FRÉDÉRIC BLAS[**]

Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales[*]

SUMARIO

Introducción. I. Las transferencias internacionales de datos en la Directiva 95/46/CE y en la Ley Orgánica de Protección de Datos[1] (LOPD). A. Las transferencias en la Directiva 95/46/CE. B. El régimen de la LOPD. C. La Instrucción 1/2000. D. La notificación al Registro General de Protección de Datos. E. Los países con nivel de protección equiparable al español. F. Las garantías para dar la autorización. G. La suspensión de la transferencia. II. La regulación del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD)[2] sobre las transferencias internacionales de datos. A. El cambio del ámbito territorial de las transferencias internacionales. B. Refuerzo del principio de cumplimiento previo de la legislación interna española. C. Países con nivel de protección adecuado. D. Garantías en caso de transferencia a países sin nivel adecuado de protección. E. Suspensión de transferencias. F. Procedimientos relacionados con las transferencias internacionales de datos. G. Las transferencias internacionales de datos y las denominadas Binding Corporate Rules. III. Instrumentos *ad hoc* de transferencia. A. Los principios de puerto seguro. B. Datos relativos a los pasajeros (PNR). IV. La necesaria búsqueda de estándares globales. A. El desarrollo de las BCR. B. "One world, one privacy". C. International Organization for Standardization (ISO).

* Fecha de recepción: 18 de agosto de 2009. Fecha de aceptación: 13 de octubre de 2009.

** Licenciado en derecho por la *Université du Littoral Côte d'Opale* (Francia); magíster en abogacía internacional por el Instituto de Estudios Bursátiles (Madrid); magíster en asesoría jurídica de empresas por la Universidad Politécnica de Madrid; especialista en derecho empresarial por la Universidad Politécnica de Madrid. En la actualidad forma parte del departamento legal de International Business Machines (IBM), donde asesora a los responsables ejecutivos de protección de datos en materia de transferencias internacionales de datos, *outsourcing* estratégico y políticas de privacidad para Europa, Oriente Medio y África. [blasfrederic@gmail.com]

1. [www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf].

2. [www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf].

D. La 30.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. v. Conclusiones

RESUMEN

El propósito de este artículo reside en (1) el análisis técnico-jurídico del sistema de protección de datos de la Unión Europea ciñéndose a las herramientas que ofrecen las legislaciones comunitaria y española para las transferencias internacionales de datos y (2) en destacar las propuestas más adecuadas para la creación de un sistema universal de privacidad.

PALABRAS CLAVES

Transferencias internacionales de datos, estándares globales de privacidad.

ABSTRACT

The purpose of this paper lies in (1) the technical and legal analysis of the data protection policies of the European Union keeping to the tools offered by European and Spanish legislations for international data transfers and (1) to highlight the most suitable proposals to create a universal privacy system.

KEYWORDS

International data transfers, cross border data transfers, global privacy standards, Safe Harbor Principles, Binding Corporate Rules.

INTRODUCCIÓN

Para una empresa multinacional es tan importante estar presente a nivel global, ofreciendo servicios y productos con los mismos estándares de calidad, como la posibilidad de poder compartir datos e información con sus distintas sedes, filiales y sucursales para centralizar o descentralizar el tratamiento de esta información y utilizarla como simple referente informacional o interpretarla de forma conjunta o sectorial con el fin de elaborar tendencias o propuestas estratégicas para mejorar la eficiencia o gestión empresarial.

También es cada vez más frecuente ver cómo las empresas, sin importar su tamaño, delegan o externalizan parte de sus servicios o tareas ("*outsourcing*") a otras empresas que les prestan dicho servicio en un país tercero, fuera del

Espacio Económico Europeo (servicios de "*call center*" o tratamiento de datos). Mucha de esta información contiene datos personales cuyo tratamiento y transferencia está sometido a numerosas limitaciones normativas con el fin de preservar la privacidad del individuo en cuestión.

La Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), preceptúa en su artículo 3.º la definición del dato de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". Esta conceptuación es muy amplia y posibilita numerosas interpretaciones cuya justificación es la posibilidad de adaptar la ley a los avances informáticos.

Según la Directiva 95/46/CE del 24 de octubre de 1995[3], en su artículo 2.a, "Identificable es toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

La LOPD, transposición de la directiva, fue hace poco completada por el Real Decreto 1720/2007, del 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, del 13 de diciembre, de protección de datos de carácter personal (RLOPD). Se desarrolla con esta norma no sólo un nuevo o modificado régimen en cuanto a las medidas de seguridad exigibles de conformidad con el principio de seguridad, sino todo el articulado de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal, habiendo además traído consigo un necesario desarrollo reglamentario específico de los ficheros no automatizados de datos de carácter personal.

Desde un punto de vista técnico-jurídico, habrá que entender como transferencia internacional de datos aquella que se da cuando exista comunicación por transmisión, difusión o cualquier otra forma de puesta a disposición de estos datos entre España y un país que no forma parte del Espacio Económico Europeo (EEE).

Los datos transferidos no deben tratarse posteriormente de manera incompatible con esta finalidad: el responsable de tratamiento debe poder establecer que la razón por la cual los datos se transfieren es compatible con las razones por las cuales se recogieron inicialmente los datos. Los datos transferidos deben ser adecuados, pertinentes y no excesivos respecto de las finalidades por las cuales se transfieren.

Cabe entonces plantearse los problemas de legitimidad de la transferencia y la pertinencia de los datos respecto de la finalidad de la transferencia. En efecto, aunque la Agencia Española de Protección de Datos (AEPD) no ponga en entredicho el método de funcionamiento de grupos internacionales, la existencia de vínculos de capital entre sociedades no podría en sí mismo justificar una centralización generalizada de los datos recogidos por

3. [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML]

las sociedades de un grupo, en particular, de la sociedad de cartera de éste. Una transferencia de datos que no responde a estas condiciones sería ilegal y podría, a este respecto, generar la responsabilidad (incluso hasta penal en países como Chipre o Italia) del responsable de tratamiento.

Lógicamente, ese trasiego de información conlleva el acceso remoto o el traslado de un lugar a otro y de un país a otro de enormes cantidades de datos de carácter personal sin cuyo movimiento a través de las fronteras difícilmente podría ser una realidad el comercio mundial.

Para evitar los posibles perjuicios que a la privacidad de las personas físicas podría causar ese trasiego de datos, los estados nacionales así como las uniones geopolíticas han establecido normas jurídicas o convenios para regular el intercambio. Ejemplo próximo de esto ha sido el establecimiento del Convenio de los llamados principios de "puerto seguro" (*safe harbor*) entre los Estados Unidos y la Unión Europea, que abre las puertas al intercambio de datos entre empresas estadounidenses y europeas, algo necesario para la revitalización del comercio mundial aunque ello reporte graves deficiencias para la seguridad de los datos y para la propia privacidad de las personas, como señalan algunos autores de forma muy objetiva.

En España, una transferencia internacional de datos que se efectúe sin respetar las normas conlleva numerosas consecuencias legales, siendo seguramente la más relevante (desde un punto de vista empresarial) la relativa a las elevadísimas sanciones que dicha conducta puede generar, con multas de hasta 600.000 euros por este tipo de falta muy grave.

En su artículo 33, la LOPD nos explica lo que sería la norma general para tener en cuenta, prohibiéndose cualquier tipo de transferencia de datos, ya fuese temporal o definitiva a países que no proporcionen un nivel de protección equiparable al que otorga la LOPD. La excepción a ello es que se haya obtenido la autorización previa del director de la Agencia Española de Protección de Datos.

En un primer tiempo analizaré detenidamente la legislación española y comunitaria sobre las transferencias internacionales de datos (I) antes de centrarme en las repercusiones del nuevo reglamento LOPD en ellas (II). También apuntaré algunos mecanismos específicos de movimientos internacionales de datos por su especialización sectorial o geográfica (III). Por fin, y frente a la versatilidad de los criterios de privacidad, procuraré resaltar entre los diferentes instrumentos y las propuestas de cambio, lo que a mi entender es el mejor camino hacia la búsqueda de estándares internacionales de protección de datos si, como es necesario, queremos mejorar la fluidez de las transferencias internacionales de datos y a la vez preservar altos niveles de protección (IV).

I. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN LA DIRECTIVA 95/46/CE Y EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD)

A. LAS TRANSFERENCIAS EN LA DIRECTIVA 95/46/CE

Las transferencias de datos tienen en el derecho español una regularización peculiar, con una sistemática y un enfoque diferentes de los que encontramos en la Directiva 95/46/CE. Cabe destacar al respecto que la regulación comunitaria europea se preocupa únicamente de regular la transferencia internacional de datos a países terceros, ya que dentro de la Unión Europea la circulación de datos personales es completamente libre (art. 1.2 Directiva 95/46/CE). Además, establece un criterio material para delimitar el concepto de transferencias internacionales de datos: será transferencia internacional cualquier salida fuera del territorio de la Unión Europea, con independencia de la causa que legitime ese tratamiento de datos. Por eso el legislador comunitario insiste tanto en que las transferencias deberán cumplir previamente las normas de protección de datos del estado miembro de procedencia de los datos (el exportador de datos).

También reitera la regla fundamental de que no pueden realizarse transferencias a países sin nivel de protección equiparable. Por excepción, se permite a los estados miembros que puedan autorizar la transferencia en una serie de situaciones concretas y, además, incluso fuera de esas situaciones, cuando el destinatario ofrezca garantías suficientes, incluso por vía contractual, de protección de la vida privada y de los derechos y libertades fundamentales de las personas, permitiendo a los afectados el ejercicio de sus derechos. En fin, se preocupa de unificar la praxis de los estados miembros en esta materia, de modo que no haya disparidad de criterios entre ellos. El enfoque de la Directiva 95/46/CE se dirige, sobre todo, a procurar la libertad de circulación de datos personales dentro del territorio de la Unión Europea y a que los estados miembros adopten una política comercial en las restricciones a la transferencia a países sin nivel de protección adecuado.

Como indica AGUSTÍN PUENTE ESCOBAR[4], en la directiva hay tres niveles sucesivos en el control de las transferencias internacionales. El primero cuando se pretende realizar la transferencia a un estado con un nivel adecuado de protección, supuesto de hecho en el que el exportador de datos debe limitarse a cumplir su normativa interna de origen (art. 25.1 Directiva 95/46/CE). El segundo es cuando el Estado no tiene un nivel de protección adecuado, pero concurre alguna de las circunstancias del artículo 26.1 de la Directiva 95/46/CE, supuesto en el cual también podrá realizarse la transferencia. El tercero y último es cuando no se da ninguno de los casos anteriores, en cuyo

4. AGUSTÍN PUENTE ESCOBAR. "Reflexiones sobre el desarrollo reglamentario de la Ley Orgánica de Protección de Datos de carácter Personal" en *La protección de datos*, Boletín del Ilustre Colegio de Abogados de Madrid, 2007, p. 109.

caso sólo podrá realizarse la transferencia internacional previa autorización del organismo competente.

B. EL RÉGIMEN DE LA LOPD

Como señala la sentencia de la Audiencia Nacional del 15 de marzo de 2002[5], el legislador español, sin apartarse en lo fundamental de la regulación comunitaria, sigue una sistemática distinta. La LOPD establece simplemente una norma general y una lista de excepciones. La norma general es la que aparece en el artículo 33 de la LOPD, a cuyo tenor "no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente ley, salvo que, además de haberse observado lo dispuesto en está, se obtenga autorización previa del director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas". Por lo tanto, sólo podrá producirse la transferencia a países sin nivel de protección equiparable al español, previa autorización del director de la AEPD. Por su parte, la lista de excepciones, o como dice el artículo 34 LOPD[6], los supuestos en que el anterior artículo no se aplicaría,

5. Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Secc. 1.ª, del 15 de marzo de 2002, rec. n.º 271/2001.

6. Artículo 34 LOPD. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación (se autorizarán las transferencias internacionales de datos):

a. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b. Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c. Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d. Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e. Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f. Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j. Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k. Cuando la transferencia tenga como destino un estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

son una lista con 11 epígrafes, sin ningún criterio sistemático ni lógico. De hecho, los cuatro primeros (letras *a* hasta la *d* del artículo 34 LOPD) son una reproducción prácticamente literal de los motivos de excepción que aparecían en la Ley Orgánica 5/1992, del 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD - cf. art. 33 LORTAD, vigente hasta el 14 de enero de 2000), mientras que los seis siguientes lo son de la lista de excepciones de la Directiva 95/46/CE (letras e hasta la j del art. 34 Directiva 95/46/CE). La última letra, artículo 34k de la LOPD, es un intento tanto de recoger en el derecho español la libertad de circulación de datos dentro de la Unión Europea como de reconocer una primacía de la Comisión Europea en determinar el nivel de adecuación de terceros países: "cuando la transferencia tenga como destino un estado miembro de la Unión Europea, o un estado respecto del cual la Comisión Europea, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado" (art. 34k LOPD). En relación con este apartado de la LOPD, la sentencia del 15 de marzo de 2002 afirma que es una forma muy modesta de plasmar en el ordenamiento español un principio básico del derecho comunitario. Además de la letra k, debe señalarse por su importancia el supuesto de la letra d: "cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista" (art. 34d LOPD).

Hay que tener en cuenta, y esto es fundamental para entender el sistema español de transferencias internacionales, que aunque muchas de las circunstancias del artículo 34 LOPD sean idénticas o similares a alguna de las circunstancias recogidas en los artículos 6 y 11 LOPD, dicho artículo no establece causas de legitimación del tratamiento, en este caso de la transferencia internacional de datos. Su significado es únicamente enumerar los supuestos de hecho que excluyen a la transferencia de la necesidad de autorización del director. Es decir que habrá que ver si la transferencia es legítima o no, de conformidad con las normas internas de la LOPD. También habrá que cerciorarse de que se cumplen el resto de principios del tratamiento (deber de información, proporcionalidad, respeto a la finalidad inicial…). Por tanto, aquí puede señalarse una regla fundamental en materia de transferencias internacionales, que no está debidamente resaltada en la LOPD:

–El exportador de datos debe cumplir, en primer lugar, la normativa interna española, y la transferencia sólo se podrá realizar si la legislación de protección de datos española lo autoriza, ya se trate de una transferencia-cesión, de una transferencia-encargo del tratamiento o de cualquier otro tipo.

Uno de los puntos fundamentales de toda la normativa sobre transferencias internacional de datos es el cumplimiento previo de la legislación interna, especialmente de lo relativo a la legitimidad de la cesión.

La regla del cumplimiento de la normativa interna española se deriva indirectamente de varios preceptos. La Directiva 95/46/CE comienza a regular la transferencia de datos personales a países terceros haciendo la salvedad de que esa transferencia deberá realizarse "sin perjuicio del cumplimiento

de las disposiciones del derecho nacional adoptadas con arreglo a las demás disposiciones de la presente directiva".

En la misma línea, el artículo 2.º de la Decisión 2001/497/CE señala que dicha norma "no afecta a la aplicación de otras disposiciones nacionales por las que se aplique la Directiva 95/46/CE". En el derecho español, el requisito aparece de modo fragmentario en el artículo 33.1 de la LOPD, para aquellas transferencias de datos que se realicen a países sin nivel de protección. Ya de forma completa para todos los tipos de transferencias, se recogió de forma expresa en el párrafo primero de la norma 2 de la Instrucción AEPD 1/2000 ("la transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia de verificar su cumplimiento").

Como ha recordado la sentencia del 15 de marzo de 2002, la ley no pretende que el responsable "quede liberado del conjunto de deberes y obligaciones que le impone la Ley Orgánica 15/1999; ni que pueda eludir las responsabilidades derivadas de su actuación. Únicamente queda liberado de la exigencia de autorización previa de la transferencia por el director de la Agencia".

C. LA INSTRUCCIÓN 1/2000

En relación con las transferencias internacionales, la Instrucción 1/2000 fue bastante útil. Hay que recordar que esta instrucción (Instrucción 1/2000, del 1.º de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos) ha sido, hasta la aprobación del RLOPD, la base fundamental de la regulación de los aspectos de detalle de las transferencias internacionales de datos, obviamente bajo la primacía de los artículos 33 y 34 LOPD.

De hecho, parte del contenido de la Instrucción 1/2000 fue anulado por los tribunales del orden contencioso-administrativo, precisamente por ser contrario a la LOPD. La Instrucción 1/2000 estableció que cuando el responsable pretenda inscribir una transferencia internacional de datos basada en alguna de las circunstancias del artículo 34 LOPD, la AEPD pudiera requerir al responsable del fichero para que aportara prueba de que se cumplía dicha circunstancia. Esas partes de la Instrucción fueron anuladas. La sentencia del 15 de marzo de 2002, posteriormente confirmada por la sentencia del Tribunal Supremo, Sala Tercera, del 25 de septiembre de 2006, rec. n.º 3223/2002, anuló la norma 4.1, la norma 3.2 y la norma 6 de la Instrucción 1/2000, si bien las dos últimas en cuanto pretenden extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción del artículo 34 de la LOPD. La norma 4.1 decía que en los casos de transferencias internacionales a países respecto de lo que se hubiera declarado un suficiente nivel de protección, la AEPD podía requerir la aportación

de documentación acreditativa de que se cumplían las disposiciones de la LOPD, y particularmente que existía consentimiento o el receptor de los datos era un encargado del tratamiento.

Por su parte, las normas 3.2 y 6 establecían una obligación similar pero sin distinguir unos países de destino y otro. Si no se facilitaba la información, la consecuencia es que se negaba la inscripción registral de la transferencia y por tanto ésta se hacía imposible. Para la Audiencia Nacional, las normas impugnadas pretenden "establecer unos mecanismos de control al margen de lo dispuesto en los artículos 33 y 34 de la LOPD" sin que pueda resultar "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 aún 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".

El Tribunal Supremo confirma la sentencia y considera lógica la interpretación que aparece en ella. Dice la Sala que el principio de jerarquía normativa impone la anulación de las normas referidas, ya que si la propia LOPD en su artículo 34, tal y como ya había regulado el artículo 26 de la Directiva 95/46/CE, establece unas excepciones en cuanto al control del director de la Agencia de Protección de Datos en las transferencias internacionales de datos, no puede la Instrucción 1/2000 establecer otros controles adicionales a un tipo de tratamiento de datos exentos de autorización administrativa.

Por tanto, el sistema español de transferencias internacionales de datos es bastante más sencillo de lo que aparentan la farragosa sistemática de la LOPD y la Instrucción 1/2000. El punto clave es el cumplimiento de la legislación interna: por ejemplo, sólo podrá procederse a una transferencia-cesión si la cesión de datos está legitimada conforme al artículo 11 LOPD o cualquier otro supuesto de legitimación. Una transferencia-encargo del tratamiento sólo será posible si el importador presta un servicio al responsable del fichero y se ha firmado el oportuno contrato del artículo 12 LOPD… Y además, en ciertos casos, será necesaria la autorización del director de la AEPD: cuando, en primer lugar, se destinen los datos a un país que no proporcione un nivel de protección equiparable al de la LOPD (art. 33.1 LOPD y art. 34k LOPD) y además, no se esté en alguno de los otros casos del artículo 34 LOPD. La autorización es, por así decirlo, una capa que se superpone a la normativa general.

D. LA NOTIFICACIÓN AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

Hay un requisito adicional más de índole formal, previsto en el artículo 26.2 LOPD, que es proceder a la notificación de las transferencias internacional "que se prevean realizar" mediante la oportuna inscripción o modificación

registral en el Registro General de Protección de Datos. Pero ese requisito no puede convertirse, como hemos visto, en una pseudoautorización de la AEPD, por vía de verificar el cumplimiento de dichos requisitos.

E. LOS PAÍSES CON NIVEL DE PROTECCIÓN EQUIPARABLE AL ESPAÑOL

La Directiva 95/46/CE habla de países con el nivel de protección adecuado (art. 25.1 Directiva 95/46/CE), mientras que la LOPD lo hace de países que proporcionen "un nivel de protección equiparable al que presta la presente Ley" (art. 33.1 LOPD). Se trata de una diferencia de expresión para reflejar una misma realidad. El artículo 33.2 LOPD reproduce casi literalmente los textos del artículo 25.2 Directiva 95/46/CE, para delimitar los criterios que llevan a considerar un país como con un nivel de protección adecuado o equiparable al español: "Se tomará en consideración la naturaleza de los datos de 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, el contenido de los informes de la Comisión de la Unión europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

La normativa española (cf. art. 34k LOPD) y la práctica de la AEPD dan una enorme importancia a las decisiones de los organismos comunitarios para delimitar qué países tienen un nivel de protección adecuado. Hay que recordar que la Directiva 95/46/CE parte del reconocimiento de un doble nivel de autoridades con potestad de declarar la adecuación de un país tercero: la Comisión Europea y las autoridades, que son las que determinan el derecho interno de cada país miembro. La directiva busca coordinar ambos grupos de autoridades, en varias formas: estableciendo criterios comunes para determinar el nivel de adecuación (art. 25.2 Directiva 95/46/CE), obligándolas a intercambiarse información recíprocamente (art. 25.3 Directiva 95/46/CE), estableciendo que los estados miembros deberán respetar las decisiones negativas de adecuación de la Comisión, es decir la declaración de que un tercer país no garantiza un nivel adecuado (art. 25.4 Directiva 95/46/CE) y que en tal supuesto la Comisión deberá iniciar negociaciones para "remediar la situación" (art. 25.5 Directiva 95/46/CE), y finalmente, estableciendo que la "Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado" (art. 26.6 Directiva 95/46/CE). En ejercicio de la potestad conferida por estos preceptos, la Comisión ha declarado la adecuación de varios países, o ciertos tratamientos de datos realizados en algunos países[7].

7. Suiza (Decisión 2000/518/CE, del 26 de julio de 2000) y desde marzo de 2009 en el marco de los principios de puerto seguro; Estados Unidos, en el marco de los principios de

El órgano al que el derecho español otorga potestad para determinar que un tercer país tiene un nivel adecuado de protección es la AEPD, que entre otros criterios deberá tener en cuenta "el contenido de los informes de la Comisión de la Unión Europea" (art. 33.2 LOPD). Sin embargo, hasta la fecha no ha efectuado ninguna declaración positiva ni negativa de adecuación de un país tercero. La práctica de la AEPD ha sido la de asumir todas las declaraciones positivas de la Comisión, considerando que los países declarados con nivel adecuado por las decisiones del órgano comunitario lo son a efectos del derecho interno español. La lectura de la norma 4 de la Instrucción 1/2000 produce la impresión de que la AEPD consideraba automáticamente como poseedores del nivel de protección equiparable al español, a efectos del derecho interno, a aquellos países respecto de los que la Comisión había realizado una declaración positiva de adecuación. También se consideran adecuados los países del Espacio Económico Europeo, o sea los 27 estados miembros de la Unión Europea más Noruega, Islandia y Liechtenstein.

F. LAS GARANTÍAS PARA DAR LA AUTORIZACIÓN

El artículo 33 LOPD preceptúa que en los casos en que para realizar la transferencia internacional sea necesaria la autorización previa del director de la AEPD, éste sólo podrá otorgarla si se obtienen las garantías adecuadas.

La LOPD guarda silencio sobre esas garantías, pero la normativa de la Unión Europea y la Instrucción 1/2000 apuestan claramente por la solución contractual. Esta solución consiste en exigir que el exportador de datos firme con el importador un contrato en que se comprometa a garantizar los niveles de protección de datos similares a los comunitarios o españoles. La solución contractual comunitaria se encuentra desarrollada en una serie de decisiones de la Comisión Europea, adoptadas de conformidad con el artículo 26.4 de la Directiva 95/46/CE:

a. Decisión de la Comisión 2001/497/CE y 2004/915/CE de las Comunidades Europeas, del 15 de junio de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país de conformidad con

puerto seguro (Decisión 2000/520/CE, del 26 de julio de 2000); Canadá, respecto de la Personal Information and Electronics Documents Act (Decisión 2002/2/CE, del 20 de diciembre de 2001); Argentina (Decisión 2003/490/CE, de 30 de junio de 2003); Guernsey (Decisión 2003/821/CE, del 21 de noviembre de 2003), Isla de Man (Decisión 2004/411/CE, del 28 de abril de 2004); Estados Unidos, respecto de los registros de nombres de los pasajeros (*passenger name record*) que se transfieren al servicio de aduanas y protección de fronteras (Decisión 2004/535/CE, del 14 de mayo de 2004, anulada por la Sentencia del 30 de mayo de 2006, asuntos acumulados C-317/04 y C-318/04, nueva autorización con la Decisión 2007/551/CFSP/JHA del 23 de julio de 2007); Canadá respecto de los registros de nombres de los pasajeros (*passenger name record*) que se transfieren a la Agencia de Servicios de Fronteras (Decisión 2006/253/CE, del 6 de septiembre de 2005); Islas Feroe (Dictamen 9/2007, del 9 de octubre de 2007); Jersey (Decisión 2008/393/CE, del 8 de mayo de 2008).

la Directiva 95/46/CE, modificada por la Decisión de la Comisión 2004/915/CE de las Comunidades Europeas, del 27 de diciembre de 2004 (transferencia de responsable a responsable).

b. Decisión de la Comisión 2002/16/CE de las Comunidades Europeas, del 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a los encargados del tratamiento establecidos en terceros países.

Estas decisiones llegan a incorporar un clausulado modelo para insertar en los contratos. Respecto de la Instrucción 1/2000, su norma 5 también incorpora una serie de cláusulas que obligatoriamente deben incorporarse al contrato, si se quiere obtener la autorización. Y al igual que ocurre con las decisiones de adecuación de un país tercero, la AEPD acepta sin reparos como garantías contractuales correctas las derivadas de las decisiones comunitarias citadas.

Ambos conjuntos de cláusulas son similares. Lo más destacado de ellas es que incorporan la responsabilidad frente a terceros que no son parte del contrato; al menos en el caso de los propios afectados sería válida en el derecho español, de conformidad con el artículo 1257, p. 2.º del Código Civil, que establece la validez de la llamada "estipulación a favor de tercero". La sentencia de la Audiencia Nacional del 15 de marzo de 2002, que enjuició la Instrucción 1/2000, avaló que se pudieran establecer garantías contractuales en transferencias-encargo a países sin nivel de protección adecuado.

Sin duda, la utilización de contratos se presenta como una forma útil y efectiva para permitir transferencias a terceros estados desde el punto de vista de los intereses de los operadores (artículo 33.1 de la LOPD). Los modelos contractuales presentados para las transferencias entre responsables de tratamiento de datos, el de 2001 elaborado por la Comisión, y el modelo de 2004 íntegramente propuesto por una coalición de empresarios liderada por la Cámara Internacional de Comercio de París, han sido considerados adecuados por la Comisión y capaces de asegurar los derechos de los interesados y de conciliarlos con las necesidades del tráfico privado de datos. Sin embargo, no cabe duda de que su articulación se muestra compleja y de difícil entendimiento para aquellos que no sean técnicos o especialistas en la materia.

G. LA SUSPENSIÓN DE LA TRANSFERENCIA

La genérica potestad de la AEPD de ordenar la cesación de los tratamientos (art. 37f LOPD) se convierte, en el caso de las transferencias internacionales de datos, en la posibilidad de suspender temporalmente la transferencia (norma 4.2 Instrucción 1/2000). Esta suspensión se producirá porque conste o haya indicios de que el destinatario ha vulnerado las normas o principios de protección de datos de su derecho interno (norma 4.2 Instrucción 1/2000).

II. LA REGULACIÓN DEL REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (RLOPD) SOBRE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

A. EL CAMBIO DEL ÁMBITO TERRITORIAL DE LAS TRANSFERENCIAS INTERNACIONALES

El nuevo Reglamento introduce una definición de transferencia internacional de datos: "tratamiento de datos que supone una transmisión de los mismos fuera del Espacio Económico Europeo […]" (art. 5t RLOPD)[8]. Consecuentemente, en el RLOPD los movimientos de datos a la Unión Europea ya no aparecen en la enumeración de las transferencias exceptuadas de la necesidad de autorización del director, a diferencia del resto de casos del artículo 34 LOPD (cf. art. 70 RLOPD).

Salta a la vista que el concepto de transferencia internacional de datos en la LOPD es completamente distinto, ya que en ella país tercero es, simplemente, cualquier país distinto de España. El artículo 34k de la LOPD hace imposible una conclusión distinta, ya que dicho precepto se refiere de forma meridiana al movimiento de datos a países de la Unión Europea u otros países respecto de los que se haya declarado un nivel adecuado de protección, como supuesto de transferencias internacionales. El RLOPD cambia radicalmente el ámbito territorial de las transferencias internacionales de datos ya que para la citada y posterior norma sólo existirá cuando los datos salgan fuera de las fronteras del EEE. Se ha justificado este cambio radical de definición como una necesidad de interpretar o adaptar el derecho español a la Directiva 95/46/CE. Sin embargo, la directiva tiene una finalidad muy distinta de la de la LOPD: lo que pretende la norma europea es, por un lado, armonizar las legislaciones de protección de datos de los estados miembros y de ahí la libertad de circulación de datos dentro de las fronteras de la Unión y, por otro, establecer una política común para la transferencia de datos fuera de esas fronteras. La LOPD es ajena a esa problemática, puesto que es una simple norma nacional sobre protección de datos. En realidad, el cambio que opera el Reglamento es de dudosa legalidad, por contravenir el tenor literal de la LOPD. Ahora bien, justo es reconocer que respeta el espíritu de la Directiva 95/46/CE en cuanto liberaliza completamente el movimiento de datos dentro de las fronteras del EEE.

8. El Espacio Económico Europeo (EEE) es el resultado de un acuerdo firmado entre los estados miembros de la Comunidad Europea, ahora Unión Europea, y los de las Asociación Europea de Libre Comercio. En la actualidad se aplica, además de a los miembros de la Unión Europea, a Islandia, Noruega y Liechtenstein, ya que Suiza, miembro de la Asociación Europea de Libre Comercio, rechazó por referéndum su ingreso en el EEE. La protección de datos se ha incorporado al Acuerdo del EEE en virtud de varias decisiones del Comité Mixto del EEE, por lo que, a estos efectos, los tres países mencionados están totalmente homologados a los estados miembros de la Unión Europea, participando en el Grupo de trabajo del artículo 29 de la Directiva 95/46/CE.

En efecto, con la nueva regulación no es sólo que nos será necesario pedir autorización al director de la AEPD (interpretación a contrario del art. 34k de la LOPD), sino que ya ni siquiera será necesario notificarlo al Registro General de Protección de Datos como tal transferencia internacional de datos.

B. REFUERZO DEL PRINCIPIO DE CUMPLIMIENTO PREVIO DE LA LEGISLACIÓN INTERNA ESPAÑOLA

En el artículo 63 del RLOPD aparece, con carácter universal para todas las transferencias, el principio de que antes de realizar una transferencia internacional de datos debe cumplirse con la normativa interna española: "La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, del 13 de diciembre, y en el presente Reglamento".

C. PAÍSES CON NIVEL DE PROTECCIÓN ADECUADO

Con el Reglamento se gana en seguridad jurídica en cuanto a la determinación de los países con adecuado nivel de protección de datos. No cambia ni la autoridad que debe declarar cuáles son esos países (el director de la AEPD), ni los criterios que debe seguir (art. 65.1 RLOPD). Pero se establece que las resoluciones por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el Boletín Oficial del Estado (art. 65.1 LOPD, p. 3.º), y que el director de la AEPD deberá publicar y actualizar una lista de países cuyo nivel de protección haya sido considerado equiparable (art. 65.2 LOPD).

Finalmente, se establece una base jurídica más clara para la aceptación automática de las decisiones de adecuación tomadas por la Comisión de la Unión Europea. Dice el artículo 66 RLOPD que "no será necesaria la autorización del director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuviera por importador una persona o entidad, pública o privada, situada en el territorio de un estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección". De hecho, el Reglamento considera en pie de igualdad al director de la AEPD y a la Comisión Europea, como órganos con capacidad de hacer declaraciones de adecuación.

D. GARANTÍAS EN CASO DE TRANSFERENCIA A PAÍSES SIN NIVEL ADECUADO DE PROTECCIÓN

El nuevo Reglamento acaba con la dualidad entre cláusulas contractuales de garantía existente entre las procedentes del derecho comunitario derivado

y las específicas del derecho interno español, establecidas en la Instrucción 1/2000.

El RLOPD se limita a decir, en este aspecto, que es preciso que exista un contrato escrito celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos (art. 68.2 RLOPD). Se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las decisiones de la Comisión referidas o que puedan dictarse en el futuro (art. 68.2, p. 2º RLOPD).

E. SUSPENSIÓN DE TRANSFERENCIAS

Se regulan con mayor amplitud y detalle las causas de suspensión temporal de las transferencias internacionales de datos. De este modo, no sólo se recogen los supuestos previstos en la Instrucción 1/2000, esto es, el incumplimiento real o potencial por el destinatario de su legislación interna de protección de datos (art. 67.1 RLOPD).

Aparecen ahora nuevos casos de suspensión relacionados no sólo con la aptitud del destinatario para cumplir las garantías exigidas contractualmente, sino también con la situación del país o simplemente con las circunstancias concurrentes si éstas pudieran poner en situación de riesgo de daño efectivo a los afectados (art. 68.1 LOPD). Esto nuevos casos de suspensión son relativamente amplios e inconcretos, por lo que se aumentan las potestades de la AEPD para decidir. Estas mismas causas lo son de denegación de la autorización (art. 68 RLOPD).

F. PROCEDIMIENTOS RELACIONADOS CON LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

Siguiendo una tendencia general de todo el Reglamento, se regulan con detalle todos los aspectos procedimentales que tienen que ver con las transferencias internacionales de datos:

–Procedimiento de autorización de transferencias internacionales de datos, con un periodo máximo de duración de tres meses y silencio positivo en caso de transcurso de dicho plazo sin emitir resolución (art. 136-138 RLOPD).

–Procedimiento de autorización temporal de transferencias internacionales de datos, en el que siempre se dará audiencia al exportador. Si se acuerda (o se levanta) la suspensión, esta circunstancia se inscribirá en el Registro General de Protección de datos (art. 139-142 RLOPD).

–El procedimiento de inscripción de la creación, modificación o supresión de ficheros (art. 129-133 RLOPD), en el que deben notificarse a la AEPD las transferencias internacionales de datos. En la regulación de este procedimiento se acepta la doctrina de la sentencia de la Audiencia Nacional del 15 de marzo y del Tribunal Supremo del 25 de septiembre de 2006, de modo que dentro del procedimiento de inscripción de transferencias internacionales de datos ya no se exige a los responsables que acrediten que se encuentran en algunos de los casos exceptuados del control administrativo de la AEPD.

G. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS Y LAS DENOMINADAS BINDING CORPORATE RULES

Dentro del apartado dedicado a las transferencias a países sin nivel de protección adecuado, el RLOPD dedica un apartado (art. 68.4 RLOP) a establecer una regulación embrionaria de las transferencias realizadas en el seno de grupos multinacionales de empresas, amparadas por las denominadas en inglés Binding Corporate Rules (BCR) o normas corporativas vinculantes.

El concepto de BCR es algo peculiar: una compañía se hace una promesa a sí misma, o sus filiales a su casa matriz: la de respetar la política intracorporativa de protección de datos. Las empresas han empezado recientemente a establecer normas de carácter interno, de obligado cumplimiento por todas las empresas del grupo, que regulan aspectos determinados generalmente relacionados con la seguridad de la información, código de conducta de empleados…

La doctrina civilista española mayoritaria expresa serias dudas sobre el carácter vinculante de las declaraciones unilaterales de voluntad y es que, salvo algún caso aislado expresamente reconocido por la ley, la voluntad unilateral que se estima vinculante para quien la declara es la que va acompañada del consentimiento del que la recibe, por lo que en realidad se trata de un control unilateral, con obligaciones para una sola de las partes. Por eso, en el artículo 68.4 RLOPD se acepta la posibilidad de dar una autorización a solicitudes en que se aporte como garantía la existencia de unas normas corporativas vinculantes, pero bajo una serie de requisitos: que las normas tengan un contenido acorde al nivel de protección de datos reconocido en la LOPD (art. 68.4, p. 1.º LOPD), que las normas o reglas resulten vinculantes para las empresas del grupo y exigibles conforme al ordenamiento jurídico español (art. 68.4, p. 2.º). Habrá que especificar los procesos para su ejecución interna tales como: auditoría, transparencia y publicidad frente a terceros, medios por los que los afectados podrán conocer su cumplimiento, procedimiento de tramitación de reclamaciones, sanciones... Finalmente, es necesario que el contenido de dichas normas sea exigible tanto por la AEPD como por los afectados (art. 68.4, p. 3.º LOPD), posibilidad que, como hemos

visto, es válida al menos en el caso de los afectados como consecuencia por aplicación del artículo 1257, p. 2.º del Código Civil.

III. INSTRUMENTOS AD HOC DE TRANSFERENCIA

A. LOS PRINCIPIOS DE PUERTO SEGURO

Uno de los intercambios de información que se realizan en la aldea global económica es el que viene sucediendo entre la Unión Europea y los Estados Unidos de América. La decisión de la Comisión del 26 de julio de 2000 (2000/520/CE) con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes (FAQ), publicadas por la Federal Trade Commission (Departamento de Comercio de los Estados Unidos de América).

El derecho a la privacidad se concibe en Estados Unidos de manera diferente de como se hace en Europa. En la concepción estadounidense, la importancia que se atribuye a otros derechos explícitamente garantizados por la Constitución, como la libertad de expresión, hace que el juego de equilibrios entre éstos y la privacidad sea diferente de su correspondiente en Europa. También el modelo de regulación de la privacidad en Estados Unidos es diferente del europeo.

El modelo europeo se construye a partir de normas de alcance general que aseguran niveles elevados de protección y permite también la autorregulación dentro del marco legal. El modelo estadounidense se caracteriza por su fragmentación y por su heterogeneidad. Existen varios niveles de regulación en Estados Unidos: el nivel federal por un lado, con un derecho de privacidad implícito en la Constitución que actúa como un régimen de mínimos; también a nivel estatal existen numerosas regulaciones derivadas de la autorregulación, sin alcance general y de adhesión voluntaria.

A pesar de estas diferencias, el común interés por asegurar un tráfico de datos fluido entre Estados Unidos y Europa ha motivado la adopción de los Safe Harbour Principles (SHP). Se trata de un cuerpo normativo adoptado por la FTC, tras un periodo de negociación con las autoridades europeas y para facilitar la recepción de datos enviados por responsables europeos. Lo que es característico de los SHP es que carecen de alcance general: sus reglas son de adhesión voluntaria y sólo cuando se suscriben son obligatorias. Esto es, las normas de protección de datos que contiene no son normas con rango legal (federal o estatal) obligatorias para todos, sino normas privadas de adopción voluntaria por parte de los empresarios establecidos en Estados Unidos.

Una vez suscritos los SHP, el empresario queda obligado y recibe la acreditación para tratar y comerciar con datos originarios de Europa. En concreto, el empresario se obliga a: respetar los principios de protección que constituyen el *safe harbor*, divulgar sus políticas de protección de la

vida privada y aceptar la competencia de la FTC como autoridad de control. En consecuencia, las transferencias que se dirigen a un empresario que ha suscrito los SHP no necesitan autorización de la AEPD (artículos 34.k de la LOPD y 68 del Reglamento PD). Por el contrario, las que se dirigen a un empresario estadounidense que no ha suscrito este régimen sí la necesitan.

Los SHP han sido criticados por la doctrina europea. Uno de los reproches es no definir de manera suficiente el principio de la finalidad del tratamiento, determinada y legítima. Éste aparece bajo la rúbrica de la "Notificación", completándose con un principio de "Opción", que permite que las entidades "ofrezcan a los particulares la posibilidad de decidir […] si su información personal […] puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida".

Según el considerando 5: el nivel adecuado de protección de la transferencia de datos desde la Unión Europea a Estados Unidos de América, reconocido por la presente Decisión, debe alcanzarse si las entidades cumplen los principios de puerto seguro para la protección de la vida privada, con objeto de proteger los datos personales transferidos de un estado miembro a los Estados Unidos de América, así que las FAQ, en las que se proporciona orientación para aplicar los principios, publicadas por el Gobierno de Estados Unidos de América con fecha 21 de julio de 2000.

Además, las entidades deben dar a conocer públicamente sus políticas de protección de la vida privada y someterse a la jurisdicción de la FTC a tenor de lo dispuesto en el artículo 5.º de la Federal Trade Commision Act, en el que se prohíben actos o prácticas desleales o fraudulenta en el comercio o en relación con él, o a la jurisdicción de otros organismos públicos que garanticen el cumplimiento efectivo de los principios y su aplicación de conformidad con las FAQ. La presente Decisión sólo se aplicará a los sectores y tratamientos que estén sujetos a la jurisdicción de la Federal Trade Commission o al Departamento de Transporte de los Estados Unidos de América.

Para garantizar la correcta aplicación de esta decisión, la FTC o su representante publicarán una lista de las entidades que autocertifiquen su adhesión a los principios y su aplicación de conformidad con las FAQ y que estén sujetos a uno de los organismos enumerados anteriormente.

1. Notificación

Las entidades informarán a los particulares: de los fines con los cuales se recoge y utiliza información sobre ellos, la forma de contactar con ellos para cualquier pregunta o queja, los tipos de terceros a los cuales se revelará la información, los medios y opciones que la entidad ofrece a los particulares para limitar su uso y su divulgación, la notificación se hará en lenguaje claro y transparente la primera vez que se invite a los particulares a proporcionar a la entidad información personal o, luego, tan pronto como sea posible, pero

en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que la transfiere o la divulga por primera vez a un tercero.

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

2. Opción

Las entidades ofrecerán a los particulares la posibilidad de decidir (por exclusión [*opt out*]) si su información personal puede divulgarse a un tercero o puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida, sin que haya sido autorizado luego por el particular. Se debe proporcionar a los particulares mecanismos claros y transparentes, fácilmente disponibles y accesibles para ejercer su derecho de opción.

Si se trata de información delicada o especialmente protegida como datos sobre estado de salud, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, vida sexual de la persona, la opción de participar debe ser afirmativa o explícita (aceptación [*opt in*]) si la información va a revelarse a un tercero o a utilizarse para un fin distinto del que inicialmente motivó la recogida de información o de una manera distinta de la autorizada después por éste al optar por la aceptación. En cualquier caso, una entidad debe tratar como delicada toda información recibida de un tercero cuando dicho tercero la identifique y trate como información delicada.

3. Transferencia ulterior

Para revelar información a terceros deberán aplicar los principios de notificación y opción. Cuando una entidad desee transferir los datos a un tercero que actúe como agente, podrá hacerlo si previamente se asegura de que éste:

a. suscribe los principios;
b. si es objeto de una resolución sobre su "adecuación" con arreglo a la directiva y otra disposición o
c. si firma con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios.

Si la entidad cumple estos requisitos, no será responsable (a menos que la propia entidad acuerde lo contrario) del tratamiento realizado por el tercero a quien haya transferido este tipo de información y que cumpliere las limita-

ciones o estipulaciones establecidas, a menos que la entidad sepa, o debiera saber, que el tercero realizaría dicho tratamiento y no haya adoptado medidas razonables para impedir o detener el tratamiento.

4. Seguridad

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

5. Integridad de los datos

La información de carácter personal, de acuerdo con los principios, debe ser pertinente para los fines con que se utiliza. Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el interesado.

En la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales.

6. Acceso

Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder: corregir, modificar, suprimir dicha información si resultase inexacta excepto en los casos siguientes:

–Cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleva para la vida privada de la persona.
–Cuando los particulares vulnerar los derechos de otras personas.

7. Aplicación

Para garantizar la conformidad con los principios se incluirán mecanismos que contengan:

–una vía de recurso independiente, asequible e inmediatamente disponible para investigar y resolver con arreglo a los principios las denuncias y litigios de los particulares y otorgar daños y perjuicios donde determinar la legislación aplicable a las iniciativas del sector privado.

–procedimientos de seguimiento para comprobar que los certificados y declaraciones de las empresas sobre sus prácticas en materia de vida privada se ajustan a la verdad y que dichas prácticas se aplican en consecuencia.
–una obligación de subsanar los problemas derivados del cumplimiento de los principios para las entidades que se hayan adherido a ellos y las sanciones correspondientes contra ellas, que serán suficientemente rigurosas para garantizar su cumplimiento.

B. DATOS RELATIVOS A LOS PASAJEROS (PNR)

Sobre la base del Título V del Tratado de la Unión Europea, la Unión Europea y los Estados Unidos han adoptado el Acuerdo sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros por las compañías aéreas al US Department of Homeland Security (Departamento de Seguridad del Territorio Nacional de los Estados Unidos [DHS]) (Acuerdo PNR 2007)[9]. Este acuerdo obliga a las compañías aéreas que realicen vuelos a Estados Unidos a transferir el registro de nombres de los pasajeros (PNR) al DHS. Los datos recogidos incluyen los datos relativos a la identidad del pasajero, los datos relativos al viaje (pago, itinerario, equipaje) y también datos sensibles que son aquellos relativos al origen étnico, religioso (que hicieron que el pasajero optara por un determinado menú), político, a la afiliación sindical o a la salud (*i. e*. el pasajero tenía movilidad reducida y necesitaba asistencia especial). En contrapartida, el DHS se compromete a tratar los datos de acuerdo con la carta que se adjunta al acuerdo, y sólo para los fines que fueron recogidos (seguridad pública y lucha contra el terrorismo).

Es importante subrayar que en estos casos la transferencia no se dirige a un sujeto de derecho privado sino a un sujeto de derecho público (DHS) y tiene su fundamento en un motivo de seguridad pública. Por este motivo, el Tribunal de Justicia en su sentencia del 30 de mayo de 2006[10] anuló la decisión de la Comisión que consideraba adecuada la protección de los datos personales incluidos en los registros de nombres de pasajeros que se transfieren al Servicio de Aduanas de Estados Unidos (Decisión 2004/535/CE). El Tribunal consideró que esa decisión caía fuera del ámbito de aplicación de la Directiva 95/46, y en concreto de su artículo 3.2. Este precepto indica que el ámbito de aplicación de la directiva no comprende los tratamientos

9. Decisión 2007/551/PESC/JAI: Decisión del Consejo, del 23 de julio de 2007, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007).

10. STJCE del 30 de mayo de 2006, as. C-317/04 y C-318/04.

de datos relativos a la seguridad nacional o al derecho criminal, como resultaban ser los tratamientos que comprendía la decisión[11]. En consecuencia, la competencia de la Comisión para adoptar la Decisión 2004/535/CE no podía en ningún caso derivar del artículo 25.6 de la directiva, razón por la cual la decisión se anulaba. A partir de ese momento comenzó un proceso de negociación entre la Unión Europea y Estados Unidos. Sobre una base de cooperación y a partir del título competencial derivado del Título V del TUE, se inició un proceso que ha resultado en la adopción de la Decisión 2007/551/PESC/JAI del Consejo[12].

IV. LA NECESARIA BÚSQUEDA DE ESTÁNDARES GLOBALES

Un sistema realista de estándares debe emerger. Es absolutamente imprescindible que estos estándares estén alineados con las realidades comerciales y políticas de hoy, pero deben también reflejar realidades tecnológicas. Tales estándares deben ser fuertes y creíbles, pero sobre todo, deben ser claros y realizables.

A. EL DESARROLLO DE LAS BCR

El sistema de BCR es probablemente, por lo menos a nivel intracorporativo, el instrumento más avanzado en materia de transferencia y política global de privacidad. Sin embargo, queda mucho por desarrollar ya que viendo los costes necesarios y la complejidad y variedad de los criterios para tener aprobadas las BCR en 30 países, es un ejercicio extremadamente lento y costoso. El elevado costo de las BCR al requerir a la compañía documentar sus procesos de tratamiento de datos a la satisfacción de cada autoridad nacional reguladora de protección de los datos en cada jurisdicción en la cual funcione en Europa es capaz de desanimar a las empresas más grandes y modernas.

Un esfuerzo reciente de simplificación ha sido la adopción del concepto de *lead regulator* o *leading authority* pero aún conservando la obligación legal de obtener la aprobación del resto de reguladores[13]. El *lead regulador* deberá ser el de la sede europea del grupo, de la filial a la que se hayan delegado responsabilidades en materia de protección de datos, la que toma las decisio-

11. Decisión de la Comisión del 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de Aduanas y Protección de Fronteras de los Estados Unidos (Bureau of Customs and Border Protection), Decisión 2004/535/CE (DOUE, L 235, del 6 de julio de 2004).

12. Sobre ese proceso y los actos conexos a la Decisión 2007/551/PESC/JAI, ver [http://europa.eu/scadplus/leg/es/lvb/l33277.htm].

13. Recomendación WP74 del Grupo de trabajo del artículo 29, del 10 de enero de 2007. [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf]

nes sobre los tratamientos, la que tenga el mayor número de transferencias o distinguirse por otros factores significativos (número de empleados…). En todo caso, la decisión será adoptada por consenso entre todas las autoridades implicadas. El objetivo es principalmente evitar el *forum shopping* y facilitar el diálogo entre el grupo empresarial y la *leading authority*.

El problema de partida que habrá que remediar en el futuro es que en los sistemas español, francés e italiano, las declaraciones unilaterales de voluntad no son fuentes de obligaciones (art. 1089 Código Civil español). En consecuencia, al no existir un posible recurso a la autoridad administrativa o judicial en caso de incumplimiento de la declaración unilateral de voluntad, el derecho a la protección de datos no quedaría garantizado. Como soluciones, cabe la posibilidad de incluir las BCR en los contratos con los clientes o los convenios colectivos con lo cual la obligación nace de un contrato. Otra solución podría ser la regulación legal expresa de las BCR como fuente de las obligaciones a favor de los afectados.

Puesto que todos estos reguladores independientes están libres de tener opiniones distintas de la que sostiene la *leading authority* es extremadamente difícil, en la práctica, conseguir la unanimidad requerida para tener sus Binding Corporate Rules aprobadas y, en la práctica, casi ninguno las tiene. General Electric obtuvo la aprobación de sus BCR después de gastar mucho tiempo y dinero, pero sólo para sus datos de recursos humanos. Philips obtuvo la aprobación de sus BCR (datos de recursos humanos y clientes) en mayo de 2007 y Accenture consiguió obtener esta aprobación en 20 países en mayo de 2009. En la actualidad, muchas empresas están interesadas en aprobarlas y es importante procurar simplificar el proceso sin bajar el nivel de seguridad (hasta el momento es probablemente el más exigente del mundo) para que esta solicitud no signifique años y años de negociaciones técnico-jurídicas con las 30 autoridades reguladoras de protección de datos.

Un gran y muy reciente avance en esta dirección es el paso que dio el Grupo de Trabajo del artículo 29 en su 69.ª reunión el 2 de octubre de 2008 al lanzar un procedimiento del reconocimiento mutuo entre 17 autoridades reguladoras de protección de datos, que son las autoridades de Francia, Alemania, Irlanda, Italia, Lituania, Luxemburgo, Países Bajos, España, Reino Unido, Noruega, Islandia, Liechtenstein, Chipre, República Checa, Malta, Eslovenia y Bulgaria. Se comprometieron a reconocer mutuamente las BCR enviadas mediante el procedimiento de coordinación. El reconocimiento mutuo es una obligación política, más que un cambio legal. Se basa en la confianza y en la consideración de que estos sistemas legislativos están basados en la directiva europea. La esencia del reconocimiento mutuo es que las autoridades reguladoras confían en que una vez la autoridad guía (*lead authority*) dé el visto bueno sobre el nivel de protección y los estándares ofrecidos, otras autoridades reguladoras de protección de datos acepten esta opinión como suficiente para proporcionar su propio permiso para las BCR solicitadas. Cabe esperar que otras autoridades reguladoras de protección de

datos se sumen al grupo de reconocimiento mutuo en los meses que vienen. Estos esfuerzos considerables y la prioridad dada a este asunto constituyen una señal muy positiva hacia las compañías multinacionales por parte del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE[14].

A mi entender es una solución muy positiva, a condición de que facilite el procedimiento. Para la empresa, facilita el libre flujo de información y supone la existencia de un valor añadido. Para los ciudadanos, les ofrece la publicidad de sus derechos y procedimientos más ágiles para su ejercicio. Por fin, para la sociedad, representan la implicación de la cultura de la protección de datos en la empresa y la colaboración con las autoridades de control.

B. "ONE WORLD, ONE PRIVACY"

Un mundo, un sistema de protección de datos, es el reclamo de numerosas instituciones y de gran parte del mundo empresarial. Es tan necesario para la seguridad jurídica de todos como difícil de poner en práctica por la variedad de sistemas que podemos encontrar en el mundo, sin hablar de los países donde no hay ningún marco normativo al respeto.

Los futuros estándares globales de privacidad habrán de basarse en numerosos principios básicos, piedras angulares de la protección de datos como:

–El consentimiento: en cuanto a recopilación, uso o revelación de nuestros datos personales, salvo en los casos permitidos por la ley. Cuanto más sensibles sean los datos, más claro e inequívoco deberá ser el consentimiento.

–La responsabilidad: la recopilación de datos conllevará con ella la carga de la prueba en cuanto al respeto de los procedimientos y las políticas de privacidad que deberán ser documentados y comunicados de forma transparente así como asignados a un responsable dentro de la organización. En caso de transferencia a terceros países será necesaria la búsqueda de un nivel equivalente de protección mediante contratos o cualquier otra herramienta.

–El propósito: una organización deberá especificar las razones por las cuales se recopilan, usan, comunican o revelan los datos personales y comunicárselas a los particulares mientras lo hacen o antes de ello. Los objetivos deberán ser claros, relevantes y limitados según las circunstancias.

–Limitación a la recopilación, el uso y la revelación: éstos habrán de ser justos, legales y limitados a los objetivos.

–Exactitud: información completa y actualizada como para cumplir con los objetivos.

14. [www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/d1813d5911e138b-dc2256cbd00313d1c/c5ffdf5b790ad656c2256cbe0036f9d8/$file/press%20release_en.pdf]

–Seguridad: asumir la responsabilidad de la seguridad de los datos personales durante sus ciclos de vida con estándares de seguridad (físicos, técnicos y administrativos) reconocidos internacionalmente.

–Acceso: la posibilidad de acceder, rectificar, cancelar sus propios datos o de oponerse a su tratamiento.

–Cumplimiento: es necesario establecer políticas de protección de datos transparentes y públicas sobre el tratamiento y el acceso a los datos así como sobre el proceso de reclamación o denuncia.

C. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

Si la protección y los flujos internacionales de datos personales plantean numerosas problemáticas jurídicas, los aspectos técnicos y las medidas de seguridad son indisociables de ellos. La 29.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad[15], que tuvo lugar en Montreal en septiembre de 2007, puso en evidencia esta necesidad y apoya una serie de medidas para la elaboración de normas eficaces y universalmente aceptadas en materia de protección de la información personal y pondrá a disposición de la ISO los conocimientos técnicos y especializados que tiene sobre dichas normas.

La Conferencia hizo un llamado a sus miembros a participar más activamente en el proceso de elaboración de normas de la ISO por medio de sus respectivos organismos normativos nacionales. Dada la limitación de recursos que enfrentan muchos miembros, la Conferencia los invitó a encontrar la manera idónea de combinar sus conocimientos y capacidades técnicas con el fin de poner dichos conocimientos y capacidades técnicas a disposición de la ISO así como a encontrar la mejor vía para coordinar sus aportes al proceso de elaboración de normas, con el fin de asegurar que dichos aportes sean uniformes entre los miembros de la Conferencia.

Las normas que actualmente están siendo elaboradas por el nuevo grupo de trabajo de la ISO son la norma ISO 29101 (marco de referencia sobre la privacidad que establece las mejores prácticas para la implementación técnica uniforme de los principios de privacidad), la norma ISO 29100 (marco sobre privacidad que define los requisitos de privacidad para el procesamiento de información de carácter personal en cualquier sistema de información de cualquier jurisdicción) y la norma ISO 24760 (marco para que la gestión de información sobre la identidad se realice de manera segura, fiable y respetuosa de la privacidad).

15. [www.agpd.es/portalweb/canaldocumentacion/comparecencias/common/03_Resolucion_datos_de_los_pasajeros.pdf]

D. LA 30.ª CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Esta última conferencia, que tuvo lugar en el mes de octubre de 2008 en Estrasburgo, confirma la tendencia a la universalidad de la protección de datos recordando toda la buena voluntad demostrada y los esfuerzos de estandarización que se están haciendo al día de hoy:

–La elaboración de un Convenio universal forma parte del programa de trabajo de la Comisión de Derecho Internacional de las Naciones Unidas.

–El Consejo de Europa está a favor de la adhesión al Convenio 108 de estados no miembros que cuenten con una adecuada legislación de protección de datos, y ha mostrado su determinación para promover este instrumento a nivel mundial. El Consejo ha destacado asimismo la vocación potencialmente universal del Convenio 108, especialmente en la Cumbre Mundial de la Sociedad de la Información de Túnez (noviembre de 2005) y en el marco del Foro de Gobierno de Internet en Atenas (2006) y Río de Janeiro (2007).

–La OCDE adoptó el 12 de junio de 2007 una recomendación relativa a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad, que pretende optimizar los marcos normativos nacionales para una mejor aplicación de las leyes sobre privacidad. Y ello principalmente para permitir que las autoridades nacionales puedan cooperar de un modo más eficaz con autoridades de terceros países y para que se puedan elaborar mecanismos internacionales eficaces que faciliten la cooperación internacional en la aplicación de las leyes de privacidad.

–Las conferencias regionales de la Unesco de 2005 (Asia-Pacífico) y 2007 (Europa) subrayan el carácter prioritario de la protección de datos.

–Las distintas iniciativas del Grupo de Trabajo del artículo 29 sobre la protección de datos personales para simplificar los procedimientos de aprobación de normas corporativas vinculantes (BCR), que permiten el intercambio transfronterizo de datos mediante la aprobación de políticas internas de protección de datos en empresas multinacionales.

–Los jefes de Estado y de Gobierno de los países francófonos se comprometieron en su 11.ª Cumbre, celebrada en Budapest en septiembre de 2006, a intensificar, en el plano nacional, los trabajos legislativos y reglamentarios necesarios para el establecimiento del derecho fundamental a la protección de datos y a trabajar, a un nivel global, de cara a la elaboración de un convenio internacional que garantice efectivamente el derecho a la protección de datos.

–El Foro de Cooperación Económica Asia Pacífico (APEC) aprobó en noviembre de 2004 su Marco de Privacidad, con el ánimo de fortalecer la protección de la privacidad y permitir los flujos de información. En septiembre de 2007 el APEC lanzó asimismo el *Privacy Pathfinder*, que tiene por objeto impulsar la aprobación de normativas que permitan esclarecer responsabilidades en los flujos internacionales de datos derivados de las necesidades empresariales, reducir los costos de cumplimiento con la normativa, facilitar a los consumi-

dores instrumentos efectivos de protección de sus derechos, dotar de mayor eficacia a los reguladores y minimizar las cargas administrativas.

–La Asociación Francófona de Autoridades de Protección de Datos Personales (AFAPDP), creada en Montreal de forma paralela a la 29.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, incluye entre sus objetivos la elaboración de un convenio universal y la realización de esfuerzos para promover la adhesión al Convenio 108 de estados no miembros del Consejo de Europa.

–La Red Iberoamericana de Protección de Datos (RIPD)[16] adoptó una declaración con motivo de su sexto encuentro, celebrado en Colombia en mayo de 2008[17], en la que invitaba a todas las conferencias internacionales en materia de protección de datos, independientemente de su ámbito geográfico, a concentrar sus esfuerzos con vistas a adoptar un instrumento jurídico conjunto.

–Las Autoridades de Protección de Datos de Europa Central y del Este (CEEDPA), en su última reunión celebrada en junio de 2008 en Polonia, manifestaron su deseo de continuar e impulsar la realización de actividades comunes en el marco de la CEEDPA, en concreto la elaboración de soluciones comunes y el apoyo a nuevos miembros en la implantación de su legislación de protección de datos.

V. CONCLUSIONES

1. Con el crecimiento de la sociedad de la información, el derecho a la protección de datos y a la privacidad es una condición indispensable en una sociedad democrática y liberal para garantizar el respeto de los derechos humanos así como la libre circulación de información en una economía de mercado.

La globalización de los intercambios y tratamientos de datos personales, la complejidad de los sistemas informáticos, los potenciales perjuicios derivados de la mala utilización de unas tecnologías cada vez más potentes y el incremento de las medidas de seguridad requieren de una respuesta rápida y adecuada, con vistas a garantizar el respeto a los derechos y libertades fundamentales y en concreto al derecho a la privacidad.

Las diferencias persistentes en materia de protección de datos y respeto de la privacidad en el mundo, y especialmente la ausencia de garantías en muchos estados, perjudican los intercambios de datos personales y la puesta en práctica de una protección de datos efectiva y global. El desarrollo de reglas internacionales que garanticen, de un modo uniforme, el respeto a la protección de datos y a la privacidad resulta prioritario. El reconocimiento de

16. [www.agpd.es/portalweb/internacional/red_iberoamericana/index-ides-idphp.php].

17. [www.agpd.es/portalweb/internacional/red_iberoamericana/encuentros/VI_Encuentro/common/acta_vi_encuentro_2008.pdf].

estos derechos pasa por la adopción de un instrumento legislativo universal y vinculante, que haga uso, consagre y complemente los principios comunes de protección de datos y de respeto a la privacidad enunciados en los diferentes instrumentos existentes, y que refuerce la cooperación internacional entre autoridades de protección de datos.

2. La adopción de recomendaciones elaboradas por organizaciones como la APEC o la OCDE, especialmente en lo relativo a la creación de marcos internacionales que permitan impulsar el respeto a los derechos de protección de datos y privacidad en el contexto de las transferencias internacionales de datos, supone un positivo avance de cara a lograr este objetivo.

3. La adhesión a instrumentos vinculantes universales, como el Convenio del Consejo de Europa para la protección de las personas con respecto del tratamiento automatizado de datos de carácter personal (STE n.º 108) y su Protocolo adicional relativo a autoridades de supervisión y flujos internacionales de datos (STE n.º 181), que incluyen principios básicos de la protección de datos, probablemente facilitará el intercambio de datos entre las partes al promover mecanismos y plataformas de cooperación entre autoridades de protección de datos. Asimismo prevé la creación de autoridades que ejerzan sus funciones con completa independencia, promoviendo también la implementación de un adecuado nivel de protección.

4. En cuanto al nuevo RLOPD, debe destacarse la importante novedad que supone el cambio del ámbito territorial en el propio concepto de transferencia internacional de datos ya que se ajusta al espíritu de la Directiva 95/46/CE, que no es otro que remover todo obstáculo al movimiento de datos personales dentro de las fronteras de la Unión, y por extensión el EEE. A raíz de la entrada en vigor del Reglamento es mucho más fácil enviar datos a otros países europeos.

5. Entre la firmeza de las normas comunitarias y la flexibilidad del marco de la APEC existe una tercera vía que es la que desarrolla Canadá. Desde la adopción en 2000 del Federal Personal Information Protection and Electronic Documents Act (PIPEDA), Canadá apunta a tener la flexibilidad de las pautas de la OCDE mientras que proporciona el rigor del acercamiento europeo. En Canadá, como en los Estados Unidos, la ley establece diversos regímenes para los sectores públicos y privados, que permite un mayor foco en cada uno.

Como también ha estado sucediendo en los Estados Unidos en años recientes con leyes del Estado, las leyes provinciales han desempeñado recientemente un papel principal en el desarrollo el modelo canadiense a pesar del hecho de que el PIPEDA crea un marco de protección de datos que requiere de las leyes provinciales ser substancialmente similares al estatuto federal. Se trata aquí de una legislación híbrida que favorece a los ciudadanos y a las empresas y podría representar perfectamente el principio de un modelo para seguir al

balancear muy cuidadosamente la protección de datos con las necesidades del negocio e intereses comerciales.

6. Como lo hemos visto, son numerosos los distintos convenios con vocación internacional, pero no favorecen la uniformidad del derecho de protección de datos y, por consecuencia, las transferencias internacionales de datos. La aprobación de un instrumento universal precisa la ayuda y colaboración de aquellas organizaciones que son lo suficientemente importantes para tener una voz global pero lo suficientemente humanas para preocuparse realmente por la protección de datos. Necesitan demostrar que es posible y deseable crear un marco de estándares globales para satisfacer no sólo sus intereses sino también los de los individuos.

El mundo de los negocios debe demostrar a las autoridades reguladoras que es capaz de operar de forma global, interactuar a través de redes y aún así respetar la privacidad. No se trata de adoptar una política ligera de protección de datos sino de demostrar que la privacidad cuenta y que están preparados para colaborar con las autoridades reguladoras para encontrar una solución global a este reto global. Es lo que estamos viendo con las últimas conferencias internacionales de autoridades de protección de datos y privacidad y los *international workshop*[18] (talleres), que permiten el encuentro entre los responsables de protección de datos (*Chief Privacy Officer*) de importantes empresas que tratan grandes cantidades de datos (Google, Philips, IBM, Facebook, Hewlett Packard, Microsoft…) con los directores de agencias de protección de datos, formando grupos de trabajo que van proponiendo soluciones cada vez más interesantes y respetuosas de este derecho fundamental.

7. Debido a la fecha del cierre editorial de esta revista, me es imposible comentar la 31.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad[19] (Madrid, 4, 5 y 6 de noviembre 2009), en la cual se habrá propuesto la adopción de un texto común, muy orientado a lo que es la visión europea de protección de datos y con vocación universal.

Participamos, en nombre de IBM, comentando los primeros borradores de este proyecto (The Road Toward Global Privacy Standards[20]) cuya redacción está al cargo de la AEPD, dejando en claro la importancia, en cuanto a las medidas de seguridad por aplicar, de restar cualquier tipo de responsabilidad al encargado del tratamiento ya que éste debe recibir las medidas de seguridad aplicables del mismo responsable de tratamiento sin perjuicio de que se vea obligado a responder por sus faltas por medio de los mecanismos de la responsabilidad contractual. También resaltamos, para que el texto acordado no

18. *Workshop on international data transfers of personal data* [http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/index_en.htm].

19. [www.privacyconference2009.org/privacyconf2009/index-ides-idweb.html].

20. [www.agpd.es/portalweb/canaldocumentacion/comparecencias/common/IAPP_Privacy_Summit_09.pdf].

se convierta en papel mojado, que la aprobación de estándares globales de protección de datos, sea por convenio, tratado u otra forma, deberá otorgar al país firmante la condición de país con nivel de protección equiparable según los criterios de la Comisión Europea.

La pesadilla administrativa que supone autorizar transferencias de datos en algunos países y la ausencia total de mecanismos de protección en otros hacen necesario la adopción de un texto común y es, con las Binding Corporate Rules, la solución más prometedora para el establecimiento de una regulación global o por lo menos sectorial de la privacidad.

8. La protección de datos en la Unión Europea garantiza, con diferencia, el sistema más alto de seguridad, pero la directiva europea resulta desfasada con la realidad de los negocios y de las empresas cada vez más globalmente integradas.

Importantes razones históricas justifican un nivel tan alto ya que durante la Segunda Guerra Mundial la revelación de datos acerca del origen étnico o racial conllevó a denuncias secretas, secuestros, incautaciones y atrocidades directamente relacionadas con la privacidad de los individuos.

Sin embargo, la protección de datos es todavía una política emergente en algunos países y en otros ni existe este concepto, con lo cual es primordial sentar las bases de una especie de convenio universal, Carta Magna de la privacidad por desarrollar en el futuro, siguiendo la línea del acuerdo matriz. Los nuevos estándares globales de protección de datos habrán de ser adaptados a la realidad de los flujos transfronterizos y con vocación universal.

Aunque redactados a través del prisma de la directiva europea, no deben ofrecer un nivel máximo de protección sino un nivel mínimo como para garantizar lo fundamental, para que sea un suelo de garantías (y no un techo) en el cual podamos construir una política de privacidad coherente con el mundo real.

BIBLIOGRAFÍA

Fernández López, J. M. "Movimientos internacionales de datos y buen gobierno corporativo" en *La protección de datos* (I), Boletín del Ilustre Colegio de Abogados de Madrid, 2007.

Linklaters. *A report on the status of data protection legislation in Europe in 2008*, 2008.

Puente Escobar, Agustín. "Reflexiones sobre el desarrollo reglamentario de la Ley Orgánica de Protección de Datos de carácter Personal" en *Protección de Datos*, *Otrosí*, *Boletín del Ilustre Colegio de Abogados de Madrid*, 2007.

Sancho Villa, D. *Transferencia internacional de datos personales*, Madrid, Agencia de Protección de Datos, 2003.

Sancho Villa, D. "Protección de datos personales y transferencia internacional: cuestiones de ley aplicable", en *Revista jurídica de Castilla y León*, n.º 16 (monográfico), septiembre de 2008.