Las transferencias internacionales de datos y las libertades individuales: un acercamiento a las normas de protección de datos*

Elena García-Cuevas Roque
Doctora en Derecho. Profesora Asociada
Departamento Derecho Político
Universidad Nacional de Educación a Distancia

Recibido: 01.10.2012
Aceptado. 15.10.2012

Resumen: Proteger la intimidad personal y, en general, las libertades individuales frente a la transferencia internacional de datos personales, ha sido y sigue siendo una constante preocupación, no sólo para el jurista, sino también para el ciudadano, potencial afectado. Bajo este prisma, es obligado dar a conocer las normas jurídicas existentes, tanto a nivel nacional como internacional en torno a tal problemática, amplificada por los continuos progresos de la tecnología informática.

Palabras clave: transferencia internacional, Supervisor Europeo, datos personales.

Abstract: *The protection of privacy and individual liberties in general from international data transfer has been and remains a constant source of concern not only for legal professionals but also for citizens in general, who are after all the potential victims of abuses. From this standpoint, it is essential to study and understand existing national and international legislation governing data transfer and protection, an ever-expanding field in the face of technological progress.*

Key words: *international data transfer, European Supervisor, personal data.*

1. INTRODUCCIÓN

El problema de la seguridad informática en la «telaraña mundial» es alarmante. No en vano, el Director de la Agencia Española de Protección de Datos

* Este trabajo se ha desarrollado en el marco del Proyecto de investigación «Constitución y globalización: transformaciones del Estado constitucional y constitucionalización de espacios supranacionales». Referencia del Proyecto: DER2009-10375. Entidad financiadora: Ministerio de Educación y Ciencia.

(en lo sucesivo, AEPD) ha resaltado que el desarrollo tecnológico dificulta la protección de la intimidad: «afecta grave e intensamente a los derechos fundamentales e incluso puede condicionar el contenido de las normas jurídicas»[1]. Traspasar las barreras políticas y geográficas, aunque necesario para activar la libre circulación de personas y cosas y mejorar las relaciones comerciales y culturales, presenta, sin duda, grandes inconvenientes, pues los derechos recogidos en las leyes de protección de datos pueden verse seriamente amenazados si no se actúa con cautela y bajo un control que garantice un grado de seguridad en las transmisiones. Debe procurarse, entonces, el delicado equilibrio entre intereses económico-comerciales e intimidad personal.

2. GÉNESIS DE LA REGULACIÓN JURÍDICO-INTERNACIONAL DEL MOVIMIENTO INTERNACIONAL DE DATOS

Las Directrices sobre los Principios Rectores para la reglamentación de los ficheros computarizados de datos personales de la ONU –1990–, las Líneas Directrices sobre la protección de la intimidad y los flujos internacionales de datos de la OCDE –1980–, el Convenio 108 del Consejo de Europa –1981– (véase nota 6, página 4 del presente trabajo) y la propuesta de Directiva de la Comunidad –1992– son los principales textos que abordan la ordenación de la protección de los datos personales de un modo general. En todos ellos, a pesar de sus diferencias, el movimiento internacional de datos ha sido objeto de una regulación autónoma, observándose cierta uniformidad en los mismos a la hora de abordar la cuestión.

Sabemos que la OCDE ha perseguido estimular y desarrollar la economía y comercio internacional, analizando las consecuencias de los nuevos desarrollos tecnológicos informáticos en este campo. Las actividades de la Organización, en cooperación con el Consejo de Europa, han sido diversas e intensas sobre todo en los años setenta y principios de los ochenta; fue el caso del simposio celebrado en Viena en 1977, donde se puso de manifiesto que las transmisiones internacionales de datos constituían la preocupación básica de esta organización. El fruto de este simposio fue el desarrollo de unas líneas directrices por un Grupo de Expertos en 1978 en un texto que fue adoptado por el Consejo de Ministros de la OCDE en forma de recomendación a los Estados miembros en 1980, en la línea de intentar evitar, en lo posible, el establecimiento de obstáculos a la libre circulación de datos que dificulten el necesario desarrollo económico y social; todo ello, sin olvidar la presencia de eventuales riesgos.

[1] Tras su experiencia como Director de la Agencia Española de Protección de Datos, éstas fueron las palabras vertidas por Piñar Mañas, J. L., *¿Existe la privacidad?,* Inauguración Curso Académico 2008-2009, Universidad CEU San Pablo, Fundación Universitaria San Pablo-CEU, Madrid, 2008, p. 13.

Uno de los principales objetivos del ya citado Convenio 108, que entró en vigor en 1985, ha sido conciliar «los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos», destacando sus disposiciones sobre los flujos transfronterizos de datos y de cooperación y ayuda mutua entre las partes contratantes; todo ello, tomando como base las resoluciones de 1973 y 1974 del Consejo de Europa. Por lo demás, el Convenio 108 se convierte en un transcendente instrumento de cohesión.

El objetivo de la Unión Europea (en lo sucesivo, UE) es fundamentalmente económico; sin ir más lejos, el Tratado de la UE de 1992 consiguió la creación del «Mercado interior», el cual implicó un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales quedaba garantizada de acuerdo con las disposiciones de dicho Tratado. A partir de los años noventa la UE comenzó a mostrar una mayor sensibilidad hacia el ámbito de los derechos fundamentales, siendo particularmente intensa la actividad del Parlamento Europeo, de la Comisión y del Consejo.

La solución jurídica adoptada en el ámbito internacional a la problemática del movimiento internacional de datos ha sido, en líneas generales, considerar que entre dos países afectados por flujos de datos a través de sus fronteras, la información deberá circular tan libremente como en el interior de cada uno de los territorios respectivos, siempre y cuando, como se indicará en los epígrafes siguientes, el nivel de protección otorgado al individuo en cada uno de los ordenamientos afectados sea similar[2].

3. TRANSFERENCIA INTERNACIONAL DE DATOS Y SU CONSIDERACIÓN EN LA LEGISLACIÓN ESPAÑOLA

«El libre flujo de los datos personales constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra»; así rezaba la Exposición de Motivos de la ya derogada Ley Orgánica 5/1992, de 29 de octubre (LORTAD).

Por transferencia o flujos internacionales de datos se entiende, con arreglo a las Directrices de la OCDE, los movimientos de datos de carácter personal a través de las fronteras nacionales; esta expresión, «transferencia de datos», debe considerarse aplicable a todos los flujos de datos (entre sistemas informáticos) a través de las fronteras, fuera del territorio de Espacio Económico Europeo –EEE–, que constituyan una cesión o comunicación de los mismos, ya sea entre sujetos

[2] Cfr. Ripoll Carulla, S., «El movimiento internacional de datos. Legislación española y derecho internacional», *Revista TELOS* nº 37, marzo-mayo 1994, Cuaderno Central, disponible en *http://www.campusred.net/telos/anteriores/num_037/cuaderno_central10.html*, (última consulta: 07/02/2012).

de Derecho Público[3] o de Derecho Privado, así como aquellos que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español (art. 5.1 t Reglamento de la Ley Orgánica de Protección de Datos[4] –en lo sucesivo RLOPD–), independientemente de cuál sea el soporte mediante el que se envían los datos o la forma de tratamiento, pues de no concebirse de esta manera, quedarían sin sentido algunas leyes de protección de datos[5], amparándose en el art. 12 del Convenio 108 del Consejo de Europa. Obsérvese que, en esta definición, el RLOPD circunscribe el concepto de transferencia internacional a la salida de los datos fuera del EEE, tanto si el destinatario de los datos en el extranjero tiene la consideración de cesionario o de simple encargado del tratamiento de los mismos, de lo que se infiere que la comunicación o cesión de datos entre países de la UE no tendrán consideración de transferencia internacional, no necesitando, entonces, la notificación para su inscripción en el Registro General de Protección de Datos; en efecto, el movimiento de datos entre los países de la Comunidad Europea es libre por aplicación del art. 1.2 de la Directiva 95/46 CE[6]; por lo tanto, en el seno de la UE no deberán existir problemas; éstos pueden surgir entre la UE como un todo y los países terceros, esto es, los Estados no miembros. Se ha puesto de manifiesto, asimismo, que la comunicación o cesión de datos se refiere a una «salida física» de los mismos y no «salida jurídica», ya que puede continuar siendo de aplicación la legislación nacional; en consecuencia, no se puede identificar el carácter internacional de la transferencia con la pérdida de competencia de la Ley Española[7].

---

[3] Es el caso del tráfico que se produce en el marco de la cooperación internacional en materia penal, policial o aduanera: el Convenio de aplicación del Acuerdo de Schengen que contempló la supresión gradual de controles en las fronteras o el Convenio de creación de la Oficina Europea de Policía en la UE son buenos ejemplos.

[4] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal. La necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva 95/46/CE (véase nota 6, página 4 del presente trabajo) y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que estos años de vigencia han puesto de manifiesto la conveniencia de una mayor precisión que doten de seguridad jurídica al sistema, justificaron la creación de este Reglamento. Véase nota 10, página 4 del presente trabajo.

[5] Velázquez Bautista, R., *Protección jurídica de datos personales automatizados,* Colex, Madrid, 1993, p. 171.

[6] Directiva del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta Directiva y el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, mencionado en páginas anteriores, constituyen la piedra angular en materia de protección de datos.

[7] Verdaguer López, J. y Bergas Jané, Mª A., *TODO Protección de Datos*, CISS (Grupo Wolters Kluwer), Valencia, 2012, p. 356.

Se ha visto, pues, la necesidad de que estas transmisiones de datos se sometan a algún control, pues de otro modo, podrían propiciarse los llamados «paraísos de datos», anulando en gran medida cualquier tipo de protección nacional. Aquélla Ley 31/1987, de 18 de diciembre, de Ordenación de las Telecomunicaciones[8] y la vigente Ley 7/2010, de 31 de marzo, General de la Comunicación audiovisual, son una buena prueba de control: «mediante ley podrá limitarse el intercambio de comunicaciones», prescripción de gran relevancia, ya que los datos personales no se tratan siempre con arreglo a la normativa o se protegen de igual forma en el país receptor y emisor.

La protección de datos está armonizada en la UE, a través de la ya mencionada Directiva 95/46/CE, a nivel de los Estados miembros y, a través del Reglamento 45/2001[9], a nivel de las instituciones europeas. Por su parte, la Ley Orgánica de Protección de Datos[10] (en lo sucesivo LOPD), bajo el epígrafe «Movimiento internacional de datos», en su título V, y el Reglamento que desarrolla la misma, regula la transferencia de datos más allá de las fronteras y sus requisitos, de acuerdo con la protección existente en el destino. En cualquier caso, estamos ante una de las actividades más delicadas que han provocado una regulación muy cautelosa por parte de estas normas, como se tendrá ocasión de comprobar. Aunque el Tribunal de Justicia de las Comunidades Europeas, en el caso de *Bodil Lindqvist* en noviembre de 2003, afirmó que la difusión de datos personales a través de Internet no se considera una transferencia internacional de datos, existen opiniones divergentes sobre el particular, lo que ha llevado a afirmar que la Directiva 95/46/CE presenta algunas deficiencias en la regulación de este fenómeno. Y así es; la Directiva parece reconocer los aspectos positivos de las Transferencias Internacionales de Datos en lo que atañe al desarrollo del comercio, pero podría no abarcar

---

[8] La adaptación del marco jurídico nacional de Telecomunicaciones al comunitario conlleva la modificación de la Ley 31/1987, de Ordenación de las Telecomunicaciones con la Ley 32/1992, de 3 de diciembre, (de modificación de la Ley 31/1987, de 18 de diciembre, de Ordenación de las Telecomunicaciones). La Comunidad Económica Europea, a través de la Comisión y del Consejo, fijó el ámbito normativo común de este sector de las comunicaciones, dictando, entre otras, las Directivas de la Comisión de las Comunidades Europeas 88/301/CEE y 90/388/CEE, relativas a la competencia en los mercados de terminales y servicios de telecomunicación, basadas en el artículo 90, apartado 3, del Tratado.

[9] Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Véase epígrafe IV del presente trabajo.

[10] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En su momento, y en la redacción de la ya derogada Ley Orgánica 5/1992 y la actual Ley Orgánica 15/1999, fueron especialmente útiles para la comprensión de la protección de los derechos de las personas frente a las tecnologías, la ley de *Hesse* en Alemania (1970), la *Datalag* sueca (1973), la *Privacy Act* estadounidense (1974) y la *Data Protection Act* inglesa (1984), entre otras.

algunas situaciones, en la medida en que no son las consecuencias de una transferencia de datos voluntaria directa o indirecta por parte de una persona situada en Europa (…); la transferencia al exterior de Europa es el resultado de la naturaleza mundial e interactiva de las redes utilizadas por los residentes europeos[11]. Desde este punto de vista, deberá observarse la Directiva 2002/58/CE[12] sobre la privacidad y las comunicaciones electrónicas, la cual contempla el reciente desarrollo de los servicios de Internet y la naturaleza global de su infraestructura.

3.1. Aspectos más relevantes de la Ley española

En el anteriormente mencionado título V de la LOPD se acoge el principio básico de reciprocidad del Convenio 108, que supedita el flujo internacional de datos, necesario para el desarrollo cultural, económico y de seguridad mutua de los Estados, a la existencia en el país receptor de los datos personales de garantías similares a las del transmisor[13]; en este caso, a las que se establecen en la LOPD: «No podrán realizarse transferencias temporales ni definitivas de datos (…) con destino a países que no proporcionen un nivel de protección equiparable al que presta la LOPD, salvo (…) autorización –expresa– previa del Director de la AEPD, que sólo podrá otorgarla si se obtienen garantías adecuadas»; así reza el art. 33 de dicha ley, siendo ésta la norma general; o como se afirma en el art. 25 de la Directiva, «el país tercero de que se trate garantice un nivel de protección adecuado», lo que se evaluará atendiendo a todas las circunstancias que concurran o relacionadas con la transferencia («Considerando» 57º Directiva 95/46/CE): naturaleza de los datos, la finalidad y duración del tratamiento; el país de origen y el país de destino final, las normas de Derecho, así como las normas profesionales y medidas de seguridad vigentes en dichos países[14]; estas circunstancias también están reflejadas en el art. 67 RLOPD. Estos criterios son indicativos; un criterio adicional podría ser el de que un nivel de protección inadecuado pudiera

---

[11] Poullet, Y., «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», *Revista española de Protección de Datos* nº 1, Agencia de Protección de Datos de la Comunidad de Madrid-Civitas, julio-diciembre 2006, pp. 99-100.

[12] Directiva del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

[13] Pérez Luño, A.-E., *Manual de Informática y Derecho,* Ariel, Barcelona, 1966, p. 53, en su análisis de la estructura normativa de la Ley.

[14] A pesar de las similitudes existentes entre el art. 33 LOPD y el art. 25 Directiva 95/46 en lo que se refiere a este extremo, se ha puesto de relieve la conveniencia de que la Ley española determine de un modo concreto, en la transposición, un sistema que garantizara el principio establecido en la Directiva; no olvidemos que la norma europea establece unas obligaciones dirigidas a los Estados miembros, no a los responsables de los tratamientos. Aparicio Salom, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2000, p. 188.

causar perjuicios a los afectados[15]. Con ello «no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales (…)», atendiendo, además, a las formalidades que se precisen, como, por ejemplo, haber obtenido el consentimiento para la cesión o haber formalizado, en su caso, el contrato de servicios. Se observa que los principios inspiradores de este precepto y siguientes se basan en el Convenio 108 del Consejo de Europa y en el Acuerdo de Schengen. Entraré, más adelante, en el sentido que debemos otorgar a lo que se ha llamado «protección equivalente».

En su momento fue de gran ayuda, en la interpretación de este artículo, la Instrucción 1/2000, de 1 de diciembre, de la AEPD, relativa a las normas por las que se rigen los movimientos internacionales de datos[16], arrojando algo de luz en cuestiones tan complejas y señalando los criterios orientativos, ante el elevado número de dudas que se suscitaron por parte de los responsables de los ficheros y la sociedad en general; la adaptación de las normas reguladoras en esta materia a lo estipulado en los artículos 25 y 26 Directiva 95/46 ha generado una abundante casuística en la actuación de la Agencia, no recogida sistemáticamente, hasta la mencionada instrucción, en ningún texto. Pero, sabemos que las Instrucciones no aportan innovación alguna en la normativa existente; su finalidad es aclarar y facilitar, en un único texto, el procedimiento seguido por la Agencia «para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos». La Instrucción 1/2000 contemplaba supuestos específicos atendiendo al país al que los datos se destinen o en función de la finalidad última que motiva la transferencia.

La definición de Transferencia Internacional de Datos que proporcionó esta Instrucción es claramente distinta a la que, una vez aprobado el RLOPD, se encuentra en el ya referenciado art. 5.1 t de este último, motivo por el cual, se debe entender que aquella Instrucción ha sido derogada por el mencionado Reglamento, al menos en todo aquello que se oponga o contradiga al mismo. En todo caso, el régimen regulador del movimiento internacional de datos se encuentra gobernado por el principio general incluido en el mencionado art. 25 de la Directiva, consistente en que «la transferencia a empresas o Administraciones ubicadas en el territorio de terceros Estados deberá entenderse sin perjuicio del cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las disposiciones de la presente Directiva».

---

[15] Así rezan las enmiendas 78.ª, 80.ª y 127.ª del dictamen del Parlamento Europeo. Heredero Higueras, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal*, Aranzadi, Pamplona, 1997, p. 189.

[16] Disponible en *http://campus.usal.es/~derinfo/derinfo/PTD/INSTDINT.htm* (última consulta: 14/02/2012).

La regla general, pues, es el principio de reciprocidad en cuanto que este artículo 33 LOPD exige, a los países destino, un nivel de protección de los datos automatizados de carácter personal equiparable al de la LOPD. Pero se pone en manos del Director de la AEPD el determinar qué se entiende por «equiparable» y, por tanto, si hay o no garantía en otros países para transmitir los datos de carácter personal. Ahora bien, «protección equiparable» significa semejante, «equivalente» –expresión utilizada en el art. 12 del Convenio 108, pero no idéntico[17]; por su parte, la Directiva 95/46/CE se basa en el concepto de «nivel de protección adecuado», carácter que se refiere al nivel de la protección, no a la protección como tal; se ha considerado que este último concepto es más débil y abierto, así como menos restrictivo que el de «protección equivalente»[18] o protección suficiente»; y así es, la equivalencia hubiera exigido una comparación analítica entre dos documentos: la ley extranjera y la de la UE, con el efecto de la adopción por parte del país tercero de una legislación, copia de la Directiva; en cambio, la protección adecuada de la Directiva tiene en consideración el objeto y efectividad de la protección[19]. Debe considerarse, en principio, que un Estado tercero ofrece un nivel de protección «adecuado» si ha ratificado el Convenio 108 (art. 25.6 Directiva 95/46/CE). Obviamente, a tales efectos se realizará una valoración de conjunto (que no se reserva a la AEPD) del sistema de protección, es decir, se valorarán las ya enumeradas circunstancias bajo las cuales vaya a tener lugar la transferencia de datos: la naturaleza de los mismos, la finalidad a que se destinan y la duración del tratamiento, país de origen y país de destino, las normas vigentes sobre tratamiento, medidas de seguridad, normas profesionales propias del país de destino o códigos deontológicos (art. 25. 2 Directiva 95/46/CE) y, por último, el contenido de los informes de la Comisión de la Unión Europea

---

[17] Cfr. Ull Pont, E., *Derecho Público de la Informática (Protección de datos de carácter personal)*, UNED, Madrid, 2000, pp. 148 y ss, así como, Aparicio Salom, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, *cit.,* p. 189. Parece que la Directiva 95/46/CE establece dos criterios diferentes en lo que se refiere a la utilización de estos términos: a) entre los estados miembros, «nivel equivalente» de protección; b) en las relaciones con terceros países, «nivel adecuado». Sobre ello, cfr. Estadella Yuste, O., «La transmisión internacional de datos personales y su control» en *Jornadas sobre el Derecho Español de la Protección de Datos Personales,* Agencia de Protección de datos, Madrid, 1996, p. 202.

[18] Heredero Higueras, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal, cit.*, p. 187, para quien «el nivel de protección adecuado» se configura como una norma en blanco a rellenar por la Comisión. Verdaguer López, J., y Bergas Jané, Mª A., *TODO Protección de Datos, cit.,* p. 361, considera también que la terminología que emplea la LOPD es más restrictiva que la que utiliza la Directiva.

[19] Poullet, Y., «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», *cit.,* pp. 102-103, siguiendo las opiniones vertidas por el *MethodologyPaper,* adoptado por el Grupo *Artículo 29*, *Data Protection Working Party, Working Document: Transfers pf personal data to third countries: Applying Articles 25 y 126 of the EU Data Protection Directiva,* 24 de julio de 1998, WP 12.

sobre dicho país; a la vista de lo expuesto, se tendrán en cuenta las normas no jurídicas que puedan existir en el tercer país en cuestión, siempre que estas normas «se cumplan». Por lo demás, es interesante el sistema de coordinación que establece la Directiva en el citado artículo en cuanto a las condiciones para autorizar o denegar las transferencias, al disponer que los Estados miembros y la Comisión se informarán recíprocamente de los casos en que se consideren que un tercer país no garantiza un nivel de protección adecuado, siendo esta última quien inicie, en el momento que considere oportuno, negociaciones con terceros países que no garanticen un nivel de protección adecuado; asimismo, y con arreglo al art. 26 Directiva 95/46/CE, los Estados miembros informarán a la Comisión y a los demás Estados de la UE acerca de las autorizaciones singulares de transferencias internacionales que concedan. Como consecuencia de todo ello, la AEPD, al igual que el resto de autoridades nacionales de protección de datos comunitarias, perderá cierto protagonismo en el ámbito internacional.

En esta equiparación, arriba referenciada, de la protección jugaron un papel decisivo la Orden del Ministerio de Justicia e Interior de 2 de Febrero de 1995, que contiene la Primera Relación de Países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos, así como, la Orden del Ministerio de Justicia de 31 de Julio de 1998, por la que se amplía dicha relación a Italia y a Grecia[20], en virtud de la facultad (que no competencia exclusiva) que confirió la disposición final, 1ª, RD 1332/1994 LORTAD al Ministro de Justicia e Interior. Las legislaciones de los distintos países se encuentran en un proceso de continua evolución, de modo que la relación de países presenta un carácter abierto («lista blanca»); además, estas legislaciones son heterogéneas entre sí, por lo que dicha relación debe integrarse por varias relaciones parciales, especificando de forma separada los países que proporcionan un nivel de protección equiparable al español, según se trate de ficheros de titularidad pública o de ficheros de titularidad privada.

Aunque se deduce cierta inseguridad de todo lo expuesto, y pueden surgir dudas respecto de algunos Estados que no sean «seguros» al no existir una declaración oficial, debe imperar una interpretación del sistema establecido por la LOPD lo más acorde posible con la Directiva; ello significa que «no podrán realizarse exportaciones de datos a países terceros salvo que se hayan declarado como destinos seguros por el Ministerio de Justicia (Órdenes de 1995 y 1998) o se haya obtenido previamente autorización de la AEPD»[21] (véase de nuevo art. 33.2 LOPD y 25.2 Directiva 95/46).

---

[20] Órdenes disponibles en *http://noticias.juridicas.com/base_datos/Admin/o020295-mji.html* y *http://www.juridicas.com/base_datos/Admin/o310798-mj.html* (última consulta: 17/01/2012).

[21] Cfr. Aparicio Salom, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, *cit*., pp. 188-189.

Lo cierto es que el Director de la AEPD acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado «equiparable», conforme a lo detallado con anterioridad; esta lista se publicará y mantendrá actualizada a través de medios informáticos o telemáticos (art. 67.2 RLOPD).

Efectivamente, este es el último aspecto relevante que se debe subrayar del mencionado artículo 33 LOPD y la prescripción del art. 66 del RLOPD: la necesaria «autorización» del Director de la AEPD en las cesiones de datos a países que no ofrezcan un nivel equiparable de protección[22], autorización que sólo podrá otorgar si se obtienen las garantías adecuadas aportadas por el exportador (art. 70 RLOPD). Dichas garantías fueron concretadas en la Decisión de la Comisión 2001/497/CE de las Comunidades Europeas, de 15 de junio de 2001, modificada por la Decisión de la Comisión 2004/915/CE de las Comunidades Europeas, de 27 de diciembre de 2004, la cual cubre las transferencias efectuadas por responsables del tratamiento establecidos en la Comunidad a otros destinatarios establecidos en terceros países que actúan como responsables del tratamiento y, por último, la Decisión 2002/16/CE, de 27 de diciembre de 2001. La autorización «podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte 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. 70.2 RLOPD). La autorización se tramitará conforme al procedimiento establecido en los arts. 137 a 140 del RLOPD.

En ocasiones, se efectúan transferencias de datos sin atender a estas prescripciones de la Ley, lo que conlleva unas sanciones con multas muy cuantiosas al encontrarnos ante faltas graves o muy graves.

Por último, cabe la posibilidad de que el Director de la AEPD deniegue o suspenda temporalmente, previa audiencia del exportador, la transferencia (art. 37.1 f LOPD), cuando concurran las concretas circunstancias recogidas en el art. 70.3 RLOPD. En estos casos, se notificará la resolución a la Comisión de las Comunidades Europeas cuando así sea exigible.

Ahora bien; existen determinadas excepciones (art. 34 LOPD) a la exigencia de la obtención de la autorización de la AEPD, basado en el art. 26 Directiva 95/46/CE[23]:

---

[22] No olvidemos que, con arreglo al art. 68 RLOPD, no será necesaria dicha autorización (…) para la realización de una transferencia internacional de datos que tuvieran 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.

[23] En este punto, nos hemos dejado llevar por las detalladas exposiciones realizadas por Verdaguer López, J. y Bergas Jané, Mª A., *TODO Protección de Datos*, *cit*., pp. 376-380, así como por Heredero Higueras, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal*, *cit*., pp. 190-194.

a) Cuando exista un tratado o Convenio del que España sea parte; hasta el momento, el único existente que vincula a España en materia de Protección de Datos es el Convenio 108.

b) Cuando se preste o solicite auxilio judicial internacional; un ejemplo ya reflejado por la AEPD ha sido el de las compañías aseguradoras en el caso de accidentes de circulación entre vehículos de distintas nacionalidades.

c) Intercambio de datos de carácter médico entre facultativos o instituciones sanitarias; no debe olvidarse, sin embargo, la naturaleza «sensible» (art. 7 LOPD) de los datos de carácter médico. De nuevo, las compañías aseguradoras se amparan a menudo en esta excepción, de modo que la AEPD ha considerado la transferencia, en estos casos, únicamente en la medida en que los datos sean determinantes de una situación personal evolutiva o definitiva de lesiones o secuelas de daños físicos.

d) Transferencias dinerarias conforme a su legislación específica en esta materia[24].

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia, para lo cual es de suma importancia para su eficacia la información relativa a la falta de protección adecuada en el país receptor de la transferencia. Esta excepción puede parecer una obviedad, ya que no tendría ninguna lógica prohibir una transferencia consentida por el interesado. Sin embargo, cobra especial relevancia en los supuestos de gestión centralizada de los servicios de recursos humanos de las grandes multinacionales.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero. El ejemplo propuesto por la AEPD es el del sector de la hostelería, donde son muy frecuentes las comunicaciones de datos a entidades ubicadas en cualquier país del mundo que operan dentro del sector turístico.

g) Cuando 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. Esto último puede generar cierto escepticismo por la propia relatividad de dichos intereses que pueden provocar la realización de transacciones perjudiciales. En cuanto a esta excepción, de gran complejidad por referirse a los contratos suscritos en el marco del proceso de ampliación de los mercados de valores que vienen desarrollándose en España, se ha insistido en el hecho de que todos los datos transferidos deben ser necesarios para la ejecución de los mismos, excluyendo los complementarios o no esenciales[25].

---

[24] RD 2660/1998, de 14 de diciembre, sobre el cambio de moneda extranjera en establecimientos abiertos al público distintos de las Entidades de Crédito y Orden de 16 de noviembre de 2000, de regulación de determinados aspectos del régimen jurídico de los establecimientos de cambio de moneda y sus agentes, y de desarrollo de la Ley 9/1999 de 12 de abril sobre régimen jurídico de las transferencias entre estados miembros de la UE.

[25] Así se infiere del *Working Document: Transfers of personal data to third countries: Applying Article 25 and 26 of the EU Data Protection Directiva*, adoptado por *Data*

h) Cuando sea necesaria para la salvaguarda de un interés público; por ejemplo, la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias («Considerando» 58º Directiva 95/46/CE); obviamente, debe tratarse de un interés de relieve y entidad, ya que, de otro modo, esta excepción podría servir de excusa para autorizar, de una forma genérica, las transferencias entre Administraciones Públicas. En cualquier caso, hubiera sido deseable concretar este concepto jurídico indeterminado mediante una relación de supuestos.

i) Cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, similar al auxilio judicial.

j) Cuando se efectúe desde un Registro público, a petición de persona con interés legítimo y los datos tengan relación con la finalidad pretendida. En torno a esta excepción existe un sistema de cooperación entre Estados para la protección del niño y la adopción internacional. Este apartado se incluyó para cubrir la preocupación manifestada por la delegación alemana, en alguna ocasión, relativa a las repercusiones que la Directiva podría tener en el régimen de los registros públicos (Mercantil, Inmobiliario…). En estos casos, la transferencia no debe afectar a la totalidad de los datos que contenga el Registro («Considerando» 58º Directiva 95/46/CE).

k) Cuando la transferencia tenga como destino un Estado miembro de la UE o un Estado respecto del cual la Comisión haya declarado que garantiza un nivel de protección adecuado.

En este último punto (k), deben tenerse en cuenta las Decisiones de la Comisión de las Comunidades Europeas 2000/518/CE, 2000/519/CE y 2000/520/CE de 26 de julio de 2000, que consideraron adecuado el nivel de protección de datos personales en Suiza y Hungría, así como el conferido por los principios de Puerto Seguro (*Safe Harbor*) para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los EEUU[26]. En efecto, como consecuencia de la entrada en vigor de la Directiva europea sobre protección de datos el 25 de octubre de 1998, el Departamento de Comercio de los EEUU publicó el 21

Protection Working Party, el 24 de julio de 1998 (*WP* 12). Aparicio Salom, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, *cit*., pp. 190 y 274-282. Sabemos que en la Directiva comunitaria no se crea una autoridad comunitaria de protección de datos, sino este Grupo de Protección de las Personas en lo que respecta al tratamiento de datos personales y un Comité, cuyo estudio excedería del ámbito de este trabajo.

[26] Junto a estas adecuaciones, debemos destacar, asimismo, la Decisión 2002/2/CE de 20 de diciembre de 2001, por la que se considera adecuado el nivel de protección de datos personales en Canadá, la Decisión 2003/490/CE, de 30 de junio de 2003, sobre la adecuación en Argentina, la Decisión 2003/821/CE de la Comisión de 21 de noviembre de 2003, relativa a Guernesey y, por último, la Decisión 2004/411/CE, de 28 de abril de 2004, concerniente a la Isla de Man. Vid. Charlesworth, A., «Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual», *Law and the Internet.*

de julio de 2000 el grupo de principios de Puerto Seguro, cuya finalidad consistió en que las empresas u operadores americanos que aplicasen los siete principios básicos, contenidos en este Acuerdo, tendrían el visto bueno de la UE y, por lo tanto, en el ámbito de protección de datos evitarían este control que impera en la Comunidad[27], permitiéndose, por ende, la libre transferencia internacional de datos a dichos operadores.

A modo de recapitulación, los países que ofrecen un nivel de «protección adecuado», en el sentido arriba indicado, son todos aquellos que pertenecen al espacio europeo de protección (los comunitarios y los pertenecientes al EEE como Noruega, Islandia y Liechtenstein), así como aquellos, ajenos a la integración, que disponen de un sistema de protección cuya suficiencia haya sido reconocida por la Comisión de las Comunidades Europeas (Suiza, Canadá, Hungría y EEUU). En lo que respecta a Canadá y EEUU, la Decisión que reconoce su nivel de protección adecuado, está limitada a los destinatarios a los que resulta de aplicación la *Personal Information and Electronic Documents Act* de 13 de abril de 2000 en el primer caso, y a los destinatarios adheridos a los Acuerdos de Puerto Seguro, en el segundo. En cambio, las Decisiones sobre la adecuación en Suiza, Argentina, Gernesey e Isla de Man son de aplicación a todas las transferencias sin restricción (véase nota 26 *infra*).

En cuanto a los problemas que puede plantear la Transferencia Internacional de Datos figuran, en un lugar preferente, la evaluación del nivel de protección de terceros Estados, la dificultad en el ejercicio de los derechos individuales, la responsabilidad en el supuesto de transferir datos a un tercer país que no disponga de dicho nivel de protección y, finalmente,

---

Edwards, L., Waelde, C. (eds.), Hart, Oxford, 2000, pp. 79-122, 84-106, citado por Sancho Villa, D., «Normas corporativas vinculantes (*binding corporate rules)*: aspectos sustantivos y de cooperación internacional de autoridades», *Revista española de Protección de Datos* nº 4, enero-junio, 2008, Agencia de Protección de Datos de la Comunidad de Madrid-Civitas, p. 42 en nota 23.

[27] Sin embargo, el número de empresas que figuran en aquélla relación no es muy elevado y puede resultar insuficiente, habida cuenta del volumen empresarial existente en EEUU. Por este motivo, si se transfieren datos a una empresa de EEUU no incluida en el listado cabe la solución de elaborar un documento a través del cual se garantice que dicha empresa extranjera se somete a la jurisdicción española y a la Agencia de Protección de Datos en todo lo relacionado con el tránsito en cuestión, comprometiéndose asimismo a facilitar al titular de los datos el ejercicio de los derecho que en España hubiese podido tener. La notificación de este contrato se efectuará, como mínimo, anualmente, obteniendo de este modo la denominada certificación de Puerto Seguro. Así describe el caso especial de EEUU, Hernández Martínez, J., «Protección de datos: Transferencias internacionales de datos», *Baquia.com*, 24/02/2003. Sobre los principios de Puerto Seguro, cfr. del Peso Navarro, E. y Ramos González, M., *La seguridad de los datos de carácter personal*, Díaz de Santos, Madrid, 2002, pp. 118 y ss, así como, Verdaguer López, J., Bergas Jané, Mª A., *TODO Protección de Datos, cit.,* pp. 364 y ss.

la polémica capacidad extraterritorial de las autoridades nacionales de protección de datos.

La sociedad de la información exige un continuo intercambio de información entre los Estados, lo que puede dañar la privacidad de las personas. Como se ha puesto de relieve, los Estados generan las normas jurídicas precisas e incluso Convenios entre Uniones geopolíticas para evitar esta colisión de derechos. La necesidad de esta conciliación quedó ya reflejada en el Preámbulo de la Recomendación de la OCDE de 23 de septiembre de 1980. Lo importante y difícil es encontrar un equilibrio entre:

Protección intimidad/datos personales vs.	intereses económico-comerciales
Protección intimidad/datos personales vs.	libertad información y comunicación

4. LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA: EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Junto a los controles ejercidos por las autoridades nacionales de protección de datos, se ha visto la necesidad de un control ejercido por una autoridad supranacional que permita resolver conflictos provocados por las transmisiones internacionales de datos, sin que, por ello, disminuyan las competencias de las autoridades nacionales[28]. Resulta evidente, pues, que la protección de datos es un derecho fundamental protegido, no sólo por el ordenamiento jurídico nacional, sino también por la legislación europea, ya que el mismo está consagrado en el art. 8 de la Carta de los Derechos fundamentales de la UE. De este modo, y a raíz del ya mencionado, en páginas anteriores, Reglamento 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, que dicta las reglas aplicables a nivel comunitario (véase nota 9, página 4 del presente trabajo), y de conformidad con el art. 286 del Tratado de la Comunidad Europea, se crea la figura del Supervisor Europeo de Protección de Datos (en lo sucesivo SEPD), con sede –la oficina– en Bruselas, también conocido como el «guardián europeo de la protección de datos de carácter personal»; la responsabilidad de este organismo de vigilancia independiente radica en garantizar que las instituciones y organismos de la UE, anteriormente mencionados, respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales, siempre que unas y otros procesen datos. Obviamente, el Supervisor trabaja con los responsables de la protección de datos de cada institución u organismo de la UE, con objeto de asegurar la correcta aplicación de las normas de confidencialidad de dichos datos[29].

---

[28] Necesidad puesta de relieve expresamente por ESTADELLA YUSTE, O., «La transmisión internacional de datos personales y su control», *cit.,* p. 147.

[29] Información disponible en *http://europa.eu/about-eu/institutions-bodies/edps/index_es.htm* (última consulta: 17/01/2012).

El SEPD y el Supervisor Adjunto, auténticos promotores de buenas prácticas sobre la privacidad en el seno de la UE, son designados por un período renovable de 5 años, por decisión conjunta del Parlamento Europeo y del Consejo.

Como ya indican las leyes sobre protección de datos, el «tratamiento» o «procesamiento» cubre actividades tales como la recogida, el registro y el almacenamiento de la información, la recuperación para su consulta, el envío o la puesta a disposición de otras personas, así como el bloqueo, el borrado o la destrucción de datos. En este sentido, existen normas estrictas de protección de la intimidad que regulan estas actividades. Así, no se permite que las instituciones y organismos de la UE procesen los datos personales que revelen origen racial o étnico, opiniones políticas, creencias filosóficas o religiosas o la afiliación a sindicatos, salvo «en circunstancias específicas»; tampoco datos sobre la vida sexual o sanitaria salvo que sea necesario por motivos médicos o sanitarios; incluso en ese caso, los datos deben ser procesados por un profesional sanitario u otra persona que deba atenerse al secreto profesional. El caso de las profesiones sanitarias es, en exceso, delicado y el SEPD considera que la comunicación de sanciones de estos profesionales y la denominada Tarjeta Profesional Europea pueden plantear problemas de protección de datos[30]. Los datos de la alerta y otra información incluida en el fichero creado con el Sistema de Información del Mercado Interior sobre delitos o sanciones administrativas, precisan una protección reforzada bajo el art. 8.5 de la Directiva 95/46/CE y el art. 10.5 del Reglamento 45/2001, ya que este sistema de alerta va a afectar a la protección de datos de un gran número de personas y grupos profesionales en todos los Estado miembros, incluyendo obviamente a los profesionales de la medicina.

El SEPD trabaja con los responsables de la protección de datos de cada institución u organismo de la UE con objeto de garantizar que se apliquen las normas de confidencialidad de dichos datos, para lo cual se reúnen regularmente en encuentros bilaterales o durante las reuniones de la red de Responsables de la protección de datos (en lo sucesivo, RPD). No debe olvidarse que cada institución y organismo de la Comunidad tiene la obligación de nombrar

[30] Por este motivo, deben precisarse mucho más los casos concretos que pueden alertarse y definir con rigor el tipo de datos que se pueden incluir, tal y como se infiere del informe emitido por el SEPD sobre la modernización de la Directiva 2005/36/CE, de cualificaciones profesionales. Así, el nuevo art. 56 bis de la propuesta de esta Directiva crea un «mecanismo de alerta» para las profesiones sanitarias: «Las autoridades competentes de un Estado miembro informarán a las autoridades competentes de todos los demás Estados miembros y a la Comisión acerca de la identidad de un profesional al que las autoridades o los órganos jurisdiccionales nacionales hayan prohibido, incluso con carácter temporal, el ejercicio de las actividades profesionales siguientes en el territorio de dicho Estado miembro: a) doctor en medicina general en posesión de un título de formación (…); b) doctor en medicina especialista en posesión de un título (…)». Más detalles en *http://www.medicosypacientes.com/noticias/2012/04/02/12_04_02_UE* (última consulta: 03/05/2012).

un RPD cuyo cometido es garantizar de forma independiente que la institución o el organismo de que se trate respeta sus obligaciones en materia de protección de datos, así como de informar a los responsables del tratamiento y a los titulares de los datos de sus derechos y obligaciones; no en vano, el RPD puede ser el punto de contacto entre el SEPD y el responsable del tratamiento y es quien notifica al Supervisor la conveniencia de efectuar un control previo[31].

En líneas generales, la labor de supervisión se centra en las notificaciones de los tratamientos que presentan riesgos específicos, debiendo ser revisadas previamente; puede limitarse a asesorar al titular de los datos objeto de tratamiento, pero también puede dirigir una advertencia o amonestación a la institución correspondiente –o imponerle una prohibición de tratamiento– e incluso someter el asunto al Tribunal de Justicia Europeo. El Supervisor analizará el tratamiento de datos personales de acuerdo con el Reglamento 45/2001. En la mayoría de los casos, esta actuación lleva a una serie de recomendaciones que la institución o el organismo debe respetar a fin de garantizar el cumplimiento de las normas de protección de datos (véase epígrafe Intervenciones Significativas del Supervisor).

Aunque, en principio, en la mayoría de los casos la información personal que se almacena sobre una persona (actividades ligadas a la contratación, recopilación de datos sobre salud en expedientes médicos, la vigilancia por vídeo…) únicamente se utilizará para fines legítimos, sin implicaciones o consecuencias ulteriores, el tratamiento de dicha información puede entrañar también riesgos; éstos pueden derivarse, por ejemplo, de la inexactitud de datos o comunicación de éstos a personas no autorizadas, lo que conducirá a situaciones nada deseables como la denegación de un contrato o la prohibición de acceder a un edificio o, incluso, presenciar la comisión de delitos de suplantación de identidad[32].

Desde este punto de vista, es de vital importancia que, dado que estas situaciones afectan a los miembros del personal de la UE y, de un modo derivado, al resto de la población, todos deben ser conscientes de sus derechos y obligaciones. En estos supuestos, y dejando claro que el SEPD no tiene competencia sobre cuestiones de ámbito nacional[33], si una persona tiene razones

[31] European Data Protection Supervisor, «El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismos comunitarios» en *www.edps.europa.eu*, Oficina de Publicaciones de la UE. Comunidades Europeas, Luxemburgo, 2009, p. 9.

[32] Son situaciones descritas en European Data Protection Supervisor, «El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismos comunitarios», *cit*., p. 2.

[33] Esto no es óbice para que el SEPD coopere con las autoridades nacionales (por ejemplo, el ya mencionado Grupo de Trabajo del *Artículo 29*), no siendo, sin embargo, jerárquicamente superior a las mismas (autoridades nacionales o regionales); de hecho, las decisiones de estas últimas no pueden ser recurridas ante el SEPD.

para asegurar que su derecho a la intimidad ha sido infringido por una institución u organismo de la UE, debe acudir, en primera instancia, a los responsables del tratamiento de sus datos y pedirles que tomen medidas; de no estar satisfecho con la respuesta o resultados, contactará con el funcionario de protección de datos pertinente, que puede encontrar en la página web del SEPD, pudiendo, asimismo, presentar una denuncia ante el Supervisor, el cual efectuará las averiguaciones necesarias. Y así es; el SEPD puede recibir quejas de los Estados miembros de la UE, así como de otras personas que consideren que sus datos personales han sido objeto de un tratamiento inadecuado por parte de una institución u organismo europeo. Si la queja es admisible, el SEPD por lo general lleva a cabo una investigación, si bien, procurará siempre que sea posible, alcanzar una solución amistosa. Los resultados se comunican al demandante y se adoptan las medidas necesarias. Si el ciudadano no está conforme con la decisión del Supervisor Europeo, aquél podrá acudir ante el Tribunal de Justicia Europeo[34]; este último puede destituir al Supervisor y al Adjunto si uno de los dos (o ambos) no ejercen adecuadamente sus funciones o si incurren en una conducta indebida grave.

El SEPD aprueba dictámenes sobre las medidas administrativas relativas a la protección de datos adoptadas por las instituciones y organismos europeos, que pueden consultarse, clasificadas por años, en su página web. Durante su primer mandato, el SEPD emitió casi 50 dictámenes sobre propuestas legislativas referentes a temas importantes para la protección de datos[35]. Podrá, asimismo, llevar a cabo investigaciones por iniciativa propia; éstas y las inspecciones son herramientas esenciales para una autoridad de control, ya que le permitirán recoger la información, así como disponer de los medios para la investigación de los hechos, el seguimiento de casos y controles de cumplimiento de las normas en general. En suma, realiza investigaciones y/o

[34] Son interesantes las decisiones del Tribunal de Justicia en torno a la Directiva 96/9/CE, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos en sus sentencias de 5 de marzo de 2009 (relativa a la interpretación del art. 7 de la mencionada Directiva) y de 9 de octubre de 2008; asimismo, sobre el tratamiento y circulación de datos fiscales de carácter personal, véase la sentencia de 16 de diciembre de 2008; por último, en lo que atañe a la Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, es relevante la sentencia de 18 de enero de 2001 en la que se vio implicada la República francesa al no cumplir con las obligaciones derivadas del art. 15 de esta última Directiva.

[35] Merecen especial atención entre las cuestiones tratadas, en estos dictámenes, con arreglo al Documento European Data Protection Supervisor, «El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismo comunitarios», *cit.*, pág. 6, la Decisión marco sobre protección de datos en el ámbito de la cooperación policial y judicial, la Directiva sobre la conservación de datos de telecomunicaciones, el Reglamento relativo al acceso del público a los documentos, el intercambio de datos con EEUU, la Directiva sobre la intimidad y las comunicaciones electrónicas, y la comunicación sobre identificación por radiofrecuencia.

audiencias, emitiendo opiniones o comentarios en relación con las propuestas legislativas comunitarias que puedan incidir en la protección de datos personales; trabaja, por último, de forma coordinada con los organismos competentes para la protección de datos personales en la UE.

A fin de supervisar el cumplimiento del Reglamento 45/2001, el SEPD se apoya en gran medida en los delegados o representantes de Protección de Datos (OPD) que son nombrados en cada institución u organismo. Aparte de las reuniones y contactos bilaterales con los RPD, el SEPD también participa, como se ha indicado líneas atrás, en las reuniones periódicas de la red de RPD.

Desde enero de 2004, el SEPD supervisa la unidad central de Eurodac. Esta supervisión se caracteriza fundamentalmente por la cooperación con las autoridades nacionales de supervisión y el establecimiento de recomendaciones para soluciones comunes a los problemas existentes.

El SEPD publica guías temáticas sobre los temas críticos que sirven como documentos de referencia para la administración europea, así como un informe anual que recoge sus actividades en ese período, cuyo texto íntegro y/o resumen pueden consultarse en varios idiomas. Dicho informe se remite a las principales instituciones de la UE, pudiendo ser discutido por el Parlamento Europeo. Con la publicación de estos informes, notas de prensa y *newsletters*, contribuye a crear una «cultura de la protección de datos en Europa», mejorando así la gobernanza. La incorporación, cuando proceda, de garantías de protección de datos en la legislación y las políticas de la UE, es condición necesaria para que estos instrumentos den los deseados resultados.

En diciembre de 2010 el SEPD adoptó un documento de política titulado «Seguimiento y Control de cumplimiento del Reglamento 45/2001».

4.1. Intervenciones significativas del Supervisor

El acceso a documentos en la UE y su adecuación a la normativa sobre protección de datos es una cuestión compleja y «sensible», en la cual, en principio, la UE no tiene competencia para armonizar; en este sector, el Reglamento 45/2001no otorga al SEPD la competencia de garantizar el acceso a los documentos de las instituciones. Es el Reglamento 1049/2001[36] el que, a nivel de la UE, determina el derecho de todo ciudadano de la Unión, así como de toda persona física o jurídica establecida en un Estado miembro, a acceder a los documentos de las instituciones. Este último Reglamento se aplica a los documentos del Consejo, del Parlamento y de la Comisión, pero ha repercutido en las demás instituciones y organismos; el Tribunal de Justicia Europeo, por un lado, ha interpretado de forma extensiva este derecho, hablando de derecho a la información; por otro, ha interpretado de forma restrictiva las excepciones a este

[36] Reglamento (CE) n° 1049/2001 begin_of_the_skype_highlightingdel Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

derecho[37]. Con motivo de un litigio entre el Sr. *Rijkeboer* y el *College van burgemester en wethouders van Rotterdam*, relativo a la desestimación parcial por este último de la solicitud de acceso de aquél a la información sobre la comunicación a terceros de sus datos personales durante los dos años anteriores a su solicitud, el Tribunal, en su sentencia de 7 de mayo de 2009, reitera la obligación de los Estados miembros de establecer que el Responsable del tratamiento ha de dar a la persona afectada acceso a la información relativa a los destinatarios y a los datos comunicados, con arreglo al art. 12 Directiva 95/46/CE.

Pero el Reglamento 1049/2001 indica que el derecho de acceso a los documentos está limitado por una serie de excepciones, entre las cuales destaca la intimidad y la protección de datos, que conducirán a la denegación del documento. El SEPD realiza una lectura muy firme de este precepto, al afirmar que deben cumplirse tres condiciones para dicha denegación: poner en peligro la intimidad del interesado (debe contener detalles «personales» o «privados»), afectar «sustancialmente» (y no superficialmente) al interesado dicho acceso del público y, por último, ser contrario –el acceso– a la legislación sobre protección de datos (en la medida en que el Reglamento sobre Protección de Datos prohíba la divulgación de los mismos). La jurisprudencia del Tribunal de Justicia y la presión del Parlamento Europeo llevaron a la propuesta de modificación del Reglamento 1049/2001 en este extremo.

Por lo demás, el Tratado de Lisboa, por el que se modifica el Tratado de la UE y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007 y cuya entrada en vigor se sitúa el 1 de diciembre de 2009, supone una mejora en cuanto al ámbito de aplicación para el derecho de acceso a documentos.

Otra intervención relevante del SEPD ha sido una reciente advertencia o denuncia vertida sobre el documento conocido como ACTA (*Anti-Counterfeiting Trade Agreement*) o *Acuerdo comercial anti-falsificación*)[38]; en su opinión, las medidas allí expuestas, que persiguen defender los derechos de la propiedad intelectual, y su imprecisión pueden derivar en amenazas para la privacidad y la protección de datos si no se aplican con corrección y cautela, al no ofrecer suficientes garantías; las amenazas se producen en el contexto de la monitorización de los usuarios y de sus comunicaciones electrónicas, lo que puede entrar en conflicto con la Carta de Derechos Fundamentales y la Directiva 95/46/CE[39].

---

[37] Cfr. Scirocco, A., «Acceso a documentos y protección de datos personales: la experiencia del Supervisor Europeo de Datos Personales» en *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos Personales,* Agencia de Protección de Datos de la Comunidad de Madrid, 2008, pp. 295, 296.

[38] Disponible en *http://www.edri.org/files/juri_draft.pdf* (última consulta: 04/05/2012).

[39] Camós J., «El Supervisor Europeo de Protección de Datos carga contra ACTA» en *nacionred.com*, 25-04-2012, fuente: *http://www.nacionred.com/proteccion-de-datos/el-supervisor-europeo-de-proteccion-de-datos-carga-contra-acta*.

5. OTRAS NORMAS DE PROTECCIÓN: *LAS BINDING CORPORATE RULES*

El intercambio de datos personales entre empresas establecidas en los diferentes Estados ha experimentado un extraordinario desarrollo. En este contexto, una posible alternativa a los contratos de carácter multilateral en el ámbito de las herramientas jurídicas disponibles para transferir datos del EEE a terceros Estados son las denominadas Normas corporativas vinculantes (*binding corporate rules)*, como conjunto de reglas uniformes para el tratamiento de datos, dentro de un grupo multinacional de empresas; es el caso del Grupo *General Electric* o *Philips*. Constituyen, entonces, nuevos mecanismos de cooperación internacional de autoridades estatales de protección, en la búsqueda de un modelo de integración plena, tal y como las contempla el Grupo *Artículo 29*, *Data Protection Working Party* en su Documento de trabajo de 3 de junio de 2001; en este contexto, se defiende «un procedimiento de cooperación establecido para conciliar el criterio de solicitud única con el de la autorización múltiple»[40]. Estas normas, deducidas implícitamente del art. 26.2 Directiva 95/46/CE y art. 33.1 LOPD, fueron incluidas en el RLOPD en su art. 70.4 como «reglas internas adoptadas por grupos multinacionales de empresas» que permitirán gobernar el conjunto de las exportaciones de datos desde cada una de las sedes europeas hacia las sedes del grupo en terceros Estados; en dichas reglas o nor» de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados; la autorización del Director de la AEPD, que implicará la exigibilidad de lo previsto en estas normas, sólo procederá cuando éstas resulten vinculantes para las empresas del grupo y exigibles conforme al ordenamiento jurídico español[41]. En efecto, este último precepto del RLOPD contempla esta nueva posibilidad, además de la descrita con anterioridad (véase página 8 del presente trabajo), relativa a la solicitud de la autorización para la transferencia internacional al amparo de un contrato que reúne las condiciones establecidas en la Decisión 2001/497/CE.

---

[40] Cfr. *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directiva to Binding Corporate Rules for International Data Transfers*, adoptado por el Grupo *Artículo 29*, *Data Protection Working Party*, el 3 junio de 2001 (*WP* 74). La profesora Sancho Villa, D., ofrece un minucioso e interesantísimo análisis de estos nuevos mecanismos de cooperación en «Normas corporativas vinculantes (*binding corporate rules)*: aspectos sustantivos y de cooperación internacional de autoridades», *cit.*, pp. 35-60. Deseo dejar constancia en este instante del hecho de que el actual SEPD, el Sr. Hustinx, presidió entre 1996 y 2000 el mencionado Grupo de Trabajo del *Artículo 29* (o Grupo de protección de las personas en lo que respecta al tratamiento de datos personales).

[41] Verdaguer López, J., Bergas Jané, Mª A., *TODO Protección de Datos, cit.,* pp. 374-375.

Habitualmente, en este cometido se utilizan centros de servicios compartidos y las denominadas «herramientas multi-acceso», que posibilitarán que los datos personales sean transferidos internacionalmente a sociedades de diversos países del mundo. De nuevo, resulta muy complicado el cumplimiento estricto de los requisitos jurídicos establecidos en las respectivas normativas de los distintos países.

6. REFLEXIONES FINALES

Aunque es deseable que los sistemas de tratamiento de datos estén «al servicio del hombre y (…), respeten sus libertades y sus derechos fundamentales, en particular, la intimidad, y contribuyan al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos» («Considerando» 2º Directiva 95/46/CE), la dinámica, sin embargo, está siendo mucho más compleja.

«La confianza en nuestras tecnologías sin fronteras tiene un precio»[42] y éste es la invasión de la privacidad de las personas en una dimensión altamente peligrosa. Una muestra fehaciente de esta intrusión fue la aprobación en EEUU de la *Patriot Act* en noviembre de 2001, tras los terroríficos atentados del 11 de septiembre, en aras, no obstante, de una mayor seguridad mundial. Esta normativa, que obliga a las compañías aéreas –que operen con aquel país– a facilitar a las autoridades estadounidenses el acceso electrónico a unos datos contenidos en sus sistemas informáticos conocidos como *Passenger Name Records (PRN),* dio mucho que hablar, al ser inicialmente considerada, por la Comisión Europea, contraria a la normativa comunitaria en materia de protección de datos. Tras diversas negociaciones y vicisitudes, finalmente el Tribunal de Justicia Europeo consideró, en su sentencia de 30 de mayo de 2006, que esta transferencia de datos de los *PNR* tenía por objeto garantizar la seguridad pública, por lo que queda fuera del ámbito de aplicación de la Directiva 95/46/CE. Pues bien; este es un ejemplo idóneo del nivel de penetración, alcanzado por las Nuevas Tecnologías, en la privacidad de las personas.

Hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio, tratamiento y cesión de datos personales, a través de las técnicas y herramientas que proporcionan las Nuevas Tecnologías, ha sido, y sigue siendo, una de las labores más ingentes protagonizada por los legisladores e instituciones europeos e internacionales; todos ellos, al menos es nuestro deseo, se han esforzado en buscar una solución global, desde el punto de vista internacional, que proporcione la mayor seguridad en estas transmisiones, a través de una legislación armonizada que facilite «la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes

[42] Es el mensaje que lanza POULLET, Y., «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», *cit.,* p. 113.

de telecomunicaciones en la Comunidad» («Considerando» 6º Directiva 95/46/CE).

No es una novedad que los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social entre los distintos Estados, impulsados en su momento por el Mercado único (europeo), constituyen una incuestionable necesidad y, por supuesto, realidad. La conciliación de estos flujos con la protección de la intimidad, representa una constante tanto a nivel de la UE como a escala internacional.

En esta complicada pero loable empresa tienen una presencia decisiva las instituciones, organismos, agencias… europeos e internacionales. En el seno de la UE, junto a las ya tradicionales instituciones, como el Defensor del Pueblo, el Parlamento Europeo, el Consejo de la UE, la Comisión Europea o el Tribunal de Justicia –de las que han emanado no pocas Directivas, Reglamentos, Decisiones o Sentencias–, las intervenciones del SEPD, en forma de advertencias, denuncias, audiencias, opiniones, comentarios o investigaciones en general, han contribuido a arrojar luz sobre aquellas cuestiones sensibles o delicadas, tal y como he tenido ocasión de transmitir en epígrafes anteriores. Esta figura, nacida en 2001, supone un paso decisivo en este cometido de armonía, ya que trabaja de forma coordinada con los organismos competentes para la protección de datos personales en la UE y contribuye a inculcar una «cultura de la protección de datos en Europa».

En lo que respecta a la legislación española, ha quedado muy patente que tanto la LOPD como su posterior Reglamento han realizado una fiel adaptación al texto de la Directiva europea. El RLOPD, además, se ha encargado de contemplar aquellos extremos en los que la experiencia ha aconsejado un cierto grado de precisión o desarrollo que dote de seguridad jurídica al sistema.

Tras lo expuesto, parece que la solución jurídica internacional que se está intentado poner en práctica para abordar debidamente las implicaciones derivadas de los movimientos internacionales de datos ha sido, en líneas generales, la de considerar que entre dos países afectados por flujos de datos a través de sus fronteras, la información deberá fluir tan libremente como en el interior de cada uno de los territorios respectivos, con las debidas precauciones; la única exigencia al respecto es, como se ha constatado, que el nivel de protección otorgado al individuo en cada uno de los ordenamientos afectados sea similar.

Reitero lo que en alguna ocasión[43] he manifestado ante la dicotomía planteada en estas reflexiones: las Nuevas Tecnologías han generado una nueva forma de ver el mundo; se ha producido un proceso de concentración y expansión de la información y del acceso a esta información que ha forzado a

[43] García-Cueva Roque, E., «La desigualdad de acceso a Internet desde la doble perspectiva política y social», *En torno a la igualdad y a la desigualdad,* Sánchez González, S. (Coordinador), Dykinson, Madrid, 2009, p. 252.

replantearse todos los principios que hasta hace unos cuantos años regían. Pero, ¿debemos renunciar a ciertos derechos básicos del hombre como la privacidad y la seguridad en favor del avance de la técnica? o, por el contrario, ¿renunciamos a los incalculables beneficios que las avanzadas tecnologías podrían proporcionar a la humanidad para resguardar los derechos individuales? Lo deseable es hacer congeniar ambos y, en esta línea, ya dibujada en este breve estudio, se está trabajando en los distintos Estados.