere el artículo 41712 del título 49 del United States Code.

ANEXO II

PREGUNTAS MÁS FRECUENTES (FAQ)

FAQ nº 1 — Datos especialmente protegidos

P: *¿Debe una entidad ofrecer siempre de modo explícito la opción de participar cuando se trate de datos especialmente protegidos?*

R: No, puesto que no es necesario optar cuando el tratamiento: 1) se realiza en función de intereses vitales de la persona afectada o de otra persona; 2) es necesario para preparar un recurso o acción en justicia; 3) se requiere para hacer un diagnóstico médico; 4) se lleva a cabo en el marco de las legítimas actividades de una fundación, asociación o cualquier otro organismo sin fines lucrativos que persiga un objetivo político, filosófico, religioso o sindical, a condición de que el tratamiento se refiera exclusivamente a los miembros del organismo o a las personas que tienen contactos habituales con él relacionados con sus fines, y a condición de que los datos no se revelen a terceros sin el consentimiento de los interesados; 5) es necesario para que la entidad cumpla sus obligaciones en materia de Derecho laboral; o 6) se refiere a información hecha pública de modo manifiesto por el particular.

FAQ nº 2 — Excepciones del periodismo

P: *Habida cuenta del amparo que la Constitución de Estados Unidos de América ofrece a la libertad de prensa, así como de las excepciones que contempla la Directiva en materia de periodismo, ¿se aplican los principios de puerto seguro a la información de carácter personal recogida, mantenida o divulgada con fines periodísticos?*

R: Cuando el derecho a la libertad de prensa consagrado en la Primera Enmienda de la Constitución de Estados Unidos de América entra en conflicto con los intereses de la protección de la vida privada, la Primera Enmienda debe regir el equilibrio de tales intereses en lo tocante a las actividades de particulares o entidades estadounidenses. La información personal que se recoge con fines de publicación, transmisión u otras formas de comunicación pública de material periodístico, aunque no se utilice, así como la información que se recabe de material de archivo publicado anteriormente, no están sujetas a los requisitos de los principios de puerto seguro.

FAQ nº 3 — Responsabilidad subsidiaria

P: *Los proveedores de servicios Internet, los operadores de telecomunicaciones u otras entidades, ¿son responsables desde el punto de vista de los principios de puerto seguro cuando, en nombre de otra entidad, se limitan a transmitir, encaminar, intercambiar o almacenar temporalmente información contraviniendo sus preceptos?*

R: No. Tal como la propia Directiva, el puerto seguro no genera una responsabilidad subsidiaria. Si una entidad actúa como mero conducto de los datos transmitidos por terceros y no es determinante ni de la finalidad ni de los medios de tratamiento de los datos personales, no será responsable.

FAQ nº 4 — Bancos de inversiones y sociedades de auditoría

P: *Las actividades de bancos de inversiones y sociedades de auditoría podrían suponer el tratamiento de datos personales sin autorización o conocimiento del interesado. ¿En qué circunstancias autorizan este proceder los principios del puerto seguro relativos a la notificación, la opción y el acceso?*

R: Los bancos de inversiones o las sociedades de auditoría pueden tratar información sin conocimiento del interesado sólo en la medida y durante el período necesarios para cumplir las normas o satisfacer las exigencias del interés público, así como en otras circunstancias en que la aplicación de estos principios perjudicaría los intereses legítimos de la entidad. Entre éstos se cuenta la supervisión del cumplimiento por las empresas de sus obligaciones legales y las actividades legítimas de contabilidad, así como la necesidad de secreto relacionada con posibles adquisiciones, fusiones, *joint ventures* u otras operaciones similares llevadas a cabo por los bancos de inversiones o las sociedades de auditoría.

FAQ nº 5 [1] **— La función de las autoridades de protección de datos**

P: *¿Qué forma adoptarán y cómo se aplicarán los compromisos de colaboración de las empresas con las autoridades de protección de datos (APD) de la Unión Europea?*

R: Las entidades estadounidenses que reciban datos personales procedentes de la Unión Europea deberán comprometerse a utilizar mecanismos eficaces para dar cumplimiento a los principios del puerto seguro. En concreto y con arreglo al principio de aplicación, dichos mecanismos establecerán: a) vías de recurso para los particulares a que se refieran los datos; b) procedimientos de seguimiento para comprobar la sinceridad de las afirmaciones y declaraciones de las entidades sobre el respeto de la intimidad, y c) la obligación de éstas de subsanar los problemas que surjan por el incumplimiento de los principios, así como de asumir sus consecuencias. Una entidad puede satisfacer las letras a) y c) del principio de aplicación si se adhiere a los requisitos de colaboración con las autoridades de protección de datos (APD) de la presente FAQ.

Una entidad puede comprometerse a colaborar con las APD declarando en su certificación de puerto seguro dirigida al Departamento de Comercio (véase la FAQ nº 6 sobre autocertificación) que:

1) opta por cumplir las letras a) y c) del principio de aplicación del puerto seguro comprometiéndose a colaborar con las APD competentes;

2) colaborará con las APD competentes en la investigación y resolución de las quejas que se formulen con arreglo al puerto seguro;

3) cumplirá las decisiones de la APD cuando ésta determine que la entidad debe tomar medidas concretas para cumplir los principios de puerto seguro, y en particular el pago de indemnizaciones o compensaciones en beneficio de los afectados por el incumplimiento de los principios, y notificará por escrito a la APD la adopción de dichas medidas.

Las APD colaborarán con información y asesoramiento, que se prestarán de la manera siguiente:

— Las APD proporcionarán asesoramiento a través de un panel informal de APD de ámbito europeo, que permitirá, entre otras cosas, seguir un enfoque armonizado y coherente.

— El panel asesorará a las entidades estadounidenses involucradas en quejas no resueltas de particulares, sobre el tratamiento de información personal transferida desde la Unión Europea dentro del puerto seguro. Esta actividad de asesoramiento tendrá como finalidad la correcta aplicación de los principios de puerto seguro y conllevará la indemnización de los afectados que las APD consideren adecuada.

— El panel proporcionará este tipo de asesoramiento en respuesta tanto a los casos que le remitan las entidades afectadas, como a las quejas que reciba directamente de particulares contra entidades que se hayan comprometido a colaborar con las APD en el marco del puerto seguro. Simultáneamente, animará y, en su caso, ayudará a los particulares en un primer momento a hacer uso de las modalidades internas de resolución de litigios que ofrezcan las entidades.

— Sólo se proporcionará asesoramiento una vez que las partes en litigio hayan dispuesto de una oportunidad razonable de hacer sus observaciones y aportar las pruebas que deseen. El panel tratará de dar su consejo tan pronto como lo permita esta exigencia de garantía jurisdiccional y, de modo general, en un plazo de sesenta días tras recibir la queja o la remisión, o antes si es posible.

— El panel hará público los resultados de sus deliberaciones sobre las quejas si lo considera conveniente.

— El asesoramiento del panel no conllevará responsabilidad alguna ni para éste ni para una APD en concreto.

[1] La inclusión de esta FAQ en el expediente depende del acuerdo que se alcance con las APD, las cuales han debatido la actual redacción en el Grupo de trabajo del artículo 29. Aunque a la mayoría le parece aceptable, sólo se podrá adoptar un punto de vista definitivo en el marco del dictamen general que evacuará el Grupo de trabajo sobre el expediente final.

Como se señaló anteriormente, las entidades que escojan esta opción para la resolución de litigios deben comprometerse a cumplir el consejo de la APD. Si una entidad persiste en el incumplimiento transcurridos veinticinco días desde que se recibió consejo y no ha dado una explicación satisfactoria sobre el retraso, el panel notificará su intención ya sea de someter la cuestión a la Comisión Federal de Comercio u otro organismo federal o estatal de Estados Unidos de América con jurisdicción para actuar en casos de fraude o engaño, o de certificar que se ha vulnerado gravemente el acuerdo de cooperación, por lo que deberá considerarse nulo de pleno derecho. En este último caso, el panel informará al Departamento de Comercio (o a su representante) de la consiguiente modificación de la lista de participantes del puerto seguro. Todo incumplimiento del compromiso de cooperar con las APD, así como de los principios de puerto seguro, podrá originar un procedimiento por fraude de conformidad con el artículo 5 de la Ley de la Comisión Federal de Comercio o norma similar.

Las entidades que escojan esta opción deberán pagar una tasa anual para cubrir el coste de funcionamiento del panel. Además, podría solicitárseles que se hagan cargo de los gastos de traducción derivados de las deliberaciones del panel sobre las quejas que les afecten. La tasa anual no sobrepasará los 500 dólares estadounidenses y será de menor cuantía para las empresas más pequeñas.

Las entidades que suscriban el puerto seguro podrán optar por cooperar con las APD durante un período de tres años. Al final de dicho período, las APD podrán reconsiderar el acuerdo si el número de las entidades estadounidenses que hayan escogido esta opción resulta excesivo.

FAQ nº 6 — Autocertificación

P: *¿De qué modo una entidad autocertifica su adhesión a los principios de puerto seguro?*

R: Los beneficios del puerto seguro se garantizan desde la fecha en que una entidad autocertifica ante el Departamento de Comercio, o su representante, su adhesión a los principios de conformidad con las directrices que se indican a continuación.

Para proceder a la autocertificación, las entidades pueden proporcionar al Departamento de Comercio (o a su representante) una carta firmada por uno de los responsables de la empresa en nombre de la entidad que se adhiere al puerto seguro, que contendrá cuando menos la información siguiente:

1) nombre de la entidad, señas postales y de correo electrónico, teléfono y fax;

2) descripción de las actividades de la entidad en lo relativo a la información personal recibida de la Unión Europea; y

3) descripción de su política de protección de la vida privada respecto de dicha información personal, con indicación de: a) el lugar donde puede consultarla el público; b) la fecha de entrada en vigor de dicha política; c) una oficina de contacto para la tramitación de las quejas, las solicitudes de acceso y cualquier otra cuestión relacionada con los principios de puerto seguro; d) el organismo oficial concreto con jurisdicción para entender de cualquier queja contra la entidad por posibles prácticas desleales o fraudulentas y vulneraciones de las leyes o normas sobre la vida privada (y citado en el anexo de los principios); e) el nombre de los programas de protección de la vida privada a los que esté adscrita la entidad; f) el método de verificación (por ejemplo, interna, por terceros) ([2]); y g) la instancia independiente de recurso que se ocupará de investigar las quejas no resueltas.

Si la entidad desea que los beneficios del puerto seguro se apliquen a la información sobre recursos humanos transferida desde la Unión Europea para usarla en el contexto de la relación laboral, puede hacerlo siempre que exista un organismo oficial con jurisdicción para entender de cualquier queja contra la entidad provocada por información sobre recursos humanos citado en el anexo de los principios. Además, la entidad deberá indicarlo en su carta y expresar su compromiso de cooperar con las autoridades comunitarias de conformidad con las FAQ nºs 9 y 5, según el caso, y que cumplirá las recomendaciones de dichas autoridades.

El Departamento (o su representante) llevará una lista de las entidades que presenten dichas cartas, dispensándoles por consiguiente los beneficios del puerto seguro. Asimismo, actualizará la lista con las cartas anuales y las notificaciones recibidas de conformidad con la FAQ nº 11. Las cartas de autocertificación se presentarán por lo menos una vez al año. De lo contrario, la entidad será eliminada de la lista y dejarán de dispensársele los beneficios del puerto

([2]) Véase la FAQ nº 7 sobre verificación.

seguro. Tanto la lista como las cartas de autocertificación remitidas por las entidades se harán públicas. Las entidades que autocertifican su adhesión a los principios de puerto seguro indicarán también este extremo en las declaraciones relativas a su política de protección de la vida privada.

El compromiso de adhesión a los principios de puerto seguro respecto a los datos recibidos durante el período en que la entidad disfruta de los beneficios del puerto seguro no está limitado en el tiempo. Según este compromiso, continuarán aplicándose los principios a dichos datos mientras la entidad los almacene, utilice o divulgue, aunque posteriormente se desvincule del puerto seguro por cualquier motivo.

Una entidad que deje de existir como persona jurídica independiente a resultas de una fusión o adquisición deberá notificarlo previamente al Departamento de Comercio (o su representante). La notificación deberá indicar también si la entidad adquirente o la entidad resultante de la fusión: 1) mantendrá su adhesión a los principios de puerto seguro en virtud de la normativa sobre adquisiciones o fusiones, o bien 2) opta por autocertificar su adhesión a los principios de puerto seguro o establece otras salvaguardias, por ejemplo un acuerdo escrito que garantice la adhesión a los principios de puerto seguro. Si no se aplican los anteriores puntos 1 o 2, cualquier dato que se haya adquirido en el marco del puerto seguro deberá suprimirse inmediatamente.

La entidad no necesita someter a los principios de puerto seguro toda la información personal, perso sí deberá aplicar los principios de puerto seguro a todos los datos personales recibidos desde la Unión Europea a partir del momento en que se adhiera al puerto seguro.

Cualquier deficiencia de la información dada a conocer al público en lo relativo a la adhesión de la entidad a los principios de puerto seguro podrá denunciarse ante la Comisión Federal de Comercio u otra instancia oficial competente. Las deficiencias de la información proporcionada al Departamento de Comercio (o a su representante) podrán perseguirse en virtud de la False Statements Act (Ley sobre declaraciones falsas, 18USC § 1001).

FAQ nº 7 — Verificación

P: *¿Qué procedimientos ofrecen las entidades para verificar que los certificados y declaraciones que presentan las empresas sobre sus prácticas de protección de la vida privada de puerto seguro son ciertos y que estas prácticas se han aplicado de la manera indicada y de conformidad con los principios de puerto seguro?*

R: Para reunir los requisitos de verificación del principio de aplicación, una entidad puede verificar los certificados y declaraciones mencionados mediante autoevaluación o mediante verificaciones por terceros.

Siguiendo el método de autoevaluación, la verificación debería indicar que la política de protección de la vida privada respecto a la información personal recibida de la Unión Europea y hecha pública por la entidad es precisa, completa, está expuesta de manera destacada, se ha aplicado en su totalidad y es accesible. Asimismo, debería indicar que dicha política cumple los principios de puerto seguro; que los particulares reciben información sobre los mecanismos de resolución de quejas de que disponen; que ha puesto en marcha los procedimientos, ofrece formación a los trabajadores para su aplicación y aplica medidas disciplinarias en caso de que no los cumplan; y que ha puesto en marcha procedimientos internos para efectuar periódicamente revisiones objetivas sobre el cumplimiento de todo lo anterior. Un directivo u otro representante autorizado de la empresa debería firmar un informe de verificación de la autoevaluación como mínimo una vez al año y éste debería difundirse a petición de los consumidores o en el contexto de posibles investigaciones o quejas por incumplimiento.

Las entidades deberían conservar registros sobre la aplicación de sus prácticas de puerto seguro de protección de la vida privada, y ponerlos a disposición cuando se soliciten en caso de investigaciones o quejas por incumplimiento ante los organismos independientes encargados de ellas o competentes en materia de prácticas desleales y fraudulentas.

Cuando la entidad haya elegido someterse a la verificación por terceros, dicha verificación deberá demostrar que la política de la entidad en cuanto a la vida privada relativa a la información personal recibida de la Unión Europea se ajusta a los principios de puerto seguro, que se está cumpliendo y que los particulares reciben información sobre los mecanismos de queja. Los métodos de verificación pueden incluir, a título meramente enunciativo, auditorías, comprobaciones imprevistas, el uso de «señuelos» o de herramientas tecnológicas, según se considere apropiado. El

informe de que se ha completado satisfactoriamente la verificación por terceros deberá portar la firma del revisor o del directivo u otro representante autorizado de la empresa, se elaborará como mínimo una vez al año y se difundirá a petición de los consumidores o en el contexto de posibles investigaciones o quejas por incumplimiento.

FAQ nº 8 — Acceso

Principio de «acceso»

Los particulares tendrán acceso a la información personal que sobre ellos detenten las entidades. Podrán corregirla o modificarla si es inexacta, excepto en dos casos: cuando ello suponga una carga o dispendio claramente desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la intimidad de la persona; o cuando puedan vulnerarse los legítimos derechos de otras personas.

P. 1: *¿Es el derecho de acceso un derecho absoluto?*

R. 1: No. De acuerdo con los principios de puerto seguro, el derecho de acceso es fundamental para la protección de la intimidad. En particular, permite a las personas verificar la presión de la información existente sobre ellas. No obstante, la obligación que tiene una entidad de proporcionar acceso a la información personal que posee sobre una persona está sujeta al principio de proporcionalidad o razonabilidad y debe suavizarse en determinados casos. De hecho, la exposición de motivos de las Directrices sobre intimidad de la Organización de Cooperación y Desarrollo Económico (OCDE) de 1980 establece claramente que la obligación de ofrecer acceso de una entidad no es absoluta. No exige la búsqueda excesivamente detallada requerida, por ejemplo, para una citación judicial, ni tampoco exige dar acceso a todos los formatos distintos en los que la entidad puede mantener la información.

La experiencia ha demostrado que, al responder a las peticiones de acceso de los afectados, las entidades deben guiarse por los motivos de preocupación que provocaron inicialmente la petición. Por ejemplo, si una petición de acceso es vaga o muy amplia, la entidad puede dialogar con el afectado para comprender mejor los motivos de la petición y localizar la información correspondiente. La entidad podría indagar sobre los departamentos con los que ha tenido contacto el afectado o sobre la naturaleza (o el uso) de la información a la que solicita acceder. No obstante, los afectados no tienen que justificar las peticiones de acceso a sus propios datos.

Las cargas y dispendios son factores importantes y deberían tenerse en cuenta, pero no son determinantes a la hora de decidir si es razonable facilitar el acceso. Por ejemplo, si la información se está utilizando para tomar decisiones que afectarán significativamente a la persona (por ejemplo, la concesión o denegación de ventajas importantes, como un seguro, una hipoteca o un puesto de trabajo), de conformidad con los demás preceptos de estas FAQ, la entidad debería proporcionar la información aunque sea relativamente difícil o costoso.

Si la información solicitada no se refiere a datos especialmente protegidos o no se emplea en decisiones que afecten significativamente a la persona (por ejemplo, información de márketing que no incluye datos especialmente protegidos y que se utiliza para decidir si se envía un catálogo a una persona), pero es fácil de consultar y no cuesta nada, la entidad tendría que proporcionar acceso a los datos que tiene almacenados sobre el afectado. La información pertinente podría incluir datos proporcionados por el propio individuo, datos recopilados en el transcurso de una transacción o datos obtenidos a través de terceros y que estén relacionados con la persona.

De conformidad con la naturaleza fundamental del acceso, las entidades siempre deben esforzarse de buena fe en facilitar el acceso. Por ejemplo, cuando se necesite proteger cierta información y ésta pueda separarse fácilmente del resto de información sujeta a una petición de acceso, la entidad debería guardar la información protegida y facilitar el resto. Si una entidad decide que debe denegar el acceso en algún caso concreto, debe ofrecer a la persona que solicita dicho acceso una explicación de los motivos que han provodado tal decisión e indicarle un punto de contacto en caso de duda.

P. 2: *¿Qué es la información comercial confidencial? ¿Pueden las entidades denegar el acceso para protegerla?*

R. 2: La información comercial confidencial (en el uso dado al término *«confidential commercial information»* en la Ley federal de enjuiciamiento civil en materia de divulgación de la información) son los datos que una entidad ha considerado que debe proteger contra la divulgación, dado que su conocimiento ayudaría a un competidor en el mercado. Un programa informático utilizado por la entidad, por ejemplo, un programa de modelización, o los

detalles de dicho programa pueden ser información comercial confidencial. Cuando la información comercial confidencial se pueda separar fácilmente del resto de información sujeta a una petición de acceso, la entidad debería guardar la información comercial confidencial y facilitar la información no confidencial. Las entidades pueden denegar o limitar el acceso para no revelar su propia información comercial confidencial, en la acepción mencionada (predicciones de márketing o clasificaciones confeccionadas por la entidad), o la de otra entidad, cuando dicha información esté sujeta a una obligación contractual de confidencialidad, en aquellas circunstancias en las que normalmente se cumpliría o se impondría tal obligación de confidencialidad.

P. 3: *A la hora de proporcionar el acceso ¿puede una entidad facilitar a los afectados la información personal de que disponga sobre ellos extraída de sus bases de datos o se exige el acceso a la propia base de datos?*

R. 3: El acceso se puede facilitar directamente a través de un informe de la entidad al afectado y no exige que dicha persona acceda a la base de datos de la entidad.

P. 4: *¿Deben las entidades reestructurar sus bases de datos para poder facilitar el acceso?*

R. 4: Solamente es necesario facilitar el acceso en la medida en que la entidad almacene información. El principio de acceso no crea de por sí ninguna obligación de obtener, mantener, reorganizar ni reestructurar ficheros de datos personales.

P. 5: *Estas respuestas aclaran que el acceso se puede denegar en determinadas circunstancias. ¿En qué otras circunstancias podrían las entidades denegar a los afectados el acceso a su información personal?*

R. 5: Estas circunstancias son limitadas y las razones para denegar el acceso deben ser específicas. Una entidad puede negarse a proporcionar acceso a la información en la medida en que sea probable que su difusión interfiera con la protección de intereses públicos importantes equivalentes, como la seguridad del Estado, la defensa o la seguridad pública. Además, si la información personal se trata exclusivamente para fines de investigación o estadísticos, el acceso se puede denegar. Entre otros motivos para denegar o limitar el acceso cabe citar los siguientes:

a) interferencia en la ejecución o aplicación de la ley, especialmente en la prevención, investigación o detección de delitos o el derecho a un juicio justo;

b) interferencia en juicios privados, especialmente en la prevención, investigación o detección de reclamaciones contenciosas o el derecho a un juicio justo;

c) divulgación de información personal relativa a terceras personas en caso de que no se puedan separar dichas referencias;

d) vulneración de un privilegio o una obligación jurídica o profesional;

e) incumplimiento de la confidencialidad necesaria de negociaciones presentes o futuras, como las relacionadas con la adquisición de empresas cotizadas en bolsa;

f) perjuicio para investigaciones sobre seguridad de los trabajadores o procedimientos de resolución de conflictos;

g) perjuicio para el sigilo que pueda ser necesario durante períodos limitados en relación con la planificación de la sucesión de trabajadores y la reorganización empresarial;

h) perjuicio de la confidencialidad necesaria para las funciones de control, inspección o regulación relacionadas con la buena gestión económica o financiera;

i) otras circunstancias en que la carga o dispendio necesarios para facilitar el acceso sean desproporcionados o se vulneren los derechos o intereses legítimos de otras personas.

Una entidad que se acoja a una excepción tendrá que demostrar que corresponde aplicarla (como suele suceder). Como se indica anteriormente, se debe informar al afectado de los motivos por los que se deniega o limita el acceso y se le debe proporcionar un contacto para consultas posteriores.

P. 6: *¿Pueden las entidades cobrar una cuota para cubrir el coste del acceso?*

R. 6: Sí. Las directrices de la OCDE admiten que las entidades cobren una cuota, siempre que no sea excesiva. Por tanto, las entidades pueden cobrar una cuota razonable por el acceso, lo que puede resultar de utilidad para evitar peticiones repetitivas y enojosas.

Por tanto, las entidades dedicadas a la venta de información de dominio público podrán cobrar los honorarios habituales para responder a las peticiones de acceso. Alternativamente, los afectados podrán acceder a su información directamente a través de la entidad que haya compilado los datos inicialmente.

No podrá denegarse el acceso por motivos de coste si el particular se ofrece a pagarlo.

P. 7: *¿Deben las entidades proporcionar acceso a información personal extraída de registros públicos?*

R. 7: En primer lugar, es preciso aclarar que los registros públicos son los registros que mantienen los órganos o entidades gubernamentales de cualquier nivel y que los ciudadanos pueden consultar. No es necesario aplicar el principio de acceso a estos datos siempre que no se combinen con otra información personal, excepto en el caso de que se usen algunos datos de registros que no sean públicos para indizar u organizar la información de los registros públicos. Sin embargo, deberán respetarse las condiciones de consulta establecidas por la jurisdicción correspondiente. Asimismo, cuando la información de registros públicos se combina con información de otros registros que no sean públicos (con la excepción indicada anteriormente) las entidades deben facilitar el acceso a toda la información, suponiendo que no esté sujeta a otras excepciones permitidas.

P. 8: *¿Debe aplicarse el principio de acceso a la información personal de dominio público?*

R. 8: Como sucede con la información de los registros públicos (véase la P. 7), no es necesario facilitar el acceso a la información de dominio público siempre que no se combine con información que no sea de dominio público.

P. 9: *¿Cómo puede protegerse una entidad contra las peticiones de acceso repetitivas o vejatorias?*

R. 9: Las entidades no tienen que responder a estas peticiones de acceso. Éste es el motivo de que las entidades puedan cobrar una cuota razonable y establecer límites razonables en cuanto al número de veces que responderán en un período determinado a las peticiones de acceso de cada persona. Al definir estos límites, la entidad debe analizar factores tales como la frecuencia con que se actualiza la información, los fines para los que se usan los datos y la naturaleza de éstos.

P. 10: *¿Cómo puede protegerse una entidad contra las peticiones de acceso fraudulentas?*

R. 10: No se exige a las entidades que proporcionen acceso a menos que reciban información suficiente para confirmar la identidad de la persona que realiza la petición.

P. 11: *¿Existe un plazo para responder a las peticiones de acceso?*

R. 11: Sí, las entidades deben responder sin demoras excesivas y en un plazo de tiempo razonable. Este requisito se puede cumplir de distintos modos, como se indica en el memorándum explicativo de las Directrices sobre intimidad de la OCDE de 1980. Por ejemplo, el responsable de un fichero de datos que facilite información a intervalos regulares puede estar exento de la obligación de responder inmediatamente a peticiones individuales.

FAQ nº 9 — Recursos humanos

P. 1: *¿Está cubierta por los principios de puerto seguro la transferencia de la Unión Europea a Estados Unidos de América de información personal obtenida en el contexto de la relación laboral?*

R. 1: Sí, cuando una empresa ubicada en la Unión Europea transfiera información personal de sus trabajadores (pasada o presente) obtenida en el contexto de la relación laboral a una matriz, filial o a un proveedor de servicio no asociado ubicado en Estados Unidos de América que se haya adherido al puerto seguro, la transferencia disfruta de

las ventajas del puerto seguro. En tal caso, la recogida de la información y su tratamiento previo a la transferencia se habrá sometido a la legislación nacional del país de la Unión Europea donde se haya realizado y a cualquier condición o restricción aplicable a su transferencia de conformidad con la normativa vigente.

Los principios de puerto seguro solamente son pertinentes cuando se transfieran registros identificados de manera individual o se acceda a ellos. Los informes estadísticos basados en datos generales sobre empleo o el uso de datos disociados o en los que se hayan utilizado seudónimos no plantean problemas para el derecho a la vida privada.

P. 2: *¿Cómo se aplican los principios de notificación y opción a dicha información?*

R. 2: Aquellas entidades estadounidenses que hayan recibido de la Unión Europea información sobre los trabajadores dentro del puerto seguro podrán revelarla a terceros y utilizarla con fines diferentes exclusivamente con arreglo a los principios de notificación y de opción. Por ejemplo, cuando las entidades estadounidenses deseen utilizar la información personal obtenida a través de la relación laboral para fines no relacionados con los laborales, como comunicaciones de márketing, deberán facilitar a los afectados el ejercicio de la opción antes de hacerlo, a menos que éstos hayan autorizado la utilización de la información para tales fines. Es más, esta opción no se utilizará para limitar sus oportunidades laborales ni para sancionarles.

Debe advertirse que es preciso cumplir algunas condiciones de aplicación general a las transferencias procedentes de los Estados miembros, las cuales pueden excluir otras utilizaciones de la información incluso después de su transferencia fuera de la Unión Europea.

Además, los empresarios deberán realizar todos los esfuerzos razonables para responder a las preferencias de sus trabajadores en cuanto a la vida privada. Esto incluirá, por ejemplo, restringir el acceso a los datos, disociar determinados datos o bien asignar códigos o seudónimos cuando no se necesiten los nombres para la finalidad de gestión de que se trate.

La entidad no aplicará los principios de notificación y opción en la medida y tiempo necesarios para que no haya perjuicio de sus intereses legítimos cuando tome decisiones sobre ascensos, nombramientos y otras decisiones laborales similares.

P. 3: *¿Cómo se aplica el principio de acceso?*

R. 3: Las FAQ sobre acceso ofrecen orientación sobre los motivos que pueden justificar la denegación o limitación del acceso previa petición en el ámbito de los recursos humanos. Por supuesto, los empresarios de la Unión Europea deben cumplir las normativas locales y garantizar que los trabajadores europeos tienen acceso a la información de la forma exigida por ley en sus países, independientemente del lugar donde se traten y almacenen los datos. Los principios de puerto seguro exigen a las entidades que tratan estos datos en Estados Unidos de América que cooperen a la hora de facilitar el acceso directamente o a través del empresario de la Unión Europea.

P. 4: *¿Cómo se gestionará la aplicación forzosa de los principios de puerto seguro para los datos sobre trabajadores?*

R. 4: En la medida en que la información se utilice exclusivamente en el contexto de la relación laboral, la responsabilidad principal sobre los datos relativos al trabajador recae en la entidad de Estados Unidos de América. De ello se deduce que, cuando los trabajadores europeos planteen quejas sobre la violación de sus derechos de protección de datos y no estén satisfechos con los resultados de los procedimientos de verficiación interna, queja y apelación (o con cualquier procedimiento de resolución de conflictos a tenor de un contrato con organizaciones sindicales), deben dirigirse a la agencia nacional de protección de datos o a la autoridad en materia laboral correspondiente a su jurisdicción. Se incluyen también los casos en que la presunta gestión inadecuada de la información personal haya tenido lugar en Estados Unidos de América, sea responsabilidad no del empresario sino de la entidad estadounidense que haya recibido la información a través del empresario y, por consiguiente, suponga un presunto incumplimiento de los principios de puerto seguro y no de la legislación nacional por la que se transpone la Directiva. Será el método más eficaz para abordar los derechos y obligaciones, con frecuencia coincidentes, impuestos por la legislación local en materia de empleo y por los convenios colectivos, así como por la legislación sobre protección de datos.

Una entidad estadounidense adherida al puerto seguro que utilice datos europeos sobre recursos humanos transferidos desde la Unión Europea en el contexto de la relación laboral y que desee que dicha transferencia también esté cubierta por el acuerdo de puerto seguro deberá comprometerse a cooperar en las investigaciones de las autoridades de la Unión Europea competentes y a acatar sus recomendaciones en dichos casos. Las APD que deci-

dan cooperar de esta forma lo notificarán a la Comisión Europea y al Departamento de Comercio. Cuando una entidad estadounidense adherida al puerto seguro desee transferir información sobre recursos humanos desde un Estado miembro en el que la APD no lo permita, se aplicarán las disposiciones de la FAQ nº 5.

FAQ nº 10 — Contratos del artículo 17

P: *Cuando se transfieren datos de la Unión Europea a Estados Unidos de América exclusivamente para tratamiento, ¿es necesario un contrato, participe o no el encargado del tratamiento en el puerto seguro?*

P: Sí. Los responsables del tratamiento en Europa tienen siempre que celebrar un contrato al realizar una transferencia para el simple tratamiento de los datos, con independencia de que la operación tenga lugar dentro o fuera de la Unión Europea. La finalidad del contrato es proteger los intereses del responsable del tratamiento, es decir, de la persona u organismo que determina los fines y los medios de dicho tratamiento, y sobre la cual recae toda la responsabilidad de los datos ante los afectados. Así pues, en el contrato se estipula qué tipo de tratamiento se va a realizar y las medidas necesarias para garantizar la seguridad de los datos.

Las entidades de Estados Unidos de América que participen en el puerto seguro y reciban información personal de la Unión Europea para su mero tratamiento no están por tanto obligadas a aplicar los principios a dicha información, pues el responsable europeo de los datos sigue teniendo la responsabilidad sobre ella frente a los particulares, de conformidad con los preceptos comunitarios correspondientes (que pueden ser más rigurosos que los principios de puerto seguro equivalentes).

Puesto que los participantes en el puerto seguro proporcionan la protección necesaria, los contratos concertados con ellos que tengan por objeto el simple tratamiento de los datos no requieren la autorización previa (o ésta sería concedida automáticamente por los Estados miembros) que se exigiría a los receptores que no participen en el puerto seguro o que no garanticen la protección adecuada.

FAQ nº 11 — Resolución de litigios y ejecución

P: *¿Cómo deberán cumplirse los requisitos de resolución de litigios impuestos por el principio de aplicación y cómo se deberá actuar ante el caso de que una entidad incumpla sistemáticamente los principios?*

R: El principio de aplicación establece los requisitos en virtud de los cuales se regulan los mecanismos de aplicación del puerto seguro. La FAQ sobre verificación (FAQ nº 7) establece la forma de reunir los requisitos de la letra b) del principio. En la presente FAQ nº 11 se abordan las letras a) y c), que requieren instancias independientes de recurso. Dichas instancias pueden adoptar formas diversas, pero siempre deben reunir los requisitos exigidos por el principio de aplicación. Las entidades podrán cumplirlos de la manera siguiente: 1) conformidad con programas de protección de la vida privada concebidos por el sector privado que incorporen los principios de puerto seguro en sus normas y cuenten con mecanismos de aplicación eficaces, similares a los descritos en el principio de aplicación; 2) conformidad con lo dispuesto por las autoridades de control establecidas legal o reglamentariamente que prevean la tramitación de las quejas individuales y la resolución de litigios; o 3) compromiso de colaboración con las autoridades de protección de datos establecidas en la Comunidad Europea o sus representantes autorizados. Esta lista se ofrece a título ilustrativo y no es de ninguna manera taxativa. El sector privado puede crear otros mecanismos de aplicación, siempre que reúnan los requisitos contemplados en el principio de aplicación y en las FAQ. Obsérvese que los requisitos del principio de aplicación se añaden al requisito expuesto en el apartado 3 de la introducción a los principios, en el sentido de que las iniciativas autorreguladoras deberán ser vinculantes con arreglo al artículo 5 de la Federal Trade Commission Act (Ley de la Comisión Federal de Comercio) o legislación similar.

Instancias de recurso:

Se alentará a los consumidores a presentar cualquier queja que tengan ante la entidad correspondiente antes de acudir a las instancias de recurso independientes. La independencia de éstas es una cuestión de hecho que puede demostrarse de varias formas, por ejemplo, por la transparencia de su composición y de su financiación o por exhibir unos antecedentes reconocidos. Tal como exige el principio de aplicación, los recursos que se pongan a disposi-

ción de los particulares deberán ser rápidos y asequibles. Los organismos de resolución de litigios aceptarán a trámite todas las quejas que reciban de los particulares, a menos que sea patente su falta de base o ésta sea de poca entidad, lo cual no impedirá que la entidad gestora de la instancia de recurso establezca condiciones de admisibilidad. Sin embargo, dichas condiciones deberán ser transparentes y justificarse debidamente (por ejemplo, para excluir las quejas que no entran en el ámbito de aplicación del programa y que merecen consideración en otra instancia), y no deberán obstaculizar el compromiso de aceptar a trámite las quejas legítimas. Además, las instancias de recurso proporcionarán a los particulares toda la información disponible sobre el funcionamiento del procedimiento de resolución de litigios cuando presenten la queja. Esta información deberá incluir la notificación de las prácticas de protección de la vida privada que utilian tales instancias, de conformidad con los principios de «puerto seguro» ([3]). También deberán colaborar en el desarrollo de herramientas tales como formularios normalizados de queja para facilitar el proceso de resolución de las quejas.

Vías de recurso y sanciones:

En virtud de los remedios proporcionados por el organismo de resolución de litigios, la entidad corregirá o anulará los efectos del incumplimiento, en la medida de lo posible; cualquier tratamiento que la entidad haga en el futuro se adecuará a los principios; y, cuando proceda, se interrumpirá el tratamiento de los datos personales del particular que haya presentado la queja. Las sanciones tienen que ser lo suficientemente rigurosas para que la entidad cumpla los principios. Una gama de sanciones con distintos grados de severidad permitirá a los organismos de resolución de litigios responder debidamente a los diferentes niveles de incumplimiento. Las sanciones deberán incluir la publicidad de los casos de incumplimiento y la obligación de suprimir datos en determinadas circunstancias ([4]). Otras sanciones pueden consistir en la suspensión y levantamiento de una licencia, la compensación a los afectados por pérdidas en que hayan incurrido como resultado del incumplimiento y medidas provisionales. Cuando las entidades del puerto seguro incumplan sus decisiones, los organismos de resolución de litigios del sector privado y los de autorregulación deben notificarlo a los tribunales o a los organismos de la administración competentes según los casos, así como al Departamento de Comercio (o a su representante).

Recurso ante la FTC:

La FTC se ha comprometido a tramitar prioritariamente los casos presentados por los organismos de autorregulación privados, como BBBOnline y TRUSTe, y de los Estados miembros de la Unión Europea que aleguen el incumplimiento de los principios de puerto seguro, a fin de determinar si se ha vulnerado el artículo 5 de la Ley FTC, por la que se prohíben los actos o prácticas desleales o fraudulentos en el comercio. Si la FTC ve indicios de que se ha vulnerado el artículo 5, podría solucionar el asunto solicitando una decisión administrativa de cese de las prácticas denunciadas o presentando una denuncia ante un tribunal federal de primera instancia (Federal District Court). Si ésta prospera, puede originar una resolución al efecto de un tribunal federal. La FTC puede tanto conseguir una sanción civil si se quebrantan las decisiones administrativas de cese, como ejercer acciones civiles o penales en los casos de incumplimiento de las resoluciones de los tribunal federales de primera instancia. La FTC pondrá en conocimiento del Departamento de Comercio todas las acciones de este tipo que emprenda. El Departamento de Comercio alienta a otros organismos públicos a notificarle el resultado final de estos asuntos o cualquier otra resolución sobre la adhesión a los principios de puerto seguro.

Incumplimiento sistemático:

Si una entidad incumple sistemáticamente los principios, cesará su derecho a beneficiarse del puerto seguro. Se considera incumplimiento sistemático cuando una entidad que haya autocertificado su adhesión a los principios ante el Departamento de Comercio (o su representante) se niega a cumplir las resoluciones de cualquier organismo de autorregulación o público, o si uno de estos organismos considera que una entidad incumple con frecuencia los principios, hasta el punto en que deja de ser creíble su participación en el puerto seguro. En estos casos, la entidad deberá notificar inmediatamente los hechos al Departamento de Comercio (o su representante). El incumplimiento de esta obligación puede ser punible en el marco de la False Statements Act (Ley relativa a las declaraciones falsas).

El Departamento (o su representante) indicará en la lista de entidades que autocertifican su adhesión a los principios de puerto seguro toda notificación de incumplimiento sistemático que le remita la propia entidad, cualquier organismo de autorregulación o la administración, pero proporcionará un plazo de treinta días para notificar este extremo a la entidad incumplidora y le concederá la oportunidad de alegar. Por consiguiente, la lista pública del Departamento de Comercio (o su representante) precisará las entidades que se acogen a los beneficios del puerto seguro y las que han dejado de acogerse.

([3]) No se exige a los organismos de resolución de litigios que se ajusten al principio de aplicación. También pueden desviarse de los principios cuando se enfrenten a conflictos de obligaciones o autorizaciones explícitas en la ejecución de sus tareas específicas.

([4]) Los organismos de resolución de litigios tienen la potestad de decidir las circunstancias de aplicación de las sanciones. El carácter delicado de la información es uno de los factores que se tomarán en consideración al decidir sobre la exigencia de suprimir los datos, al igual que si una entidad ha recogido, utilizado o divulgado información incumpliendo manifiestamente los principios.

Una entidad que solicite participar en un organismo de autorregulación con el fin de volver a acogerse a los principios de puerto seguro deberá facilitar a dicho organismo información completa sobre su participación anterior en el puerto seguro.

FAQ nº 12 — Opción — Momento de la exclusión

P: *¿Permite el principio de opción que una persona ejerza su derecho de opción solamente al principio de una relación o en cualquier momento de la misma?*

R: En general, el objeto del principio de opción es garantizar que la información personal se utiliza y difunde de manera coherente con las expectativas y opciones del afectado. Por tanto, cualquier persona debería tener la posibilidad de ejercer el derecho de «exclusión» (u opción) de su información personal con fines de márketing directo en cualquier momento, con los límites de tiempo razonables establecidos por la entidad, como dejar un plazo suficiente para que ésta pueda aplicar dicho derecho de exclusión. Asimismo, una entidad puede requerir información suficiente para confirmar la identidad de la persona que solicita la «exclusión». En Estados Unidos de América, se puede ejercer esta opción mediante un programa central de «exclusión» como el «Mail Preference Service» de la Direct Marketing Association. Las entidades que participen en el «Mail Preference Service» de la Direct Marketing Association deberán fomentar esta posibilidad entre los consumidores que no deseen recibir información comercial. En cualquier caso, todo ciudadano debe tener acceso a un mecanismo rápido y asequible para ejercitar esta opción.

De la misma forma, una entidad puede utilizar la información para determinados fines de márketing directo cuando sea imposible proporcionar al afectado la oportunidad de ejercer su derecho de exclusión antes de usar la información, siempre que le ofrezca de inmediato dicha posibilidad (previa pertición en cualquier momento) de negarse (sin coste alguno para el consumidor) a recibir posteriores envíos de márketing directo y que la entidad se ajuste a los deseos del afectado.

FAQ nº 13 — Información sobre viajes

P: *¿Cuándo se puede transferir a entidades situadas fuera de la Unión Europea la información de las reservas de billetes de avión u otra información sobre viajes, por ejemplo, la relativa a personas con tarjetas de fidelidad o a reservas hoteleras y a necesidades especiales, como la dieta por motivos religiosos o la asistencia física?*

R: Esta información se puede transferir en diversas circunstancias. De conformidad con el artículo 26 de la Directiva, podrá 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: 1) la transferencia sea necesaria para proporcionar los servicios solicitados por el consumidor o cumplir un convenio, como el programa de fidelización «frequent flyer»; o 2) el consumidor haya dado su consentimiento inequívocamente. Las organizaciones estadounidenses que suscriben los principios de puerto seguro ofrecen una protección adecuada de los datos y por consiguiente pueden recibir datos transferidos de la Unión Europea sin cumplir estas condiciones u otras condiciones expuestas en el artículo 26 de la Directva. Dado que el puerto seguro incluye normas específicas para datos especialmente protegidos, dicha información (que puede ser preciso recoger, por ejemplo, en relación con las necesidades de asistencia física de los clientes) puede incluirse en las transferencias a participantes en el puerto seguro. No obstante, en todos los casos, la organización que transfiere la información ha de cumplir la legislación del Estado miembro de la Unión Europea en el que opera, que, entre otras cosas, puede imponer condiciones especiales para el tratamiento de datos especialmente protegidos.

FAQ nº 14 — Productos médicos y farmacéuticos

P. 1: *Si se recogen datos personales en la Unión Europea y se transfieren a Estados Unidos de América con fines de investigación farmacéutica u otros, ¿se aplican las leyes de los Estados miembros o los principios de puerto seguro?*

R. 1: Las leyes de los Estados miembros se aplican a la recogida de los datos personales y a cualquier tratamiento previo a su transferencia a Estados Unidos de América. Los principios de puerto seguro se aplican a los datos una vez que se han transferido a Estados Unidos de América. Los datos personales utilizados con fines de investigación farmacéutica u otros deben ser convertidos en datos anónimos cuando resulte adecuado.

P. 2: *Los datos personales conseguidos en estudios de investigación médica o farmacéutica suelen desempeñar un valioso papel en futuras investigaciones científicas. Cuando se transfieren datos personales recogidos para un estudio de investigación a una entidad estadounidense acogida al puerto seguro, ¿podrá dicha entidad utilizar los datos en una nueva actividad de investigación científica?*

R. 2: Sí, si desde el primer momento se ha procedido a la correspondiente notificación y se proporciona la posibilidad de optar. En la notificación se proporcionará información sobre la utilización concreta que se dará a los datos, a saber, seguimiento, otros estudios o márketing. Se sobreentiende que no podrán especificarse todas las utilizaciones futuras de los datos, ya que éstas pueden resultar de un nuevo enfoque de los datos originales, de nuevos descubrimientos y avances médicos, y de novedades en materia legislativa y de salud pública. Por consiguiente, la notificación debería incluir, si procede, una referencia a la posible utilización de los datos personales en futuras actividades de investigación médica y farmacéutica que todavía se desconocen. Será necesario obtener un nuevo consentimiento si la utilización no es coherente con las finalidades de investigación general para las que se recogieron originalmente los datos o dieron posteriormente los particulares su consentimiento.

P. 3: *¿Qué ocurre con los datos de un particular si un participante decide voluntariamente o a petición del patrocinador retirarse de un ensayo clínico?*

R. 3: Los participantes pueden decidir voluntariamente o a instancias de terceros retirarse de un ensayo clínico en cualquier momento. No obstante, los datos recogidos con anterioridad a la retirada podrán seguir siendo tratados con los demás datos del ensayo clínico si este extremo quedó claro en la notificación a los participantes desde el momento en que dieron su conformidad para participar.

P. 4: *Las sociedades de productos farmacéuticos y médicos tienen autorización para facilitar datos personales obtenidos en ensayos clínicos realizados en la Unión Europea a las autoridades de regulación de Estados Unidos de América con fines de regulación y control. ¿Están autorizadas las transferencias similares a terceros que no sean las autoridades de regulación, como las filiales de las empresas u otros investigadores?*

R. 4: Sí, con arreglo a los principios de notificación y de opción.

P. 4: *Muchas veces, para garantizar la objetividad de los ensayos clínicos, se priva a los participantes y, con frecuencia, también a los investigadores, de la información sobre el tratamiento. Este proceder podría poner en peligro la validez de los estudios de investigación y de sus resultados. ¿Tendrán los participantes en este tipo de ensayos clínicos (denominados «experimentos a ciegas») acceso a los datos sobre su tratamiento durante el ensayo?*

R. 5: No, no deberá proporcionarse este acceso a los participantes si se les explicó tal restricción cuando se unieron al ensayo y si la revelación de la información puede poner en peligro la integridad de la investigación. Consentir la participación en los ensayos dentro de estas condiciones constituye un modo razonable de renunciar al derecho de acceso. Tras la conclusión del ensayo y el análisis de los resultados, los participantes tendrán acceso a sus datos si lo solicitan. En primer lugar, se dirigirán al médico o profesional sanitario de quien recibieron tratamiento en el marco del ensayo clínico y, en segundo lugar, a la empresa patrocinadora.

P. 6: *¿Tiene una empresa de productos médicos o farmacéuticos que aplicar los principios de puerto seguro, en lo relativo a la notificación, opción, transferencia ulterior y acceso, en las actividades que realiza para garantizar la seguridad de los productos y controlar su eficacia, entre ellas la información sobre circunstancias adversas y el seguimiento de pacientes/individuos que utilicen determinadas medicinas o dispositivos médicos (por ejemplo, marcapasos)?*

R. 6: No, si la adhesión a los principios interfiere con el cumplimiento de las exigencias legales. Esto se aplica tanto a los informes de los profesionales sanitarios dirigidos a las empresas de productos médicos y farmacéuticos, como a los de éstos a organismos de la administración como la Food and Drug Administration.

P. 7: *El investigador principal codifica siempre los datos de la investigación, en su origen, con una clave única, para que no se conozca la identidad de los interesados. Las empresas farmacéuticas que patrocinan la investigación no reciben la clave. El código original sólo lo conoce el investigador, de modo que sólo él puede identificar al sujeto de la investigación en determinadas circunstancias (por ejemplo, cuando es necesario un acompañamiento médico). Una transferencia de datos codificados de esta forma desde la Unión Europea a Estados Unidos de América, ¿constituye una transferencia de datos personales sujeta a los principios de puerto seguro?*

R. 7: No, no se trata de una transferencia de datos personales sujeta a los mencionados principios.

FAQ nº 15 — Información extraída de registros públicos e información de dominio público

P: *¿Deben aplicarse los principios de notificación, opción y transferencia ulterior a la información extraída de registros públicos y a la información de dominio público?*

R: No es necesario aplicar los principios de notificación, opción y transferencia ulterior a la información extraída de registros públicos siempre que no se combine con información de otros registros no públicos y se cumplan las condiciones de consulta establecidas por la jurisdicción competente.

Asimismo, generalmente no es necesario aplicar los principios de notificación, opción y transferencia ulterior a la información de dominio público a menos que el transferidor europeo de dicha información indique que está sujeta a restricciones que exijan la aplicación de tales principios por parte de la entidad para los usos a los que piensa destinarla. Las entidades no tendrán ninguna responsabilidad sobre el uso de la información por quienes la obtengan de materiales publicados.

Cuando se descubra que una entidad ha hecho pública intencionadamente información personal contraviniendo los principios, para beneficiarse de estas excepciones o beneficiar a terceros, la entidad dejará de estar cualificada para disfrutar de los beneficios del puerto seguro.

ANEXO III

Informe sobre la aplicación del puerto seguro

Competencia estatal y federal en materia de «prácticas desleales y fraudulentas» y protección de la vida privada

El presente memorando explica la competencia que el artículo 5 de la Federal Trade Commission Act (USC, título 15, §§ 41-58, modificado) confiere a la Federal Trade Commission (FTC) para actuar contra los que vulneran la obligación de proteger la confidencialidad de la información personal, con arreglo a las declaraciones efectuadas o los compromisos adquiridos. Asimismo, aborda las excepciones a dicha competencia y la capacidad de actuación de otros organismos estatales y federales en los casos en los que la FTC no está facultada para hacerlo [1].

Competencia de la FTC en materia de prácticas desleales y fraudulentas

El artículo 5 de la Federal Trade Commission Act declara ilegales los actos o prácticas desleales o fraudulentos en el comercio o relacionados con el comercio, véase el USC, título 15, § 45(a)(1). La FTC está autorizada, en virtud de dicho artículo, a actuar contra tales actos y prácticas, véase el USC, título 15, § 45(a)(2). En consecuencia, la FTC puede dictar un mandamiento ordenando el cese de las prácticas denunciadas, previa audiencia formal, véase el USC, título 15, § 45(b). La FTC también puede solicitar a un tribunal de distrito de Estados Unidos de América una prohibición temporal o medidas cautelares temporales o permanentes por motivos de interés público, véase el USC, título 15, § 53(b). Cuando los actos o prácticas desleales o fraudulentos tengan lugar de forma continuada, o si ya se han dictado mandamientos para el cese de los mismos, la FTC puede promulgar una norma administrativa que prohíba los actos o prácticas en cuestión, véase el USC, título 15, § 57a.

El incumplimiento de una decisión de la FTC puede ser objeto de una sanción civil de hasta 11 000 dólares estadounidenses, y cada día de incumplimiento se considera un nuevo delito [2], véase el USC, título 15, § 45(1). Igualmente, quien viola conscientemente una disposición de la FTC puede ser objeto de una sanción de 11 000 dólares estadounidenses, por cada violación, véase el USC, título 15, § 45(m). El Departamento de Justicia o, en su defecto, la FTC pueden adoptar las medidas de ejecución, véase el USC, título 15, § 56.

Competencia de la FTC y protección de la vida privada

Al ejercer la competencia que le confiere el artículo 5, la FTC considera que proporcionar intencionadamente a los consumidores información inexacta sobre el motivo de la recogida de datos personales y la utilización de dichos datos constituye una práctica fraudulenta [3]. Por ejemplo, en 1998, la FTC presentó una denuncia contra GeoCities por revelar a terceros con fines comerciales información que había recogido en su sitio Web, sin permiso previo, a pesar de haber manifestado lo contrario [4]. Asimismo, la FTC afirma que la recogida de información personal procedente de menores y la venta y revelación de dicha información sin el consentimiento paterno puede constituir también una práctica fraudulenta [5].

---

(1) No se debaten aquí las diversas Leyes federales que tratan de la protección de la vida privada en contextos específicios o las Leyes estatales y el *common law* aplicables. Entre las Leyes federales que regulan la recogida y utilización de la información personal cabe citar las siguientes: Cable Communications Policy Act (USC, título 47, § 551), Driver's Privacy Protection Act (USC, título 18, § 2721), Electronic Communications Privacy Act (USC, título 18, § 2701 et seq.), Electronic Funds Transfer Act (USC, título 15, §§ 1693, 1693m), Fair Credit Reporting (USC, título 15, § 1681 et seq.), Right to Financial Privacy Act (USC, título 13, § 3401 et seq.), Telephone Consumer Protection Act (USC, título 47, § 227) y Video Privacy Protection Act (USC, título 18, § 2710). Muchos Estados cuentan con una legislación análoga en estos ámbitos. Véase, por ejemplo, Mass. Gen. Laws capítulo 167B, § 16 (que prohíbe a las instituciones financieras revelar a terceros la información financiera de los clientes sin el consentimiento de los mismos o sin que exista un procedimiento judicial), N.Y. Pub. Health Law § 17 (que limita la utilización y revelación de informes médicos o de salud mental y otorga a los pacientes el derecho a acceder a los mismos).

(2) En este caso, el tribunal de distrito de Estados Unidos de América puede también ordenar medidas provisionales y equitativas adecuadas para hacer cumplir la decisión de la FTC; véase el USC, título 15, § 45(1).

(3) «Práctica fraudulenta» se define como una declaración, omisión o práctica que puede realmente inducir a error a un consumidor razonable.

(4) Véase la dirección en Internet siguiente: www.ftc.gov/opa/1998/9808/geocitie.htm.

(5) Véase la nota enviada al Center for Media Education (www.ftc.gov/os/1997/9707/cenmed.htm). Por otro lado, la Children's Online Privacy Protection Act de 1998 confiere a la FTC autoridad legal específica para regular la recogida de información personal procedente de menores mediante operadores de los servicios en línea y de Internet. Véase el USC, título 15, §§ 6501-6506. En particular, la Ley obliga a los operadores en línea a informar y obtener el consentimiento paterno verificable antes de recoger, utilizar o revelar información personal procedente de menores. *Id.*, § 6502(b). Asimismo, la Ley confiere a los padres derecho de acceso y la posibilidad de denegar la autorización para el uso continuado de la información. *Id.*

En una carta dirigida al Director General John Mogg de la Comisión Europea, el presidente de la FTC Pitofsky señaló las limitaciones de la competencia de la FTC para proteger la vida privada si no han existido declaraciones falsas (o ningún tipo de declaración) sobre los fines de la información recogida [carta del presidente de la FTC a John Mogg (23 de septiembre de 1998)]. No obstante, las empresas que desean beneficiarse del puerto seguro propuesto deberán certificar que protegerán la información que recojan de conformidad con las orientaciones estipuladas. En consecuencia, si una empresa certifica que protegerá la confidencialidad de la información y posteriormente no lo hace, habrá incurrido en declaración falsa o «práctica fraudulenta» con arreglo a lo dispuesto en el artículo 5.

Dado que la jurisdicción de la FTC se extiende a los actos o prácticas desleales o fraudulentos relacionados con el comercio, la FTC no tiene jurisdicción respecto a la recogida y utilización de información personal con fines no comerciales, por ejemplo, para la recogida de fondos con fines benéficios. Véase la carta de Pitofsky, página 3. Sin embargo, la utilización de la información personal en cualquier transacción comercial satisface este requisito jurisdiccional. Así, por ejemplo, la venta por parte de un empresario de información personal relativa a sus empleados a una empresa de márketing directo pertenece al ámbito de aplicación del artículo 5.

Excepciones al artículo 5

El artículo 5 establece una serie de excepciones a la competencia de la FTC sobre los actos o prácticas desleales o fraudulentos en los casos siguientes:

— instituciones financieras, incluidos bancos, cooperativas de ahorro y préstamo y cooperativas de crédito,

— telecomunicaciones y empresas de transporte interestatal,

— compañías aéreas,

— envasadores y explotadores de áreas para ganado.

Véase el USC, título 15, § 45(a)(2). A continuación se comenta cada excepción y la autoridad reglamentaria correspondiente.

Instituciones financieras ([6])

La primera excepción se aplica a los bancos, cooperativas de ahorro y préstamo que se describen en el artículo 18(f)(3) [véase el USC, título 15, § 57a(f)(3)] y a las cooperativas de crédito que se describen en el artículo 18(f)(4) [véase el USC, título 15, § 57a(f)(4)] ([7]). Estas instituciones financieras están sujetas a las reglamentaciones de los organismos siguientes: Federal Reserve Board, Office of Thrift Supervision ([8]), y la National Credit Union Administration Board, respectivamente, véase el USC, título 15, § 57a(f). Estos organismos pueden prescribir las normas necesarias para evitar prácticas desleales y fraudulentas por parte de estas instituciones financieras ([9]) y crear una división independiente para tramitar las denuncias de los consumidores. Véase el USC, título 15, § 57a(f)(1). Por último, la competencia de ejecución se deriva del artículo 8 de la Federal Deposit Insurance Act (véase el U.S.C., título 12, § 1818), en el caso de los bancos y cooperativas de ahorro y préstamo, y de los artículos 120 y 206 de la Federal Credit Union Act, en el caso de las cooperativas federales de crédito. Véase el USC, título 15, §§ 57a(f)(2)-(4).

Aunque el sector de los seguros no figura expresamente en la lista de excepciones del artículo 5, la McCarran-Ferguson Act (véase el USC, título 15, § 1011 et seq.) delega de manera general en los Estados la regulación de esta

([6]) El 12 de noviembre de 1999, el Presidente Clinton firmó la Gramm-Leach-Bliley Act (Pub. L. 106-102, codificada en el USC, título 15, § 6801 et seq.). La Ley limita la revelación por parte de las instituciones financieras de información personal sobre sus clientes. Entre otras cosas, la Ley obliga a las instituciones financieras a notificar a todos los clientes sus políticas y prácticas de protección de la vida privada en la transmisión de información personal a los afiliados y no afiliados. La Ley autoriza a la FTC, a las autoridades bancarias federales y a las demás autoridades a promulgar reglamentos que apliquen las medidas de protección de la vida privada que exige la Ley. Estos organismos han publicado la normativa propuesta al efecto.

([7]) Tal como está formulada, esta excepción no se aplica al sector de las sociedades de valores. Por tanto, los corredores y agentes de bolsa y demás operadores del sector de las sociedades de valores están sujetos a la jurisdicción concurrente de la Securities and Exchange Commission y la FTC en caso de actos y prácticas desleales o fraudulentos.

([8]) La excepción del artículo 5 se refería en un principio al Federal Home Loan Bank Board, que se suprimió en agosto de 1989 tras la Financial Institutions Reform, Recovery and Enforcement Act de 1989. Sus funciones se transfirieron a la Office of Thrift Supervision y a la Resolution Trust Corporation, la Federal Deposit Insurance Corporation y el Housing Finance Board.

([9]) Aunque el artículo 5 elimina a las instituciones financieras de la jurisdicción de la FTC, prevé que si la FTC promulga una norma en materia de prácticas y actos desleales o fraudulentos, los organismos de reglamentación del sector financiero deberán adoptar normas paralelas en un plazo de sesenta días, véase el USC, título 15, § 57a(f)(1).

actividad ([10]). Por otro lado, con arreglo al artículo 2(b) de dicha Ley, ninguna ley federal podrá invalidar, perjudicar o sustituir la reglamentación estatal a menos que dicha Ley se refiera específicamente a la actividad de las entidades aseguradoras, véase el USC, título 15, § 1012(b). No obstante, los preceptos de la Ley FTC se aplican subsidiariamente en aquellos Estados que no hayan regulado la actividad. *Id*. Asimismo, debe señalarse que la Ley McCarran-Ferguson delega en los Estados únicamente respecto a la actividad aseguradora. Por tanto, la FTC conserva una competencia residual sobre las prácticas desleales o fraudulentas de las compañías de seguros que se realicen al margen de la actividad aseguradora, por ejemplo, si venden información personal sobre los titulares de las pólizas a empresas de márketing directo de productos no relacionados con los seguros ([11]).

Compañías de servicio público de transportes y telecomunicaciones

La segunda excepción del artículo 5 se refiere a aquellas empresas públicas «sujetas a las leyes que regulan el comercio», véase el USC, título 15, § 45(a)(2), es decir, el subtítulo IV del título 49 del United States Code y la Communications Act de 1934 (véase el USC, título 47, § 151 et seq.) (la Ley de comunicaciones), véase el USC, título 15, § 44.

El subtítulo IV del título 49 de la USC (Transporte interestatal) afecta al transporte ferroviario, por carretera y por vía navegable, agentes, transitarios y transportistas por oleoducto, véase el USC, título 49, § 10101 et seq. Estas empresas de transporte están sometidas a la jurisdicción del Surface Transportation Board, organismo independiente del Departamento de Transporte, véase el USC, título 49, §§ 10501, 13501, y 15301. Las leyes federales prohíben a los transportistas revelar información sobre la naturaleza, el destino y otros aspectos de la carga que pudieran utilizarse en detrimento del expedidor, véase el USC, título 49, §§ 11904, 14908, y 16103. Cabe destacar que estas disposiciones se refieren a la información relativa a la carga del expedidor, por lo que no parecen afectar a la información personal del expedidor que no guarde relación con el envío en cuestión.

Respecto a la Communications Act, prevé la regulación del «comercio interestatal y extranjero de la comunicación por cable y radio», por parte de la Federal Communications Commission (FCC), véase el USC, título 47, §§ 151 y 152. Además de a las empresas de servicio público de telecomunicaciones, la Communications Act se aplica también a empresas de difusión de radio y televisión y a los proveedores de servicios por cable que no son compañías de servicio público. Como tales, estas últimas empresas no pueden acogerse a las excepciones previstas en el artículo 5 de la Ley FTC, por la que la FTC puede someterlas a investigación por prácticas desleales o fraudulentas, mientras que la FCC tiene jurisdicción concurrente para aplicar su competencia independiente en este ámbito tal como se describe a continuación.

En el marco de la Communications Act, todas las empresas de servicio público de telecomunicaciones, incluidas las empresas locales, tienen la obligación de proteger la confidencialidad de la información de red exclusiva del cliente ([12]). Véase el USC, título 47, § 222(a). Además de esta autoridad general de protección de la vida privada, la Communications Act fue modificada por la Cable Communications Policy Act de 1984 (Ley del cable), véase el USC, título 47, § 521 et seq., que establece específicamente que las empresas de distribución por cable deben proteger la confidencialidad de la información personal identificable sobre sus abonados, véase el USC, título 47, § 551 ([13]). La Ley del cable restringe la recogida de información personal por parte de empresas de distribución por cable y les obliga a notificar al abonado la naturaleza de la información recogida y el uso que se hará de la misma. Asimismo, confiere a los abonados el derecho de acceso a la información que les afecta y obliga a las empresas a destruir la información cuando ya no sea necesaria.

La Communications Act faculta a la FCC a aplicar estas dos disposiciones relativas a la protección de la vida privada, ya sea por propia iniciativa o como respuesta a una denuncia exterior ([14]), véase el USC, título 47, §§ 205, 403; *id*. § 208. Si la FCC determina que una empresa de servicios públicos de telecomunicaciones (incluidas las de distribución por

([10]) «La actividad de las empresas aseguradoras y de las personas que operan en este sector estará sujeta a las leyes de los Estados federales relativas a la regulación o fiscalidad de dichas empresas», véase el USC, título 15, § 1012(a).

([11]) La FTC ha ejercido su jurisdicción sobre compañías de seguros en diferentes contextos. En un caso, la FTC denunció por publicidad engañosa a una empresa en un Estado en que no estaba autorizada a operar. La jurisdicción de la FTC fue confirmada sobre la base de que no existía ningún reglamento estatal aplicable puesto que la empresa se encontraba efectivamente fuera de la jurisdicción del Estado en cuestión; véase «FTC v. Travelers Health Association», 362 U.S. 293 (1960).
En cuanto a los Estados, diecisiete han adoptado el modelo de la Insurance Information and Privacy Protection Act, preparado por la National Association of Insurance Commissioners (NAIC). La Ley incluye disposiciones relativas a la notificación, utilización y revelación, y acceso. Asimismo, casi todos los Estados han adoptado el modelo «Unfair Insurance Practices Act» de la NAIC, que se centra específicamente en las prácticas comerciales desleales en el sector de los seguros.

([12]) El término «información de red exlusiva del cliente» significa la información relativa a la cantidad, configuración técnica, tipo, destino y cantidad de uso de un servicio de telecomunicaciones por parte de un abonado y la información de las facturas de teléfonos, véase el USC, título 47, § 222(f)(1). No obstante, el término no incluye la información sobre la lista de abonados. *Id*.

([13]) La Ley no define expresamente la expresión «información personal identificable».

([14]) Esta autoridad incluye el derecho a reparación por violación de la intimidad en virtud del artículo 222 de la Communications Act o, en el caso de los abonados a servicios por cable, en virtud del artículo 551 de la Ley del cable que modifica la anterior. Véase también la USC, título 47, § 551(f)(3) (la acción civil en un tribunal federal de distrito es un recurso no exclusivo que se ofrece «además de las demás vías de recurso a disposición de los abonados a un servicio por cable»).

cable) ha vulnerado las disposiciones del artículo 222 o del artículo 551, puede emprender tres acciones básicas. En primer lugar, tras celebrar una audiencia y determinar la violación, la Comisión puede ordenar a la empresa el pago de sanciones pecuniarias ([15]), véase el USC, título 47, § 209. En segundo lugar, la FCC puede ordenar a la empresa el cese de las prácticas o la omisión, véase el USC, título 47, § 205(a). Por último, la Comisión puede también ordenar a la empresa que cumpla y respete los reglamentos o prácticas que la FCC pueda prescribir. *Id*.

Los particulares que consideren que una empresa de telecomunicaciones o de distribución por cable ha vulnerado las disposiciones correspondientes de la Communications Act o de la Cable Act pueden presentar una denuncia ante la FCC o plantear su reclamación ante un tribunal federal de distrito, véase el USC, título 47, § 207. Si el demandante obtiene una sentencia favorable en un juicio ante un tribunal federal contra una empresa de telecomunicaciones que no ha cumplido la obligación de proteger la información de red exclusiva del cliente en virtud del artículo 222 de la Communications Act puede obtener indemnizaciones por daños efectivamente causados y el reembolso de los honorarios de abogados, véase el USC, título 47, § 206. En el marco del artículo 551 de la Cable Act, se pueden obtener también indemnizaciones punitivas y resarcimiento de costes procesales razonables, véase el USC, título 47, § 551(f).

La FCC ha adoptado normas detalladas de aplicación del artículo 222, véase el CFR, título 47, 64.2001-2009. Las normas establecen salvaguardas específicas de protección contra el acceso no autorizado a la información de red exclusiva del cliente. Las empresas de telecomunicaciones deben:

— desarrollar y aplicar sistemas de *software* para la señalización automática del aviso/aprobación del cliente cuando sus datos aparezcan por primera vez en pantalla,

— mantener un «seguimiento» electrónico para controlar el acceso a la cuenta de un cliente, en particular cuándo, quién y con qué fin se abre el registro de un cliente,

— formar a su personal sobre la utilización autorizada de la información de red exclusiva del cliente, con medidas disciplinarias adecuadas,

— establecer un proceso de revisión y supervisión para garantizar el cumplimiento cuando se realicen actividades de márketing externo,

— certificar anualmente a la FCC el cumplimiento de estas obligaciones.

Compañías aéreas

Las compañías aéreas extranjeras y estadounidenses que están sujetas a la Federal Aviation Act de 1958 tampoco entran en el ámbito de aplicación del artículo 5 de la FTC Act; véase el USC, título 15, § 45(a)(2). Se trata de las empresas que se dedican al transporte interestatal o al extranjero de mercancías o pasajeros, o al transporte aéreo de correo, véase el USC, título 49, § 40102. Las compañías aéreas están sometidas a la autoridad del Departamento de Transporte. A este respecto, la Secretaría de Transporte puede actuar para evitar prácticas anticompetitivas, fraudulentas, desleales o abusivas en el transporte aéreo, véase el USC, título 49, § 40101(a)(9). Del mismo modo, puede investigar por motivos de interés público si una compañía aérea estadounidense o extranjera, o una agencia de viajes, ha llevado a cabo prácticas engañosas o desleales, véase el USC, título 49, § 41712. Tras una audiencia, la Secretaría de Transporte podrá ordenar el cese de la práctica ilegal. *Id*. Según los datos de que disponemos, nunca ha utilizado esta competencia para proteger la confidencialidad de la información personal relativa a los pasajeros de las líneas aéreas ([16]).

Existen dos disposiciones de protección de la confidencialidad de la información personal que se aplican a las compañías aéreas en contextos específicos. En primer lugar la Federal Aviation Act protege la vida privada de los candidatos a piloto, véase el USC, título 49, § 44936(f). Si bien las compañías aéreas pueden obtener información profesional de los candidatos, la Ley confiere a estos últimos el derecho a comunicar que esta información se les ha solicitado, acceder a la solicitud, corregir las imprecisiones y transmitir la información exclusivamente a los que participan en el proceso de contratación. En segundo lugar, los Reglamentos del Departamento de Transporte prevén que la información de la lista de pasajeros recogida oficialmente en caso de accidente aéreo será confidencial y solo podrá revelarse al Departamento estadounidense de Estado, al National Transportation Board (si la solicita), y al Departamento estadounidense de Transporte, véase el CFR, título 4, parte 243, § 243.9(c) (modificado por 63 FR 8258).

([15]) No obstante, la ausencia de daños directos al denunciante no es motivo para desestimar una denuncia, véase el USC, título 47, § 208(a).

([16]) Sabemos que se está trabajando en el sector de los transportes aéreos para abordar el problema de la protección de la vida privada. Los representantes de la industria han debatido los principios propuestos de puerto seguro y su posible aplicación a las compañías aéreas. El debate ha incluido una propuesta al respecto según la cual las empresas que participen estarán sujetas expresamente a la jurisdicción del Departamento de Transporte.

Envasadores y explotadores de áreas para ganado

Respecto a la Packers and Stockyards Act de 1921 (véase el USC, título 7, § 181 et seq.), la Ley declara ilegal que los envasadores de productos animales, carne, productos cárnicos o productos animales no manufacturados, o que los comerciantes de aves respecto a aves vivas, recurran a prácticas o dispositivos desleales, injustamente discriminatorios o engañosos; véase el USC, título 7, § 192(a); también véase el USC, título 7, § 213(a) (que prohíbe la prácticas o dispositivos desleales o injustamente discriminatorios o engañosos en relación con el ganado). La Secretaría de Agricultura es responsable en primera instancia de aplicar estas disposiciones, si bien la FTC conserva una competencia residual sobre las transacciones al por menor y las relativas a la industria avícola, véase el USC, título 7, § 227(b)(2).

No está claro si la Secretaría de Agricultura considerará práctica «engañosa» con arreglo a la Packers and Stockyards Act el incumplimiento de un compromiso declarado de proteger la vida privada por parte de los envasadores y explotadores de áreas para ganado. Sin embargo, la excepción del artículo 5 se refiere a las personas, socios o empresas únicamente en la medida en que estén sujetos a la Packers and Stockyards Act. Por tanto, si la protección de la vida privada no entra en el ámbito de la Packers and Stockyards Act, la excepción del artículo 5 puede no ser aplicable a este sector, que estaría sometido entonces a la competencia de la FTC a este respecto.

Competencia estatal en materia de prácticas desleales y fraudulentas

Según un análisis preparado por el personal de la FTC, los cincuenta Estados más el distrito de Columbia, Guam, Puerto Rico, y las Islas Vírgenes han adoptado leyes similares a la Federal Trade Commission Act (FTCA) para evitar prácticas desleales y fraudulentas. FTC fact sheet, reimprimida en «Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation, 59 Tul. L. Rev. 427 (1984)». En todos los casos, un organismo público estatal, encargado de velar por la aplicación de la normativa, se ocupa de las investigaciones, mediante mandamientos judiciales o requerimientos de investigación, de obtener compromisos de cumplimiento voluntario, de emitir mandamientos ordenando el cese de las prácticas incorrectas y de obtener requerimientos judiciales. *Id*. En 46 jurisdicciones la Ley permite emprender acciones privadas para obtener indemnizaciones simples, dobles, triples o punitivas y, en algunos casos, recuperar las costas y los honorarios de los abogados. *Id*.

La Deceptive and Unfair Trade Practices Act de Florida, por ejemplo, autoriza al Fiscal General a investigar e interponer una demanda judicial contra los métodos de competencia desleales, y las prácticas comerciales desleales, fraudulentas o abusivas, incluida la publicidad falsa o engañosa, las franquicias o las oportunidades comerciales engañosas, la venta telefónica fraudulenta y los regímenes piramidales. Véase también la N.Y. General Business Law § 349 (que prohíbe actos o prácticas desleales y engañosos en las actividades comerciales).

En una encuesta realizada este año por la Asociación Nacional de Fiscales (NAAG), se confirman estas conclusiones. De los 43 Estados que respondieron, todos disponen de leyes similares a la FTC con protección comparable. En esta misma encuesta, 39 Estados declararon estar dispuestos a conocer de las denuncias de no residentes. Respecto a la protección de la vida privada de los consumidores, 37 de los 41 Estados que respondieron indicaron que responderían a las denuncias contra empresas establecidas en su jurisdicción que no cumplan la política de protección de la vida privada tras haberse adherido a la misma.

ANEXO IV

Memorando sobre daños por violación de las reglas sobre protección de la intimidad, autorizaciones explícitas y fusiones y absorciones en el Derecho estadounidense

Este documento viene a responder a las aclaraciones solicitadas por la Comisión Europea sobre la legislación estadounidense en materia de: a) demandas de indemnización de daños y perjuicios por violación del derecho a la intimidad, b) «autorizaciones explícitas» para la utilización de datos personales sin atenerse a los principios de puerto seguro de puerto seguro y c) efectos de las fusiones y absorciones sobre las obligaciones contraídas en virtud de dichos principios.

A. **Indemnización de daños y perjuicios por violación del derecho a la intimidad**

El incumplimiento de los principios de puerto seguro puede dar lugar a diversas reclamaciones de particulares, en función de las circunstancias del caso. En especial, las entidades que se adhieren a los principios de puerto seguro pueden ser responsables de falsa declaración por incumplir sus normas de protección de la intimidad. El *common law* prevé también acciones de particulares para reclamar una indemnización de daños y perjuicios por violación del derecho a la intimidad. Muchas leyes federales y estatales sobre el derecho a la intimidad disponen asimismo la indemnización de los daños y perjuicios sufridos por los particulares como consecuencia de tales incumplimientos.

El common law *estadounidense establece con claridad el derecho a la indemnización de los daños y perjuicios por invasión de la intimidad personal*

El uso de datos personales sin atenerse a los principios de puerto seguro puede dar lugar a responsabilidad legal en virtud de diversas teorías jurídicas. Por ejemplo, tanto el responsable de la transmisión de datos como las personas afectadas pueden demandar por falsa declaración a la entidad adherida a estos principios que incumpla sus compromisos en este campo. Con arreglo al Restatement of the Law (Repertorio de Derecho vigente), volumen 2, Responsabilidad Extracontractual ([1]):

> Quien realice fraudulentamente una falsa declaración de hechos, opiniones, intenciones o normas jurídicas con el fin de inducir a otro a actuar o abstenerse de actuar por tal motivo, será responsable frente a quien ha sido objeto del engaño de las pérdidas económicas que éste hubiera sufrido por haberse basado justificadamente en tal falsa declaración.

Repertorio, § 525. La falsa declaración es «fraudulenta» cuando se realiza con el conocimiento o en la creencia de su falsedad. *Id.*, § 526. Como regla general, quien realiza una falsa declaración es potencialmente responsable frente a todos aquellos que pretende o prevé conseguir que se basen en ella respecto de cualesquiera pérdidas económicas que estos pudieran sufrir por tal causa. *Id.* 531. También puede serlo frente a terceros si quien realizó el ilícito pretende o prevé que su falsa declaración sea repetida ante dicho tercero y éste actúe basándose en ella. *Id.*, § 533.

En el ámbito de los principios de puerto seguro, la declaración en cuestión es aquella en la que la entidad manifiesta públicamente que cumplirá dichos principios. Asumido tal compromiso, el incumplimiento consciente de estos principios puede ser fundamento de una acción por falsa declaración por parte de quienes hayan actuado basándose en ella. Dado que el compromiso de cumplir tales principios se formula respecto al público en general, tanto las personas a que se refiere la información en cuestión como el responsable del tratamiento en Europa que transmite datos personales a la entidad estadounidense pueden tener fundamentos para demandar a ésta por falsa declaración ([2]). La entidad estadounidense será también responsable frente a aquellos por «falsa declaración continuada» por la totalidad del tiempo durante el que actúen en perjuicio propio basándose en tal declaración, Repertorio, § 535.

([1]) Second Restatement of the Law — Torts; American Law Institute (1997).

([2]) Éste podría ser el caso, por ejemplo, de aquellas personas que se basen en los compromisos de protección de confidencialidad de la entidad estadounidense para autorizar a quien controle los datos a transmitir sus datos personales a Estados Unidos de América.

Quienes se basan en una falsa declaración fraudulenta tienen derecho a la indemnización de los daños y perjuicios sufridos. Según el Repertorio:

> El destinatario de una falsa declaración fraudulenta tiene derecho a la indemnización de los daños y perjuicios, mediante una acción por falsedad, frente al causante de las pérdidas económicas que la ley considere derivadas de la declaración.

Repertorio, § 549. La indemnización comprende tanto las pérdidas efectivas como la pérdida de la «ventaja de negociación» en una transacción comercial. *Id.*; véase, v.g., «Boling v. Tennessee State Bank», 890 S.W.2d 32 (1994) (el banco es responsable frente a los prestatarios por 14 825 dólares estadounidenses en concepto de indemnización de daños y perjuicios por revelación de sus datos personales y planes de negocio al presidente del banco, quien tenía intereses contrapuestos.)

Aunque para que exista una falsa declaración fraudulenta se requiere conocer efectivamente su falsedad, o al menos creer que lo es, puede derivarse también responsabilidad de una falsa declaración negligente. Según el Repertorio, quien realiza una falsa declaración en el curso de su negocio, profesión o empleo, o en cualquier transacción económica, puede ser responsable si «no actúa con la competencia o la diligencia debidas para obtener o comunicar la información.». Repertorio, § 552(1). A diferencia de lo que ocurre con la falsa declaración fraudulenta, la indemnización en caso de negligencia se limita a las pérdidas efectivas. *Id.*, § 552B(1).

En un caso reciente, por ejemplo, el Tribunal Superior de Connecticut consideró que la no revelación por una empresa de suministro de electricidad de los datos de pago de un cliente a los organismos nacionales de crédito era base para una acción por falsa declaración. Véase «Brouillard v. United Illuminating Co.», 1999 Conn. Super. LEXIS 1754. En este caso, el demandante vio cómo se le denegaba un crédito porque el demandado calificaba de «pagos demorados» los efectuados treinta días después de la fecha de facturación. El demandante alegó que no había sido informado de esta práctica cuando abrió una cuenta de servicio de suministro de electricidad para su vivienda. El tribunal consideró expresamente que «la existencia de falsa declaración negligente puede fundamentarse en el silencio del demandado, pues tenía el deber de comunicar la información». Este caso muestra también que el elemento intencional o fraudulento no es imprescindible para fundamentar una acción de esta naturaleza. Por tanto, si una entidad estadounidense deja de revelar de forma negligente cómo va a utilizar los datos personales que recibe con arreglo al puerto seguro, podrá ser considerada responsable de falsa declaración.

Si la infracción de los principios de puerto seguro implica la utilización indebida de datos personales, podrá fundamentar también una demanda del sujeto por violación de la intimidad, según los principios de *common law*. El Derecho estadounidense reconoce desde hace tiempo acciones por tal concepto. En un caso de 1905 ([3]), el Tribunal Supremo de Georgia consideró que el derecho a la intimidad se basa en el Derecho natural y el *common law*, fallando a favor de una persona cuya fotografía había sido utilizada por una compañía de seguros de vida, sin su consentimiento ni conocimiento, para ilustrar un anuncio publicitario. Articulando conceptos hoy arraigados en la jurisprudencia estadounidense en materia de derecho a la intimidad, el tribunal estimó que la utilización de la fotografía fue «maliciosa», «falsa» y «ponía al demandado en ridículo ante el mundo» ([4]). Los fundamentos de la resolución Pavesich se han mantenido, con mínimas variaciones, hasta convertirse en la piedra angular del Derecho estadounidense en esta materia. Los tribunales estatales han estimado sistemáticamente acciones por violación del derecho a la intimidad, y al menos 48 estados reconocen ya judicialmente este fundamento ([5]). Por otra parte, al menos doce Estados disponen de normas constitucionales que salvaguardan el derecho de sus ciudadanos a no sufrir actos intrusivos ([6]), lo que en algunos casos comprende la protección frente a la intrusión de entidades no oficiales, véase, v.g., Hill v. NCAA, 865 P.2d 633 (Ca. 1994); véase también S. Ginder, «Lost and Found in Cyberspace: Information Privacy in the Age of the Internet», 34 S.D. L. Rev. 1153 (1997) («Las constituciones de algunos Estados tienen normas de protección del derecho a la intimidad de más alcance que las de la Constitución de los EE UU; Alaska, Arizona, California, Florida, Hawai, Illinois, Luisiana, Montana, Carolina del Sur y Washington ofrecen una protección más amplia.»).

El Segundo Repertorio sobre Responsabilidad Extracontractual ofrece una panorámica muy autorizada de cómo se regula esta materia. En consonancia con la práctica judicial común, el Repertorio explica que el «derecho a la intimidad» comprende cuatro causas de responsabilidad extracontractual. Véase el Repertorio, § 652A. En primer lugar, puede actuarse por «intrusión en la intimidad» contra un demandado que se inmiscuya, físicamente o de otro modo, en la sole-

([3]) «Pavesich v. New England Life Ins. Co.», 50 S.E. 68 (Ga. 1905).

([4]) *Id.*, 69.

([5]) Una búsqueda electrónica en la base de datos Westlaw halló 2 703 casos de acciones civiles ante tribunales estatales en materia de «intimidad» desde 1995. Ya hemos entregado a la Comisión los resultados de esta búsqueda..

([6]) Véanse, v.g., las constituciones de Alaska, artículo 1, sección 22; Arizona, artículo 2, sección 8; California, artículo 1, sección 1; Florida, artículo 1, sección 23; Hawaii, artículo 1, sección 5; Illinois, artículo 1, sección 6; Louisiana, artículo 1, sección 5; Montana, artículo 2, sección 10; New York, artículo 1, sección 12; Pennsylvania, artículo 1, sección 1; South Carolina, artículo 1, sección 10; y Washington, artículo 1, sección 7.

dad o la intimidad, o en los asuntos o intereses privados de otra persona ([7]). En segundo lugar, puede existir «apropiación» si se utiliza o aprovecha en beneficio propio el nombre o la apariencia de otro ([8]). En tercer lugar, puede alegarse la «publicación de datos privados» si el asunto es de tal naturaleza que resultaría sumamente ofensivo para una persona razonable y no es de legítimo interés público ([9]). Por último, procede una acción por «publicidad denigratoria» si el demandado sitúa deliberada o imprudentemente a una persona ante la opinión pública con información que resultaría sumamente ofensiva para una persona razonable ([10]).

En el ámbito que nos ocupa, la «intrusión en la intimidad» podría comprender la obtención no autorizada de datos personales, en tanto que su utilización no autorizada para fines comerciales podría fundamentar una acción de apropiación. De modo similar, la revelación de datos personales incorrectos podría dar lugar a responsabilidad extracontactual por «publicidad denigratoria» si la información cumple el requisito de ser sumamente ofensiva para una persona razonable. Por último, la violación de la intimidad consecuencia de la publicación o revelación de datos personales sensibles podría dar lugar a una acción por «publicación de datos privados» (véanse a continuación ejemplos de casos ilustrativos).

Sobre la posible indemnización de daños y perjuicios, quien sufre una violación del derecho a la intimidad tiene derecho a la reparación de:

a) la lesión de su derecho consecuencia de la violación de la intimidad;

b) sus trastornos psicológicos acreditados, si son del tipo normalmente producido por tal violación de la intimidad; y

c) daños y perjuicios específicos con fundamento en la violación del derecho a la intimidad.

Repertorio, § 652H. Dada la aplicabilidad general de la normativa de responsabilidad extracontractual y la multiplicidad de acciones por distintos aspectos del derecho a la intimidad, quienes sufran una violación de estos derechos por incumplimiento de los principios de puerto seguro tendrán probablemente derecho a una indemnización económica.

De hecho, en los tribunales estatales se ven multitud de casos en los que se alega la violación del derecho a la intimidad en situaciones análogas. El asunto Ex Parte AmSouth Bancorporation et al., 717 So. 2d 357, por ejemplo, responde a una acción colectiva en la que alega que el demandado «traicionó la confianza de los depositantes en el Banco, compartiendo datos confidenciales relativos a éstos y sus cuentas» para que una filial del banco vendiera fondos de inversión colectiva y otras inversiones. En estos supuestos suelen concederse indemnizaciones de daños y perjuicios. En el caso Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985), un tribunal de apelación revocó la sentencia del tribunal inferior, al considerar que la utilización de fotografías del demandante «antes» y «después» de una cirugía plástica en la presentación de unos grandes almacenes constituía una violación del derecho a la intimidad por publicación de hechos privados. En Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986), la compañía de seguros demandada utilizó para una campaña publicitaria un accidente en el que la esposa del demandante resultó gravemente lesionada, alegando éste violación del derecho a la intimidad. El tribunal consideró que el demandante tenía derecho a una indemnización de daños y perjuicios por trastorno emocional y usurpación de identidad. Caben acciones por apropiación indebida aunque el demandante no sea personalmente célebre. Véase, v.g., Staruski v. Continental Telephone Co., 154 Vt. 568 (1990) (el demandado obtuvo ventajas comerciales utilizando el nombre y la fotografía del empleado en publicidad en periódicos). En el caso Pulla v. Amoco Oil Co., 882 F.Supp. 836 (S.D Iowa 1995), una empresa vulneró la intimidad del empleado demandante al disponer que otro empleado investigara los registros de operaciones de sus tarjetas de crédito para comprobar sus bajas por enfermedad. El tribunal confirmó la decisión del jurado de 2 dólares estadounidenses por daños y perjuicios efectivo más 500 000 dólares estadounidenses de indemnización punitiva. Otro empleado fue considerado responsable de publicar en la revista de la empresa un reportaje sobre un empleado despedido por falsificar supuestamente su historial de empleo, véase Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987). Esta información violaba el derecho a la intimidad del demandante al publicar un asunto personal, porque la revista circulaba en la comunidad. Por último, una facultad que hacía pruebas de VIH a los estudiantes diciéndoles que se trataba sólo de detectar la rubeola fue considerado responsable de intrusión en la intimidad, véase Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998) (véanse otros casos en el Repertorio, § 652H, Apéndice).

Con frecuencia se critica a Estados Unidos de América por exceso de litigiosidad, pero esto significa también que las personas tienen la posibilidad real, y la aprovechan, de obtener una reparación legal cuando consideran que han sufrido

([7]) *Id.*, capítulo 28, artículo 652B.
([8]) *Id.*, capítulo 28, artículo 652C.
([9]) *Id.*, capítulo 28, artículo 652D.
([10]) *Id.*, capítulo 28, artículo 652E.

un acto ilícito. Muchos aspectos del sistema judicial estadounidense facilitan al demandante la presentación de una demanda individual o colectiva. El número de abogados, comparativamente más numeroso que en la mayoría de los países, facilita el recurso a la asistencia letrada. Los abogados de los demandantes en demandas privadas actúan normalmente con honorarios condicionales en función de la indemnización percibida, lo que permite exigir una reparación incluso a los más pobres o indigentes. Esto pone sobre la mesa otro importante factor: en Estados Unidos de América, cada parte suele cargar con los honorarios de sus propios abogados y demás costas, a diferencia de lo que ocurre en Europa, donde lo habitual es que la parte perdedora deba reembolsar tales gastos a la otra. Sin entrar a juzgar las ventajas relativas de ambos sistemas, la práctica estadounidense no ejerce un efecto disuasorio frente a las reclamaciones legítimas de personas que no podrían pagar las costas de ambas partes en caso de perder el litigio.

También puede reclamarse una reparación aunque la demanda sea relativamente pequeña. En la mayoría de las jurisdicciones estadounidenses, si no en todas, existen tribunales para reclamaciones de pequeña cuantía que siguen procedimientos simplificados y más baratos para resolver las controversias que no alcancen los mínimos legales ([11]). La posibilidad de obtener una indemnización punitiva ofrece también una recompensa económica a las personas que hayan sufrido daños directos de escasa cuantía y llevan ante los tribunales una conducta indebida censurable. Por último, las personas que hayan sufrido un mismo tipo de daños pueden mancomunar sus recursos y sus reclamaciones, ejercitando una acción colectiva.

Un buen ejemplo de la posibilidad de solicitar una reparación son los litigios pendientes contra Amazon.com por violación del derecho a la intimidad. Este gran minorista de servicios en línea es objeto de una acción colectiva en la que los demandantes alegan falta de información y de consentimiento para la obtención de datos personales al utilizar un programa de *software* propiedad de esta empresa denominado «Alexa». En este caso, los demandantes alegan infracción de la Ley de Fraude y Utilización Indebida de la Informática por acceso ilegal a sus comunicaciones almacenadas, y de la Ley de Intimidad de las Comunicaciones Electrónicas, por interceptación ilegal de sus comunicaciones electrónicas y por cable. También alegan la violación del derecho a la intimidad con arreglo al *common law*. Esto es consecuencia de una demanda presentada en diciembre por un experto en seguridad de Internet. En total se reclama una indemnización de daños y perjuicios de 1 000 dólares estadounidenses por cada demandante colectivo, más los honorarios de abogados y los beneficios obtenidos gracias a la infracción de las leyes, y como el número de demandantes puede ser de millones, la indemnización puede ascender a miles de millones de dólares. La FTC (Comisión Federal de Comercio) está investigando también estas alegaciones.

La legislación federal y estatal sobre derecho a la intimidad contempla a menudo acciones de indemnización económica

Además de dar lugar a responsabilidad civil extracontractual, el incumplimiento de los principios de puerto seguro puede constituir también una infracción de otras de los cientos de leyes federales y estatales sobre el derecho a la intimidad. Muchas de ellas, relativas a la utilización de datos personales por los sectores público y privado, permiten a las personas demandar la indemnización de daños y perjuicios. Por ejemplo:

La Electronic Communications Privacy Act (Ley de Intimidad de las Comunicaciones Electrónicas) de 1986. La ECPA prohíbe la interceptación no autorizada de llamadas de teléfonos celulares y transmisiones entre ordenadores. Las infracciones pueden dar lugar a responsabilidad civil en cuentía no inferior a 100 dólares estadounidenses diarios. La protección se extiende también al acceso no autorizado a comunicaciones electrónicas almacenadas, o su revelación. Los infractores son responsables de los daños y perjuicios sufridos, incluido el lucro cesante.

La Telecommunications Act (Ley de Telecomunicaciones) de 1996. Con arreglo a su artículo 702, la información de red exclusiva del cliente (IREC) no puede utilizarse para ningún fin distinto de la prestación de servicios de telecomunicación. Los abonados del servicio pueden presentar una queja ante la Federal Communications Commission (Comisión Federal de Comunicaciones) o una demanda ante un tribunal federal de distrito reclamando la indemnización de los daños y perjuicios más los honorarios de abogados.

La Consumer Credit Reporting Reform Act (Ley de Reforma de los Informes de Crédito de Consumidores) de 1996. La Ley de 1996 modifica la Fair Credit Reporting Act (Ley de Informes de Crédito Justos) de 1970 (FCRA) y exige la mejora del proceso de notificación y reconoce a los sujetos el derecho de acceso a sus informes de crédito. La Ley de Reforma impone también nuevas restricciones a los revendedores de informes de crédito de consumo. Los consumidores pueden obtener la indemnización de los daños y perjuicios, más los honorarios de abogados.

([11]) Ya habíamos proporcionado a la Comisión información sobre las acciones en reclamación de pequeña cuantía.

Las legislaciones estatales también protegen la intimidad personal en diversas situaciones. Las áreas cubiertas comprenden los registros bancarios, las suscripciones a televisión por cable, los informes de crédito, los registros de empleo, los registros oficiales, los datos genéticos e historiales médicos, los registros de seguro, los historiales académicos, las comunicaciones electrónicas y el alquiler de vídeos ([12]).

B. **Autorizaciones legales explícitas**

Los principios de puerto seguro recogen una excepción cuando las normas legales o reglamentarias o la jurisprudencia crean «obligaciones en contrario o autorizaciones explícitas, siempre que en el ejercicio de tal autorización la entidad acredite que el incumplimiento de dichos principios se limita a lo necesario para satisfacer los intereses legítimos que tal autorización considera deben prevalecer». Es evidente que, si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de los principios de puerto seguro. Con respecto a las autorizaciones explícitas, aunque estos principios tienen como finalidad salvar las diferencias entre los regímenes estadounidense y europeo de protección de la intimidad, debemos respetar las facultades legislativas de nuestros legisladores. Esta limitada excepción del cumplimiento estricto de los principios de puerto seguro trata de encontrar un equilibrio entre los intereses legítimos de cada parte.

La excepción se circunscribe a los casos en los que haya una autorización explícita. Por tanto, como cuestión de partida, la norma legal o reglamentaria o la resolución judicial en cuestión debe autorizar expresamente la conducta concreta de las entidades adheridas a los principios de puerto seguro ([13]). En otras palabras, la excepción sólo será aplicable si la autorización explícita entra en conflicto con el cumplimiento de dichos principios. Aun en tal caso, la excepción «está limitada a lo necesario para satisfacer los intereses legítimos que tal autorización considera deben prevalecer». A modo de ejemplo, si la Ley se limita a autorizar a una empresa a proporcionar datos personales a las autoridades públicas, la excepción no sería de aplicación. Por el contrario, si la Ley autoriza expresamente a la empresa a proporcionar información personal a organismos oficiales sin el consentimiento del interesado, esto constituiría una «autorización explícita» para actuar de modo contrario a lo establecido en los principios de puerto seguro. Por su parte, las excepciones concretas a los requisitos expresos de notificar y prestar consentimiento caerían en el ámbito de la excepción (dado que sería equivalente a una autorización explícita a revelar los datos sin notificación ni consentimiento). Por ejemplo, una ley que autorice a los médicos a proporcionar los historiales médicos de sus pacientes a las autoridades sanitarias sin el previo consentimiento de éstos puede permitir una excepción de los principios de notificación y opción. Esta autorización no permitiría al médico entregar estos mismos historiales a las organizaciones de protección de la salud o los laboratorios farmacéuticos comerciales, que quedarían fuera del ámbito de los fines autorizados por la ley y, por tanto, de la excepción ([14]). La autorización legal en cuestión puede ser una autorización «aislada» para hacer determinadas cosas con los datos personales, pero, como ilustran los ejemplos siguientes, será probablemente una excepción a una norma más amplia que prohíba obtener, utilizar o revelar datos personales.

Ley de Telecomunicaciones de 1996

En la mayoría de los casos, los usos autorizados se ajustan a lo exigido en la Directiva y los principios o están permitidos por una de las otras excepciones autorizadas. Por ejemplo, el artículo 702 de la Ley de Telecomunicaciones (codificada en el USC, título 47, § 222) impone a las empresas de telecomunicaciones mantener la confidencialidad de los datos personales que obtengan en el curso de la prestación de sus servicios a sus clientes. Esta disposición autoriza específicamente a dichas empresas a:

1) emplear los datos del cliente para prestar servicios de telecomunicaciones, incluida la publicación de guías de abonados;

2) proporcionar a terceros información sobre el cliente, a solicitud escrita de éste; y

3) proporcionar información de clientes en forma agregada.

([12]) Una reciente búsqueda electrónica de la base de datos Westlaw ofreció 994 casos relativos a indemnización de daños y perjuicios por violación del derecho a la intimidad.

([13]) Como aclaración, la autoridad legal correspondiente no tendrá que hacer referencia específica a los principios de puerto seguro.

([14]) De modo similar, el médico de este ejemplo no podría basarse en la autorización legal para invalidar el ejercicio personal del derecho a excluirse del márketing directo establecido en la FAQ nº 12. El ámbito de cualquier excepción de «autorizaciones explícitas» está necesariamente limitado al de la autorización con arreglo a la norma en cuestión.

Véase el USC, título 47, § 222(c)(1)-(3). La Ley permite también a las empresas de telecomunicaciones, como excepción, utilizar los datos del cliente para:

1) iniciar, prestar, facturar y cobrar sus servicios;

2) protegerse de actos fraudulentos, indebidos o ilegales; y

3) prestar servicios de telemárketing, remisión o administración durante una llamada iniciada por el cliente ([15]).

Id., § 222(d)(1)-(3). Por último, las empresas de telecomunicaciones deben suministrar información relativa a la lista de abonados, que sólo puede incluir su nombre, dirección, número de teléfono y línea de negocio de los clientes comerciales, a los editores de directorios telefónicos. *Id*., § 222(e).

La excepción de las «autorizaciones explícitas» podría entrar en juego cuando las empresas de telecomunicaciones utilizan la IREC para evitar fraudes u otros actos ilegítimos. Aun en tal caso, estas actuaciones podrían calificarse como de «interés público» y quedar así permitidas por los principios.

Normas propuestas por el Departamento de Servicios Humanitarios y de Sanidad

El Departamento de Servicios Humanitarios y de Sanidad (SHS) ha propuesto unas normas relativas a los requisitos de intimidad en materia de los datos sanitarios individualmente identificables, véase 64 Fed. Reg. 59.918 (3 de noviembre de 1999) (por codificar en 45 C.F.R. puntos 160-164). Estas reglas serían la plasmación de los requisitos de intimidad de la Health Insurance Portability and Accountability Act (Ley de Transferibilidad y Responsabilidad del Seguro Sanitario) de 1996, Pub. L. 104-191. Las normas propuestas prohíben en general a las entidades sujetas (es decir, planes sanitarios, cámaras de compensación de asistencia sanitaria y prestadores de asistencia sanitaria que transmitan información sanitaria en formato electrónico) utilizar o revelar datos sanitarios protegidos sin autorización personal. Véase la propuesta 45 CFR § 164.506. Las normas exigirían la revelación de la información sanitaria protegida únicamente para dos fines: 1) permitir a las personas inspeccionar y copiar datos sanitarios propios, véase *id*., § 164.514; y 2) exigir el cumplimiento de las normas, véase *id*., § 164.522.

Las normas propuestas permitirían la utilización o revelación de información sanitaria protegida sin autorización específica de la persona en circunstancia limitadas, tales como la supervisión del sistema de asistencia sanitaria, la vigilancia del cumplimiento de la ley o las situaciones de emergencia. Véase *id*., § 164.510. En ellas se detallan los límites de tales formas de utilización y revelación que además estarían circunscritas al volumen mínimo necesario de información. Véase *id*., § 164.506.

Los usos explícitamente autorizados por las normas propuestas suelen atenerse a los principios de puerto seguro o estar autorizados por otra excepción. Por ejemplo, se permite la vigilancia del cumplimiento de la ley (función de policía) y la función judicial, al igual que la investigación médica. Otros usos, tales como la supervisión del sistema de asistencia sanitaria, la función de salud pública y la operación de las redes de datos oficiales, son de interés público. Las revelaciones de datos para tramitar pagos y primas de asistencia sanitaria son necesarias para la prestación de la misma. Los usos en caso de emergencias, para consultar a familiares sobre un posible tratamiento cuando el consentimiento del paciente «no puede obtenerse razonablemente» o para determinar la identidad o la causa de la muerte, protegen los intereses vitales de la persona en cuestión y de otros sujetos. Los usos para la gestión de personal en servicio militar activo y otras categorías especiales de personas ayudan a la correcta realización de la función de defensa o situaciones igualmente exigentes; y, en cualquier caso, estas formas de utilización tendrán escasa o nula repercusión en los consumidores en general.

Ello nos deja tan sólo con la utilización de datos personales por parte de los centros de asistencia sanitaria para elaborar directorios de pacientes. Aunque este uso podría no alcanzar el nivel de interés «vital», los directorios benefician a los

([15]) El ámbito de esta excepción es muy limitado. Con arreglo a ella, la empresa de telecomunicaciones puede usar la IREC sólo durante una llamada iniciada por el cliente. Además, la Comisión Federal de Comunicaciones nos ha indicado que la empresa no puede utilizar la IREC para comercializar servicios fuera del ámbito de la solicitud del cliente. Por último, dado que el cliente debe autorizar el uso de la IREC para este fin, esta disposición no constituye en realidad una «excepción» en modo alguno.

pacientes y a sus amigos y parientes. Además, el ámbito de este uso autorizado es limitado por naturaleza. Por tanto, basarse en la excepción de los principios para usos «explícitamente autorizados» por la ley para este fin supone un riesgo mínimo para la intimidad de los pacientes.

Ley de Informes de Crédito Justos

La Comisión Europea ha manifestado su preocupación por el hecho de que la excepción de «autorizaciones explícitas» podría «constituir efectivamente una conclusión de adecuación» a efectos de la Ley de Informes de Crédito Justos (FCRA). No es así. A falta de una conclusión de adecuación específica para la FCRA, las organizaciones de Estados Unidos de América que en otro caso se basarían en tal conclusión tendrán que adherirse a los principios de puerto seguro a todos los efectos. Esto significa que, si los requisitos de esta Ley superan el nivel de protección previsto en los principios, a las entidades estadounidenses les bastaría con atenerse a lo dispuesto en ella. A la inversa, si la FCRA resultara insuficiente, dichas entidades tendrían que ajustar sus prácticas informativas a lo previsto en los principios. La excepción no desvirtuaría esta conclusión básica. Según lo establecido, la excepción se aplica sólo si la norma en cuestión autoriza expresamente actos que contradicen los principios de puerto seguro, y no se extendería al ámbito en que los requisitos de la FCRA simplemente no se ajustan a dichos principios ([16]).

En otras palabras, no consideramos que la excepción signifique que todo lo que no está exigido queda por tanto «explícitamente autorizado». Además, la excepción se aplica sólo si lo explícitamente autorizado por la legislación estadounidense es contratario a los requisitos de los principios de puerto seguro. La legislación aplicable debe cumplir estos dos elementos para que se permita no atenerse a los principios.

El artículo 604 de la FCRA, por ejemplo, autoriza explícitamente a las agencias de informes de consumidor emitir tales informes es una serie de situaciones determinadas. Véase la FCRA, § 604. Si al hacer esto el artículo 604 autoriza a las agencias a actuar de forma contraria a los principios de puerto seguro, éstas deberán basarse en la excepción (a menos, obviamente, que sea de aplicación otra excepción). Las agencias deben obedecer los mandamientos judiciales y de gran jurado, y el uso de los informes de crédito por los organismos públicos de concesión de licencias, sociales y de apoyo a la infancia sirve al interés público. *Id.*, § 604(a)(1), (3)(D) y (4). Por tanto, la agencia no estará obligada a basarse en la excepción de «autorización explícita» para estos fines. Si actúa con arreglo a instrucciones escritas del consumidor, habrá cumplido plenamente los principios de puerto seguro. *Id.*, § 604(a)(2). Del mismo modo, sólo pueden obtenerse informes de consumidor para fines de empleo con la autorización escrita de éste [*id.*, §§ 604(a)(3)(B) y (b)(2)(A)(ii)] y para operaciones de crédito o seguro no iniciadas por el consumidor, sólo si éste no ha decidido excluirse de tales ofertas [*id.*, § 604(c)(1)(B)]. La FCRA prohíbe también a las entidades de informes de crédito proporcionar información médica para fines de empleo sin el consentimiento del consumidor. *Id.*, § 604(g). Estos usos se atienen a los principios de notificación y de opción. Otros fines autorizados por el artículo 604 implican operaciones en que interviene el consumidor y, por tal motivo, estarán permitidas por los principios. Véase *id.*, § 604(a)(3)(A) y (F).

La utilización restante «autorizada» por el artículo 604 se refiere a los mercados secundarios de crédito. *Id.*, § 604(a)(3)(E). No hay conflicto entre el uso de informes de consumidor para este fin y los principios de puerto seguro *per se*. Si bien es cierto que la FCRA no exige a las entidades de informes de crédito, por ejemplo, notificar y obtener el consentimiento de los consumidores cuando emiten informes para tal fin, debemos reiterar que la ausencia de un requisito no equivale a una «autorización explícita» para actuar de manera diferente a la exigida. De modo similar, el apartado 608 permite a las entidades de informes de crédito proporcionar algunos datos personales a los organismos públicos. Esta «autorización» no justifica que la entidad pase por alto su compromiso de cumplir los principios de puerto seguro. Esto contrasta con nuestros restantes ejemplos, en los que las excepciones a las exigencias de notificación y elección positiva vienen a autorizar explícitamente usos de los datos personales sin notificación ni elección.

Conclusión

Puede observarse una pauta clara, incluso a partir de lo limitado de nuestro examen de estas Leyes:

— La «autorización explícita» de la Ley permite en general la utilización o revelación de datos personales sin el previo consentimiento de la persona; por tanto, la excepción estará limitada a los principios de notificación y de elección.

([16]) Nuestro análisis de este extremo no debe considerarse una admisión de que la FCRA no establece una protección «adecuada». Cualquier análisis de la FCRA debe considerar la protección ofrecida por la ley en su conjunto en lugar de centrarse exclusivamente en las excepciones, como hemos hecho aquí.

— En la mayoría de los casos, las excepciones autorizadas por la Ley están estrictamente definidas para su aplicación en situaciones y para fines específicos. En todos los casos, la Ley prohíbe cualquier otro supuesto de uso o revelación no autorizados de datos personales no comprendidos en estos límites.

— En la mayoría de los casos, y como reflejo de su carácter legislativo, la utilización o revelación autorizada sirve al interés público.

— Prácticamente en todos los casos, los usos autorizados se ajustan plenamente a los principios de puerto seguro o bien están comprendidos en una de las restantes excepciones autorizadas.

En conclusión, la excepción de «autorizaciones explícitas» de la Ley será probablemente, por su propia naturaleza, muy limitada en su alcance.

C. **Fusiones y absorciones**

El Grupo de trabajo del artículo 29 manifestó su preocupación por los casos en que una entidad adherida a los principios de puerto seguro resulte absorbida por otra que no se haya comprometido a seguirlos, o se fusione con ella. En cualquier caso, el Grupo de trabajo parece haber considerado que la empresa subsistente no estaría obligada a aplicar dichos principios a los datos personales en manos de la empresa absorbida, pero esto no es necesariamente así con arreglo a la legislación estadounidense. La regla general en Estados Unidos de América en materia de fusiones y absorciones es que la sociedad que adquiere el capital en circulación de otra asume en general las obligaciones y deudas de ésta. Véase 15 Fletcher Cyclopedia of the Law of Private Corporations § 7117 (1990); véase también Model Bus. Corp. Act § 11.06(3) (1979) («la empresa superviviente hace suyas las obligaciones de todas las sociedades participantes en la fusión»). En otras palabras, la sociedad superviviente en una fusión o absorción de este tipo de una entidad adherida a estos principios quedaría vinculada por los compromisos de protección asumidos por ésta.

Por otra parte, aun si la fusión o absorción se realizara mediante la adquisición de activos, las obligaciones de la empresa adquirida seguirían vinculando a la adquirente en determinados casos, véase 15 Fletcher, § 7122. Aun en el caso de que las obligaciones no sobrevivieran a la fusión, debe señalarse que tampoco lo harían en una fusión en la que los datos se transfirieran desde Europa en virtud de un contrato, la única alternativa viable a los principios de puerto seguro de que tratamos para las transferencias de datos a Estados Unidos de América. Por otra parte, los textos relativos a estos principios, según la revisión hecha, exigen a toda entidad adherida notificar cualquier absorción al Departamento de Comercio y sólo permite la continuación de la transmisión de datos a la organización sucesora si ésta asume estos principios, véase la FAQ nº 6. De hecho, Estados Unidos de América ha revisado su marco de protección para exigir a las entidades de este país que se encuentren en tal situación que eliminen la información que hayan recibido en virtud de estos principios si no van a continuar asumiéndolos o que establezcan otras garantías adecuadas.

ANEXO V

14 de julio de 2000

John Mogg
Director, Dirección General XV
Comisión Europea
Despacho C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles/Brussel

Estimado Sr. Mogg:

Entiendo que han surgido diversas dudas en relación con la carta que le remití con fecha de 29 de marzo de 2000. Para aclararle nuestra competencia en las áreas que han provocado las dudas, le remito la presente que, para facilitar la referencia en el futuro, se añade al texto de la correspondencia anterior y recapitula parte del mismo.

En el transcurso de sus visitas a nuestras oficinas y en su correspondencia, ha planteado diversas cuestiones sobre la competencia de la Comisión Federal de Comercio (FTC) de Estados Unidos de América en el área de protección de la vida privada en línea. He pensado que sería útil resumir mis respuestas anteriores y facilitar información adicional sobre la jurisdicción de dicho organismo en cuestiones de vida privada del consumidor planteadas en su última carta. Concretamente, Ud. pregunta: 1) si la FTC tiene jurisdicción sobre transmisión de datos relacionados con el empleo si se realiza incumpliendo los principios de puerto seguro de Estados Unidos de América; 2) si la FTC tiene jurisdicción sobre programas de carácter no lucrativo de protección de la vida privada («seal» o «programs»); 3) si la Ley FTC se aplica a los datos en línea al igual que a los datos fuera de línea; y 4) qué sucede cuando la jurisdicción de la FTC se superpone con la de otros órganos encargados de la aplicación de la Ley.

Aplicación de la Ley FTC a la protección de la vitada privada

La competencia jurídica de la Comisión Federal de Comercio en este ámbito se fundamenta en el artículo 5 de la Ley de la Comisión Federal de Comercio (en adelante, «Ley FTC»), que prohíbe «actos o prácticas desleales o fraudulentos» en el comercio o en relación con él [1]. Una práctica fraudulenta se define como una manifestación, omisión o práctica que probablemente inducirá a error de manera significativa a consumidores razonables. Una práctica es desleal si provoca, o podría provocar, daños o perjuicios importantes para los consumidores que no se pueden evitar razonablemente y no están compensados por contrapartidas beneficiosas para los consumidores o la competencia [2].

Ciertas prácticas de recogida de información tienen muchas probabilidades de infringir la Ley FTC. Por ejemplo, si un sitio web afirma cumplir una política determinada de protección de la vida privada o un conjunto de directrices de autorregulación y esto no es cierto, el artículo 5 de la Ley FTC ofrece la base jurídica para denunciar dicha manifestación falsa como fraudulenta. De hecho, hemos logrado aplicar la Ley para establecer este principio [3]. Además, la FTC ha tomado la postura de que puede recusar prácticas de protección de la vida privada especialmente flagrantes alegando que son desleales a tenor del artículo 5 si dichas prácticas están relacionadas con menores o con el uso de información muy delicada, como datos financieros [4] y expedientes médicos. La Comisión Federal de Comercio ha puesto en marcha, y continuará haciéndolo, tales acciones de aplicación de la Ley mediante sus esfuerzos activos de supervisión e investigación, y a través de los casos que nos remiten los organismos de autorregulación y otros, incluidos los Estados miembros de la Unión Europea.

---

[1] Véase el USC, título 15, § 45. La Fair Credit Reporting Act también se aplicaría a la recogida de datos y las ventas en Internet que respondan a las definiciones de «consumer report» (informe del consumidor) y «consumer reporting agency» (agencia de información del consumidor) incluidas en dicha Ley.

[2] USC, título 15, § 45(n).

[3] Véase GeoCities, expediente Nº C-3849 (Final Order de 12 de febrero de 1999) (www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., expediente Nº C-3891 (Final Order de 12 de agosto de 1999) (www.ftc.gov/opa/1999/9905/younginvestor.htm). Véase también Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. parte 312 (www.ftc.gov/opa/1999/9910/childfinal.htm). La norma COPPA Rule, que entró en vigor el mes pasado, exige a los operadores de sitios web destinados a menores de 13 años, o que recojan voluntariamente información personal de menores de 13 años, la aplicación de las normas para prácticas leales de información enunciadas en ella.

[4] Véase FTC v. TouchTone, Inc., Civil Action Nº 99-WM-783 (D.Co.) (presentada el 21 de abril de 1999) en www.ftc.gov/opa/1999/9904/touchtone.htm. Carta de opinión del personal, 17 de julio de 1997, enviada en respuesta a una petición presentada por el Center for Media Education, en www.ftc.gov/os/1997/9707/cenmed.htm.

Apoyo a la autorregulación

La FTC dará prioridad a los casos de incumplimiento de directrices de autorregulación remitidos por organizaciones como BBBOnline y TRUSTe ([5]). Este enfoque sería coherente con nuestra relación con el National Advertising Review Board (NARB) del Better Business Bureau, que remite a la FTC las quejas relacionadas con la publicidad. La National Advertising Division (NAD) de NARB resuelve, a través de un proceso de resolución judicial, las denuncias relativas a la publicidad nacional. Cuando una parte se niega a cumplir un fallo de la NAD, se remite el caso a la FTC. El personal de la FTC revisa la publicidad denunciada según un sistema de prioridades a fin de determinar si incumple la Ley FTC y con frecuencia logra poner fin a la conducta denunciada o convencer a la parte para que vuelva al proceso iniciado en el NARB.

Igualmente, la FTC dará prioridad a los casos que reciba sobre incumplimiento de los principios de «puerto seguro» procedentes de Estados miembros de la Unión Europea. Como sucede con los casos remitidos por las entidades de autorregulación estadounidenses, nuestro personal analizará todos los datos relativos a si la conducta objeto de denuncia infringe el artículo 5 de la Ley FTC. Este compromiso también se puede observar en los principios de puerto seguro recogido en una de las preguntas más frecuentes sobre aplicación (FAQ nº 11).

GeoCities: primer caso sobre protección de la vida privada en línea de la FTC

El primer caso sobre protección de la vida privada en Internet que se presentó ante la Comisión Federal de Comercio, GeoCities, se basaba en la competencia que le confiere el artículo 5 ([6]). En dicho caso, la FTC alegó que GeoCities realizó declaraciones engañosas, tanto a adultos como a niños, relativas al uso de su información personal. La denuncia de la Comisión Federal de Comercio alegó que GeoCities declaró que determinados datos de identificación personal recogidos en su sitio web se utilizarían únicamente para fines internos o para proporcionar a los clientes las ofertas publicitarias y los productos o servicios específicos que éstos solicitaran, y que determinada información «opcional» adicional no se transmitiría a terceros sin el consentimiento del consumidor. En realidad, esta información se facilitaba a terceros que la utilizaban para enviar a los clientes ofertas distintas a las acordadas por la entidad miembro. La denuncia también acusaba a GeoCities de participar en prácticas fraudulentas relacionadas con la recogida de información procedente de menores. Según la denuncia de la FTC, GeoCities afirmaba gestionar una zona de su web destinada a menores y que la información en ella recogida no era transmitida a terceros. En realidad, estas áreas de su sitio web eran operadas por terceros que recogían y mantenían la información.

El acuerdo extrajudicial prohíbe a GeoCities que realice declaraciones engañosas relativas al fin para el que recoge o utiliza la información de identificación personal de sus clientes, incluidos los menores. La orden exige a la empresa que incluya en su sitio web una advertencia sobre protección de datos clara y en lugar destacado donde indique a los consumidores la información que está recogiendo y para qué fines, a quién la transmitirá y la manera en que los consumidores pueden acceder a dichos datos y eliminarlos. Para garantizar el control de los padres, el acuerdo también exige a GeoCities que obtenga el consentimiento de los padres antes de recoger información de identificación personal de menores de 12 años. La orden también incluye la exigencia de que GeoCities envíe una notificación a sus miembros y les ofrezca la oportunidad de eliminar sus datos personales de las bases de datos de GeoCities y de terceros. El acuerdo menciona explícitamente que GeoCities enviará una notificación a los padres de los menores de 12 años y que eliminará la información relativa a ellos, a menos que uno de los padres consienta específicamente su conservación y uso. Por último, GeoCities deberá ponerse en contacto con los terceros a los que previamente reveló la información y les solicitará que también eliminen dichos datos ([7]).

ReverseAuction.com

En enero de 2000, la FTC aprobó una denuncia y elaboró un acuerdo de consentimiento relativos a ReverseAuction.com, un sitio de subastas en línea que, presuntamente, obtenía información de identificación personal de los consumidores de un sitio competidor (eBay.com) y les enviaba mensajes por correo electrónico no solicitados y fraudulentos para atraer sus negocios ([8]). Nuestra denuncia alegaba que ReverseAuction incumplía el artículo 5 de la Ley FTC al obte-

([5]) De hecho, la FTC presentó recientemente una denuncia ante el Tribunal Federal de Primera Instancia contra una entidad con la certificación de TRUSTe, Toysmart.com, para obtener desagravios cautelares y declarativos para impedir la venta de información confidencial y personal de clientes recogida en el sitio web de la empresa incumpliendo su propia declaración de protección de la vida privada. La FTC fue informada de esta posible infracción de la Ley directamente por TRUSTe. Véase FTC v. Toysmart.com, LLC, Civil Action Nº 00-11341-RGS (D.Ma.) (presentada el 11 de julio de 2000) en www.ftc.gov/opa/2000/07/toysmart.htm).

([6]) GeoCities, expediente Nº C-3849 (Final Order de 12 de febrero de 1999) (se puede consultar en www.ftc.gov/os/1999/9902/9823015d%26o.htm).

([7]) Posteriormente, la Comisión decidió en un segundo aspecto relacionado con la recogida en línea de información personal sobre niños. Liberty Financial Companies, Inc., operaba el sitio web Young Investor, destinado a niños y adolescentes y centrado en cuestiones relacionadas con el dinero y la inversión. La FTC alegó que este sitio afirmaba falsamente que la información personal solicitada a los menores en una encuesta se mantendría anónima y que los participantes recibirían un boletín informativo por correo electrónico, así como premios. De hecho, la información personal sobre los menores y la situación financiera de sus familias se conservaba de manera identificable y no se enviaron ni boletines informativos ni premios. El acuerdo de consentimiento prohíbe estas manifestaciones falsas en el futuro y exige que Liberty Financial incluya en sus sitios web destinados a menores una advertencia sobre protección de datos y obtenga el consentimiento paterno verificable antes de recoger información personal de identificación de los menores. Liberty Financial Cos., expediente Nº C-3891 (Final Order de 12 de agosto de 1999) (en www.ftc.gov/opa/1999/9905/younginvestor.htm).

([8]) Véase ReverseAuction.com, Inc., Civil Action Nº 000032 (D.D.C.) (presentada el 6 de enero de 2000) (nota de prensa y escritos procesales en www.ftc.gov/opa/2000/01/reverse4.htm).

ner la información identificable individualmente, incluidas las direcciones de correo electrónico de los usuarios de eBay y sus nombres de identificación de usuario personalizados («user IDs») y al enviar los correos electrónicos fraudulentos.

Como se explica en la denuncia, antes de obtener la información, ReverseAuction se registró como usuario de eBay y aceptó cumplir el acuerdo de usuario y la póliza de protección de datos de eBay, que protegen la vida privada de los consumidores prohibiendo a los usarios de eBay la recogida y el uso de información de identificación personal para fines no autorizados, como el envío de mensajes electrónicos comerciales no solicitados. Por tanto, nuestra denuncia alegó en primer lugar que ReverseAuction realizó manifestaciones falsas en el sentido de que cumpliría el acuerdo de usuario y la póliza de protección de datos de eBay, una práctica fraudulenta a tenor del artículo 5. Además, la denuncia alegaba que el uso por ReverseAuction de la información para enviar el correo electrónico comercial no solicitado, incumpliendo el acuerdo de usuario y la póliza de protección de datos, era una práctica comercial desleal según el artículo 5.

En segundo lugar, la denuncia alegaba que los mensajes electrónicos a los consumidores incluían un título engañoso que les informaba de que su identificación como usario de eBay «vencerá pronto». Por último, la denuncia alegaba que los mensajes electrónicos afirmaban de manera fraudulenta que eBay facilitaba directa o indirectamente a ReverseAuction la información identificable persona de los usuarios de eBay, o participaba de otra forma en la difusión de los correos electrónicos no solicitados.

El acuerdo obtenido por la FTC prohíbe a ReverseAuction volver a cometer estas infracciones en el futuro. Asimismo, exige a ReverseAuction que envíe una notificación a los consumidores que, tras recibir un correo electrónico de ReverseAuction, se registraron o se registrarán en el futuro en dicha empresa. Esta notificación debe informar a los consumidores que la identificación de los usuarios de eBay no estaba a punto de vencer y que eBay no conocía la difusión por ReverseAuction del mensaje electrónico no solicitado, ni la autorizó. La notificación también ofrecerá a estos consumidores la oportunidad de cancelar el registro en ReverseAuction y eliminar su información de identificación personal de la base de datos de dicha empresa. Además, la orden exige a ReverseAuction eliminar y abstenerse de utilizar o revelar la información de identificación personal de los miembros de eBay que recibieron el mensaje electrónico de ReverseAuction pero que no se hayan registrado. Por último, de manera coherente con las órdenes sobre protección de la vida privada obtenidas previamente por esta agencia, el acuerdo exige a ReverseAuction presentar su propia política de protección de la vida privada en su sitio Internet, y contiene disposiciones completas sobre el mantenimiento de registros que permitirán a la FTC controlar su cumplimiento.

El caso ReverseAuction demuestra que la FTC se ha comprometido a poner en práctica el principio de aplicación para reforzar las acciones de autorregulación de la industria en el área de protección de la vida privada en línea. De hecho, este caso recusaba directamente una conducta que minaba una póliza de protección de datos y un acuerdo de usuario que protegían la vida privada de los consumidores y que podría hacer peligrar la confianza de los consumidores en las medidas de protección de dados puestas en marcha por las empresas en línea. Dado que este caso se refiere a la apropiación indebida por una empresa de información de consumidores protegida por la política de protección de datos de una segunda empresa, también puede ser de especial importancia para las dudas sobre la protección de la vida privada planteadas por la transmisión de datos entre empresas de distintos países.

Pese a las acciones encaminadas a exigir la aplicación de la ley emprendidas por la Comisión Federal de Comercio en GeoCities, Liberty Financial Cos. y ReverseAuction, la competencia de esta agencia en algunas áreas de la vida privada en línea es más limitada. Como se ha indicado anteriormente, la recogida y el uso de información personal sin consentimiento debe constituir una práctica comercial desleal o fraudulenta para incluirse en el ámbito de la Ley FTC. Por tanto, la Ley FTC probablemente no sería de aplicación en las prácticas de un sitio web que recogiera información personal identificable de consumidores, pero que no realizara manifestaciones engañosas sobre el fin para el que la recoge, ni utilizara o divulgara la información de manera que pudiera causar daños y perjuicios importantes a los consumidores. Además, actualmente la FTC puede no estar facultada para exigir en general a las entidades que recogen información en Internet que se adhieran a una política de protección de la vida privada general ni particular ([9]). Como se ha afirmado anteriormente, sin embargo, el hecho de que una empresa no acate una política de protección de la vida privada declarada probablemente puede considerarse una práctica fraudulenta.

([9]) Por este motivo, la Comisión Federal de Comercio afirmó en una declaración ante el Congreso que probablemente sería necesaria una nueva norma para obligar a todos los sitios web comerciales de Estados Unidos de América destinados a los consumidores a acatar práctica específicas de información leal: «Consumer Privacy on the World Wide Web» ante el Subcomité de Telecomunicaciones, Comercio y Protección del Consumidor del «House Committee on Commerce United States House of Representatives», 21 de julio de 1998 (esta declaración se puede consultar en www.ftc.gov/os/9807/privac98.htm). La FTC optó por aplazar la solicitud de dicha legislación para dar la oportunidad de que los esfuerzos de autorregulación demuestren la adopción extendida de prácticas informativas leales en los sitios web. En el informe de la Comisión Federal de Comercio al Congreso sobre protección de la vida privada en línea «Privacy Online: A Report to Congress» de junio de 1988 (el informe se puede consultar en www.ftc.gov/reports/privacy3/toc.htm), la FTC recomendó incluir en la legislación la exigencia de que los sitios web comerciales obtengan el consentimiento paterno antes de obtener información personal identificable de niños menores de 13 años. Véase la anterior nota 3. El año pasado, el informe de la FTC «Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress», de julio de 1999 (que se puede consultar en www.ftc.gov/os/1999/9907/index.htm#13) consideró que había progresos suficientes en la autorregulación y, por tanto, optó en aquel momento por no recomendar una legislación.
En mayo de 2000, la FTC presentó un tercer informe ante el Congreso, «Privacy Online: Fair Information Practices in the Electronic Marketplace» (se puede consultar en www.ftc.gov/os/2000/05/index.htm#22) que analiza el reciente estudio realizado por la FTC sobre sitios web comerciales y su cumplimiento de las prácticas leales de información. Este informe también recomienda (por mayoría de la FTC) que el Congreso elabore nueva legislación para definir un nivel básico de protección de la vida privada en los sitios web comerciales orientados al consumo.

Además, la jurisdicción de la FTC en este ámbito cubre los actos o prácticas desleales o frauduentos solamente «en el comercio o en relación con él». La recogida de información por entidades comerciales en sus actividades de promoción de productos o servicios, incluida la recogida y el uso de información para fines comerciales, cumplirían presumiblemente el requisito de «comercio». Por otro lado, muchas personas o entidades pueden estar recogiendo información en línea sin fines comerciales y, por tanto, no entrar en la jurisdicción de la Comisión Federal de Comercio. Un ejemplo de esta limitación son los «foros electrónicos» si son gestionados por entidades no comerciales, como organizaciones de caridad.

Por último, hay diversas limitaciones jurídicas, totales o parciales, en la jurisdicción básica de la FTC respecto a prácticas comerciales que limitan la capacidad de la FTC para ofrecer una respuesta completa a los problemas de protección de la vida privada en Internet. Entre ellas se incluyen la exención de numerosas entidades de consumo que utilizan gran cantidad de información, tales como bancos, compañías de seguros y líneas aéreas. Como sabe, la jurisdicción sobre dichas entidades corresponde a otras agencias federales o estatales, como las agencias federales de banca o el Departamento de Transporte.

En los casos que no entran en su jurisdicción, la FTC acepta y, si lo permiten los recursos, actúa en respuesta a las quejas de los consumidores recibidas por correo y teléfono en su centro de atención al cliente (Consumer Response Center, CRC) y, más recientemente, en su sitio web ([10]). El CRC acepta quejas de todos los consumidores, incluidos los recidentes en Estados miembros de la Unión Europea. La Ley FTC proporciona a la Comisión Federal de Comercio competencia equitativa para obtener desagravios cautelares frente a futuras infracciones de la Ley FTC, así como reparación para los consumidores perjudicados. No obstante, intentaríamos ver si la empresa ha participado en un modelo de conducta inadecuada, dado que no resolvemos litigios de consumidores individuales. En el pasado, la Comisión Federal de Comercio ha obtenido reparación para ciudadanos estadounidenses y de otros países ([11]). La FTC continuará imponiendo su autoridad, en los casos adecuados, para ofrecer reparación a los ciudadanos de otros países que hayan sufrido daños y perjuicios por prácticas fraudulentas dentro de su jurisdicción.

Datos sobre la relación laboral

En su última carta deseaba más aclaraciones sobre la jurisdicción de la FTC en el ámbito de los datos laborales. En primer lugar, plantea la cuestión de si la FTC podría emprender acciones, a tenor del artículo 5, contra una empresa que afirme cumplir los principios de puerto seguro estadounidenses pero que transmita o utilice datos laborales de manera incompatible con dichos principios. Deseamos asegurarle que hemos revisado atentamente la legislación que habilita a la FTC, documentos relacionados y jurisdicción pertinente, y hemos llegado a la conclusión de que, en las situaciones relativas a datos laborales, la FTC tiene la misma jurisdicción que se le otorga en general en el artículo 5 de la Ley FTC ([12]). Es decir, suponiendo un caso que cumpliera nuestros criterios actuales (información desleal o fraudulenta) de cumplimiento relacionado con la vida privada, podríamos iniciar acciones si se tratara de datos laborales.

Asimismo, deseamos negar la opinión de que la capacidad de la FTC para incoar acciones de aplicación relacionadas con la vida privada se limita a situaciones en las que una empresa ha actuado de manera fraudulenta hacia consumidores individuales. De hecho, como aclara su reciente acción en el asunto ReverseAuction ([13]), la FTC incoará acciones de aplicación relacionadas con la vida privada en situaciones con transmisión de datos entre empresas en las que una empresa presuntamente haya actuado ilegalmente respecto a otra, provocando posibles daños y perjuicios a consumidores y empresas. Suponemos que este tipo de situaciones son las que más probabilidades tienen de plantear problemas con los datos laborales, cuando se hayan transmitido datos de este tipo sobre ciudadanos europeos de empresas europeas a empresas estadounidenses que hayan declarado acatar los principios de puerte seguro.

No obstante, deseamos destacar una circunstancia en la que la acción de la FTC sí se vería limitada. Esto sucedería cuando el asunto ya se estuviera tratando en el contexto de un litigio de Derecho laboral tradicional, probablemente un procedimiento de resolución de conflictos o de arbitraje o una denuncia por práctica laboral desleal ante el National Labor Relations Board (el tribunal nacional de relaciones laborales). Esto ocurriría, por ejemplo, si un empresario

([10]) Véase el formulario de queja en línea de la Comisión Federal de Comercio en http://www.ftc.gov/ftc/complaint.htm.

([11]) Por ejemplo, en un caso reciente relacionado con un sistema piramidal en Internet, la FTC obtuvo reembolso para 15 622 consumidores por un importe aproximado de 5,5 millones de dólares estadounidenses. Los consumidores eran residentes en los Estados Unidos y 70 países más. Véase www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([12]) Exceptuando las limitaciones explícitas incluidas en la legislación habilitadora de la FTC, su jurisdicción a tenor de la Ley FTC sobre prácticas «en el comercio o en relación con él» es igual de amplia que el poder constitucional del Congreso a tenor de la Cláusula sobre Comercio, Estados Unidos contra American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975). Asi, la jurisdicción de la FTC abarcaría prácticas relativas a datos laborales en empresas e industrias de comercio internacional.

([13]) Véase «Online Auction Site Settles FTC Privacy Charges», nota de prensa de la FTC (6 de enero de 2000) en http://www.ftc.gov/opa/2000/01/reverse4.htm.

hubiera aceptado un compromiso en un convenio colectivo en relación con el uso de los datos personales y un empleado o sindicato denunciara el incumplimiento de dicho compromiso. La FTC respetaría dicho procedimiento ([14]).

Jurisdicción sobre los programas de protección de la vida privada

En segundo lugar, pregunta si la FTC tendría jurisdicción sobre los programas de protección de la vida privada que administran mecanismos de resolución de conflictos en Estados Unidos de América en los que se hicieran manifestaciones engañosas sobre su función al aplicar los principios de «puerto seguro» y gestionar quejas individuales, aunque tales entidades técnicamente fueran «sin ánimo de lucro». Al determinar si tenemos jurisdicción sobre una entidad que se presenta como sin ánimo de lucro, la FTC analiza detalladamente si dicha entidad, aunque no obtenga beneficios de por sí, favorece el beneficio de sus miembros. La FTC ha reivindicado con éxito su jurisdicción sobre dichas entidades y recientemente, el 24 de mayo de 1999, el Tribunal Supremo de los Estados Unidos, en California Dental Association contra Comisión Federal de Comercio, aceptó por unanimidad la jurisdicción de la FTC sobre una asociación voluntaria sin ánimo de lucro de sociedades dentales locales en un asunto antimonopolio. El Tribunal falló lo siguiente:

> La Ley FTC hace lo posible por incluir claramente no sólo las entidades «organizadas para realizar negocios en su propio lucro» (véase el USC, título 15, § 44) sino también las que hacen negocios en beneficio «de sus miembros» […] En realidad, difícilmente, se puede suponer que el Congreso pretendiera aplicar una noción tan restringida de organizaciones de apoyo, con las oportunidades que esto daría de evitar la jurisdicción cuando los fines de la Ley FTC solicitan, obviamente, su reivindicación.

En resumen, para decidir si se reivindica la jurisdicción sobre una entidad «sin ánimo de lucro» concreta que administre un programa de protección de la vida privada sería necesaria una revisión objetiva de en qué medida la entidad aporta beneficios económicos a sus miembros con ánimo de lucro. Si dicha entidad gestionara el programa de protección de la vida privada de manera que sus miembros obtuvieran un beneficio económico, la FTC reivindicaría su jurisdicción, probablemente. Independientemente de lo anterior, la FTC tendría probablemente jurisdicción sobre un programa de protección de la vida privada fraudulento que se declarara engañosamente entidad sin ánimo de lucro.

Protección de la vida privada fuera de línea

En tercer lugar, Ud. observa que nuestra correspondencia anterior se ha centrado en la vida privada en el mundo en línea. Aunque la protección de datos en línea ha sido motivo de gran interés para la FTC como componente crucial del desarrollo del comercio electrónico, la Ley FTC data de 1914 y se aplica igualmente al mundo fuera de línea. Por tanto, podemos investigar a empresas de este tipo que participen en prácticas comerciales desleales o fraudulentas en relación con la vida privada de los consumidores ([15]). De hecho, en un caso planteado por la FTC el año pasado, FTC contra TouchTone Information, Inc. ([16]), se acusó a un «*broker* de información» de obtener y vender ilegalmente información financiera privada de los consumidores. La FTC alegó que TouchTone obtenía información de los consumidores «pretextando», término acuñado por el sector de la investigación privada para describir la práctica de obtener información personal de otros de manera fraudulenta, normalmente por teléfono. El caso, presentado el 21 de abril de 1999 ante los Tribunales Federales en Colorado, desea la cesación y todos los beneficios obtenidos ilegalmente.

Esta experiencia de aplicación de la Ley, así como la reciente inquietud por la fusión de bases de datos en línea y fuera de línea, la difuminación de las diferencias entre comercio en línea y fuera de línea, y el hecho de que se recogen y utilizan fuera de línea enormes cantidades de información de identificación personal, garantizan mucha atención a los aspectos de la vida privada fuera de línea.

Jurisdicción coincidente

Por último, plantea la cuestión de la interrelación de la jurisdicción de la FTC con la de otras agencias de aplicación de la Ley, especialmente en los casos de posible conflicto jurisdiccional. Hemos desarrollado unas estrechas relaciones de

([14]) La decisión sobre si una conducta es una «práctica laboral desleal» o infringe un convenio colectivo es una decisión técnica que normalmente se reserva a los tribunales especializados en materia laboral que entenderán de las denuncias, tales como juntas de arbitraje y el NRLB.

([15]) Como sabe por conversaciones anteriores, la Fair Credit Reporting Act también otorga a la FTC la competencia de proteger los datos financieros privados de los consumidores en el ámbito de la Ley, y la FTC emitió recientemente una decisión relacionada con esta cuestión. Véase «In the Matter of Trans Union», expediente Nº 9255 (1 de marzo de 2000) (la nota de prensa y el dictamen se pueden consultar en www.ftc.gov/os/2000/03/index.htm#1).

([16]) Civil Action 99-WM-783 (D.Colo.) (se puede consultar en http://www.ftc.gov/opa/1999/9904/touchtone.htm) (pendiente de *tentative consent decree*).

cooperación con numerosas agencias de aplicación de la Ley, incluidas las agencias federales de banca y los fiscales generales estatales. Con mucha frecuencia coordinamos investigaciones para maximizar nuestros recursos en casos de superposición de la jurisdicción. También es frecuente que remitamos ciertos casos a la agencia federal o estatal apropiada para su investigación.

Espero que este repaso le sea de utilidad. Si necesita más información, no dude en hacérmelo saber.

Atentamente,

Robert Pitofsky

ANEXO VI

John Mogg
Director General, Dirección General XV
Comisión Europea
Despacho C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles/Brussel

Sr. Director General:

Me dirijo a usted a petición del Departamento de Comercio de Estados Unidos de América para explicarle el papel del Departamento de Transportes en la protección de la intimidad de los consumidores en relación con la información que éstos suministran en las compañías aéreas.

El Departamento de Transportes fomenta la autorregulación por constituir el medio que interfiere menos y resulta más eficaz para garantizar la confidencialidad de la información que los consumidores suministran a las compañías aéreas y, por consiguiente, apoya el establecimiento de un régimen de «puerto seguro» que permitiría a las compañías aéreas cumplir las exigencias de la Directiva de protección de datos personales por lo que respecta a su transferencia fuera de la Unión Europea. El Departamento reconoce, no obstante, que para que surtan efecto las iniciativas de autorregulación es fundamental que las compañías aéreas comprometidas con los principios de protección de la intimidad enunciados en el régimen de puerto seguro se atengan a ellas efectivamente. A este respecto, la autorregulación debería ir acompañada por el cumplimiento de la legislación. Por consiguiente, en ejercicio de su actual autoridad legal de protección de los consumidores, el Departamento garantizará el cumplimiento por parte de las compañías aéreas de sus compromisos de protección de la intimidad con el público y perseguirá los casos de presunto incumplimiento que le remitan las organizaciones de autorregulación y otros interesados, como los Estados miembros de la Unión Europea.

La competencia del Departamento para imponer el cumplimiento de la legislación en este ámbito deriva del texto legal del USC, título 49, sección 41712, que prohíbe a las empresas de transporte aplicar «prácticas desleales o engañosas o métodos desleales de competencia» en la prestación del transporte aéreo que supongan o puedan suponer un perjuicio para el consumidor. La sección 41712 se inspira en la sección 5 de la Ley de la Comisión Federal de Comercio (véase el USC, título 15, 45). Sin embargo, la Comisión Federal de Comercio, con arreglo a lo dispuesto en el USC, título 15, 45(a)(2), exime a las compañas aéreas de las normas que establece la sección 5.

Mis servicios están investigando y siguiendo causas con arreglo al USC, título 49, sección 41712 (véanse, por ejemplo, órdenes del Departamento de Transportes 99-11-5, de 9 de noviembre de 1999; 99-8-23, de 26 de agosto de 1999; 99-6-1, de 1 de junio de 1999; 98-6-24, de 22 de junio de 1998; 98-6-21, de 19 de junio de 1998; 98-5-31, de 22 de mayo de 1998; y 97-12-23, de 18 de diciembre de 1997). Incoamos este tipo de causas basándonos en nuestras investigaciones, así como en las denuncias formales o informales que recibimos de particulares, agencias de viajes, compañías aéreas y oficinas de la administración estadounidense o de otros países.

Quisiera señalar que el incumplimiento por parte de una empresa de transporte del respeto de la confidencialidad de la información obtenida de los pasajeros no constituye *per se* una vulneración de la sección 41712. Sin embargo, una vez que una empresa de transporte se compromete formal y públicamente con los principios de puerto seguro de tratar confidencialmente la información sobre los consumidores que obtiene, el Departamento está facultado para hacer uso de las competencias legales que establece la sección 41712 para garantizar el cumplimiento de dichos principios. Por consiguiente, cuando un pasajero proporciona información a una empresa de transporte que se ha comprometido a cumplir los principios de puerto seguro, cualquier incumplimiento en este sentido puede constituir un perjuicio para el consumidor y una vulneración de la sección 41712. Mis servicios otorgarán un gran prioridad a la investigación de todas las supuestas actividades de este tipo y la persecución de todos los casos en los que se observen muestras de tales actividades. También informaremos al Departamento de Comercio de las consecuencias de todos los casos de este tipo.

Las vulneraciones a la sección 41712 pueden dar lugar a mandamientos de cese de tales prácticas y a la imposición de sanciones civiles por vulneración de dichos mandamientos. Pese a que carecemos de competencia para asignar indemnizaciones o conceder reparaciones pecunarias a cada denunciante, tenemos poder para aprobar soluciones derivadas de las investigaciones y los casos presentados por el Departamento que supongan elementos de valor para los consumidores, bien para aliviar el perjuicio, bien para compensar las sanciones monetarias que de otro modo habrían de pagarse. Ésta ha sido la práctica anteriormente, y en el futuro se seguirá aplicando en el ámbito de los principios de puerto seguro cuando las circunstancias lo justifiquen. Las infracciones repetidas a la sección 41712 por cualquier compañía aérea estadounidense también plantearía cuestiones acerca de la predisposición de la compañía al cumplimiento de los principios, que, en situaciones extremas, podría suponer que se considerara que una compañía aérea ya no es apta para seguir operando y, por consiguiente, perdiera su autorización para operar económicamente (véanse las órdenes del Departamento de Transportes 93-6-34, de 23 de junio de 1993, y 93-6-11, de 9 de junio de 1993. Aunque este proce-

dimiento no afectó a la sección 41712, supuso la suspensión de la autorización para operar de una empresa de transporte por absoluto desacato a lo dispuesto en la Federal Aviation Act, Ley federal de aviación, un acuerdo bilateral, y las normas y reglamentos del Departamento.)

Espero que esta información le sea útil. Se desea preguntarme algo o necesita más información, no dude en dirigirse a mí.

Atentamente,

Samuel Podberesky

Consejero General Adjunto de
Aviation Enforcement and Proceeding

ANEXO VII

En lo referente a la letra b) del apartado 2 del artículo 1, los organismos públicos estadounidenses, facultados para investigar las quejas que se presenten y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como reparaciones para los particulares, independientemente de su país de residencia o de su nacionalidad, en caso de incumplimiento de los principios aplicados de conformidad con las FAQ, serán los siguientes:

1) La Federal Trade Commission y

2) El Departamento de Transporte de Estados Unidos de América.

La Federal Trade Commission actúa en el ejercicio de su competencia, que le confiere el artículo 5 de la Federal Trade Commission Act. Según el artículo 5, la Federal Trade Commission carece de jurisdicción en lo tocante a bancos, cooperativas de ahorro y crédito, compañías de servicio público de telecomunicaciones y de transporte, compañías aéreas y envasadores y operarios de áreas para ganado. Aunque el sector de los seguros no figura expresamente en la lista de excepciones del artículo 5, la McCarran-Ferguson Act [1] delega de manera general en los Estados la regulación de esta actividad. No obstante, los preceptos de la FTC Act se aplican subsidiariamente en aquellos Estados que no hayan regulado la actividad. Del mismo modo, la FTC conserva una competencia residual sobre las prácticas desleales o fraudulentas de las compañías de seguros que se realicen al margen de la actividad aseguradora.

El Departamento de Transporte de Estados Unidos de América actúa en el ejercicio de su competencia, que le confiere la sección 41712 del título 49 del United States Code. Incoa los procedimientos basándose tanto en sus propias investigaciones como en las acusaciones formales e informales recibidas de particulares, agentes de viajes, compañías aéreas, organismos públicos estadounidenses y extranjeros.

[1] Véase el USC, título 15, § 1011 y siguientes.