LA PROGRESIVA CONFIGURACION DE LAS TRANSFERENCIAS DE DATOS COMO OBJETO DEL TRAFICO COMERCIAL INTERNACIONAL

Helena Ancos Franco*

El desarrollo del comercio electrónico depende, en gran medida, del nivel de protección que consiga darse a los datos en circulación. El carácter global de las redes y el libre tránsito de los datos exigen una normativa de protección, también global, que permita respetar los derechos humanos y las libertades fundamentales, y servir los intereses del comercio internacional. En este artículo se pone de relieve el abandono de la consideración del derecho de protección de datos personales como derecho fundamental y su progresiva configuración como objeto del tráfico comercial internacional, sobre todo a través de la negociación de acuerdos de comercio bilaterales.

Palabras clave: *comercio internacional, transmisión de datos, flujo transnacional de datos, EDI, derechos fundamentales, acuerdos comerciales, acuerdos bilaterales.*

Clasificación JEL: *F10, K33, O33.*

1. Introducción

El desarrollo de la economía digital ha estimulado poderosamente el movimiento internacional de datos personales, hasta el punto de convertirse al mismo tiempo en un valioso input de todo negocio en la red y en condicionante de su desarrollo futuro.

Y es que está comúnmente aceptado que el crecimiento de la sociedad de la información, y en particular del comercio electrónico, depende —además de otros factores, como el libre acceso a los mercados, la gestión y calidad del servicio, etcétera— del nivel de protección que se otorgue a los datos en circulación. El carácter global de las redes, y la implementación de estándares abiertos, hace que la transmisión de datos sea fácil y rápida poniendo los datos de carácter personal a disposición de millares de usuarios geográficamente dispersos y permitiendo la segmentación de las operaciones de recogida, tratamiento, cesión y cruce de informaciones en diferentes países.

El carácter global de las redes y el libre tránsito de los datos que por ellas circulan exigen una normativa también de carácter global, cuyo diseño constituye un auténtico desafío regulador. Y ello, fundamentalmente, porque la protección de las transferencias internacionales de datos implica cohonestar los derechos humanos y las libertades fundamentales con los intereses del comercio internacional.

Si los tradicionales instrumentos reguladores contemplaban la protección de los datos personales como una esfera más de la intimidad del individuo, estamos asistiendo en los últimos años —a medida que aumenta la importancia de las transacciones electrónicas—, a su creciente consideración como mercancía objeto del tráfico comercial internacional en detrimento de su

* C. U. Francisco de Vitoria. Universidad Complutense de Madrid.

consideración como bien jurídico a proteger en cuanto susceptible de violación de la intimidad.

Por tanto, el planteamiento original «libre circulación de datos-protección intimidad» aparece claramente escorado hacia la promoción de la libertad de tránsito y la eliminación de barreras a la entrada de dichos flujos. La consecuencia jurídica más directa será la concepción del nivel de protección otorgado por las legislaciones nacionales a las transferencias internacionales de datos como barrera técnica en el comercio electrónico interestatal.

El presente artículo pretende poner de relieve el abandono de la consideración del derecho a la protección de datos personales como derecho fundamental y su progresiva configuración en tanto que objeto del tráfico comercial internacional, sobre todo a través de la negociación de acuerdos comerciales bilaterales. Se analizarán para ello, partiendo de las disposiciones sobre transferencias internacionales de datos (TID) de la Directiva 95/46/CE, las recientes negociaciones comerciales UE-terceros Estados que han supuesto la incorporación de cláusulas sobre protección de datos en los instrumentos bilaterales y, en particular, la conclusión del acuerdo entre la Comisión Europea y el Departamento de Comercio norteamericano sobre los llamados principios de «puerto seguro».

2. Las transferencias internacionales de datos en la Directiva 95/46/CE: la exportación de los estándares de protección comunitarios

El origen de la normativa convencional en materia de protección de datos lo encontramos en las normas sobre derechos humanos. Así, el Pacto de Derechos Civiles y Políticos de 1966 y el Convenio de Roma para la protección de los Derechos Humanos y las Libertades Fundamentales de 4 de noviembre de 1950. En el mismo sentido, el Convenio de Estrasburgo de 28 de enero de 1981, que va a constituir el antecedente más directo de la Directiva 95/46/CE. Paralelamente, las Líneas Directrices de la OCDE sobre protección de la intimidad y los flujos transfronterizos de datos personales de 23 de septiembre de 1980 y las directrices de Naciones Unidas sobre archivos automatizados de datos personales de 14 de diciembre de 1980[1], fueron producto de un profuso desarrollo legislativo convencional, inusual en el caso de otros derechos fundamentales.

Este consenso internacional permitió consolidar una serie de principios mínimos de protección, que tendrían quizá su más clara expresión en las directrices de la OCDE de 1980. Pero esta espiral de reconocimiento internacional resultaba engañosa: mientras estos principios propiciaban la aparición de leyes nacionales de protección de datos, eran en todo punto insuficientes para garantizar una protección adecuada[2].

Precisamente, el afán de superación de estos estándares mínimos es el que motivará la aparición de la Directiva 95/46 de la CE. Su antecedente más directo, el Convenio 108 del Consejo de Europa, no había sido firmado por todos los países miembros y, aunque tenía fuerza obligatoria, no preveía el establecimiento por las partes contratantes de mecanismos institucionales de supervisión. Por su parte, las directrices de la OCDE carecían de fuerza vinculante y tampoco establecían medios para asegurar su cumplimiento y una protección efectiva de los particulares.

La mencionada directiva pretende superar estas deficiencias, elevando el nivel de protección del convenio y promoviendo, al mismo tiempo, la adhesión de todos los países miembros de la Comunidad que no lo habían ratificado en su totalidad. Entre las mejoras que incorporaba, se encontraba la regulación de las transferencias internacionales de datos, para las que no existía previsión alguna en el convenio del Consejo de Europa[3]. Sin

[1] Estos instrumentos han de completarse con otros nuevos más recientes adoptados como consecuencia de los nuevos desarrollos tecnológicos: Recomendación del Consejo de Europa n.º R (99) 5, adoptada el 23 de febrero de 1999, para la protección de los particulares respecto a la recogida y procesamiento de datos personales en las autopistas de la información; el Informe de la OCDE sobre «La implementación de las Directrices sobre privacidad en el marco electrónico respecto a Internet», de septiembre de 1998; y la Declaración de la OCDE sobre la protección de la privacidad en las redes globales, como conclusión a la Conferencia de Otawa de octubre de 1998.

[2] DUMOTIER, J. y GOEMANS, C.*: Personal Data Protection in the Digital Economy: The Role of Standardisation*, octubre, 1999, página 9.

[3] El Convenio 108 sólo recogía en su artículo 12, de forma tangencial, las relaciones entre los flujos transfronterizos de datos de carácter personal y el Derecho interno de los Estados partes.

embargo, distintos preceptos de la directiva van a permitir cuestionar su verdadero propósito, haciendo patente una clara toma de partido por la libre circulación de los datos personales y la eliminación de cualquier obstáculo que pudiera poner en peligro «un área de información común dentro de la Comunidad»[4].

El primer indicio lo encontramos en el hecho de que haya sido el artículo 95 (antiguo artículo 100 A) del TCEE el que ha servido de fundamento a la directiva y no el artículo 293 (antiguo artículo 220) del TCEE, pese a que, como se menciona en este último: «Los Estados miembros entablarán, en tanto sea necesario, negociaciones entre sí, a fin de asegurar a favor de sus nacionales: la protección de las personas, así como el disfrute y la tutela de los derechos en las condiciones reconocidas por cada Estado a sus propios nacionales (…)», lo cual era un reflejo, sin duda, de la relevancia que para el desarrollo del mercado interior tenía la libre circulación de datos.

En segundo lugar, la Comunidad va a pretender exportar sus estándares de protección en aras de proteger sus propios intereses comerciales. Esta aplicación extraterritorial de la directiva —que tendrá su correspondencia en el papel preponderante de la Comisión en la vigilancia de las transferencias internacionales de datos frente a la actuación de las autoridades nacionales— hay que entenderla por el temor a una deslocalización masiva de ficheros y actividades informáticas, que afectarían además a los servicios y sectores intensivos en informática y telecomunicaciones como banca, seguros, agencias de viajes y servicios médicos.

Para argumentar la anterior hipótesis nos apoyaremos tanto en criterios sustantivos como procedimentales. Veamos cuáles son.

Ambito de aplicación

En primer lugar, si se atiende al ámbito de aplicación de la directiva, en el artículo 4 se distinguen dos criterios de delimitación: las normas comunitarias serán aplicables cuando: a) el establecimiento del responsable del tratamiento se halle en territorio comunitario; b) cuando para el tratamiento de los datos se empleen medios— automatizados o no— sitos en cualquiera de los Estados miembros.

Rápidamente se observa que no existe simetría reguladora, por cuanto olvida la directiva el supuesto de transferencias pasivas que tengan como destino la Comunidad, a las que, a tenor de la letra del artículo 4, no se les aplicarán las normas nacionales. Este dato tiene más relevancia de lo que a primera vista pudiera parecer. En principio, el criterio del tratamiento en sede comunitaria para inferir la jurisdicción de los Estados miembros parece ser un criterio razonable desde el momento en que la naturaleza cuasipenal de la vulneración de los datos personales aconseja la utilización de un criterio con cierta estabilidad, como es el criterio territorial. Sin embargo, por un lado, se obvia la posibilidad de que aquellas transferencias de datos con destino en un primer momento a Estados a los que la Comunidad haya considerado de «protección adecuada» hayan sido reenviadas a terceros Estados que no gocen de esta consideración y posteriormente, tras tratamientos ulteriores en estos Estados, remitidas a la Comunidad. Por otra parte, esta protección sesgada resulta poco acorde con la pretendida calificación de la protección de la intimidad como derecho fundamental. En tercer lugar, los medios de resarcimiento de los particulares en supuestos de violación de la privacidad de sus datos personales, distan mucho de ser efectivos. Por último. y como tendremos ocasión de ver, la escasa operatividad del procedimiento de declaración de la protección adecuada ha llevado a la Comunidad a conversaciones con terceros Estados, movida por circunstancias coyunturales y comerciales que, aparte de cuestionar su adecuación a los principios del GATS, ponen en entredicho el carácter coherente y completo de su política de protección de la intimidad.

Nivel de protección adecuado

Por otra parte, el artículo 25 se basa en el mismo principio del artículo 12 del Convenio 108 del Consejo de Europa: la transmisión a terceros países es ilícita a menos que se den unas condicio-

[4] En este sentido se pronunciaba el *Libro Blanco sobre el crecimiento, la competitividad y el empleo*, haciendo alusión a la necesidad de un mercado interior de la información semejante al existente para las mercancías, servicios y libre tránsito de personas. Véanse, asimismo, los especialmente considerandos 5, 6, 7 y 8 de la Directiva.

nes de licitud, que son la existencia de un nivel de protección adecuado en el Estado de destino o, en defecto de tal nivel, una de las condiciones que enumera el artículo 26. Mientras que la «protección equivalente» del Convenio 108 aparecía ligada a determinadas categorías de datos cuya naturaleza exigiera una protección especial o instrumentos adicionales de salvaguardia, el «nivel de protección adecuado» no se predica ahora de grupos de datos concretos sino, que hace referencia (artículo 25.2) al grueso de la legislación estatal, a la par que implica el recurso a un completo listado de criterios que convierten al procedimiento de evaluación en un proceso complejo, riguroso y, sobre todo, que torna difícil el reconocimiento de la homologación. Esta exigencia de «nivel de protección adecuada» va a permitir la «legitimación» de la extensión de la directiva fuera del territorio comunitario.

Procedimiento de autorización

Si se observa, por su parte, el procedimiento de autorización, se encuentran argumentos adicionales. En caso de no concesión de la autorización por parte de los Estados miembros o de una decisión no favorable de la Comisión, existen dos alternativas: bien la adopción de garantías adecuadas para paliar la insuficiencia del nivel de protección en el tercer país por parte del responsable del tratamiento, bien la iniciación de negociaciones entre la Comisión y las autoridades nacionales del Estado no miembro.

Los artículos 25, 26 y 31 de la directiva establecen un sistema de competencias compartidas entre las autoridades nacionales de los Estados miembros y la Comisión. En ausencia de decisión de la Comisión, las autoridades nacionales decidirán sobre la autorización o no de las transferencias, sin perjuicio de la información recíproca entre la Comisión y los Estados miembros de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado.

En aras de asegurar la coherencia de las decisiones adoptadas a nivel nacional y las valoraciones que la propia Comisión pudiera emitir, ésta se reserva la facultad de investigar los supuestos de no adecuación a las disposiciones de la directiva, pudiendo adoptar los Estados miembros medidas provisionales de bloqueo de la transferencia si se reúnen las condiciones establecidas en la decisión del artículo 25.6. La Comisión iniciará entonces las negociaciones destinadas a remediar esta situación, teniendo en cuenta el dictamen del Comité consultivo del artículo 31 y según el procedimiento previsto en el artículo 31.2 de la directiva. En todo caso, los Estados miembros habrán de conformarse a la decisión de la Comisión.

Con motivo de las negociaciones que la Comunidad ha entablado con EE UU, se ha redactado un borrador que lleva por título *Description of the procedures established for handling complaints about transfers of personal data to third country recipients who are the subject of an «Adequate protection» finding under article 25.6 of the data protection Directive (95/46/EC)*, que pretende clarificar las competencias entre las autoridades nacionales y las Comisión en la adopción de una decisión sobre el nivel de protección y cuyas líneas generales se exponen a continuación.

Si no existe una decisión en base al artículo 25.6 por parte de la Comisión, la valoración de la «adecuación» es un proceso descentralizado. Ahora bien, el artículo 25.4 establece un proceso en el que cualquier disparidad de criterios se armoniza a nivel comunitario, de tal manera que si la Comisión emite una decisión de autorización, las decisiones nacionales habrán de ajustarse a lo establecido por la Comisión y, por tanto, cualquier bloqueo efectuado habrá de ser levantado. Del mismo modo, las notificaciones o autorizaciones previas exigidas en las legislaciones nacionales serán obviadas o concedidas automáticamente.

En el borrador se establece que aquellos países receptores de los que se afirme que no alcanzan el nivel de protección exigido en la directiva han de tener la certeza de que sus transferencias sólo serán bloqueadas por una decisión de la Comisión, y solamente después de que las autoridades nacionales de estos países (si lo desean) hayan tenido la oportunidad de plantear sus alegaciones. Las acciones nacionales de bloqueo estarían, sin embargo, justificadas en base a las circunstancias excepcionales establecidas en la propia decisión de la Comisión.

Resulta interesante, como comentario a este borrador, establecer una comparación con el mecanismo de cooperación entre autoridades del derecho de la competencia comunitario, recurriendo a la

comunicación de la Comisión relativa a la cooperación entre la Comisión y los órganos jurisdiccionales nacionales para la aplicación de los artículos 85 y 86 del TCEE de 13 de febrero de 1993.

Como se recordará, en derecho de la competencia, el artículo 88 del TCEE confiere plena competencia a la Comisión y a las autoridades nacionales para la aplicación de los artículos 85.1 y 86. Por su parte, el Reglamento 17/62 mantiene esta competencia compartida pero su artículo 9 confiere a la Comisión competencia exclusiva para autorizar acuerdos prohibidos y para expedir declaraciones negativas. La competencia concurrente con las autoridades nacionales para aplicar la prohibición del párrafo primero del artículo 85 y declarar la nulidad del acuerdo, así como para la aplicación del artículo 86, se subordina en el Reglamento 17/62 al hecho de que la Comisión no haya iniciado procedimiento alguno. Sin embargo, la Comunicación de la Comisión de 1993 modifica esta circunstancia, pues la competencia del órgano nacional no desaparece porque la Comisión esté conociendo, sino que «puede aplazar» su decisión —cuando el propio órgano nacional lo considere necesario o apropiado (artículo 22)— o, por el contrario, pronunciarse sobre las cuestiones relacionadas con los artículos 85.1 y 86. Es decir, en definitiva, únicamente la Comisión aplica el artículo 85.3 concediendo exenciones, pero los órganos nacionales pueden ejercer sus competencias respecto del artículo 85.1 cuando se cercioren de que no puede existir exención (por no concurrir notificación de la Comisión o debido a cualquier otra circunstancia). Existe, evidentemente, en esta comunicación, una clara intención de la Comisión de transferir competencias a los órganos nacionales en materia de libre competencia.

En el caso, por el contrario, de los flujos transfronterizos de datos, cualquier intervención de la Comisión bloqueará la actuación de las autoridades nacionales, y éstas habrán de conformarse a la decisión de la Comisión, cualquiera que fuese su pronunciamiento. Este poder decisiorio de la Comisión marcha parejo a la negociación de acuerdos comerciales con los terceros Estados y pone de manifiesto la importancia de retener el control del flujo transfronterizo de datos, un bien del que la Comunidad es crecientemente exportadora.

En la práctica, además, la asunción de competencias por la Comisión se corresponde con un procedimiento de examen a nivel nacional difícil y poco eficaz, a pesar de los esfuerzos del grupo de trabajo por otorgar una metodología eficaz de evaluación de las transferencias. Prueba de ello es la escasísima práctica de las Agencias de Protección de Datos nacionales en esta materia (véanse Informes anuales de 1997 y 1998 del Grupo de Trabajo)[5].

3. El diálogo UE-terceros países en materia de protección de datos personales

La actitud de la UE frente a terceros Estados en materia de protección de datos debe entenderse en un contexto económico donde la importancia de la economía digital está adquiriendo tintes de auténtica revolución. Así, según un informe reciente de la Comisión Europea, se prevé que el volumen de comercio electrónico europeo pase de 17.000 millones de dólares a finales de 1999 a cerca de 360.000 millones de dólares en 2003, duplicándose cada año. Esta cifra, no obstante, está muy lejos de alcanzar el volumen de EE UU, cuya previsión de negocio se eleva hasta los 654.000 millones de dólares, partiendo de los 71.000 millones de 1999.

Junto a lo anterior, la falta de consideración a nivel multilateral de los obstáculos no arancelarios en el comercio electrónico quizá pueda argüirse como justificación de la posición comunitaria[6]. El estado actual de los acuerdos adoptados en el seno de la OMC sobre comercio electrónico —y sus implicaciones para el Anexo sobre Telecomunicaciones del Acuerdo General sobre Comercio de Servicios (GATS)— es todavía muy embrionario[7].

---

[5] *Primer Informe Anual,* DG MARKT/5025/97, WP 3, de 25 de junio 1997; *Segundo Informe Anual,* DG MARKT, D/5047/98 WP 14, de 30 de noviembre 1998.

[6] Existe, no obstante, y precisamente a iniciativa estadounidense, una propuesta a la UNCITRAL para la elaboración de un Convenio Internacional sobre Transacciones Electrónicas que tendría dos objetivos fundamentales: 1) la eliminación de las barreras legales a las transacciones electrónicas y 2) la previsión de un marco efectivo para la autenticación.

[7] El Acuerdo sobre Tecnología de la Información (ATI) de la OMC fue el primer instrumento de carácter multilateral, adoptado por 29 países en la primera Conferencia Interministerial celebrada en Singapur en diciembre de

Así, el actual Acuerdo sobre Tecnologías de la Información (ATI) se ocupa únicamente de la eliminación de aranceles y no de otros obstáculos al comercio. Sin embargo, recientemente, con motivo de la Tercera Conferencia Interministerial celebrada en Seattle en noviembre de 1999, los distintos comités de trabajo elaboraron una serie de informes donde se llegaba a la conclusión de que la inmensa mayoría de las transacciones realizadas a través de Internet son servicios abarcados por el Acuerdo General sobre Comercio de Servicios[8], con lo que podrá concluírse la extensión de las normas del GATS a las actividades de comercio electrónico. Por otra parte, la Organización Mundial del Comercio ha aceptado, a iniciativa de la UE, adoptar soluciones globales e incluir la protección de datos en su agenda de trabajo sobre aspectos relacionados con el comercio electrónico. El objetivo es un acuerdo sobre los principios básicos que permita la libre circulación de datos personales en el comercio electrónico mundial mientras se respeta el derecho a la privacidad de los individuos y se asegura, por tanto, un marco electrónico seguro.

Como ya se ha visto, el artículo 26 de la directiva preveía la posibilidad de entablar negociaciones entre la Comisión y terceros Estados en el supuesto de insuficiencia de protección por este último. La negociación de acuerdos comerciales entre la UE y terceros países ha dado lugar a la inclusión, junto a los aspectos comerciales y de desarrollo económico, de disposiciones sobre protección de datos y de la vida privada, acuerdos que han conducido a un papel preponderante de la Comisión en la determinación de aquellos países a los que se puedan autorizar las transferencias. Al margen de la actividad de la Comisión, la participación de las autoridades nacionales en la concesión de la autorización seguirá, no obstante, revistiendo una importancia capital en cuanto a la constatación del verdadero grado de cumplimiento de la legislación nacional y en relación a sectores de protección concretos.

A pesar de la reciente entrada en vigor de la directiva (octubre de 1998), la Comisión Europea se ha mostrado muy activa en la iniciación de negociaciones con sus principales socios comerciales, y ello máxime cuando el procedimiento previsto en el artículo 25.6 de la directiva todavía no se ha puesto en marcha y, por tanto, no existen decisiones formales de «inadecuación». El diálogo entre la Comisión Europea y los principales socios comerciales de la UE se ha orientado a un mejor conocimiento y comprensión de los distintos sistemas legales y resalta el carácter preventivo de la directiva mencionado anteriormente.

Estas negociaciones se han orientado a los países no firmantes del Convenio 108, que son, además, los principales destinatarios de las transferencias de datos procedentes de la Unión Europea, tal como reconoce la propia Comisión[9]. Y es que, a pesar de la justificación inicial de la directiva en cuanto que pretendía elevar el nivel de exigencia contenido en el Convenio, lo cierto es que los estándares de protección en él establecidos se consideraron suficientes por el Grupo de Trabajo de la Comi-

1996. Este acuerdo —suscrito en la actualidad por 51 países— implica que a partir del 1 de enero de 2000, a más tardar, deberán eliminarse los aranceles y todos los demás derechos y cargas que graven las importaciones de tecnología de la información contempladas en el acuerdo y procedentes de todos los miembros de la OMC. Aunque el acuerdo recoge sólo seis categorías de productos (ordenadores, programas informáticos, equipo de telecomunicaciones, semiconductores, equipo para la fabricación de semiconductores e instrumentos científicos) se están llevando a cabo negociaciones sobre la ampliación del número de productos abarcados (ATI II). En la Segunda Conferencia Ministerial, celebrada el 20 de mayo de 1998 en Ginebra, se adoptó una declaración sobre el comercio electrónico. La declaración instaba al Consejo General de la OMC a establecer un programa de trabajo amplio para examinar todas las cuestiones relacionadas con el comercio electrónico que afectan al comercio, y a presentar un informe sobre los progresos alcanzados en el programa de trabajo al tercer período de sesiones de la Conferencia Interministerial de la OMC. El 25 de septiembre de 1998 el Consejo General adoptó un programa de trabajo sobre el comercio electrónico que reenviaba a los distintos órganos sectoriales —el Consejo del Comercio de Servicios, el Consejo de Comercio de Mercancías, el Consejo de los ADPIC y el Comité de Comercio y Desarrollo— para que presentaran sus respectivos informes, que vieron la luz a finales de julio de 1999. Estos informes pueden consultarse en www.wto.org.

[8] No había acuerdo, no obstante, sobre la clasificación que debiera darse a los bienes o servicios de ciertos productos disponibles en Internet, por ejemplo, libros y soporte lógico.

[9] «Primeras orientaciones sobre las transferencias de datos personales a terceros países. Posibles formas de evaluación», DG MARKT D/5020/97, WP 4, de 26 junio de 1997, página 9.

sión, gozando, pues, los países parte del mismo, de un «nivel de protección adecuado».

Como manifestó el Grupo de trabajo[10], «algunos países pueden resultar "paraísos de datos" para los operadores económicos que busquen menores costes de tratamiento de datos. El objetivo de los acuerdos entre la Comunidad y estos países ha sido simplemente un intercambio de información (una especie de "alerta precoz") junto con una recomendación de que el país en cuestión considere cómo puede garantizar una protección adecuada a las transferencias de datos procedentes de países de la CE. La protección de datos se ha planteado de esta forma con México —rubricado el 23 de julio de 1997— y Paquistán. La lista está en constante crecimiento».

Junto a estos acuerdos mencionados hay que añadir también el Acuerdo de Cooperación entre la Comunidad Europea y Laos (DO L 334 de 5 de diciembre de 1997, páginas 15-23) donde se incluye en el apartado de la cooperación comercial una mención a la supresión de los obstáculos no arancelarios «garantizando, al mismo tiempo, la protección de datos de carácter personal».

Con algunos países las negociaciones han llevado al reconocimiento por parte de la Comisión de un nivel aceptable de protección. Tal es el caso de Japón, donde existe una ley de protección de datos que cubre el sector público, aunque con excepciones, y un proyecto en el sector privado, al mismo tiempo que se ha realizado un gran esfuerzo en materia de autorregulación. Nueva Zelanda y Hong Kong también poseen acuerdos e instituciones con un nivel de protección equiparable al de la CE. Australia y Canadá han adoptado previsiones similares en sus sectores públicos y Quebec goza de legislación aplicable al sector privado.

La directiva debería aplicarse también al Espacio Económico Europeo (EEE), que vincula a la Comunidad con Islandia, Noruega y Liechtenstein, una vez incorporada al acuerdo EEE. Según menciona el Informe de 1998, los trabajos de transposición ya han comenzado en los países no comunitarios que forman parte de este acuerdo. En cuanto a Suiza, la Comisión ha reconocido recientemente la inclusión de este país en la lista de aquéllos que gozan de una protección adecuada.

Por lo que respecta a los países de Europa Central y Oriental, la Comisión, en su Libro Blanco donde fijaba la estrategia de preparación para la adhesión a la UE de estos países, recomendó, como primera etapa en el campo de la protección de datos, que estos países se adhirieran al Convenio 108 del Consejo de Europa, previéndose en 1997, al inicio de las negociaciones de adhesión, una estrategia de preadhesión reforzada que permitiera a largo plazo la integración del acervo comunitario. Existen ya leyes de protección de datos aprobadas en Estonia, Polonia, Eslovaquia o, en tramitación legislativa, en Bulgaria, Letonia, Rumanía, República Checa y Eslovenia. En el caso de Hungría, una reciente decisión de la Comisión lo ha reconocido como país con nivel de protección adecuada[11].

Especial mención merecen, sin embargo, las negociaciones UE-Estados Unidos. Paralelamente a las negociaciones iniciadas por la UE, Estados Unidos se había dedicado a raíz de la publicación del documento «A framework for Global Electronic Commerce», en julio de 1997, a una intensa campaña de información y búsqueda de compromisos sobre los principios que el gobierno estadounidense había establecido como marco para la economía digital, y en especial en el tema que estamos tratando, sobre el papel preponderante de la iniciativa privada en el desarrollo de la red[12]. El grado de obligatoriedad de estas conversaciones quedará en la simple declaración de principios, pero el número de declaraciones suscritas y, sobre todo, el hecho de que fueran algunos países europeos los firmantes, demostraba

[10] *Primer Informe Anual,* ibídem, punto 2.5.

[11] El Grupo de Trabajo del artículo 29 de la directiva emitió un dictamen de fecha 7 de septiembre de 1999, por el que recomendaba a la Comisión y al Comité del artículo 31 de la directiva, el reconocimiento de Hungría como país garante de un nivel de protección adecuado. (dictamen 6/99 sobre el nivel de protección de los datos personales en Hungría, de 7 de septiembre de 1999, WP 24, 5070/FR/99/final).

[12] El eje central de las discusiones se centraba en el hecho de que el acercamiento de Estados Unidos a la protección de los datos personales estaba basado en un acercamiento sectorial, mezcla de legislación y autorregulación, poco acorde con la normativa comunitaria única y vinculante para los Estados miembros.

que EE UU estaba dispuesto a asumir la iniciativa en el control del comercio electrónico mundial: Irlanda (septiembre de 1998); Holanda (octubre de 1997); Corea (noviembre de 1998); APEC (noviembre de 1997); UE (diciembre de 1997); Japón (mayo de 1998); y Francia (junio de 1998).

La Unión Europea se vio, por tanto, en la necesidad de entablar negociaciones con EE UU que fueran más allá de las meras declaraciones de intenciones, negociaciones que se han venido desarrollando desde 1997 y que concluyeron en un acuerdo formal en julio de este mismo año[13]. Los interlocutores, la Comisión Europea y el Departamento de Comercio estadounidense, centraron su diálogo en los llamados «principios de puerto seguro» que constituyen un sistema voluntario ofrecido a las entidades de EE UU basado en la autocertificación y la autoevaluación, respaldado por disposiciones legales en caso de prácticas desleales o fraudulentas.

Dado su carácter voluntario, la adhesión a estos principios puede derivarse bien de un programa autorregulador propio que se adecue a los principios de puerto seguro, bien en la sujeción a normas estatutarias o administrativas que protejan la privacidad de forma idéntica a aquéllos. Los principios de puerto seguro surten efecto desde que cada organización autocertifica en el Departamento de Comercio (o la institución que éste designe) su adherencia a los principios de puerto seguro. No existe, pues, ningún tipo de verificación *a priori*, por lo que aunque se insista en que sus normas son obligatorias para todas las empresas que decidan asumirlos, las facultades de supervisión de un organismo público son esenciales para la credibilidad del acuerdo.

Los exportadores de datos comunitarios que deseen comprobar si su socio norteamericano —el destinatario de los datos— goza de la certificación de puerto seguro, podrán acudir al listado disponible en el Departamento de Comercio estadounidense. Las empresas que opten por permanecer al margen de estos principios, podrán beneficiarse no obstante de las excepciones permitidas en el artículo 26.1 de la directiva (por ejemplo, los datos transmitidos con previo consentimiento del particular) o se les exigirán salvaguardias alternativas como por ejemplo, un contrato (artículo 26.2).

Las jurisdicciones competentes para vigilar la observancia del «puerto seguro» serán la *Federal Trade Commission* y el *US Department of Transportation*[14], en el caso del transporte aéreo. La competencia de la FTC viene determinada en función de la sección 5 de la *Federal Trade Commission Act* que establece que son ilegales los actos desleales o fraudulentos si afectan «*unfair or deceptive acts or practices in or affecting commerce*» (15 U.S.C. § 45 (a) (2)), por lo que la FTC no tendrá jurisdicción sobre la recogida y uso de información personal para propósitos no comerciales, como sería en el caso de una fundación benéfica. Sin embargo, el uso de información personal en cualquier transacción comercial satisfará las premisas de su jurisdicción. Así, por ejemplo, la venta por un empresario de información personal de sus empleados a una empresa de marketing directo entraría dentro del ámbito de la sección 5.

Llegados a este punto, y si se estudia con algo de detenimiento el régimen de reparto de competencias en el derecho norteamericano, se observarán varias cuestiones de especial interés en el tema que se está tratando.

En primer lugar, la sección 5 excluye de su ámbito de aplica-

[13] Los principales antecedentes de estas negociaciones, que arrojan luz suficiente sobre la postura inicial de las partes, sobre las discrepancias y los puntos de acuerdo, los encontramos en el Proyecto de los Principios Internacionales de puerto seguro de 15 de noviembre de 1999; el Borrador de las Preguntas Más Frecuentes (o FAQ) de 15 de noviembre de 1999; el Resumen de la Decisión adoptada en virtud del apartado 6 del artículo 25; la Carta de David Aaron a John Mogg a la que adjunta los principios de puerto seguro y las FAQ de 16 de noviembre de 1999; y la Carta de John Mogg a David Aaron a la que adjunta la Decisión adoptada en virtud del apartado 6 del artículo 25 de 16 de noviembre de 1999. Estos documentos se pueden consultar en http://www.ita.doc.gob/td/ecom/menu.htm.
Por su parte, la respuesta del Grupo de Trabajo a las propuestas estadounidenses, Dictamen 7/99, aprobado el 3 de diciembre de 1999, y el Dictamen 4/2000 sobre el nivel de protección que proporcionan los «principios de puerto seguro», de 16 de mayo de 2000, pueden consultarse en http://www.europa.eu.int/comm/dg15/en/media/dataprot. El texto de la Decisión de la Comisión, por el que se llega a un acuerdo con el Gobierno estadounidense, aunque todavía no ha sido formalmente adoptada, puede consultarse en la dirección anterior.

[14] La competencia del *Department of Transportation* le viene dada sobre la base del Título 49 del *United States Code* Section 41712.

ción ciertos sectores como los servicios financieros (bancos y entidades aseguradoras), telecomunicaciones, transportes y empresas manipuladoras de productos alimenticios, que quedan al margen de las competencias de la FTC. La pregunta que surge en estos casos es si estos sectores —¡tan relevantes a efectos del tratamiento de datos!— quedan completamente al margen del Acuerdo UE-EE UU: pues bien, la respuesta es afirmativa y un breve repaso al entramado legislativo estadounidense, con concurrencia de normativas estatales y federales, confirma esta aserción.

En efecto, al margen de la FTC, serán otras entidades públicas con competencias similares las que vigilen la actuación de las empresas sometidas a su jurisdicción cuando la actuación de aquéllas atente contra los datos personales de los particulares. Como se mencionó anteriormente, la falta de evaluación previa por el Departamento de Comercio de la adecuación a los principios de «puerto seguro», por parte de las empresas que se acojan a los mismos, hace recaer todo el peso del sistema en los órganos de supervisión. En este punto, la normativa norteamericana establece un sistema de competencias separadas, pero en algunos casos concurrentes, que conviene mencionar aunque sea sólo someramente. Así, para las instituciones financieras tienen competencias reguladoras la *Federal Reserve Board*, la *Office of Thrift Supervision* y la *National Credit Union Administration Board*. Se establece una jurisdicción separada entre las instituciones financieras y la FTC, y estos organismos tienen competencia para dictar los reglamentos necesarios para impedir dentro de su ámbito las prácticas desleales o engañosas, fijando, no obstante, la sección 5 una cierta homogeneidad de actuación, al establecer que, cuando la FTC dicte una norma sobre prácticas desleales o engañosas, las entidades financieras deberán adoptar regulaciones paralelas en el plazo de 60 días (15 U.S.C. § 57 A(F) (1)).

Del mismo modo, en el caso de los transportes interestatales, los transportistas estarán sujetos al *United States Code* (Subtitle IV Title 49) y a la *Communications Act* de 1934 (47 U.S.C. § 151 *et seq.*), y a la jurisdicción de la *Surface Transportation Board*, una agencia independiente dentro del Departamento de Transporte (49 U.S.C. §§ 10501, 13501, y 15301), y, en el caso de las telecomunicaciones, por la *Federal Communications Commission* (FCC). Sin embargo, los operadores de televisión, operadores de cable y emisoras de radio, no están propiamente incluidos dentro de la excepción de la sección 5 de la *FTC Act*, por lo que la FTC tiene jurisdicción para investigar las posibles prácticas desleales o engañosas de estas empresas, mientras que la FCC tendrá una jurisdicción concurrente en las materias de su competencia[15].

Del mismo modo, los transportistas aéreos norteamericanos o extranjeros que están sujetos a la *Federal Aviation Act* de 1958 están también exentos de la *FTC Act*. En estos casos, la Secretaría de Transporte puede investigar si un transportista aéreo ha incurrido en una práctica desleal o engañosa.

Junto a toda esta maraña de competencias a nivel federal, hay que añadir que todos los Estados de la Unión, junto con el Distrito de Columbia, Guam, Puerto Rico y las Islas Vírgenes Norteamericanas, han promulgado leyes similares a la *Federal Trade Commission Act* y, en todos estos casos, una agencia independiente tendrá la responsabilidad de investigar este tipo de infracciones.

Pero en definitiva, ¿cómo se protegería el derecho a la vida privada en relación con los datos transferidos a Estados Unidos si no se respetasen los principios de «puerto seguro»?

En primer lugar, cabe una alternativa no judicial o administrativa de los conflictos planteados por la falta de conformidad a los principios. Muchas empresas con el marchamo del «puerto

[15] La *Communications Act* da a la FCC competencias para vigilar la normativa sobre privacidad, ya por propia iniciativa o en respuesta a una denuncia. Si la FCC determina que un operador de telecomunicaciones (incluyendo un operador de cable) ha violado la normativa sobre privacidad de la sección 222 o sección 551, hay tres acciones básicas. Primero, tras la apertura de un procedimiento y la determinación de la violación, la Comisión puede imponer al operador una compensación económica. Alternativamente, la FCC puede ordenar al operador el cese de las prácticas ofensivas o, en su caso, de la omisión. Finalmente, la Comisión puede ordenar al operador que adecue su comportamiento a la normativa o práctica que aquélla prescriba. Por su parte, los particulares que consideren que un operador de cable ha violado las previsiones de la *Communications Act* o de la *Cable Act* puede, bien interponer una denuncia ante la FCC, o acudir a los tribunales federales. (47 U.S.C. § 207).

seguro» podrán ser auditadas anualmente por una entidad independiente como es el caso de *BBB online*, *Webtrust* y *Trust-e*, pero estas auditorías no se han impuesto como obligatorias con el fin de no desincentivar a las pequeñas y medianas empresas a adherirse a estos principios.

Si las empresas de «puerto seguro» no cumplen las decisiones de estas entidades independientes, los casos se notificarán a la *Federal Trade Commission* o al *Departament of Transportation*. En el caso de que no cumplan con los dictados de estos organismos, se podrá excluir a estas empresas del listado del Departamento de Comercio, junto con la facultad de la *Federal Trade Commission* de tomar medidas provisionales.

Resulta a todas luces patente que este sistema presenta un alto grado de imperfección por varios motivos: en primer lugar, los organismos de resolución de litigios deberían notificar a la FTC los casos de incumplimiento de los principios, pero no tienen la obligación de hacerlo. Además, aunque las personas afectadas pueden presentar una denuncia directamente a la FTC, no existen garantías de que ésta examine su caso (tiene potestad discrecional). Por tanto, los particulares no tienen derecho a ser oídos ante la FTC ni a hacer cumplir, ni a recurrir las decisiones de los organismos de resolución alternativa de litigios (o la no adopción de las mismas). En segundo lugar, porque el esquema competencial norteamericano anteriormente expuesto resultará muy complicado para los litigantes extranjeros —consumidores— que resulten afectados. Por último, porque los sectores afectados por las exclusiones —telecomunicaciones, banca, seguros y, en menor medida, transportes— determinarán en un futuro no muy lejano gran parte del volumen del flujo de los datos personales, con lo que la efectividad práctica del sistema resulta harto mermada.

A falta de solución administrativa válida, la vía judicial tampoco ofrece muchos alicientes. Si ya se pusieron de manifiesto en el ámbito comunitario las dificultades de entablar acciones transnacionales para los ciudadanos comunitarios[16], cuánto más en un contexto donde no sólo los costes judiciales, sino la falta de armonización judicial desincentivará al actor de obtener un resarcimiento justo a la violación de sus derechos.

A pesar del esquema anterior, las autoridades nacionales de la Comunidad se retienen algunos poderes de intervención. Las autoridades competentes en los Estados miembros pueden suspender las transferencias de datos cuando la organización exportadora haya sido declarada culpable por una instancia competente, o bien cuando exista probabilidad de que viole esos principios (artículo 3, Decisión de la Comisión).

Finalmente, si atendemos a las cuestiones sustantivas, el acuerdo no ofrece ninguna destacable. Se ratifica la inclusión de todos los principios incluídos en las Directrices sobre protección de la vida privada de la OCDE, adoptadas por Estados Unidos, y ratificadas en la Conferencia de Ottawa de octubre de 1998. La confianza depositada en estos principios es significativa puesto que una de las justificaciones esgrimidas para dictar la directiva comunitaria fue la de elevar el nivel de protección por encima del establecido en el Convenio 108 del Consejo de Europa y de las Directrices de la OCDE.

Se reafirma, además, la visión unidireccional de estos principios desde el momento en que «los principios de "puerto seguro"» están diseñados para controlar el tratamiento de los datos transmitidos a EE UU por responsables de ficheros de la UE. En relación con la recogida de datos personales de los particulares en la UE, el Grupo de Trabajo recuerda que normalmente serán de aplicación las disposiciones legislativas nacionales por las que se transpone la directiva, pero no se hace mención de nuevo al trato que deba darse a las entradas de datos en la Comunidad. Nuevamente parece que las preocupaciones comunitarias se dirigen más hacia un intento de evitar que las diferencias entre los estándares de protección norteamericanos y los comunitarios puedan revertir en perjuicio de la industria comunitaria.

4. Las soluciones contractuales

La ausencia, hasta el momento, de soluciones multilaterales efectivas ha dejado paso a las iniciativas autorreguladoras, aunque desde dos perspectivas diferentes: una, propugnada por los

[16] *Access to Justice in Europe- A Single Market for Litigants?*, Hanno von FREYHOLD, 1999.

países más fieles a la tradición liberal, como en el caso de EE UU y otra, defendida por la UE, que ve en la iniciativa privada un complemento necesario allí donde fallan los instrumentos normativos.

Si atendemos a los sujetos que intervienen, estos instrumentos pueden ser de dos tipos: a) las iniciativas procedentes de la comunidad empresarial y los grupos profesionales que han intentado establecer códigos de conducta —*soft law*— como métodos de unificación jurídica complementarios —o sustitutivos— de la iniciativa reguladora; y b) la redacción de contratos que regulen entre el particular, sujeto de los datos, y las entidades transmisora y destinataria las obligaciones a las que se somete la transferencia internacional de datos.

La iniciativa privada ha tenido distinta acogida en los diferentes Estados. Así, la filosofía reguladora estadounidense ha estado siempre basada en un principio de mínima intervención estatal y la distribución de poderes entre las autoridades estatales y federales. Este principio se manifestaba también en las relaciones exteriores de EE UU al extender a terceros Estados su convicción de que el crecimiento del comercio electrónico había de dejarse en manos de la iniciativa privada.

Así, en la Declaración común sobre comercio electrónico entre Australia y EE UU, de 13 de noviembre de 1998, se apostaba por la autorregulación como principio rector de todas las cuestiones atinentes a la sociedad de la información. Así se afirmaba: «Competitive market-based solutions to specific issues for the information economy will promote optimal growth and benefits. Governments should avoid imposing unnecessary regulations. When regulation is necessary, they should rely on a "light touch" regulatory environment. Where the market alone will not solve problems, self-regulation gives maximum control and responsibility to the individual and should be the preferred approach. In some cases this may need to be facilitated by legislation to ensure effective arrangements. In light of the global nature of e-commerce, government-based or industry-based approaches should be coordinated and harmonized domestically and internationally, as far as possible.»

En Europa, por el contrario, existió siempre el consenso sobre la necesidad de que los datos personales estuvieran amparados por un marco legislativo que cubriera todos los sectores económicos y que estableciera mecanismos adecuados de protección y de sanción en caso de violación de derechos. De ahí la necesidad de que el proceso de protección fuera controlado en un principio por las autoridades nacionales. Sin embargo, la Directiva 54/96 dejaba cierto margen de maniobra para su implementación por los actores del mercado. Así, el Considerando 61 de la directiva afirmaba que los Estados miembros y la Comisión, en sus respectivas esferas de competencia, promoverán que las asociaciones comerciales y otras organizaciones representativas establezcan sus códigos de conducta para facilitar la aplicación de la directiva teniendo en cuenta las características específicas del procesamiento en ciertos sectores, y respetando las previsiones nacionales adoptadas para su implementación.

Las medidas contractuales pueden venir impuestas no sólo *ex ante* y de forma totalmente generalizada, sino también para un caso particular. Así, el artículo 26.2 establece la posibilidad de que, en caso de ausencia de protección adecuada en el sentido del artículo 25.2, sea el responsable del tratamiento el que ofrezca las garantías para paliar la insuficiencia del nivel de protección en un tercer país, pudiendo concretarse en cláusulas contractuales apropiadas, decisión que después deberá notificarse por los Estados miembros a la Comisión. En caso de oposición a la autorización, la Comisión puede anular o confirmar la decisión, de acuerdo con el procedimiento de comitología establecido en el artículo 31. Además de las autorizaciones de los Estados miembros, el artículo 26.4 de la directiva permite a la Comisión, también de acuerdo con el procedimiento de comitología establecido en el artículo 31, juzgar si ciertas cláusulas contractuales tipo ofrecen las garantías suficientes. La valoración que emita es también vinculante para los Estados miembros[17].

[17] «Primeras orientaciones sobre las transferencias de datos personales a terceros países. Posibles formas de evaluación», DG MARKT D/5020/97, WP 4, de 26 junio de 1997.

Sin embargo, el recurso a las soluciones privadas es criticable por varias razones. En primer lugar, y en el caso de la directiva, el recurso a las soluciones contractuales aparece como consecuencia de la imposibilidad para los Estados miembros de garantizar un examen detallado de todos los casos que se les presenten[18].

En segundo lugar porque, en cualquier caso, las bases para afirmar la adecuación de las salvaguardas del contrato son las mismas que las bases establecidas para evaluar con carácter general al tercer país, por lo que todas las críticas procedimentales que se han apuntado anteriormente resultan perfectamente trasladables a este caso. Puede ocurrir que la solución contractual sea el medio más adecuado en situaciones donde las transferencias de datos son similares y repetitivas pero, en cualquier caso, la efectividad final dependerá de que existan en el tercer país entidades de supervisión de estas transferencias[19] o, en su defecto, del reconocimiento de las decisiones de la autoridad del primer país[20]. El principio de mínima intervención inspirador de los contratos choca, en el caso europeo, con la reciente propuesta del Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales de incluir la protección de datos de carácter personal en la futura Carta Europea de Derechos Fundamentales[21], y con la tradición constitucional de protección reforzada de estos derechos. Esta disposición de la directiva autorizando los contratos no dejará de producir problemas, porque una cosa es el establecimiento de compromisos y garantías para que la transferencia pueda llevarse a cabo y otra la ejecución de las mismas, en los supuestos de incumplimiento de las condiciones en las que se basó la autorización de la transferencia.

Por último, por su falta de eficacia. En un estudio realizado en 1998 por la *Federal Trade Commission* entre las asociaciones de comerciantes y los grupos industriales sobre sus prácticas de protección en la red, sólo un 14 por 100 de los sitios consultados —sobre 1.400— daban algún tipo de información a sus clientes sobre sus prácticas de recogida de datos, mientras que sólo un 2 por 100 disponían de una estrategia completa de protección de la privacidad[22].

5. Conclusión

A modo de conclusión, podemos afirmar que estamos asistiendo en los últimos años a la progresiva consideración de las normativas en materia de protección de datos como barreras técnicas al comercio internacional, lo que sin duda se reflejará en los próximos años en las negociaciones del GATS.

Si bien es cierto que las acciones concertadas permitirán un aumento de la eficacia y seguridad jurídicas, impidiendo la constitución de paraísos informáticos, se corre el riesgo, en aras de conseguir un consenso multilateral, de concebir únicamente los flujos internacionales de datos en su vertiente económica.

---

[18] Véanse a este respecto las otras soluciones propuestas por el Grupo de Trabajo en el documento antes citado.

[19] DUMORTIER, J. y GOEMANS, C., *op. cit.,* página 13.

[20] *«An audit has revealed that American company Experian has revealed the financial records of up to 1.5 million South Africans including names, addresses and identity, telephone and cellphone numbers and bank account details. The records were on customers of Vodac, the Banking Council, Nedcor, First National Bank and Standard Bank»* (*Africa News,* 5 de agosto de 1999). En el mismo sentido, la fusión entre Double Click y la mayor empresa estadounidense de marketing, Abacus Direct, se ha visto como una amenaza a la privacidad de los usuarios de la red cuyos datos son recogidos mediante *cookies.* EPIC —Electronic Privacy Information Center— ha interpuesto una demanda ante la Federal Trade Commission contra estas compañías en relación con sus prácticas de recogida de información. Alega que Doubleclick —una empresa líder en la publicidad en Internet— recoge los datos sobre la actividad de los usuarios en Internet y los combina con sus datos personales contenidos en una base de datos nacional. (www.epic.org).

[21] Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, Dictamen 4/99 sobre la inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales, aprobado el 7 de septiembre de 1999. WP 26, 5143/99/FR/final. Además, el nuevo artículo 286, incluido en el TUE, dispone que los actos comunitarios relativos a la protección de las personas físicas en lo que concierne al tratamiento de los datos personales son aplicables, a partir del 1 de enero de 1999, a las instituciones y órganos de la UE.

[22] *First Annual Report,* U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, 1998, página 16.

En este sentido, las soluciones contractuales pueden constituir una solución complementaria en ciertos casos a los instrumentos normativos. Dado que el consumidor-afectado se encontrará siempre en una situación más comprometida en cuanto al control sobre sus datos personales, será aconsejable establecer un control riguroso sobre estos documentos contractuales. No obstante, el peso de la regulación deberá recaer todavía durante un tiempo en los Estados, si se quiere proteger debidamente a los consumidores y armonizar de manera efectiva esta normativa.

Referencias bibliográficas

[1] AGENCIA DE PROTECCION DE DATOS (1999): *Memoria Anual 1998*.

[2] 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. DO L 281 de 23-11-1995, páginas 31-50.

[3] DIRECTORATE-GENERAL INTERNAL MARKET AND FINANCIAL SERVICES (1998): *Handbook on Cost-effective Compliance with Directive 95/46/EC*.

[4] DUMOTIER, J. y GOEMANS, C. (1999): *Personal Data Protection in the Digital Economy: The Role of Standardisation*.

[5] ESTADELLA, O. (1999): «La transmisión internacional de datos personales y su control», Jornadas sobre el Derecho español de la protección de datos personales, Madrid, 28, 29 y 30 de octubre, Agencia de Protección de Datos.

[6] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1997): *Primer Informe Anual*, 25 de junio de 1997, DG MARKT/5025/ 97, WP 3.

[7] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1997): *Primeras orientaciones sobre las transferencias de datos personales a terceros países. Posibles formas de evaluación*, DG MARKT D/5020/97, WP 4, de 26 de junio.

[8] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1998): *Documento de Trabajo: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?*, 14 de enero de 1998, 5057/97 final, WP 7.

[9] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1998): *Segundo Informe Anual*, DG MARKT, D/5047/98 WP 14, de 30 de noviembre.

[10] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1999): *Dictamen 5/99 sobre el nivel de protección de los datos personales en Suiza*, 7 de junio de 1999, 5054/99/final, WP 22.

[11] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1999): *Documento de Trabajo sobre el estado del debate entre la Comisión Europea y el Gobierno de Estados Unidos acerca de los «Principios internacionales de puerto seguro»*, 7 de julio de 1999, 5075/88/ES/final, WP 23.

[12] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1999): *Dictamen 6/99 sobre el nivel de protección de los datos personales en Hungría*, 7 de septiembre de 1999, 5070/FR/99/final, WP 24.

[13] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1999): *Dictamen 4/99 sobre la inclusión del derecho fundamental a la protección de datos en el catálogo europe de derechos fundamentales*, aprobado el 7 de septiembre de 1999, WP 26, 5143/99/FR/final.

[14] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1999): *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 EE UU*, 3 de diciembre de 1999, 5146/99/ES/final, WP 27.

[15] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (2000): *Opinión 3/2000 sobre el diálogo UE-EE UU sobre el acuerdo de «puerto seguro»*, DG MARKT 5019/00, WP 31.

[16] GRUPO DE TRABAJO DE LA UE SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (2000): *Dictamen 4/2000 sobre el nivel de protección que proporcionan los «principios de puerto seguro»*, 16 de mayo de 2000, D MARKT CA07/434/00, WP 32. Todos estos informes se pueden consultar en http://www.europa.eu.int/comm/dg15/en/media/dataprot.

[17] HEREDERO, M. (1997): *La Directiva comunitaria de protección de datos de carácter personal*, Madrid.

[18] INTERNATIONAL CHAMBER OF COMMERCE (1998): *Model Clauses for Use in Contracts Involving Transborder Data Flows*, 23 de septiembre.

[19] OCDE, (1998): *Implementing the OECD «Privacy Guidelines» in the Electronic Environment: Focus on the Internet*, Group of Experts on Information Security and Privacy, 9 de septiembre, DSTI/ICCP/REG (97) 6/final.

[20] OCDE, (1998): *Privacy Protection in a Global Networked Society*, 29 de julio, DSTI/ICCP/REG (98) 5/final.

[21] OCDE, (1998): *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 de septiembre de 1980.

[22] OCDE, (1997): *Dismantling the Barriers to Global Electronic Commerce*, noviembre.

[23] OCDE, (1998): *A Borderless World: Realising the Potential of Global Electronic Commerce*, octubre.

[24] U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE (1998): *First Annual Report*, noviembre.

[25] U.S. DEPARTMENT OF COMMERCE (1998): *The Emerging Digital Economy*, abril.

[26] VN FREYHOLD, H. (1999): *Access to Justice in Europe- A Single Market for Litigants?*