LA REGULACIÓN DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL COMO BARRERA AL COMERCIO INTERNACIONAL: DE LA DIRECTIVA 95/46 A LOS ACUERDOS UE-TERCEROS ESTADOS

Por HELENA ANCOS FRANCO

SUMARIO

1. REFLEXIONES PRELIMINARES SOBRE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS. SU DIMENSIÓN ECONÓMICA Y JURÍDICA

La convergencia de la informática y las telecomunicaciones y el desarrollo de redes abiertas ha estimulado poderosamente el movimiento internacional de datos personales con el consiguiente riesgo de violación de la intimidad.

La implementación de redes globales y 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[1].

El flujo transfronterizo de datos de carácter personal y el diseño de una normativa reguladora eficaz constituyen un auténtico desafío para el Derecho Internacional Privado. Y ello por varios motivos. En primer lugar, por la creciente dimensión económica que está cobrando el libre tránsito de la información. El acceso y uso de la información por parte de empresas, administraciones e individuos, se ha convertido en un precioso bien intangible causa y efecto a la vez de la progresiva integración económica y social. Así, el «*Libro Blanco sobre el crecimiento, la competitividad, y el empleo*» reconocía el cambio irreversible hacia una sociedad de la información y la necesidad de la creación de un área de información común dentro de la Comunidad, similar a la existente para las mercancías, los servicios y el libre tránsito de personas.

En segundo lugar, porque junto a la dimensión económica, proteger los datos personales y la intimidad supone afrontar por vez primera la difícil tarea de cohonestar los Derechos Humanos y las Libertades Fundamentales con el comercio internacional y ello, en las distintas esferas jurídicas implicadas. La búsqueda de una solución que ampare ambos intereses en las transferencias internacionales de datos (TID) en un contexto global no es fácil, debido sobre todo, a las diferencias entre los distintos niveles de protección de los derechos y libertades de las personas y su intimidad existentes entre distintos estados. En este sentido, la búsqueda de soluciones uniformes ha de superar las distintas calificaciones en las categorías de datos personales y los distintos intereses económicos en juego, dada la original vinculación de los datos con el desarrollo del comercio internacional. Las acciones concertadas permitirían además de un aumento de la eficacia y la seguridad jurídicas, la consecución de economías sobre los costes de circulación internacional de la información, impidiendo la constitución de paraísos informáticos y la deslocalización de actividades informáticas.

[1] Así ocurre por ejemplo con la recogida de datos a través de *cookies* o los datos *clickstream* en Internet. «La preocupación de un gran número de usuarios de Internet es que la revelación de información personal que les afecta se genera, colecta, almacena, interrelaciona y se pone a disposición de muchos usos automáticamente, incluidos los fines comerciales. Este miedo se convierte en un problema para el comercio en Internet y es un obstáculo importante para el desarrollo del comercio electrónico». *Implementing the OECD «Privacy Guidelines» in the electronic environment: focus on the Internet.* October 1997, p. 11.

En tercer lugar, la especial volatilidad de las transferencias de datos complica extraordinariamente la definición del derecho sustantivo aplicable, en lo que algunos autores han calificado acertadamente como una «desterritorialización cualificada». Las características de los flujos de información y el carácter abierto de las redes hacen que los datos puedan ser accedidos, recopilados y tratados desde varios países de manera simultánea, por lo que distintos estados tendrán competencia normativa para definir los términos y las condiciones de las prácticas apropiadas en el ámbito de la información.

La preocupación por la regulación de la protección de los datos personales no es nueva. El Convenio 108 del Consejo de Europa marcó el inicio de una serie de instrumentos regulatorios que tendrían su continuidad en la Directiva 95/46/CE sobre protección en el tratamiento de datos personales y la libre circulación de esos datos[2], en la más específica 97/66 relativa al tratamiento de los datos personales y protección de la intimidad en el sector de las Telecomunicaciones[3] o en su toma en consideración en el art. XIV del GATS como excepción legítima al comercio internacional de servicios. Al mismo tiempo, iniciativas procedentes de la comunidad empresarial y los grupos profesionales, han intentado establecer códigos de conducta —*soft law*— como métodos de unificación jurídica complementarios a la alternativa reguladora. Junto a las anteriores, la redacción de contratos que regulen entre las partes implicadas las obligaciones a las que se somete la transferencia internacional de datos, se presenta también como una solución válida.

En este contexto, las disposiciones de la Directiva reguladoras de la transferencia de datos a países no comunitarios han provocado la preocupación de gobiernos y operadores económicos no comunitarios en la medida en que su aplicación puede representar un obstáculo a la libre transferencia de datos. En particular, el diálogo UE-EEUU sobre el nivel de protección de los datos en sus respectivas legislaciones ha sido muy revelador del creciente papel desempeñado por la protección de los datos en el comercio internacional.

El presente artículo pretende abordar la necesidad de una regulación

[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, 23 de noviembre de 1995, p. 31.

[3] Directiva 97/66/CE del 15 de diciembre de 1997, DO L 24 de 30.1.1998, p. 1.

de los flujos internacionales de datos desde la triple dimensión apuntada. Y es que si la intención de la Directiva comunitaria era la elevación del nivel de exigencia reflejado en el Convenio 108 del Consejo de Europa, a través de la introducción de requisitos sustantivos y procedimientos de control adicionales, la letra de la Directiva desemboca en una aplicación extraterritorial de las normas y en un papel preponderante de la Comisión en la vigilancia de tales transferencias frente a la actuación de las autoridades nacionales. Esto, junto al hecho de que la Directiva sea el primer supuesto de protección de los Derechos Humanos a través del derecho derivado[4] en una materia tan sensible desde el punto de vista de la competitividad internacional y donde es difícil diseñar soluciones tecnológicamente neutrales, justifica su estudio pormenorizado.

2. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN LA DIRECTIVA 95/46/CE. EL CRITERIO DE LA «PROTECCIÓN ADECUADA». PROBLEMAS SUSTANTIVOS Y PROCEDIMENTALES

Los acercamientos multilaterales a la regulación de las transferencias internacionales de datos tienen su origen en el Convenio de Estrasburgo de 28 de enero de 1981, que va a constituir el antecedente más directo de la Directiva 95/46. Ambos textos legislativos van a tener su justificación en la necesidad de uniformar las distintas regulaciones nacionales en una materia que por su especificidad reclamaba inexcusablemente criterios normativos homogéneos[5].

Sin embargo, los buenos propósitos de armonización que se arrogaba el Convenio del Consejo de Europa al «asegurar para todo particular, cualquiera que sea su residencia o nacionalidad, en el territorio de cada Parte, el respeto de sus derechos y libertades fundamentales, y en particular

[4] PIERCE, G. and PLATTEN, N. «Achieving Personal Data Protection in the European Union», *Journal of Common Market Studies*, Vol. 36, n.º 4, pp. 529-47.

[5] En puridad, el origen de la normativa convencional en esta materia la 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 de las libertades fundamentales de 4 de noviembre de 1950. Habrá que esperar, sin embargo, a las Líneas Directrices de la OCDE de 1980, para encontrar el primer texto que, aunque con carácter no vinculante, recogía una relación completa y coherente de medidas protectoras del manejo de información personal.

el derecho a su privacidad, respecto del tratamiento automatizado de sus datos personales», resultaron en un fracaso relativo en su consecución.

En efecto, por un lado, no sólo el Convenio no había sido ratificado por todos los Estados comunitarios, sino que establecía normas materiales mínimas (art. 4.1), lo que dejaba en manos de los Estados la implementación de las medidas necesarias para que los principios básicos del Convenio fuesen efectivos. Por otra parte, pronto se vio que los objetivos del Convenio quedaban seriamente comprometidos pues entre las lagunas que presentaba su regulación, se encontraba la falta de previsión para los supuestos de transferencias de datos a terceros Estados.

Con este referente, la Directiva va a pretender elevar el nivel de protección del Convenio, promoviendo al propio tiempo, la adhesión al mismo de todos los países miembros de la Comunidad. Precisamente, una de las novedades era la inclusión de las transferencias internacionales de datos (TID) en el texto de la Directiva, frente al tratamiento tangencial que el art. 12 del Convenio hacía de las relaciones entre los flujos transfronterizos de datos de carácter personal y el derecho interno.

En su regulación de las TID, la Directiva recogerá el acercamiento bifronte *protección de la intimidad-libre circulación de datos personales* que inspiraba el Convenio, sin embargo, los condicionantes del mercado interior determinarán que este equilibrio aparezca claramente escorado hacia la promoción de la libertad de tránsito y la eliminación de barreras a la entrada de dichos flujos.

Particularmente revelador de esta circunstancia es el hecho de que sea el art. 95 (antiguo art. 100A) TCE el que haya servido de fundamento a la Directiva y no el art. 293 (antiguo art. 220) TCE, pese a que como se menciona en este último: «Los Estados miembros entablarán, en tanto sea necesario, negociaciones entre sí, a fin de asegurar en 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 este mismo sentido, la protección comunitaria se articula sobre el establecimiento de un espacio liberalizado *ad intra* y con fuertes restricciones *ad extra*, admitiéndose únicamente la transferencia activa o pasiva de datos personales entre un Estado miembro y terceros Estados cuando éstos garanticen un *nivel de protección adecuado.*

Pero ¿suponía realmente la nueva regulación de la directiva una mejo-

ra de las disposiciones del Convenio o más bien el deseo de exportar la normativa comunitaria? ¿Ofrecía el Convenio un nivel suficientemente satisfactorio de protección que hiciera innecesaria la promulgación de la directiva?

La tesis que nos planteamos en este artículo pretende avanzar en el sentido de la exportación de los estándares de protección comunitarios. Y por ello, en orden al análisis y búsqueda de respuestas a estos interrogantes, recurriremos a un análisis comparado de los criterios del Convenio 108 y de la Directiva, atendiendo al ámbito de aplicación de la Directiva (2.1), a criterios sustantivos (2.2) y al procedimiento de evaluación de la protección otorgada por terceros Estados (2.3). Finalmente, se hará una breve referencia a la trasposición efectuada por el legislador español (2.4).

2.1. Ambito de aplicación de la directiva

La Directiva no oculta, en el difícil balance entre el libre flujo de datos y la defensa del derecho a la privacidad, su preocupación por los obstáculos a la transmisión de datos en el territorio de los estados miembros, que se hace patente en los considerandos de la Directiva (5, 6, 7 y 8).

Los criterios de aplicación territorial de la Directiva están establecidos en el art. 4. Sobre ellos existe una clara influencia de los elementos de conexión utilizados en materia de responsabilidad extracontractual. La utilización del criterio del *loci delicti* para la definición del ámbito de aplicación de las normas de la Directiva, es coherente con el carácter penal en todos los estados miembros de la vulneración de la intimidad, permitiendo, en principio, una coincidencia entre el *ius* y el *forum.*

Salvando la obvia mención del reenvío al derecho comunitario en el apartado b), el criterio del *loci delicti* ofrece, en el art. 4 de la Directiva, dos vertientes:

a) el del establecimiento del responsable del tratamiento, cuando éste se halle en territorio comunitario;
b) el de la utilización de medios —automatizados o no— sitos en cualquiera de los Estados miembros, para el tratamiento de los datos.

La preocupación comunitaria por evitar una deslocalización masiva de ficheros y actividades informáticas —que afectarían además a los servi-

cios y sectores intensivos en informática y telecomunicaciones como banca, seguros, agencias de viajes, y servicios médicos— lleva a redactar una norma de cierta artificiosidad técnica y gran dificultad en su implementación práctica.

En primer lugar, porque a pesar de la prevención de salida de flujos del territorio comunitario y de empleo de medios técnicos en sede comunitaria, no existe simetría regulatoria, 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. No se aprovechaba pues, la ocasión para colmar la laguna normativa del Convenio del Consejo de Europa.

En segundo lugar, por la introducción de la excepción en el supuesto de establecimiento del responsable sito fuera del territorio comunitario y utilización de medios dentro de la Comunidad: «*salvo que el medio se utilice con fines de tránsito*». La introducción del elemento subjetivo de la intencionalidad complica la apreciación de la existencia de esta excepción: un elemento de difícil valoración por cuanto se está distinguiendo entre transmisiones temporales y definitivas y habrá de recurrirse a la búsqueda del compromiso del responsable del tratamiento de los datos en territorio comunitario y en el tercer estado de no proceder a cesiones ni tratamientos ulteriores dentro de la UE.

En tercer lugar, porque este criterio, en el ánimo de evitar los riesgos de fraude de ley por la vía de utilización de medios de tratamiento en cualquier estado comunitario, va a permitir la «legitimación» de la extensión de la aplicación de la Directiva fuera del territorio comunitario al tener que completarse, como veremos a continuación, con lo dispuesto en el art. 25 de la Directiva, que extiende su ámbito a las transferencias internacionales con destino a países terceros.

2.2. Criterios sustantivos.

Como hemos mencionado antes, la regulación de las transferencias internacionales de datos en el artículo 25 de la Directiva tiene como punto de partida el art. 12 del Convenio. En este artículo aparecía el concepto de «protección equivalente», concepto que se invocará posteriormente por las autoridades comunitarias como antecedente de la noción de «nivel de protección adecuada» de la Directiva y la justificación de su aplica-

ción a terceros estados, aunque su significado sea bien distinto. El art. 12 se basa en el principio de que no debería haber comunicaciones transfronterizas de datos si no hay una protección de datos equivalente. Pero, ¿qué significa «protección equivalente»? «Esto significa en concreto, que desde el momento en que un Estado concretiza en su Derecho interno los principios básicos en el ámbito de la protección de datos y ratifica el Convenio, tiene a su favor una presunción de equivalencia y no debería haber obstáculos basados en la protección de la intimidad para los flujos transfronterizos de datos hacia dichos Estados»[6]. La presunción de equivalencia tiene pues aquí, una proyección *meramente interna.* Cualquier excepción al libre flujo de datos de carácter personal habrá de basarse en el mayor nivel de protección impuesto por la legislación nacional en determinadas categorías de datos. El Convenio se configura por tanto, como un convenio de mínimos.

Por su parte, el art. 25 de la Directiva regulador de las transferencias internacionales de datos va a recoger los conceptos de *protección equivalente* y de fraude de ley de los apartados a) y b) del art. 12 del Convenio, en un intento de hacer más rigurosas las exigencias a las que se someten las transferencias internacionales.

El artículo 25 se basa en el mismo principio del art. 12 del Convenio 108: la transmisión es ilícita a menos que se den unas condiciones 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 art. 26[7].

---

[6] WALTER, J-P., en *Conferencia Internacional de Autoridades de Protección de Datos*, p. 191.

[7] Esta redacción adoptada por la Directiva no gozó de mucha aceptación ni por parte del Parlamento ni del Consejo Social. El dictamen del CES (capítulo 2.2.19) consideró conveniente atenerse al concepto de protección equivalente del Convenio 108 y adoptar la regulación de éste. Para ello propugnaba una solución de orden tecnológico, no jurídico: la transmisión de los datos entre estados miembros debía ser regulada por medio de normas técnicas, por la vía de la normalización de equipos de transmisión («medidas prácticas comunes»), a cuyo efecto invocaba la propuesta de Directiva SYN 288, de protección de datos en las redes digitales de telecomunicación. El dictamen se mostraba asímismo a favor de una diversificación de tales medidas en función de clases de tratamientos que presentaran características comunes. El dictamen del Parlamento Europeo (enmiendas 79.ª a 81.ª) proponía igualmente aproximar el texto del precepto al del art. 12 del Convenio 108, en la medida en que, según la enmienda 79.ª, el nivel de protección adecuado habría de referirse a categorías concretas de «datos personales específicos»; en iguales términos

Aunque se haya justificado la redacción del artículo sobre la base de un acercamiento funcional implicando la búsqueda de los elementos fundamentales de la protección de la privacidad, más que el deseo de exportar el modelo legislativo europeo, evidentemente, el artículo 25 se manifestaba en términos mucho más amplios que su precedente en el Convenio. Mientras que la «protección equivalente» 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 predicaba de grupos de datos concretos sino que se estaba haciendo referencia (art. 25.2) al grueso de la legislación estatal, a la par de implicar el recurso a un completo listado de criterios que hacían el procedimiento de evaluación, complejo, riguroso y sobre todo, tornando difícil el reconocimiento de la homologación.

La alternativa a la negativa de autorización por parte de los Estados miembros o a una decisión no favorable de la Comisión, era la adopción bien 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.

2.3. Aspectos procedimentales

Los artículos 25, 26 y 31 de la Directiva establecen así, 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 art. 25.6. Iniciará entonces las negociacio-

se manifestaban las enmiendas 80.ª y 81.ª (Heredero, *La Directiva Comunitaria de protección de datos personales,* p. 32, Madrid, 1997).

nes destinadas a remediar esta situación, teniendo en cuenta el dictamen del Comité consultivo del art. 31 y según el procedimiento previsto en el art. 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 EEUU, 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 «Adecuate protection» finding under article 25.6 of the data protection directive (95/46/EC)»*, que pretende clarificar las competencias entre autoridades nacionales-Comisión en la adopción de una decisión sobre el nivel de protección y cuyas líneas generales exponemos a continuación.

Si no existe una decisión en base al art. 25.6 por parte de la Comisión, la valoración de la «adecuación» es un proceso descentralizado. Ahora bien, el art. 25.4 establece un proceso en el que cualquier disparidad de criterios se armoniza a nivel comunitario. Si una decisión basada en el art. 25.6 otorga la protección adecuada, 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.

Se establece en el borrador que en el caso de 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 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 art. 84 CE (antiguo art. 88) confiere plena competencia a la Comisión y a las autoridades nacionales para la aplicación de los arts. 81 y 82 CE. 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 art. 81 CE y declarar la nulidad del acuerdo, así como para la aplicación del art. 82 CE, 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 (art. 22)— o, por el contrario, pronunciarse sobre las cuestiones relacionadas con el art. 81.1 y 82 CE. Es decir, en definitiva, únicamente la Comisión aplica el art. 81.3 CE concediendo exenciones pero los órganos nacionales pueden ejercer sus competencias respecto del art. 81.1 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 de protección de las personas respecto al tratamiento de datos de carácter personal del art. 27 de la Directiva 95/46 —en adelante, Grupo de Trabajo—). En este mismo sentido se manifiesta Reidenberg[8].

Dado el gran número de transferencias de datos personales que salen

[8] *Op. cit.* p. 170.

y saldrán de la Comunidad diariamente, ningún Estado miembro podría garantizar el examen detallado de cada uno de los casos que se le presenten. En este sentido, el Grupo de trabajo, con el fin de racionalizar los procedimientos de toma de decisiones, ha previsto tres mecanismos[9]:

1) La definición de criterios que permitan distinguir categorías de transferencias que puedan suponer una amenaza para la vida privada. La finalidad de este sistema sería, sin perjuicio del mantenimiento de la obligación de garantía de una «protección adecuada», priorizar para su consideración, aquellas transferencias que supongan una preocupación en cuanto a la protección de los sujetos. El documento de trabajo establece algunos ejemplos de lo que pueden representar categorías de datos: categorías sensibles de datos del art. 8 de la Directiva, transferencias que supongan un riesgo de pérdida financiera, recogida de datos a través de *cookies* o *chivatos* en Internet, etc.

2) El establecimiento de cláusulas contractuales-tipo. La Directiva considera en el art. 26.2, la posibilidad de que 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 art. 31. Además de las autorizaciones de los Estados miembros, el art. 26.4 de la Directiva permite a la Comisión, también de acuerdo con el procedimiento de comitología establecido en el art. 31, juzgar si ciertas cláusulas contractuales tipo ofrecen las garantías suficientes. La valoración que emita es también vinculante para los Estados miembros. Tal disposición de la Directiva 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.

3) El establecimiento de listas blancas provisionales de países terceros que pueden presumirse que garantizan un nivel de protección adecuado. Estas listas, serían elaboradas en base a casos representativos de trans-

[9] Documento de Trabajo n.º 4, *Primeras orientaciones sobre las Transferencias Internacionales de datos personales a países terceros. Posibles formas de evaluación.* XV D/5020/97-final, WP 4.

ferencias a un país tercero, cuando se haya estimado en cada una de ellas, que la protección otorgada es adecuada. Cuando un país no esté incluido en la lista blanca, no significa que dicho país esté incluido implícitamente en una «lista negra», sino que no se dispone de una orientación general respecto a dicho país.

La mayor dificultad que puede presentar este procedimiento radica en el hecho de que muchos países terceros no tienen una protección uniforme en todos los sectores económicos. Así, si se examinan las listas que el Consejo de Europa elabora para señalar las características que ofrecen las legislaciones de protección de datos en cada país, se observa que muchos tienen legislaciones en esta materia en el sector público pero no en el privado. En EEUU la situación es más compleja, dado que existen leyes específicas para áreas concretas, tales como la información sobre créditos y los registros de alquiler de videos, pero no en otros. Además, los países que tienen constituciones federales no suelen presentar una uniformidad en la materia de protección de datos personales, existiendo a menudo diferencias entre los distintos países que componen una federación.

Finalmente, en el art. 26 de la Directiva se contienen las excepciones al posible bloqueo de los datos (consentimiento del interesado, salvaguardia del interés público, supuestos de informaciones necesarias para la ejecución de un contrato entre las partes, informaciones públicas...). Dado que el bloqueo de transferencias se presenta como un último recurso, el artículo 26 ofrece soluciones permanentes para situaciones en las que no se puede establecer la decisión de «protección adecuada» del art. 25.6. Es más, consciente la Comisión del grado de compromiso que implican las decisiones adoptadas en base al 25.6, no ha efectuado todavía ninguna valoración en base al art. 25.6. En el caso de Suiza por ejemplo, con una legislación de protección de datos muy similar a la comunitaria, no se ha hecho todavía una determinación de adecuación, por lo que el procedimiento descansa sobre el artículo 26.

2.4. Las transferencias internacionales de datos en la normativa española

La transposición de la Directiva al Derecho español se ha hecho a través de la Ley Orgánica del Tratamiento Automatizado de Datos de carácter personal (LORTAD) de 29 de octubre, que recoge en su artículo 32

las transferencias internacionales de datos. Aunque nuestra ley de protección de datos se adelantó a la promulgación de la Directiva, recogía en la mayoría de sus preceptos, el contenido y espíritu de aquélla, por lo que el adelanto en su publicación no supuso una antinomia con sus preceptos[10]. Tal es el caso del artículo 32 de la ley que sigue el mismo esquema del artículo 25 de la Directiva, exigiendo autorización previa del Director de la Agencia de Datos en el supuesto de transferencias de datos a países considerados como de «protección no equiparable» cuando se cumplan las exigencias de la LORTAD y si se obtienen además «las garantías adecuadas».

No se especifican sin embargo, ni el procedimiento ni los criterios en base a los que se realizará la valoración. El art. 3 del Real Decreto 1332/1994, de 20 de junio, de desarrollo de la LORTAD, ha intentado precisar estos criterios pero sin mucho éxito:

> *«1. Si la transferencia de los datos de carácter personal tuviera como destinatario un país que no proporciona un nivel de protección equiparable al que presta la Ley Orgánica 5/1992, el Director de la Agencia de Protección de Datos autorizará la transferencia de los mismos, siempre que el cedente de los datos acredite haber cumplido lo dispuesto en los preceptos de la referida Ley y otorgue las garantías que al efecto le sean exigidas. A tal fin, la autorización deberá ser sometida al cumplimiento de las condiciones o cargas modales que se consideren necesarias para que de la transferencia no se deriven perjuicios a los derechos de los afectados y se respeten los principios contenidos en el Título II de la Ley Orgánica 5/1992.*
>
> *2. En caso de incumplimiento de los términos de la autorización el cedente y el cesionario de los datos responderán solidariamente a efectos de lo previsto en el artículo 17.3 de la Ley Orgánica 5/1992.»*

¿Cuáles son esas garantías? ¿Son discrecionales por el Director? En las Memorias de la Agencia de Protección de Datos de 1995 se hizo al-

[10] Por otra parte, el nuevo proyecto de ley orgánica de protección de datos personales, que en estos momentos se encuentra en fase de tramitación en el Senado, no contiene ninguna modificación a la redacción original de la LORTAD.

guna precisión al respecto (Memoria de la Agencia de Protección de Datos, 1995, pp. 71-72):

a) información sobre las circunstancias relacionadas con la transferencia, en concreto, naturaleza de los datos, finalidad, duración del tratamiento, país de destino y normas sectoriales o profesionales que puedan existir;
b) consentimiento inequívoco del interesado o bien que el interesado sea parte de una relación contractual o precontractual que haga innecesaria la transferencia;
c) que los datos transmitidos se utilicen según la especificación manifestada al momento de inscripción del fichero y que no se cedan a terceros sin el consentimiento previo de los afectados, y
d) la titularidad del fichero continuará siendo de la entidad peticionaria de la autorización, cumpliendo las obligaciones y derechos de la normativa legal.

3. EL DIÁLOGO UE-TERCEROS PAÍSES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES. EL CASO DE EEUU

3.1. El diálogo UE-terceros países

La negociación de acuerdos comerciales entre la UE y terceros países ha dado lugar a la inclusión, junto con 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.

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[11]. 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 Comisión, gozando pues, los países parte del mismo, de un *nivel de protección adecuado.*

«Este breve análisis parece indicar que las transferencias de datos personales a países que han ratificado el Convenio 108 pueden considerarse permitidas en virtud del apartado 1 del artículo 25 de la Directiva, siempre que:

- *el país en cuestión también cuente con mecanismos institucionales adecuados, tales como una autoridad de control independiente con poderes adecuados, y*
- *el país en cuestión sea el destino final de la transferencia y no un país intermedio por el que transiten los datos».*

Como reconoce el Grupo de trabajo[12], *«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 Méjico —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, pp. 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».

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

[11] Documento de Trabajo n.º 4, p. 9.

[12] Documento de Trabajo n.º 3, *Primer informe anual sobre la protección de datos,* 25 de junio de 1997, XV D/5025 /97-final, WP 3, punto 2.5

el procedimiento previsto en el art. 25.6 de la Directiva todavía no ha sido 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.

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, «ya poseen acuerdos legales e instituciones que permiten un nivel de protección comparable al de la CE. Australia y Canadá han adoptado similares previsiones en sus sectores públicos, mientras Quebec ha adoptado recientemente legislación que se aplica a su sector privado».

La Directiva debería aplicarse también al Espacio Económico Europeo, 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 parte de este acuerdo.

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. En 1997, Hungría se adhirió al Convenio y ya existen leyes de protección de datos aprobadas en Hungría, Estonia, Polonia, Eslovaquia o en tramitación legislativa en Bulgaria, Letonia, Rumanía, República Checa y Eslovenia.

3.2. El diálogo UE-EEUU

Especialmente revelador del peso específico de la protección de datos en las negociaciones comerciales internacionales, ha sido el diálogo entre la Comisión Europea y el Ministerio Federal de Comercio estado-

unidense, diálogo que se inició con la firma de la Nueva Agenda Trasatlántica.[13]

En la Cumbre de Madrid de diciembre de 1995, culminó un gran ejercicio de redefinición y relanzamiento de la relación EEUU-UE con la firma de la Nueva Agenda Trasatlántica. Una parte esencial de este acuerdo fue el plan de acción donde se describían diversas acciones y objetivos específicos. En cumplimiento del plan de acción, el 5 de diciembre de 1997, la UE y los EEUU firmaron una declaración común sobre el comercio electrónico.

En materia de protección de datos, se han sucedido las respectivas propuestas especialmente desde junio de 1997, en vistas de conseguir un acuerdo para la cumbre de 21 de junio de 1999. Este acuerdo no ha llegado sin embargo a tiempo, en vista de las divergencias de posiciones entre ambas partes. La última posición del Ministerio de Comercio estadounidense hecha pública, de fecha 19 de abril de 1999, nos ayudará a analizar las diferencias que separan a las partes.

La propuesta de base se centra en los llamados «principios de puerto seguro», que representan el núcleo de un paquete de medidas que pretenden establecer un marco predecible para las transferencias de datos personales entre EEUU-UE. Sus objetivos: crear un marco más previsible, de mayor seguridad jurídica y menos cargas administrativas, asegurando un alto estándar de protección de datos.

Desde el punto de vista comunitario, este conjunto de principios responderían al estándar de *protección adecuada* exigido por la Directiva 95/46, que pretende establecer un marco de adhesión a suscribir por los agentes económicos y operadores norteamericanos. Sin embargo, desde un punto de vista sustantivo, los principios de base no serían los establecidos en la Directiva, sino los recogidos en las Directrices sobre protección de la intimidad de la OCDE de 1980, adoptadas por EEUU, y que se volvieron a ratificar en la Conferencia de Otawa de la OCDE sobre comercio electrónico.

Esta imposición choca precisamente, con la tradición liberal estadounidense, más partidaria de la desregulación y de dejar la sociedad de la in-

[13] Dictamen 1/99 del Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento automatizado de datos personales relativo al nivel de protección de datos en EEUU y a los debates en curso entre la Comisión Europea y el Gobierno de los EEUU. WP 15, 5092/98/ES/final. DE 26 de enero de 1999.

formación en manos privadas, esto es, sujeta a la ley del mercado, y ha sido una de las principales objeciones comunitarias a la protección estadounidense, que no ha considerado suficiente la existencia de regulación sectorial, tanto a nivel federal como estatal, combinada con la autorregulación industrial y la existencia de soluciones contractuales. Aunque la Comisión considera que el nuevo documento estadounidense presenta sustanciales mejoras respecto a versiones anteriores, se critican del texto consultivo publicado por el Ministerio de Comercio estadounidense el 4 de noviembre de 1998, las siguientes cuestiones:

Frente a las exigencias comunitarias de obligatoria adhesión a los principios de puerto seguro, los EEUU pretenden su aceptación voluntaria en el ánimo de evitar la imposición de cualquier tipo de regulación. Así, según el tercer párrafo de la introducción del documento norteamericano, la «adhesión a los principios está sujeta» a varias excepciones y limitaciones, tales como «la gestión de riesgos» y la «seguridad de la información». El Grupo de Trabajo de la Comisión ha considerado que estas nociones son demasiado vagas y de interpretación abierta, y recomienda que se clarifiquen o se supriman.

Frente a la extensión en la Directiva de su ámbito de aplicación a los datos personales automatizados y manuales, se excluyen por parte norteamericana los datos propietarios y cualquier dato tratado manualmente.

Junto a ello, se recorta el contenido de los principios básicos: el principio de «opción», que permite que datos recogidos con un propósito determinado se utilicen para otro, a condición de que exista la posibilidad de opción por parte del interesado, no proporciona protección alguna a los datos recogidos de terceros. El derecho de acceso del afectado excluye la información procedente de documentación pública y se limita a lo «razonable». Las directrices sobre intimidad de la OCDE no limitan este derecho, simplemente afirman que debe ejercitarse «de modo razonable». Uno de los temores de los americanos es que el comportamiento de los consumidores ejerciendo su derecho de acceso sea muy costoso para las empresas. Además un gran número de bases de datos de marketing no están organizadas de forma que sea fácil efectuar una búsqueda a partir de la entrada de un nombre sino sobre la base de un código postal u otras bases y sería muy costoso su modificación.

Aunque las últimas negociaciones tampoco han conducido a un consenso, está previsto ya un nuevo calendario de conversaciones, por lo que ambas partes tendrán que reconsiderar sus respectivas posiciones.

4. CONCLUSIONES

A modo de conclusión, podemos afirmar que la Directiva 95/46 no se halla justificada en razones de mejora de criterios sustantivos ni procedimentales frente a los contenidos en el Convenio del Consejo de Europa.

Aunque las respectivas legislaciones nacionales han procedido a la trasposición de la normativa comunitaria, los controles a nivel nacional se han revelado lentos, antieconómicos e ineficaces, en una materia donde la resolución de los expedientes ha de resolverse con gran celeridad. Pero es que además, la atribución de competencias a la Comisión no tiene carácter residual, como podría deducirse de la letra de los arts. 25.4 y 25.5, sino que ha adquirido una posición relevante a través de la negociación de acuerdos comerciales con terceros estados que van más allá de la mera protección de los datos personales.

Aunque el verdadero alcance de estas negociaciones y acuerdos está todavía por definir, *a priori,* no todos ofrecen el mismo nivel de exigencia por lo que pueden plantearse dudas respecto a su compatibilidad con el acuerdo del GATS. En este sentido, los principios de base utilizados en la mayoría de estos acuerdos han sido los contenidos en el Convenio 108 del Consejo de Europa mientras que en el caso de los EEUU, se ha partido de las Directrices de la OCDE, lo que independientemente de la equiparación sustantiva entre éstas y el Convenio 108, cuestiona una vez más, la necesidad de incorporar a la Directiva criterios adicionales de protección.

Consideramos sin embargo positivo, el control sobre las posibles soluciones contractuales, dado que el consumidor-afectado se encontrará siempre en una situación más comprometida en cuanto al control sobre sus datos personales. No obstante, sería aconsejable adoptar un enfoque basado en el consumidor, que permitiese abandonar en parte el tono economicista que prima en la regulación, y se revelaría como un motor efectivo en la armonización de esta normativa y en la promoción de su carácter universal, en aras de la protección de las libertades fundamentales.

JURISPRUDENCIA