ARTÍCULOS

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES Y EL NIVEL EQUIPARABLE O ADECUADO DE PROTECCIÓN

CECILIA ÁLVAREZ RIGAUDIAS
Abogada (*)

1 · INTRODUCCIÓN

La Directiva 95/46/CE 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 (la Directiva) estableció unos altos estándares de protección de la intimidad en relación con el tratamiento de datos personales. En particular, para preservar los efectos del régimen que establecía, impuso la prohibición general de transferir datos personales fuera de cualquier país de la Unión Europea (U.E.), a un país «tercero» por tanto, siendo una de las excepciones más relevantes que el país tercero de destino garantizara un nivel adecuado de protección. Al implementar la Directiva en España, dicho régimen, aunque con una sistemática distinta, ha sido recogido en la Ley Orgánica 15/1999 de protección de datos de carácter personal (LOPD).

En la práctica, esta prohibición ha llevado a imponer los estándares de protección de datos en la U.E. en otras jurisdicciones, por lo que la Directiva ha sido criticada como una seria barrera regulatoria para el comercio internacional, particularmente en el contexto de grupos multinacionales que tratan de operar bajo unos mismos estándares en todas las jurisdicciones donde están presentes.

La regulación española sobre transferencias internacionales de datos personales y su interpretación por la autoridad de control no han quedado exentas de esta crítica, lo que nos lleva a estudiar qué se entiende por un nivel adecuado de protección, comenzando por un análisis del marco jurídico español en el que se encuadran las transferencias internacionales, para determinar lo que ha de considerarse como un nivel de protección equiparable o adecuado a nuestros estándares de protección, terminando por quién y cómo se ha determinado éste hasta ahora.

2 · MARCO JURÍDICO DE LAS TRANSFERENCIAS INTERNACIONALES

2.1 · El concepto de transferencia internacional

La LOPD no contiene una definición de transferencia en general ni de transferencia internacional en particular. Sin embargo, en su artículo 3 *c)*, al definir el tratamiento de datos [1], se menciona la transfe-

* Del Departamento de C.S.D.I. de Uría Menéndez (Madrid).

1 Art. 3 de la LOPD. «A los efectos de la presente Ley Orgánica se entenderá por: [...] c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

rencia como un proceso a consecuencia del cual se produce un acto de tratamiento específico, la cesión de datos, esto es, «*toda revelación de datos realizada a una persona distinta del interesado*».

El concepto de transferencia lo podemos encontrar en el Real Decreto 1332/94 [2]: «*el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional*».

Por su parte, la Instrucción 1/2000, de la Agencia Española de Protección de Datos (AEPD) [3], relativa a las normas por las que se rigen los movimientos internacionales de datos (la Instrucción), define la transferencia internacional de datos de carácter personal como toda «*transmisión de los mismos* [datos de carácter personal] *fuera del territorio español*». La Instrucción precisa que bajo este concepto se incluyen, aunque no de forma exhaustiva, tanto las transferencias que constituyan una cesión o comunicación de datos *strictu sensu* (esto es, de responsable a responsable) como las que tengan por objeto la realización de un tratamiento por cuenta del responsable del fichero (esto es, de responsable a encargado). Teniendo en cuenta que los sujetos obligados por la LOPD sólo se corresponden con la figura del responsable y del encargado [4], resulta difícil comprender a qué otras transferencias pudiera referirse la Instrucción.

Sobre la base de lo anterior y a la luz de la sentencia de 6 de noviembre de 2003 del Tribunal de Justicia de las Comunidades Europeas (TJCE) [5], cabría definir la transferencia de datos personales como la transmisión directa de datos a consecuencia de la cual el transmitente da acceso o permite el conocimiento de ellos al destinatario (distinto del afectado), implicando por tanto una comunicación «material» de datos personales, con independencia de su finalidad (sin perjuicio de las implicaciones legales específicas previstas para las comunicaciones de datos a terceros para realizar tratamientos por cuenta del transmitente o para otras finalidades); siendo internacional cuando el destino de los datos se localiza fuera del territorio español.

La Instrucción deja fuera de su ámbito de aplicación las transferencias de datos efectuadas desde fuera del territorio español y con destino al territorio español. Sin embargo, en estos casos, la autoridad de control ha sostenido en ocasiones que la captación y transferencia efectuadas en y desde el extranjero han de enjuiciarse a la luz de las exigencias establecidas en la legislación española acerca de la obtención de consentimiento respecto al tratamiento y, en particular, a la cesión a terceros situados en España por parte del cedente extranjero.

2.2 · La prohibición general para realizar transferencias internacionales

El principio general que rige en las transferencias internacionales a un país que no tenga un «*nivel de protección equiparable*» al de la LOPD es la autorización previa de la AEPD (que deberá otorgarla si «*se obtienen garantías adecuadas*») salvo que concurra

2 Art. 1 del RD 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Aunque este Real Decreto se refiere a la LORTAD, derogada por la LOPD, este reglamento sigue vigente en todo lo que no contradiga a la LOPD (vid. D.T. 3.ª de la LOPD).

3 Art. 37 de la LOPD: «Son funciones de la Agencia de Protección de Datos: c) Dictar [...] las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley» y art. 5 c) del Estatuto de la AEPD, aprobado por RD 428/1993, de 26 marzo: «La Agencia de Protección de Datos colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia de la Ley Orgánica 5/1992, y a tal efecto: [..] c) Dictará instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica.».

4 Art. 3 de la LOPD: «A los efectos de la presente Ley Orgánica se entenderá por: [...] d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. [...] g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento».

5 En la sentencia del TJCE de 6 de noviembre de 2003, as. C-101/01, Lindqvist, se concluye, de una parte, que la difusión de datos personales en el contenido de una página web (de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquéllas que se encuentren en países terceros), no constituye una transferencia de datos a un país tercero en el sentido del art. 25 de la Directiva con respecto a cualquier potencial usuario que acceda a través de Internet a esa información; y, de otra parte, que habría comunicación de datos relevante a los efectos de los arts. 25 y 26 de la Directiva si existiera una transferencia directa entre quien revela los datos y quien los recibe (p.e., las operaciones realizadas por el proveedor de servicios de alojamiento de páginas web, en la medida en que entre éste y el titular de la página web sí existe normalmente una transmisión directa de información; requiriendo la prestación de tales servicios el acceso del proveedor a los datos, lo que justifica su consideración como encargado del tratamiento de datos personales), pero no en situaciones como las que han dado lugar a esta sentencia, donde los datos «se han transmitido con la ayuda de la infraestructura informática del proveedor de servicios de alojamiento de páginas web donde está almacenada la página».

alguna de las excepciones previstas en el artículo 34 de la LOPD.

Cualquier transferencia internacional sin la autorización previa de la AEPD, cuando sea preceptiva, constituirá infracción muy grave sancionable con multa de hasta 600.000 euros aproximadamente.

Entre las excepciones previstas en el artículo 34 de la LOPD, destaca el apartado *k)*, esto es, que el destinatario de la transferencia internacional esté establecido en un Estado miembro de la UE [6], o un Estado respecto del cual la Comisión Europea (la Comisión) haya declarado que garantiza un nivel de protección adecuado. Todos los Estados miembros de la UE gozan de «*nivel equiparable*» por definición. Por tanto, hubiera resultado más adecuado que este supuesto se incluyera en el principio general en vez de configurarse como una excepción al él.

Por otra parte, la LOPD no menciona expresamente a los Estados miembros del Espacio Económico Europeo que no forman parte de la UE (Islandia, Liechtenstein y Noruega), por lo que cabría plantearse si estos países se consideran como países «terceros». Estos países han transpuesto a su Derecho nacional las previsiones de la Directiva, motivo por el cual constituyen un ámbito geográfico armonizado con nivel de protección equiparable, como ha venido a reconocer la Instrucción [7].

En cualquier caso, la Instrucción, en el apartado 1 de la Norma 3.ª (aplicable a toda transferencia internacional) prevé que la AEPD puede solicitar al responsable documentación acreditativa: (i) de la concurrencia de cualquiera de las excepciones al principio general de recabar autorización previa (incluso si se trata de transferencias a países con nivel equiparable o adecuado de protección, de conformidad con el apartado 1 de la Norma 4.ª); y (ii) del cumplimiento de la obligación de información al afectado de quién será el destinatario de los datos, así como de la finalidad que justifique la transferencia internacional y el uso de los datos que podrá hacer el destinatario (por remisión a la Norma 2.ª).

Sin perjuicio de que la obligación de información a que nos hemos referido en el apartado (ii) anterior está configurado en la Norma 2.ª de la Instrucción como una consecuencia del artículo 5 de la LOPD, este artículo 5 no menciona de forma específica todos los extremos a que se refiere la Instrucción. Las menciones previstas en la Instrucción más bien se corresponden con lo previsto en el artículo 27 de la LOPD respecto a la información que hay que suministrar al afectado en el momento de realizarse la cesión. Este artículo 27 reconoce, no obstante, excepciones que no han sido recordadas por la Instrucción. La única excepción que recoge la Instrucción es que la finalidad de la transferencia sea la prestación de un servicio al responsable del fichero (ya que es una excepción que también se aplica a las transferencias nacionales para esta finalidad).

Sin embargo, el responsable de un fichero privado que realice una transferencia internacional (para finalidad distinta del tratamiento de datos por su cuenta) debe poder acogerse a las excepciones previstas en el artículo 27.2 de la LOPD (sin perjuicio de que determinados instrumentos contractuales que proporcionan garantías adecuadas puedan exigir un deber específico de información al afectado [8]). Y, máxime, cuando la Instrucción no puede excluir (ni modificar) la aplicación de las disposiciones contenidas en la LOPD.

En cualquier caso, los apartados primeros de las Normas 3.ª y 4.ª de la Instrucción han sido declarados nulos por la Audiencia Nacional [9] en tanto en cuanto pretenden establecer unos mecanismos de control de significación equivalente a la autorización previa también cuando concurran alguna de las excepciones del artículo 34 LOPD, entre otros, el mencionado apartado *k)* (país de destino de nivel equiparable o adecuado), lo cual ha sido excluido expresamente por el legislador [10].

6 A estos efectos, desde el 1 de mayo de 2004, también se incluyen los países europeos que se han adherido a la UE en dicha fecha. Como excepción, Hungría fue declarada previamente como un país de nivel de protección adecuado en virtud de la Decisión 2000/519/CE (vid. apartado 4.1.2).

7 Apartados 1 de Norma 4.ª y de la Norma 5.ª y apartado 3.ª de la Norma 6.ª de la Instrucción.

8 Por ejemplo, las cláusulas contractuales tipo 4 b) y f), anejas respectivamente a las Decisiones 2001/497/CE y 2002/16/CE, prevén el deber de informar al afectado de que sus datos pueden ser transferidos a un país que no proporciona una adecuada protección cuando se transfieren datos sensibles.

9 El fallo de la sentencia de la AN de 15 de marzo de 2002 (objeto de recurso de casación ante el TS), que resuelve la impugnación directa de la Instrucción, señala que «[...] debemos anular y anulamos el apartado 2) de la Norma Tercera y la Norma Sexta de dicha Instrucción, si bien ambos únicamente en cuanto pretenden extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción del artículo 34 de la Ley Orgánica 15/1999, y anulamos también el apartado 1) de la Norma Cuarta de la misma Instrucción [...]».

10 «Por supuesto, la transferencia internacional de datos —esté o no sujeta a autorización previa— no excluye que sean de aplicación el conjunto de disposiciones de la Ley Orgánica 15/1999,

3 · ELEMENTOS CONSTITUTIVOS DE UNA PROTECCIÓN ADECUADA

De acuerdo con el «*Documento de Trabajo sobre Transferencias de datos personales a terceros países y aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE*», aprobado el 24 de julio de 1998 por el Grupo 29 [11], los estándares de protección que debe ofrecer la legislación de un Estado para ser considerados como «adecuados» han de ser evaluados desde una doble perspectiva: el contenido de las normas aplicables a los datos personales y los mecanismos procedimentales existentes destinados a garantizar la eficacia de dichas normas.

En dicho documento se enumeran aquellos principios que constituyen «*un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento/de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección*» [12] y que son los siguientes:

(i) Principios de contenido: se distinguen dos tipos de principios de contenido, los «*básicos*» y los «*adicionales*» aplicables a tipos específicos de tratamiento, que se pueden resumir como sigue:

Principios básicos L*imitación de objetivos:* los datos deben tratarse con una finalidad específica y posteriormente utilizarse o transferirse únicamente en cuanto no sea incompatible con la finalidad de la transferencia (únicas excepciones: las necesarias en una sociedad democrática por alguna de las razones contempladas en el artículo 13 de la Directiva). *Proporcionalidad y calidad de los datos*: los datos deben ser exactos y, cuando sea necesario, estar actualizados, así como adecuados, pertinentes y no excesivos con relación la finalidad para la que se transfieren o traten posteriormente. *Transparencia*: debe informarse a los interesados acerca de la finalidad del tratamiento y de la identidad del responsable del tratamiento en el país tercero, y de cualquier otro elemento necesario para garantizar un tratamiento legítimo (únicas excepciones permitidas: artículos 11.2 y 13 de la Directiva). *Seguridad*: el responsable debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presente el tratamiento; toda persona que actúe bajo su autoridad, incluido el encargado, no debe tratar los datos salvo bajo sus instrucciones. *Derechos de acceso, rectificación y oposición*: el interesado debe tener derecho a obtener una copia de todos sus datos y a rectificar los inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de sus datos (únicas excepciones: en línea con el artículo 13 de la Directiva). *Restricciones respecto a ulteriores transferencias a países terceros*: únicamente deben permitirse en el caso de que el país tercero de destino garantice asimismo un nivel de protección adecuado (únicas excepciones: en línea con el artículo 26.1 de la Directiva).

Principios adicionales aplicables a tipos específicos de tratamiento *Datos sensibles*: cuando se trate de categorías de datos «sensibles» (*vid.* artículo 8 de la Directiva), deberán establecerse protecciones adicionales, tales como el consentimiento explícito del interesado. *Marketing directo*: cuando la transferencia tenga por objeto el marketing directo, el interesado deberá tener la posibilidad de negarse a que sus datos sean tratados con dicho propósito en cualquier momento. *Decisión individual automatizada:* cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

(ii) Mecanismos de procedimiento/aplicación: un sistema «adecuado» debe ofrecer tanto un

---

ni impide o menoscaba el ejercicio de las competencias (inspectoras, sancionadoras,...) que la legislación atribuye a la Agencia de Protección de Datos;...Pero no resulta aceptable que estas potestades de comprobación o incluso de inspección encaminadas a asegurar el cumplimiento de la Ley las ejerza la Agencia precisamente al tener conocimiento de que pretende realizarse una transferencia de datos para la que no es necesaria su autorización; y menos aun cabe aceptar que a los requerimientos realizados en esa ocasión se les atribuya la virtualidad de, si no son atendidos dentro del plazo señalado, impedir la inscripción y con ello la propia viabilidad de la transferencia.» (F.D. 7 de la sentencia de la AN antes citada de 15 de marzo de 2002).

11 Este grupo se creó en virtud del art. 29 de la Directiva. Se trata de un organismo de la UE, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el art. 30 de la Directiva y en el art. 15 de la Directiva 2002/58/CE. En febrero de 2004, el Director de la AEPD fue elegido Vicepresidente del Grupo 29.

12 Este documento se basa a su vez en otros documentos previos del Grupo 29: «Primeras orientaciones sobre las transferencias de datos personales a países terceros - Posibles formas de evaluar su adecuación», de 26 de junio 1997; «Evaluación de la autorregulación industrial: ¿en qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?», de 14 de enero de 1998; y «Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países», de 22 de abril de 1998.

nivel satisfactorio de cumplimiento de las normas como un apoyo y asistencia a los interesados en el ejercicio de sus derechos, y vías adecuadas de recurso a los que resulten perjudicados en el caso de que no se observen las normas.

4 · DETERMINACIÓN DEL NIVEL EQUIPARABLE O ADECUADO

De acuerdo con la Directiva, tanto los Estados miembros como la Comisión están facultados para realizar la evaluación del nivel adecuado de protección. Dicha evaluación puede proyectarse sobre el país tercero de destino (artículo 25) o bien sobre las garantías que ofrezca el responsable de tratamiento, es decir, instrumentos *ad hoc*, especialmente de naturaleza contractual (artículo 26) [13].

La LOPD ha recogido tales principios, aunque en el marco de una sistemática diferente, atribuyendo a la AEPD la facultad de realizar la mencionada evaluación cuando sea necesaria una autorización previa para llevar a cabo una transferencia internacional, esto es, cuando el destino de la transferencia es un país que no tiene un nivel equiparable a la LOPD y no concurra alguna de las excepciones previstas en su artículo 34.

4.1 · Determinación del nivel equiparable del país de destino

Las facultades de la AEPD

De acuerdo con la LOPD, la instancia competente para declarar la existencia de un nivel de protección equiparable respecto al país de destino es la AEPD [14].

Reproduciendo el artículo 25.2 de la Directiva, la LOPD establece en su artículo 33 que la evaluación ha de ser global, atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. Esta evaluación habrá de tener en cuenta, en particular: (i) los mismos parámetros previstos en el artículo 25.2 de la Directiva, esto es, la naturaleza de los datos; la finalidad y la duración del tratamiento o de los tratamientos previstos; el país de origen y el país de destino final; las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate; así como las normas profesionales y las medidas de seguridad en vigor en dichos países; y (ii) los «*informes emitidos por la Comisión*».

Bajo la vigencia de la LOPD, la AEPD no ha realizado hasta la fecha las evaluaciones globales respecto al nivel de equiparable protección de un «país tercero» a que se refiere el artículo 33 [15], por lo que habrá de estarse a las evaluaciones que ha realizado la Comisión en virtud de lo previsto en la Directiva. Las decisiones de la Comisión en este sentido obligan a los Estados Miembros, los cuales quedan asimismo obligados a impedir aquellas transferencias respecto a las cuales la Comisión considere que no garantizan un nivel de protección adecuado.

Las decisiones de la Comisión: las «listas blancas»

De conformidad con el artículo 25.6 de la Directiva, la Comisión podrá hacer constar que un país tercero garantiza un nivel de protección adecuado a efectos de la protección de la vida privada o de las libertades o derechos fundamentales de las personas, a la vista de su legislación interna o de sus compromisos internacionales.

Hasta la fecha, y sobre la base de los criterios del Grupo 29 enunciados anteriormente, la Comisión ha declarado que considera adecuado el nivel de protección de datos personales en Suiza (Decisión 2000/518/CE), Hungría (Decisión 2000/519/CE), «*el conferido por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos*» (los «Principios» y

13 Desde el punto de vista procedimental, la Directiva trata estos casos de forma muy diferente. Mientras que, en virtud del art. 25, los Estados miembros deberán notificar a los demás Estados miembros y a la Comisión los casos donde no se garantiza una protección adecuada y por lo tanto se bloquea la transferencia, en virtud del art. 26, la obligación se ve invertida y los Estados miembros deberán informar a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan.

14 Arts. 33 y 37(i) LOPD.

15 De acuerdo con la D.F. 1.ª del RD 1332/1994, se facultó al Ministro de Justicia e Interior para (previo informe de la AEPD) aprobar la relación de países que se entiende que proporcionan un nivel de protección equiparable al de LORTAD (a efectos de su art. 32 reproducido en el actual art. 33.1 de la LOPD). Bajo la vigencia de la LORTAD, se aprobaron dos relaciones de países, mediante Órdenes Ministeriales de 2 de febrero de 1995 y de 31 de julio de 1998 respectivamente, especificando aquellos países que proporcionaban un nivel de protección equiparable al español, según se trataba de ficheros de titularidad pública o privada. A este respecto, la AEPD se ha pronunciado expresamente respecto de la vigencia de tales Órdenes Ministeriales, que entiende derogadas a raíz de la promulgación de la LOPD (vid. Memoria Anual de la AEPD de 2002).

las «FAQs» [16]) (Decisión 2000/520/CE [17 y 18]), Canadá (Decisión 2002/2/CE), la Bailía de Guernsey (2003/821/CE), Argentina (Decisión de 30 de junio de 2003), la Isla de Man (Decisión de 28 de abril de 2004), así como los datos personales incluidos en los registros de nombres de los pasajeros (PNR, *Passenger Name Record*) que se transfieren al Servicio de aduanas y protección de fronteras de los EE.UU. (Decisión 2004/535/CE) [19].

Respecto a los EE.UU. (sin perjuicio de que sigue siendo un país que no ofrece, según la normativa comunitaria y nacional, un nivel de protección equiparable o adecuado), la Instrucción reconoce el nivel adecuado que prevé el sistema de autocertificación de Puerto Seguro establecido en la Decisión 2000/520/CE. A este respecto, aunque no sea necesaria la autorización previa de la AEPD, la Instrucción prevé que el transmitente «*deberá acreditar que el destinatario se encuentra entre las entidades que se han adherido a los principios, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión*» [20]. La Instrucción extiende

16 Los Principios son siete: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación. En términos de la Directiva, harían referencia al derecho de información, consentimiento, comunicación a terceros, seguridad, calidad de datos, derecho de acceso y recursos, responsabilidad y sanciones, aunque con un contenido más limitado. Estos Principios, muy generales, se completan con quince FAQs que pretenden aclarar y precisar su alcance y dar solución a algunas dudas interpretativas que pudieran surgir en su aplicación. Las FAQs hacen referencia a datos especialmente protegidos, excepciones relativas al ejercicio del periodismo, responsabilidad subsidiaria de los proveedores de servicios de Internet o telecomunicaciones, excepciones a los principios de notificación, opción y acceso para los bancos de inversiones y sociedades de auditoria, la función de las autoridades de protección de datos europeas, condiciones y compromisos adquiridos a través de la autocertificación, verificación del cumplimiento de Puerto Seguro, alcance del derecho de acceso, condiciones especiales para los datos de recursos humanos transferidos desde la UE, regulación contractual de los tratamientos por cuenta de terceros, resolución de litigios y ejecución, precisiones sobre el derecho de opción, transferencia de información sobre viajes, transferencia de datos relativos a productos médicos y farmacéuticos, y, finalmente, información extraída de registros públicos y de dominio público.

17 De conformidad con la Decisión, la Comisión analizará, en todo caso, su aplicación tres años después de su notificación a los Estados miembros. La Comisión emitió su informe el 20 de octubre de 2004 (SEC (2004) 1323), cuyas principales conclusiones básicamente se corresponden con las establecidas en su primera evaluación de 2002 (SEC(2002) 196, de 13 de febrero de 2002), al que siguió un proyecto de documento de trabajo sobre el funcionamiento del Acuerdo de Puerto Seguro (WP62) del Grupo 29, de 2 de julio de 2002.

En su informe de octubre de 2004, la Comisión destaca las deficiencias en el grado de transparencia de las entidades adheridas al sistema, ya que existe un porcentaje significativo de ellas que no han hecho pública su política de privacidad (lo que limita, en particular, las posibilidades de intervención de los organismos estadounidenses encargados de su supervisión) o ésta presenta serias deficiencias respecto del estándar marcado por Puerto Seguro, así como la falta de adhesión a Puerto Seguro o de pleno cumplimiento del mismo por las entidades arbitrales previstas en él (Alternative Dispute Resolution Bodies), lo que también debilita el sistema de cumplimiento o aplicación y la necesidad de una mayor transparencia en la página web del Departamento de Comercio de EE.UU., en particular, en cuanto a que se especifique el compromiso de las organizaciones de cumplir con la opinión del panel U.E. en caso de conflicto.

18 Dentro del programa de trabajo del Grupo 29 para el año 2004 figuraba la constatación de un nivel adecuado de protección respecto a Australia (sobre el cual ya se pronunció en su Dictamen 3/2001) y Nueva Zelanda, pero todavía no se ha concretado en ninguna decisión de la Comisión.

19 Ha sido especialmente controvertido el acuerdo alcanzado por la Comisión con las autoridades estadounidenses respecto a la transferencia de los datos de pasajeros aéreos a los EE.UU. (COM(2004) 190), habiendo incluso presentado el Parlamento Europeo una demanda ante el TJCE. El informe de la Comisión de Libertades del Parlamento Europeo de 7 de abril de 2004, que rechazaba la celebración de este acuerdo, no ha sido votado a la espera del dictamen del TJCE. El Grupo 29, en su Dictamen 6/2004, de 22 de junio de 2004, lamentó que la Comisión, en su Decisión 2004/535/CE de 14 de mayo de 2004, sólo haya tenido en cuenta parcialmente las preocupaciones expresadas por este Grupo en anteriores ocasiones (Dictamen 6/2002) respecto del ámbito de datos transferidos, su período de retención y la forma en que van a ser tratados. Por otra parte, el Grupo 29 ha elaborado asimismo otros dictámenes respecto de la transferencia de PNR a Australia (1/2004) (Australia) y Canadá (3/2004 y 1/2005).

20 Los organismos públicos estadounidenses con competencias en estas materias son actualmente la Federal Trade Commission («FTC») y el Departamento de Transporte de los EE.UU. La Decisión no se aplica ni a los sectores ni a los tratamientos de datos que no estén sujetos a la jurisdicción de estos organismos. A este respecto, la FTC carece de jurisdicción en lo referente a bancos, cooperativas de ahorro y crédito, compañías de servicio público de telecomunicaciones y de transporte, compañías aéreas, envasadores y operarios de áreas para ganado. En cuanto a los seguros, la FTC es competente respecto al cumplimiento de determinadas normas federales aplicables subsidiariamente en aquellos Estados que no hayan regulado la actividad y conserva una competencia residual sobre las prácticas desleales o fraudulentas de las compañías de seguros que se realicen al margen de la actividad aseguradora. Asimismo, la FTC se declara competente para controlar la protección de la intimidad en actividades on-line (para una mayor información al respecto puede revisarse la carta de la FTC dirigida a la Dirección General XV de la Comisión adjunta como Anexo V a los Principios y las FAQs). El Departamento de Transporte, por su parte, incoa procedimientos basándose tanto en sus propias investigaciones como en las acusaciones formales e informales recibidas de particulares, agentes de viajes, compañías aéreas, organismos públicos estadounidenses y extranjeros.

El destinatario de los datos deberá comunicar al Departamento de Comercio de EE.UU. su adscripción a los Principios y las FAQs y la determinación de la autoridad a la que haya de quedar sometido. Huelga decir que ello obligará al destinatario a cumplir con dichos principios y podrá implicar la apertura de procesos sancionatorios o indemnizatorios por los citados organismos en caso contrario.

esta previsión a todas las transferencias internacionales a países en que el nivel de protección adecuado se declare por la Comisión en relación con un sistema de autorregulación o de condiciones similares a las contenidas en la Decisión 2000/520/CE.

4.2 · Determinación del nivel adecuado de las garantías

De conformidad con el artículo 26.2 de la Directiva, los Estados miembros podrán asimismo autorizar una transferencia o una serie de transferencias de datos personales a un país tercero que no garantice un nivel de protección adecuado (con arreglo al artículo 25.2, de la Directiva) cuando el responsable del tratamiento «*ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos*». En particular, se especifica que dichas garantías podrán derivarse de cláusulas contractuales apropiadas.

En línea con lo considerado en este último punto, la Instrucción establece, en particular, dos contratos entre transmitente y destinatario que cumplirían con las premisas de ofrecer garantías adecuadas. Ello no excluye la posibilidad de que se autoricen otros contratos que se ajusten a las decisiones de la Comisión (vinculantes para los Estados miembros) o cualesquiera otros que cuenten con garantías adecuadas. A este respecto, los dictámenes y documentos de trabajo elaborados por el Grupo 29 proporcionan asimismo orientaciones valiosas para analizar nuevas vías que permitan las transferencias internacionales a países terceros.

Los contratos de la Instrucción

Las Normas 5.ª y 6.ª de la Instrucción establecen aquellas garantías contractuales que la AEPD entiende «*adecuadas*» a los efectos de otorgar la autorización pertinente, destinando la primera a cualquier transferencia internacional a país no equiparable (con independencia de su finalidad) y la segunda a cualquier transferencia internacional para la finalidad de tratamiento de datos, esto es, de responsable a encargado de tratamiento (con independencia de su destino).

La elección de una estructura que considera los criterios de destino y finalidad de forma separada no resulta acertada. En primer lugar, porque la Norma 5.ª, al no considerar la finalidad, incluye menciones que sólo deberían ser aplicables a las transferencias con encargados de tratamiento y no a las transferencias de responsable a responsable. En segundo lugar, porque los apartados 1 y 2 de la Norma 6.ª parecen pretender aplicarse a cualquier encargado internacional, cuando la Instrucción debe limitarse a establecer qué considera «*garantías adecuadas*» respecto de aquellas transferencias internacionales que requieran su autorización de acuerdo con la LOPD.

En relación al contrato a que se refiere la Norma 5.ª, además de la lógica necesidad de identificar a las partes y la finalidad de la transferencia, lo más relevante es que implica lo siguiente:

(i) la obligación del destinatario de tratar los datos recibidos exclusivamente para la finalidad de que se trate y conforme a Derecho español, en particular, adoptando las medidas de seguridad requeridas por la normativa de protección de datos personales vigente en España; de no comunicar los datos a terceros sin consentimiento del afectado y de devolver o destruir los datos una vez extinguida la relación contractual (lo cual no tiene un ajuste adecuado en una cesión que no consista en un encargo de tratamiento y que debería más bien corresponderse, en los otros casos, con el respeto del principio de calidad), y de reconocer un derecho de auditoría a la AEPD para comprobar el cumplimiento del contrato [21];

(ii) la responsabilidad solidaria de ambas partes frente a los afectados, a la AEPD y a los órganos jurisdiccionales españoles por los eventuales incumplimientos del contrato en que pudiera incurrir el destinatario, cuando sean constitutivos de infracción de la LOPD o produzcan un perjuicio a los afectados; y

(iii) la garantía de que el afectado podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, tanto ante el transmitente como ante el destinatario [22] (aunque esta men-

21 Estas últimas previsiones (destrucción y devolución de los datos y derecho de auditoría al importador por la autoridad de control del exportador) se prevén en la Decisión 2002/16/CE, esto es, en las transferencias de responsable a encargado, pero no en la Decisión 2001/497/CE.

22 En la Decisión 2001/497/CE, es el cedente el que debe atender las consultas de los afectados y de la autoridad de control en relación con el tratamiento de datos del cesionario. El cesionario queda obligado a atender las consultas del cedente o del afectado en relación con el tratamiento del importador y a cooperar con la autoridad de control sobre dicho tratamiento y a atender la opinión de tal autoridad de control al respecto. En la Decisión

ción habría de entenderse referida a la garantía del exportador de que estos derechos se ejerciten desde España y ante el responsable [23]).

Respecto del contrato a que se refiere la Norma 6.ª (que ha sido declarado nulo por sentencia de la Audiencia Nacional, como hemos comentado), es básicamente igual que el de la Norma 5.ª con excepción del punto (3) anterior (que no se deduce directamente de su redacción [24]), del hecho de que la finalidad está predeterminada y de que, por la propia aplicación del artículo 12 de la LOPD, las transferencias ulteriores sólo podrán hacerse en el marco de una subcontratación y actuando en nombre y por cuenta del transmitente.

Como hemos avanzado, la Norma 6.ª resulta confusa en su construcción pues parece aplicarse a cualquier tipo de transferencia con un encargado internacional, con independencia de que esté establecido en un país de nivel equiparable o adecuado o de que concurra otra de las excepciones del artículo 34 de la LOPD, lo cual no tiene sentido alguno y es contrario a la LOPD y a la Directiva.

Por otra parte, en la Norma 6.ª se mezclan consideraciones que son extemporáneas a las garantías «adecuadas», como son las menciones e implicaciones legales del artículo 12 de la LOPD que son aplicables a cualquier encargado. Esto tiene una gran relevancia a la vista de que la AEPD ha venido sosteniendo que, si el contrato con un encargado de tratamiento no contiene formalmente las menciones que establece como obligatorias, califica a tal transferencia como una cesión. Y ello resulta discutible porque la finalidad de la transferencia es el elemento que determina la existencia (o no) de una cesión [25]. Por tanto, no se puede pretender aplicar a una transferencia que tiene una finalidad de encargo de tratamiento (y, por tanto, que no tiene la consideración de cesión) las consecuencias previstas en la LOPD para la cesión y, en particular, las relativas al consentimiento de los afectados y a los deberes de información para con ellos, así como al tipo de contrato necesario para obtener, en su caso, la autorización de la AEPD. Otra cosa es que se incumplan las obligaciones que a un responsable y encargado competen conforme al artículo 12 de la LOPD.

En cualquier caso, la responsabilidad directa del responsable de los incumplimientos del encargado de la LOPD no debería entenderse como una mención obligatoria (como no lo es para un encargado nacional) sino como una clarificación del régimen legal de responsabilidad entre responsable y encargado establecido en el artículo 12 de la LOPD (y, por tanto, sin perjuicio de que el encargado responda de las infracciones que sólo a él le son imputables como establece el artículo 12.6 de la LOPD) que, además, se requiere solidaria frente a los afectados y las autoridades cuando esté sujeta a autorización previa de la AEPD [26].

Finalmente, no parece que esta Instrucción sea el lugar idóneo para establecer la prohibición de subcontratación del servicio de tratamiento, ya que, en su caso, sería una consecuencia de la obligación del encargado de no comunicar los datos a ningún tercero establecida en el artículo 12.2 de la LOPD (salvo, claro está, si el responsable le instruye para realizar una cesión a un tercero o le autoriza a subcontratar el servicio, en cuyo caso el encargado actuaría por cuenta del responsable). Lo que hubiera sido deseable es que la Norma 6.ª especificara que el encargado podrá comunicar a un tercero los datos objeto de tratamiento (y sólo en los términos previstos en la LOPD, es decir, por cuenta del responsable), siempre que se cumplan los requisitos adicionales que procedan si en la transferencia internacional ulterior no concurren las excepciones del artículo 34 de la LOPD.

Por tanto, en nuestra opinión, la Instrucción debería limitarse a constatar que la LOPD sigue siendo aplicable (en particular, los artículos. 5, 11, 12 y 27 de la LOPD) y que, sólo si no concurre alguna de las excepciones del artículo 34 en la transferencia internacional, establezca las menciones que a su jui-

2002/16/CE, el encargado queda sólo obligado a atender las consultas del exportador en la relación con el tratamiento del encargado, a atender la opinión de tal autoridad de control al respecto y a notificar al exportador cualquier solicitud directamente recibida del afectado sin responder a ella salvo expresa autorización del exportador.

23 Vid. Memoria Anual de la AEPD de 2002, página 83.

24 Sin embargo, en muchas autorizaciones internacionales de este tipo de transferencias otorgadas por la AEPD, se ha considerado necesario que se especifique en el contrato que estos derechos se ejerciten desde España y ante el responsable.

25 Art. 12.1 de la LOPD: «No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento».

26 Aunque la Norma 6.ª de la Instrucción no lo mencione expresamente, en el caso de que el encargado esté adherido a los Principios y las FAQs, seguirá siendo necesaria la celebración de un contrato entre responsable y encargado, pero la transferencia no requerirá autorización previa (FAQ núm. 10).

cio merecen la consideración de «*garantías adecuadas*», ajustándolas debidamente a la finalidad de los dos tipos de transferencias ante los cuales podemos encontrarnos, como ha hecho la Comisión.

Las cláusulas contractuales tipo

La Comisión tiene asimismo la facultad de decidir, *ex* artículo 26.4 de la Directiva, que determinadas cláusulas contractuales tipo ofrecen suficientes garantías (de conformidad con el artículo 26.2 de la Directiva). Los Estados miembros están obligados a adoptar las medidas necesarias para ajustarse a estas decisiones de la Comisión. Por tanto, la AEPD ha de autorizar de manera automática toda transferencia internacional basada en un contrato que incorpore las cláusulas contractuales tipo recogidas en estas decisiones.

Aunque la Instrucción sólo hace referencia expresa a estas decisiones en su Norma 5.ª [27] ha de entenderse que también es de aplicación a los contratos con encargados de tratamiento internacionales (Norma 6.ª). Tal y como se manifestaba en la contestación del Ministerio de Justicia español al cuestionario de la Comisión Europea sobre el grado de implementación de la Directiva, de julio de 2002, «*las decisiones de la Comisión Europea sobre transferencias internacionales de datos en aplicación del art 26.4 de la Directiva 95/46/CE tienen aplicación directa en España desde su publicación en el DOCE, tal y como extensamente se expuso en la razonada comunicación ad hoc emitida a solicitud de la Comisión Europea.*» [28].

Hasta la fecha, han sido tres las decisiones de la Comisión que han establecido esta clase de cláusulas contractuales tipo (CCT). La primera (Decisión 2001/497/CE, de 15 de junio de 2001), referida a las transferencias internacionales de responsable a responsable, y la segunda (Decisión 2002/16/CE, de 27 de diciembre de 2001), referida a las transferencias internacionales de responsable a encargado. La tercera (Decisión 2004/915/CE, de 27 de diciembre) modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo.

De acuerdo con las dos primeras decisiones, el contrato queda sometido a las normas de protección de datos del exportador. Las CCT responden a una estructura similar en ambos casos, previendo declaraciones y garantías de ambas partes, el régimen de responsabilidad frente a violaciones de las cláusulas establecidas en beneficio del afectado cuando se le causen perjuicios a éste (solidaria en la Decisión 2001/497/CE y subsidiaria del importador en la Decisión 2002/16/CE), obligaciones de cooperación con las autoridades nacionales de protección de datos (más amplias en la Decisión 2002/16/CE, que incluye un derecho de auditoría del importador por la autoridad de control y no sólo por el exportador) y previsiones sobre ley aplicable, mediación y jurisdicción.

Entre los principios aplicables al importador de acuerdo con la Decisión 2001/497/CE destacan, en particular, las restricciones a transmisiones ulteriores a un país que no proporcione una protección adecuada o no amparado por una decisión de la Comisión bajo el artículo 25.6 de la Directiva. En estos casos, la transferencia ulterior sólo podrá tener lugar cuando (i) los interesados hayan consentido inequívocamente si hay datos sensibles o hayan podido oponerse habiéndoseles suministrado información suficiente sobre la transferencia; o (ii) el tercero se adhiera a las CCT, previo acuerdo de exportador e importador, asumiendo las mismas obligaciones que el importador. Estos supuestos no han sido recogidos en la Norma 5.ª de la Instrucción, que requiere, en todos los supuestos, el consentimiento del afectado.

En cualquier caso, tanto la Decisión 2001/497/CE como la Decisión 2002/16/CE establecen que su aplicación sólo afecta a las transferencias de datos personales a países terceros desde la U.E. y, en ningún caso, al resto de condiciones y obligaciones establecidas en el Derecho nacional de cada Estado miembro.

Finalmente, sin perjuicio de las competencias asignadas por sus leyes nacionales, estas dos Decisiones otorgan a las autoridades nacionales de protección de datos la posibilidad de suspender o prohibir una transferencia si (i) se determina que la legislación a la que está sujeto el importador le impone desviaciones de las normas correspondientes sobre protección de datos que vayan más allá de las restricciones necesarias en una sociedad democrática, cuando tales exigencias puedan tener un importante efecto negativo sobre las garantías proporcionadas por las CCT; (ii) una autoridad competente

27 Norma 5.ª (Transferencias al territorio de otros Estados): «6. Surtirán el mismo efecto jurídico los contratos que pudieran celebrarse en el futuro al amparo de lo que, en su caso, dispongan las Decisiones de la Comisión de las Comunidades Europeas que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE, siempre que se acredite su íntegro cumplimiento.».

28 Vid. asimismo la Memoria Anual de la AEPD de 2002.

decide que el importador no ha respetado las CCT; o (iii) existe la probabilidad sustancial de que las CCT no se estén respetando o no se respeten en el futuro, y la continuación de la transferencia provoque un riesgo inminente de daños graves para los interesados.

La Instrucción recoge adecuadamente esta facultad y circunstancias en su Norma 5.ª (transferencias al territorio de otros Estados). Sin embargo, también lo hace inexplicablemente en su Norma 4.ª, respecto de transferencias a países en los que precisamente existe un nivel adecuado de protección. Y ello, a pesar de manifestar expresamente que recoge las mismas circunstancias que las previstas en estas Decisiones, cuando en realidad modifica su sentido y alcance. Por otro lado, la AEPD se atribuye también la facultad de suspender cualquier transferencia (con independencia de la concurrencia o no de las excepciones a la autorización) según lo dispuesto en la Norma 2.ª (Cumplimiento de las disposiciones de la Ley Orgánica 15/1999), lo cual supone una extralimitación de lo dispuesto en la Directiva y en la LOPD. Lo que el incumplimiento de la Norma 2.ª sólo (y nada menos) puede conllevar es la facultad de la AEPD de imponer las sanciones que sean aplicables en el marco de un expediente sancionador.

Por último, el nuevo conjunto de CCT de la Decisión 2004/915/CE, de 27 de diciembre, ofrece una alternativa más flexible al ya previsto en la Decisión 2001/497/CE, pudiéndose optar por cualquiera de los dos conjuntos como un todo (sin que quepa modificar ni combinar elementos de los dos conjuntos) [29].

El nuevo conjunto se diferencia del previsto en la Decisión 2001/497/CE fundamentalmente en los siguientes aspectos: (i) se flexibilizan los requisitos de auditoría; (ii) se precisan las normas que regulan el derecho de acceso con una mayor intervención del exportador de datos; (iii) a diferencia del régimen solidario de responsabilidad que caracteriza al conjunto de cláusulas ya existente, el exportador y el importador responden ante los interesados por el incumplimiento de sus respectivas obligaciones contractuales, siendo el exportador responsable si no realiza esfuerzos razonables para determinar si el importador es capaz de cumplir sus obligaciones (culpa *in eligendo*); y (iv) se reconoce a las autoridades de control la facultad de prohibir o suspender más fácilmente las transferencias basadas en este nuevo conjunto de cláusulas cuando el exportador rehúse tomar medidas contra el importador para hacerle cumplir las obligaciones contractuales o este último se niegue a cooperar de buena fe con las autoridades.

Las «reglas corporativas vinculantes»

El 3 de junio de 2003, el Grupo 29 publicó el documento de trabajo WP74 sobre reglas vinculantes corporativas para transferencias de datos internacionales (RCV). Su propósito era suministrar una guía para la adopción de códigos de conducta relacionados con transferencias internacionales de datos dentro de un mismo grupo. En particular, el Grupo 29 estableció que, en tanto en cuanto estas reglas corporativas sean vinculantes (por ley y en la práctica) e incorporen los principios de contenido identificados por el Documento de Trabajo WP12, de 24 de julio de 1998 (expuestos anteriormente), no hay razón por las que las autoridades nacionales de protección de datos no autoricen transferencias multinacionales dentro de un grupo de compañías.

Las RVC constituirían, pues, un instrumento adicional a los ya existentes para las transferencias internacionales y combinable con éstos, en particular, para las transferencias ulteriores desde el grupo a países terceros que no cuenten con nivel de protección adecuada.

Además de recordar los principios de contenido esenciales identificados en el Documento de Trabajo WP12 (lo cuales han de detallarse y adaptarse a los tratamientos realizados por el grupo de forma que puedan ser entendidos y efectivamente aplicables por aquellos que tienen responsabilidad de protección de datos en el grupo), el Grupo 29 identifica otros requisitos complementarios o adicionales que pueden resumirse como sigue:

— adopción de programas de formación adecuados y nombramiento de personas apropiadas con la responsabilidad de asegurar el cumplimiento de las RCV.

— auditorías (internas o externas) periódicas reportando directamente al órgano de administración de la matriz sin perjuicio de aceptar auditorías realizadas por inspectores de

29 Esta decisión responde al resultado de las negociaciones con la Comisión del proyecto de cláusulas contractuales tipo, presentado el 17 de diciembre de 2001 por la Cámara de Comercio Internacional y otras asociaciones empresariales, para su aprobación como cláusulas contractuales tipo («the alternative model contract») y sobre las que se pronunció el Grupo 29 en diciembre de 2003 (Dictamen 8/2003 WP84).

la autoridad de protección de datos o de auditores independientes actuando por su cuenta.

— un sistema que gestione las reclamaciones de los afectados con expresa identificación de un departamento específico a estos efectos.

— deberes de cooperación con las autoridades de protección de datos de manera que los afectados puedan beneficiarse de apoyo institucional.

— previsiones de responsabilidad y jurisdicción que permitan el cumplimiento real y efectivo de las RCV y la efectiva compensación de los daños causados a los afectados.

— aceptación de que los afectados pueden interponer acciones contra el grupo así como elegir la jurisdicción.

— información a los afectados de la existencia y contenido de las RCV y de que sus datos están comunicándose a otros miembros del grupo que están fuera de la U.E.

El Grupo 29 también propone la adopción de reglas de procedimiento que permitan a las compañías seguir un único proceso de legitimación ante la autoridad de protección de datos de un Estado miembro, que gestionará el otorgamiento de las autorizaciones con las distintas autoridades de los Estados miembros donde el grupo opera.

Abierto a consulta pública, se produjeron reacciones al Documento de Trabajo WP74 [30] que valoraron positivamente este instrumento, puntualizando, no obstante, algunos aspectos que requerirían una mayor clarificación. En particular, se apuntó la dificultad de suministrar un grado de detalle suficiente de todos los tratamientos realizados en el grupo, y la necesidad tanto de establecer un procedimiento de cooperación claro y realista entre las distintas autoridades nacionales de protección de datos; como de evitar un soporte contractual adicional a las RCV y de flexibilizar las transferencias fuera del grupo, y de clarificar las obligaciones del grupo en cuanto a su deber de cooperación con las autoridades nacionales de protección de datos (en particular, respecto de la entrega de las auditorías internas) y a cómo cumplir en la práctica las obligaciones de informar a los afectados de que las transferencias se sujetan a las RCV y otros deberes de información derivados del principio de transparencia [31].

La utilización e implementación de las RCV es una de las prioridades del Grupo 29 [32]. Así, el Grupo 29 ha elaborado, el 25 de noviembre de 2004 [33], un documento orientativo para grupos de empresas respecto de los extremos que ha de contener y probar una solicitud de autorización de reglas corporativas vinculantes. Finalmente, dos nuevos documentos de trabajo del Grupo 29 de 14 de abril de 2005 [34] han establecido unas guías más concretas respecto de la elección de la autoridad de protección de datos que liderará el proceso de autorización, de las cuestiones a desarrollar por el solicitante para la evaluación de su adecuación conforme al documento W74 por las autoridades de protección de datos que pueden verse implicadas en el proceso de autorización, así como unas líneas directrices para la cooperación de éstas.

Sin embargo, el Grupo 29 puntualiza en uno de estos documentos que la participación de las autoridades de protección de datos en la aprobación de las RCV es completamente voluntaria. En el Reino Unido, la autoridad de protección de datos, el *Information Commissioner*, emitió dos documentos en septiembre de 2003 y en febrero de 2004 [35] en los

30 ABN-AMRO; Accenture; American Chamber of Commerce to the European Union; Bundesverband der Deutschen Industrie; Gesellschaft für Datenschutz und Datensicherung e.V.; Confederation of British Industry; Citigroup; Daimler Chrysler; European Privacy Officers Forum; European Banking Federation; International Chamber of Commerce; International Communications Round Table; Japan Business Council in Europe; KPMG International; Coalition on Global Information Flows; Philips; Sidley Austin Brown & Wood LLP; y United States Council for International Business.

31 «Summary of the contributions received to the Article 29 Working Party, consultation on Binding Corporate Rules». European Commission, Internal Market DG, Services, Intellectual and Industrial Property, Media and Data Protection (Data Protection). LCN. October 2003.

32 Documento del Grupo 29 WP98, Document Strategy, de 29 de septiembre de 2004.

33 Documento WP 102 del Grupo 29, de 25 de noviembre de 2004, Model Checklist Application for approval of Binding Corporate Rules.

34 Documentos del Grupo 29, de 14 de abril de 2005, WP 108, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules y WP 107, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From «Binding Corporate Rules».

35 «Transfers of Personal data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. Putting the concept

cuales clarifica los requisitos que esta autoridad va a exigir, sobre la base de este Documento de Trabajo WP74, para aquellos grupos que deseen solicitar la autorización de RCV desde el Reino Unido. Sería pues deseable que la AEPD, siguiendo el ejemplo de su homóloga inglesa, estableciera una primera guía orientativa al respecto [36].

5 · REFLEXIONES FINALES

Como hemos visto, el régimen español de las transferencias internacionales, tributario de la Directiva, no deja de ser complejo y de imponer unos requisitos que no son fáciles de llevar a la práctica. La Instrucción dictada por la AEPD no deja asimismo de plantear dificultades, por lo que muchas transferencias internacionales a países terceros tratan de buscar acomodo en otras excepciones del artículo 34 de la LOPD, en particular, el consentimiento inequívoco del afectado, cuyo alcance, obtención y acreditación no está exento de problemas. Sin perjuicio de lo que resulte del recurso de casación interpuesto ante el Tribunal Supremo, sería conveniente que la Instrucción se adecuara no sólo al fallo de la Audiencia Nacional sino a las consecuencias que se derivan de su acertado razonamiento en aquellos extremos sobre los que ésta no pudo pronunciarse expresamente.

Sin embargo, no podemos desconocer que han sido positivas las iniciativas comunitarias de flexibilización e interpretación uniforme de la prohibición impuesta en la Directiva. Ciertamente, el sistema de «listas blancas» de países se ha revelado como el más útil en términos prácticos, pero, también, uno de los más difíciles de evaluar. Por otra parte, en la práctica, los sistemas de cláusulas contractuales tipo de las Decisiones 2001/497/CE y 2002/16/CE y el sistema de auto-certificación del Puerto Seguro no han sido utilizados con la frecuencia pretendida debido a las importantes cargas que asume particularmente el importador. Conscientes de que sigue siendo necesario analizar nuevas vías que permitan una adecuada ponderación entre la protección de la intimidad y los legítimos intereses empresariales en un contexto multinacional, en el seno comunitario se sigue profundizando en la simplificación y flexibilización de los sistemas existentes, en particular, con la reciente aprobación por la Comisión del nuevo conjunto alternativo de cláusulas contractuales tipo y los últimos trabajos del Grupo 29, impulsando el sistema de reglas corporativas vinculantes. Es quizás este último sistema el que está generando, al tiempo, más expectativas e incertidumbres en cuanto a su aplicación y utilidad prácticas, ya que requiere una involucración y criterios interpretativos uniformes por parte de todas las autoridades de protección de datos de la UE.

into practice in the United Kingdom.» (22 de septiembre de 2003) y «Required Contents of a Submission for Approval of "Binding Corporate Rules" to the Information Commissioner» (11 de febrero de 2004).

36 El Information Commissioner realizó una visita de trabajo el 28 de julio de 2004 a la AEPD en la que parece que examinó, entre otros, la aplicabilidad en el ámbito de las transferencias internacionales de las RCV (La Gaceta de los Negocios, 29 de julio de 2004).