CONSTITUCIONAL-ADMINISTRATIVO

TRATAMIENTO ILÍCITO INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL, COOPERACIÓN INTERNACIONAL Y AUTORIDADES DE CONTROL

Alfonso Ortega Giménez

Profesor contratado doctor de Derecho internacional privado.
Universidad Miguel Hernández (Elche, Alicante)

Este trabajo ha sido seleccionado para su publicación por: don Carlos Francisco Molina del Pozo, doña M.ª José Achón Bruñén, don Xabier Arzoz Santisteban, don Jorge Botella Carretero, don Javier Cremades García y don Vicente Moret Millás.

Extracto

La protección del derecho a la protección de datos constituye hoy una necesidad, una actuación ineludible de los Estados. La cesión internacional de datos personales ha sido, y sigue siendo, uno de los aspectos en que parece necesaria la coordinación estatal. Los Estados tienen un interés común en prevenir la creación de lugares donde el tratamiento de datos de carácter personal pueda fácilmente realizarse fuera de los límites legalmente establecidos.

Sin obviar los avances normativos acaecidos en los últimos años y la diversidad de sistemas de protección de datos y de la privacidad o, en algunos casos, la ausencia de ellos, se ha convertido en una tarea urgente la elaboración de unas directrices o estándares internacionales y la posible instauración de una autoridad supranacional que faciliten con garantías los flujos de datos en un mundo globalizado, garantizándose, así, la «libre circulación de datos de carácter personal» y la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal.

Palabras claves: cooperación internacional, autoridad de control y transferencia internacional de datos personales.

Fecha de entrada: 30-04-2015 / Fecha de aceptación: 30-06-2015

ILLICIT INTERNATIONAL TRANSFER OF PERSONAL DATA, INTERNATIONAL COOPERATION AND SUPERVISING AUTHORITIES

Alfonso Ortega Giménez

Abstract

The protection of the right to data protection is a must today, an unmissable State performance. The international transfer of personal data has been and remains, one of the ways in which the State coordination seems necessary. States have a common interest in preventing the creation of places where the treatment of personal data can easily be done outside of legal limits.

Without ignoring regulatory developments have occurred in recent years and the diversity of systems of data protection and privacy or, in some cases, the lack thereof, has become an urgent task in the development of guidelines or international standards and the possible establishment of a supranational authority guarantees that facilitate data flows in a globalized world, guaranteeing thus the «free movement of personal data» and the protection of the person entitled to the protection of data against unlawful processing international their personal data.

Keywords: international cooperation, supervisory and international transfer of personal data.

Sumario

I. Introducción: Autoridades de control, cooperación internacional y transferencia internacional de datos de carácter personal

II. Determinación de la competencia de las autoridades de control estatales en materia de transferencia internacional de datos de carácter personal

1. Distribución competencial para el control de las transferencias internacionales de datos de carácter personal
2. Determinación de la competencia de las autoridades de control en España

III. La necesidad o no de articular unas directrices o estándares internacionales comunes para la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal

IV. Cooperación internacional entre autoridades de control y conveniencia o no de crear una autoridad supranacional para la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal

V. Reflexiones finales

I. INTRODUCCIÓN: AUTORIDADES DE CONTROL, COOPERACIÓN INTERNACIONAL Y TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL

1. Las legislaciones estatales desarrolladas bajo la impronta de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE)[1] admiten un control del tratamiento de datos personales, radicado, preferentemente, en los tribunales de justicia, al cual adicionan una autoridad pública cuyo cometido específico es fiscalizar el cumplimiento de la ley: nos referimos a las denominadas «**autoridades de control**» (art. 28 de la Directiva 95/46/CE). Estas entidades son públicas, estatales, independientes, territorialmente competentes (la autoridad de control ejercerá sus funciones en su territorio, cualquiera que sea el Derecho aplicable al tratamiento) y con potestades efectivas de investigación e intervención (p. ej., bloquear y borrar datos, prohibir temporal o definitivamente su tratamiento, su transferencia internacional, etc.): constituyen un elemento esencial de la protección de datos de carácter personal.

2. La coexistencia de diversos regímenes legales (uno por cada Estado) nos obliga a buscar soluciones pacíficas que no perjudiquen el normal desenvolvimiento de las relaciones comerciales internacionales y que garanticen la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal. La política de las transferencias internacionales de datos de carácter personal, con un volumen tan extraordinariamente elevado, con la necesidad de una autorización o aprobación previa y, en consecuencia, la prohibición de transferir datos de carácter personal a países con un nivel de «protección no adecuado», si bien constituye la arista internacional de una política tendente a proteger los datos personales y a consolidar el derecho a la protección de datos, es una herramienta normativa, en cierto modo, anticuada y de escasa virtualidad práctica.

3. Los distintos instrumentos y legislaciones han establecido reglas que exigen la condición de «adecuado», «equivalente» o «igual» del nivel de protección de datos en el Estado de destino. Los estándares podrían optar por el término «similar», que debería ser interpretado en el sentido de que el Estado de destino ofrezca un nivel de protección que, como mínimo, cumpla con los estándares.

---

[1] Diario Oficial n.º L 281 de 23 de noviembre de 1995 (NSL000669).

Por su parte, el Estado de origen no podría obstaculizar una transferencia si el Estado de destino cumpliese ese nivel de «similitud» al mínimo exigible por los estándares, aun cuando las garantías de protección en dicho Estado u organización puedan ser menores a las ofrecidas en origen, siempre que se cumpla el estándar mínimo y dos condiciones mínimas: por una parte, que corresponde a quien vaya a realizar la transferencia, ya sea un responsable, ya un prestador de servicio que actúe por cuenta de este, verificar el nivel de protección previsto en el Estado de destino y no llevar a cabo la transmisión de los datos cuando ese nivel no se cumpla[2]; por otra, que en virtud de la ley nacional aplicable se pueda evaluar la concurrencia en el destinatario de un nivel de protección sustancialmente similar y adoptar, en su caso, medidas para que dicho nivel se garantice

4. No obstante, la ley nacional aplicable podrá permitir la transferencia internacional de datos de carácter personal a Estados que no ofrezcan un nivel de protección sustancialmente similar. A título de ejemplo, será posible que una transferencia internacional pueda tener como fundamento el cumplimiento de compromisos contenidos en tratados internacionales que exijan para su pleno desarrollo el intercambio de información entre los Estados parte para el logro del interés público o la colaboración perseguidos por dichos instrumentos. Igualmente, y como se ha dicho, el establecimiento de los estándares no debería poder, en ningún caso, obstaculizar o dificultar la adecuada asistencia sanitaria o la atención o salvaguarda de un interés vital o un derecho fundamental del propio individuo[3].

II. DETERMINACIÓN DE LA COMPETENCIA DE LAS AUTORIDADES DE CONTROL ESTATALES EN MATERIA DE TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL

1. DISTRIBUCIÓN COMPETENCIAL PARA EL CONTROL DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

5. La Directiva 95/46/CE confirió cierto margen de maniobra a los Estados miembros de la Unión Europea (en lo sucesivo, UE) para la configuración de sus respectivas **autoridades de control**, lo que ha permitido que ellas se adecuen a las realidades institucionales que les son pro-

---

2 Se podría prever la intervención de terceros, a modo de entidades privadas certificadoras, con el objeto de verificar el nivel de protección previsto en el Estado de destino.

3 Teniendo en cuenta que el propio reconocimiento del «derecho a la protección de datos» y el concepto de «dato de carácter personal» varían de un Estado a otro, en materia de transferencias internacionales de datos el propio catálogo de excepciones podría ser ampliado recogiendo la realidad actual y no haciendo una remisión a la ley aplicable del Estado correspondiente, lo que, en la práctica, podría dar lugar a un conflicto de leyes, tal como que la ley de un Estado A admita X excepción y la del Estado B establezca todo lo contrario.

pias. Con todo, el énfasis lo puso la Directiva 95/46/CE en la concesión de independencia a tales autoridades; que se convierten así en imprescindibles para disponer de un óptimo cumplimiento de la normativa, tanto por las entidades responsables de tratamiento del sector público como del sector privado. Se observa bastante celo en las legislaciones internas en lo relativo al nombramiento de quienes integran las autoridades de control, a las inhabilidades a que se ven afectos los mismos, a la inamovilidad de sus miembros, así como al otorgamiento de facultades reglamentarias; y, quizás, el punto que mayor esfuerzo se demanda actualmente es la atribución de recursos materiales suficientes para el cabal desempeño de su cometido.

6. En el ámbito de la UE serán los Estados miembros quienes «evaluarán, en relación con la transferencia o categoría o clase de transferencias, si un tercer Estado ofrece o no un nivel de protección adecuado sobre la base de los criterios que enumera el apartado 2 [del artículo 25 de la Directiva 95/46/CE] al efecto»[4]. Además, sobre la base de lo previsto en el Considerando 66.º de la Directiva 95/46/CE[5], se habilita a la Comisión, en los apartados 4 a 6 del artículo 25 de la citada Directiva 95/46/CE, para que evalúe si un tercer Estado garantiza dicho «nivel de protección adecuado», obligando a los Estados miembros a que adopten «las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate»[6].

La cuestión es, entonces, determinar cuándo un país ofrece un «nivel de protección adecuado»[7], esto es, cuándo se considera que su regulación incorpora ese núcleo esencial de

---

4 *Vid*. Heredero Higueras, M.: *La directiva comunitaria de protección de los datos de carácter personal: Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos*, Pamplona: Aranzadi, 1997, pág. 188.

5 Al señalar que «por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CEE del Consejo».

6 Como bien señala Heredero Higueras, «este es el único contexto para el que la Directiva ha previsto una habilitación del Consejo a favor de la Comisión en materia de ejecución». *Vid.*, *op. cit.*, pág. 188.

7 Mientras el nivel de protección «equivalente» viene referido a la idea de que los instrumentos que presente el país destinatario deberán tener un contenido sobre la protección de datos similar al que posee el transmitente de los mismos, el nivel de protección «adecuado» consiste en que el destinatario de la transferencia internacional de datos tenga normas donde su contenido sea suficiente para garantizar la protección de los datos de carácter personal, determinándose tal suficiencia en el establecimiento y respeto de los principios rectores de la protección de datos y sus mecanismos de efectividad. En este sentido, coincido con Garriga Domínguez y Estadella Yuste en que «no significa lo mismo equivalente que adecuado, ya que mientras a los Estados miembros se les exige, para que los datos puedan circular libremente por sus territorios alcanzar [un] nivel equivalente al del estado transmisor, cuando la transmisión de datos se produce hacía un país que no pertenece a la UE, solo se satisfaga un estándar mínimo de protección». *Vid*. Garriga Domínguez, A.: *La protección de los datos personales en el Derecho español*, Madrid: Dykinson, 1999, pág. 331; Estadella Yuste, O.: «La transmisión internacional de datos personales y su control», en *Jornadas sobre Derecho Español de Protección de Datos Personales*, Agencia de Protección de Datos, Madrid, 1996, pág. 202; y

principios de protección de datos que consagra nuestra Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, la LOPD), de forma que se garantice la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal.

El artículo 33.2 de la LOPD[8] y la Instrucción 1/2000, de 1 de diciembre de la Agencia [Española] de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos[9], ofrecen una solución a la cuestión –que reproduce, en lo esencial el artículo 25.2 de la Directiva 95/46/CE–, al señalar que «el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará[10] por la Agencia [Española] de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de trans-

---

Piñol i Rull, J. y Estadella Yuste, O.: «La regulación de la transmisión internacional de datos en la Ley Organica 5/1992 de 29 de octubre», en Ripoll i Carulla, S. (coord.), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Universitat Pompeu Fabra, Barcelona, 1993, págs. 84-87. Además, sin duda, el régimen previsto en el artículo 25 de la Directiva 95/46/CE no es acorde con lo previsto en el artículo 12 del Convenio 108/81/CE del Consejo, de 28 de enero, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal –Convenio 108/81/CE–, ya que mientras aquel habla de «nivel de protección adecuado», este habla de «protección equivalente»; y, como señala Heredero Higueras, «el concepto de nivel de protección adecuado es más débil que el de protección equivalente del artículo 12 del Convenio [108/81/CE] ». *Vid*. Manuel Heredero Higueras, *La directiva...*, *op. cit.*, pp. 186-188.

8 BOE núm. 298, de 14 de diciembre de 1999 (NFL003202).

9 La Instrucción 1/2000 tiene por objeto señalar los criterios orientativos seguidos por la AEPD, en relación con aquellos tratamientos que supongan una transferencia internacional de datos, poniendo de manifiesto el procedimiento que, en uso de las competencias que la ley le atribuye, se sigue por la propia AEPD en cada caso concreto. Por tanto, no es finalidad de esta instrucción efectuar innovación alguna dentro de la normativa reguladora de la protección de datos de carácter personal sino, simplemente, aclarar y facilitar a todos los interesados, en un único texto, el procedimiento seguido por la propia AEPD para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos. Por otro lado, no olvidemos que mediante la SAN, Sala de lo Contencioso-Administrativo, de 15 de marzo de 2002 se estima en parte el recurso contencioso-administrativo interpuesto anulando el apartado 2 de la norma 3.ª y la norma 6.ª de dicha instrucción, si bien ambos únicamente en cuanto pretenden extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción del artículo 34 de la LOPD, y anulando también el apartado 1 de la norma 4.ª de la misma Instrucción, desestimando en lo demás la pretensión de la demandante. *Vid.*, en particular, Davara Rodríguez, M. Á.: «La transferencia internacional de datos», en *Revista Española de Protección de Datos*, núm. 1, Madrid: Agencia de Protección de Datos de la Comunidad de Madrid-Civitas, 2007, págs. 30-46.

10 Los elementos principales que deberá valorar la entidad competente –Comisión Europea o AEPD, según el caso– al momento de efectuarse la evaluación del nivel de protección adecuado son dos: por un lado, los principios rectores de la protección de datos (finalidad, calidad de los datos, transparencia y seguridad), donde los mismos deberán ser identificados y desarrollados sin importar la naturaleza del continente de tales principios y, por otro, los mecanismos de efectividad de tales principios, que se refieren a la puesta en práctica, observación y cumplimiento de los principios. *Vid.* en relación con los principios básicos en todo análisis de adecuación, Aced Félez, E.: «Transferencias internacionales de datos», en Piñar Mañas, J. L. (dir.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos*, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia: Tirant lo Blanch, 2005, págs. 108-109.

ferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, 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». Este precepto se ve complementado por el artículo 25.4 de la Directiva 95/46/CE, según el cual siempre se considerará que ofrecen un nivel de protección adecuado aquellos terceros Estados respecto de los cuales la Comisión Europea haya declarado la existencia de esa adecuación; extremo que contempla el artículo 34 k) de la LOPD cuando afirma que no será necesaria autorización del director de la Agencia Española de Protección de Datos (en adelante, la AEPD) «cuando la transferencia tenga como destino un Estado miembro de la UE, 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».

7. La aplicación del principio de «nivel de protección adecuado»[11] antes comentado cobra vigencia cuando al efectuarse una transferencia internacional de datos se permite la misma en el momento en que se evidencie que el país destinatario posea instrumentos que garanticen la protección de los datos de carácter personal que sean transmitidos y tratados; conciliándose, de esta forma, la necesidad de la transferencia internacional de datos y la obligación de protección que deben los responsables del tratamiento a los datos de carácter personal.

8. En las transferencias internacionales de datos suelen distinguirse dos supuestos: a) aquellos en los que se está en presencia de transferencias internacionales que implican auténticas cesiones de datos; y, b) aquellos otros en los que la transferencia se efectúa para el tratamiento de los datos por cuenta de tercero. En ambos supuestos, conforme a la LOPD, nos encontraríamos ante «transferencias internacionales de datos de carácter personal» y tanto en un caso como en otro, el respeto a la ley de origen (en nuestro caso, la LOPD) para cualquier transferencia internacional de datos es pieza clave para su legitimidad.

Además, para garantizar la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal se deberá dar cumplimiento a los requisitos y obligaciones legales propias de las cesiones o comunicaciones de datos, es decir, que dicha transferencia internacional de datos de carácter personal se efectúe a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario y que la misma cuente con el previo consentimiento del interesado, otorgado con

---

11 *Vid.* sobre la transferencia internacional de datos de carácter personal y las posibles formas de evaluar el «nivel de protección adecuado», Documentos de trabajo del Grupo de trabajo del Artículo 29, «Primeras orientaciones sobre la transferencia de datos personales a países terceros. Posibles formas de evaluar la adecuación», adoptado el 26 de junio de 1997 (XV D/5020/97/ES 2-WP 4); y, «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE», aprobado el 24 de julio de 1998 (DG XV D/5025/98-WP 12).

carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar (art. 11.3 de la LOPD), salvo que se trate de alguno de los supuestos en que legalmente esta excepcionado dicho consentimiento (art. 11.2 de la LOPD).

Cuando la transferencia sea para que el cesionario de los datos realice un tratamiento sobre los datos transferidos, será de aplicación la figura del encargado del tratamiento. Por tanto, en cumplimiento del artículo 12 de la LOPD, en estos casos se deberá suscribir un contrato de tratamiento de datos por cuenta de terceros en el que el encargado de tratamiento deberá asumir las obligaciones establecidas en el mencionado artículo de la LOPD.

Otra de las obligaciones del exportador de datos de carácter personal sería dar cumplimiento a lo previsto en el artículo 5 de la LOPD –derecho de información del interesado en la recogida de datos–, esto es, informar previamente al afectado acerca de qué datos se van a transferir, dónde van a ser transferidos y el nivel de protección del país destinatario de los datos, con el fin de que aquel muestre su consentimiento inequívoco a dicha transferencia internacional de datos (art. 6 LOPD –consentimiento del afectado–)[12].

2. DETERMINACIÓN DE LA COMPETENCIA DE LAS AUTORIDADES DE CONTROL EN ESPAÑA

9. La competencia de la AEPD se corresponde con el ámbito de aplicación espacial de la legislación nacional de protección de datos, definido en el artículo 2.1 de la LOPD. La competencia de la AEPD se extenderá a las actividades desarrolladas por un responsable establecido en cualquier punto del territorio español [art. 2.1 a) LOPD], así como a aquel empresario responsable establecido en un Estado no parte de la UE, cuando utilice medios en España que no sean de mero trámite [art. 2.1 c) LOPD]. Además, puede suceder que la AEPD extienda territorialmente su competencia a un tercer Estado donde se encuentre establecido el responsable de un tratamiento de datos[13].

10. En España, con la LOPD, como ocurre en otros países *de perfil federal o autonómico* (como en Alemania, en Suiza o en Canadá), se habilita a las comunidades autónomas a crear sus propias autoridades de protección en esta materia, «cuando afecten a ficheros de datos de carácter

---

12 *Vid.* en el mismo sentido, De Miguel Asensio, P. A.: «Recensión a Diana Sancho Villa, *Transferencia internacional de datos personales*, Madrid: Agencia de Protección de Datos, 2003, 294 págs.», en *REDI*, vol. LVI (2004), 1, págs. 636-639.

13 El contrato entre el responsable del tratamiento ubicado en España y otro empresario, también responsable, puede contener el compromiso del destinatario de aceptar la competencia de la autoridad de origen para velar por el cumplimiento de los derechos del afectado y aceptar el acceso a sus establecimientos de la citada autoridad o de un auditor o agente independiente en quien delegue.

personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial»[14].

Son varias las comunidades autónomas que ha aprobado normas sobre protección de datos de carácter personal: Madrid, Cataluña, País Vasco, Comunidad Valenciana, Castilla-La Mancha, Navarra y Castilla y León; y, de todas estas, hasta la fecha, solo han sido creadas en España tres agencias autonómicas de protección de datos: la «desaparecida» Agencia de Protección de Datos de la Comunidad de Madrid[15], la Agencia Catalana de Protección de Datos[16] (hoy día, «Autoridad Catalana de Protección de Datos»)[17], y la Agencia Vasca de Protección de Datos[18], si bien otras comunidades autónomas se encuentran en estos momentos trabajando en ello: en la Comunidad Valenciana, en la futura Agencia Valenciana de Protección de Datos[19]; en Castilla-La Mancha, en la Agencia Castellano-Manchega; y, en Andalucía, en la Agencia Andaluza de Protección de Datos. Recientemente, la Agencia de Protección de Datos de la Comunidad de Madrid, por razones presupuestarias, ha sido suprimida.

11. Ahora bien, el legislador español ha diseñado un sistema de control público donde el tráfico internacional de datos personales se somete inexorablemente a la intervención de la AEPD –arts. 33 y 34 LOPD–, correspondiéndole el ejercicio del control y la adopción de las autorizaciones que procedan en relación con los movimientos internacionales de datos (art. 37.1 LOPD), función que, sin embargo, no corresponde a las autoridades de control (art. 41.1 LOPD).

Esta «reserva de competencia» a favor de la AEPD en materia de transferencias internacionales de datos (art. 41 LOPD) es consecuencia no solo de que las relaciones internacionales son

---

14 Son lo que el Consejo de Europa denomina «Agencias subestatales o subnacionales».

15 Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

16 Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos y Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades (DOGC núm. 3835, de 4 de marzo de 2003).

17 Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos (DOGC núm. 5731, de 8 de octubre de 2010 y corr. de err. DOGC núm. 5739 de 21 de octubre de 2010). Esta ley introduce algunas novedades dignas de mención: la nueva ley cambia la denominación de la agencia, que pasa a denominarse «Autoridad Catalana de Protección de Datos», adecua el ámbito de actuación de la institución a las previsiones derivadas del Estatuto de Autonomía del año 2006, cambia el sistema de designación del director que pasa a ser por designación parlamentaria, se cambian las funciones del Consejo Asesor y se introducen las figuras de las auditorías de oficio realizadas por la autoridad y también alguna referencia a las evaluaciones de impacto sobre la privacidad o sobre el acceso a la información, entre otras cuestiones.

18 Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

19 *Vid.*, p. ej., en relación con la futura Agencia Valenciana de Protección de Datos, Benedito Agramunt, J.: «Anteproyecto de Ley de creación de la Agencia Valenciana de Protección de Datos», en Troncoso Reigada, A. (dir.), *Estudios sobre Administraciones públicas y protección de datos personales. I Encuentro entre Agencias Autonómicas de Protección de Datos Personales: celebrado el día 2 de noviembre de 2004 en la Sede de la Universidad Carlos III de Madrid; organizado por la Agencia de Protección de Datos de la Comunidad de Madrid*, Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, 2006, págs. 247-257.

competencia exclusiva del Estado (art. 149.1.3.º CE) sino de un principio de eficacia práctica y de unicidad de interlocutor para cada uno de los Estados[20].

Este reparto de competencias, en lo que respecta a las transferencias internacionales de datos, ha sido criticado por algunas autoridades de control autonómicas. En concreto, la Autoridad Catalana de Protección de Datos señala que el artículo 156 a) del Estatuto de Autonomía de Cataluña del año 2006[21] atribuye a la Generalidad de Cataluña la competencia ejecutiva en materia de protección de datos de carácter personal, incluyendo en todo caso la inscripción y el control de los ficheros de titularidad pública, sin hacer distinción en cuanto a las transferencias de datos sobre las que deba efectuarse esa función de control. De ello podría deducirse (dice dicha autoridad) el obligado reconocimiento de la competencia autonómica de autorización de dichas transferencias internacionales de datos de carácter personal.

12. El artículo 156 del nuevo Estatuto de Autonomía de Cataluña[22] no se encuentra sometido a lo dictado por la LOPD, por ser ley posterior de rango jerárquico superior –no olvidemos que forma parte del «bloque de constitucionalidad»–[23]. Huyendo de «debates competenciales»[24], y centrándonos en el tema que nos interesa, si por «transferencia internacional de datos» debemos

---

20 *Vid.* Troncoso Reigada, A.: «Introducción y presentación» a Agencia de Protección de Datos de la Comunidad de Madrid, *Repertorio de Legislación y Jurisprudencia sobre Protección de Datos*, Madrid: Thomson-Civitas, 2004, pág. 86.

21 Estatut d'Autonomia de Catalunya (arts. 4.1, 15, 20, 23, 27, 28, 30, 31, 76, 78, 156, 182.3) (DOGC núm. 4680, de 20 de julio de 2006).

22 Precepto a salvo del conocido recurso de inconstitucionalidad núm. 8045-2006, interpuesto por 99 diputados del Grupo Parlamentario Popular del Congreso contra diversos preceptos de la Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña, que desembocó en la Sentencia del Pleno del Tribunal Constitucional, de fecha 28 de junio de 2010.

23 No debemos olvidar que, como señala Espín, las «Leyes del estado y leyes de las Comunidades Autónomas poseen el mismo rango y fuerza, pero tienen acotado un campo material distinto determinado por el bloque de la constitucionalidad, conjunto normativo integrado por la Constitución, los Estatutos de Autonomía y determinadas leyes estatales distributivas de competencias entre el Estado y las Comunidades Autónomas. Este criterio de separación entre los ámbitos propios de las potestades normativas del Estado y de las Comunidades Autónomas no es sino una manifestación del principio de competencia, que aquí opera como medio de delimitación del ámbito de ejercicio de las potestades normativas del Estado y de las Comunidades Autónomas. De acuerdo con el citado principio, unas y otras se despliegan en aquellas materias para las que, de acuerdo con el citado bloque de la constitucionalidad, poseen competencia legislativa». *Vid.* VV. AA.: *Derecho Constitucional. Volumen I (El ordenamiento constitucional. Derechos y deberes de los ciudadanos)*, 6.ª edición, Valencia: Tirant lo Blanch, 2003, pág. 78.

24 Así, Mortilla Martos se muestra a favor de la asunción de nuevas competencias por parte de la Generalitat Catalana, vía Estatut, sin que la previsión estatutaria provoque la inconstitucionalidad sobrevenida de las normas básicas estatales en vigor que excedan ese carácter. En un sentido contrario, se pronuncia Ortega Álvarez, para quien esa previsión estatutaria solo vincula al legislador catalán en cuanto principios, objetivos o estándares mínimos; quedando el legislador autonómico, de esta forma, sometido a un doble límite: el respeto a las bases estatales y la concreción de facultades competenciales que hace el Estatuto. *Vid.* Montilla Martos, J. A.: «La legislación básica tras las reformas estatutarias», *Revista Española de Derecho Constitucional*, año 26, núm. 78, septiembre-diciembre (2006), Madrid: Centro de Estudios Políticos y Constitucionales, 2006, págs. 123-124 y 142.

entender todo tratamiento de datos que supone una transmisión de los mismos fuera del territorio español, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español; las agencias autonómicas carecen de competencia en materia de transferencia internacional de datos, en la medida en que su competencia abarca los tratamientos realizados dentro del territorio autonómico –y, de momento, solo en relación con los ficheros de titularidad pública–[25] en el que se establecen y no fuera del territorio español[26].

13. Algunas de las recientes reformas de algunos Estatutos de Autonomía de las comunidades autónomas han introducido preceptos relativos al derecho a la protección de datos en relación con los ficheros de titularidad pública[27]. Junto a ellos, han regulado la protección de datos de carácter personal desde la perspectiva competencial, atribuyéndose competencias ejecutivas (Cataluña y Andalucía), de desarrollo legislativo y ejecución (Illes Balears) o compartidas (Aragón). En línea con dichas reformas se encuentran las ya iniciadas de otros Estatutos de Autonomía, actualmente en tramitación, caso de Castilla y León, el comentado de Castilla-La Mancha y el de Canarias.

No cabe ninguna duda de que la duplicidad entre autoridades de control autonómicas y la estatal puede llegar a ser conveniente por razones cuantitativas y cualitativas. Por un lado, porque aquellas actúan como órganos de auxilio de la AEPD; tras la ampliación de competencias de 2003, le es necesario el auxilio de órganos para cumplir sus funciones, tanto las de inscripción de ficheros, como de inspección y sanción. Por otro lado, una segunda razón justificativa de la existencia de las agencias autonómicas tiene carácter cualitativo: desarrollan una labor de promoción y de concienciación al ciudadano, a las empresas y a las instituciones, en relación con los derechos y obligaciones que les corresponden, que le sería difícil realizar, en solitario, a la AEPD[28], pero, en la práctica, esa multiplicidad de autoridades competentes podría, en última

---

25 Ya sean ficheros creados y/o gestionados por las Administraciones públicas catalanas. *Vid.*, en particular, Bacaria Martrus, J.: «La Agencia Catalana de Protección de Datos (algunos aspectos comparativos con la Agencia de Protección de Datos de la Comunidad de Madrid). La cuestión de las competencias autonómicas sobre ficheros de titularidad privada en la ley catalana», en Davara Rodríguez, M. Á. (coord.), *XVII Encuentros sobre Informática y Derecho 2002-2003*, Universidad Pontificia de Comillas, Madrid, 2003, págs. 47-56.

26 En el mismo sentido, Rebollo Delgado y Serrano Pérez señalan que «existen competencias en el ámbito del control del tratamiento de datos que han de ser ejercidas inexorablemente por órganos de carácter nacional, como son la transferencia internacional de datos, las relaciones con los órganos de la UE y con otros de carácter internacional, o la publicidad periódica de los ficheros inscritos». *Vid.* Rebollo Delgado L. y Serrano Pérez, M.ª M.: *Introducción a la protección de datos*, Madrid: Dykinson, 2006, pág. 111.

27 Artículo 31 del Estatuto de Autonomía de Cataluña; artículo 28 del Estatuto de Autonomía de las Illes Balears; artículo 32 del Estatuto de Autonomía para Andalucía; artículo 16.3 del Estatuto de Autonomía de Aragón.

28 *Vid.*, en general, Rebollo Delgado, L. y Serrano Pérez, M.ª M.: *Introducción…*, *op.cit*., pág. 112; y, en particular, Troncoso Reigada, A.: «La contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos», en Davara Rodríguez, M. Á. (coord.), *XVII Encuentros…*, *op.cit*., págs. 23-45.

instancia, obstaculizar la protección del titular del derecho a la protección de datos con ocasión del tratamiento ilícito internacional de sus datos de carácter personal.

14. El creciente protagonismo normativo e institucional de las comunidades autónomas en materia de protección de datos, en España, incluida la creación de otras futuras autoridades de control, es otra razón que sugiere la conveniencia de extremar las cautelas a la hora de determinar las condiciones básicas del ejercicio del referido derecho fundamental. A estos efectos ha de recordarse que la STC 290/2002 declaró que solo la reserva a una única autoridad (a la AEPD) de la competencia sobre todos los ficheros, con independencia de su ubicación y naturaleza, puede garantizar la efectividad del derecho a la protección de los datos de carácter personal, lo que conecta con la competencia exclusiva del Estado *ex* artículo 149.1.1 de la CE, que excepcionalmente implica, además de una reserva normativa, una perspectiva institucional. De lo anterior se ha deducido la legitimidad del monopolio de la competencia estatal (AEPD) sobre todos los ficheros privados. Pero no ha supuesto un límite a la competencia de las comunidades autónomas para crear sus propias agencias/autoridades de control (arts. 148.1.1 CE y 41 LOPD) y para otorgar a estas funciones de inscripción y control, en términos generales, sobre los ficheros de titularidad pública de la respectiva Administración pública y sus personificaciones.

La solución pasa por adoptar un «tratamiento uniforme» (STC 173/1998) con el fin de evitar el conflicto y actuar con mesura y ponderación, a fin de asegurar la igualdad de todos los españoles en el ejercicio del derecho a la protección de datos de carácter personal[29].

15. Bien es cierto que este nuevo marco competencial (AEPD *vs.* agencias autonómicas de protección de datos) puede ser modificado en el futuro de dos formas distintas: por una parte, a través de la reforma de los Estatutos de Autonomía, que podría asumir la materia de protección de datos; por otra, a través de una modificación de la propia LOPD, por la que se atribuyan mayores competencias de ejecución administrativa sobre la protección de datos a las agencias au-

29 Así, p. ej., esta es la argumentación de la Agencia de Protección de Datos de la Comunidad de Madrid sobre las definiciones de ficheros de titularidad privada y pública contenidas en el artículo 5.1 del Reglamento, letras l) («los ficheros de los que sean responsables las entidades sometidas al derecho privado, no vinculados en ningún caso con el ejercicio de potestades de derecho público, incluyendo aquellos de los que sean responsables las fundaciones del sector público, salvo en su caso, las fundaciones públicas sanitarias, las sociedades del sector público empresarial del Estado, la Comunidad Autónoma, la Provincia o el Municipio, con independencia de su estructura accionarial, y las Corporaciones de Derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica») y m) («los ficheros de los que sean responsables los Órganos constitucionales o con relevancia constitucional del Estado o las Instituciones Autonómicas con funciones análogas a las mismas, las Administraciones Públicas Territoriales, las entidades u organismos vinculados o dependientes de las mismas con personalidad jurídico pública y sometidas al derecho administrativo, las Universidades Públicas y las Corporaciones de derecho público, en este último caso, siempre y cuando dichos ficheros se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica»).

tonómicas[30]. La distribución competencial no tiene por qué merecer descalificación alguna; se trata de una opción razonable, que puede facilitar la aplicación de criterios homogéneos en toda España a la hora de tomar decisiones, siempre y cuando vaya encaminada a preservar el derecho a la protección de datos y a garantizar las transferencias internacionales de dichos datos. Además, esa acción coherente y homogénea no solo es exigida por elementales razones de igualdad en la aplicación de la ley y de unidad de mercado, sino también por la naturaleza de los riesgos que se quieren conjugar: evitar los conflictos de competencias *ad intra* a la hora de autorizar o no una transferencia internacional de datos, obligando a las autoridades de control que entran en juego a la cooperación institucional y la coordinación de los criterios o procedimientos de actuación[31].

III. LA NECESIDAD O NO DE ARTICULAR UNAS DIRECTRICES O ESTÁNDARES INTERNACIONALES COMUNES PARA LA PROTECCIÓN DEL TITULAR DEL DERECHO A LA PROTECCIÓN DE DATOS ANTE EL TRATAMIENTO ILÍCITO INTERNACIONAL DE SUS DATOS DE CARÁCTER PERSONAL

16. Son muchas las autoridades de protección de datos que hoy día conviven en el espacio, desplegando sus competencias en el marco de su ley reguladora. Esta construcción propicia la necesidad de establecer cauces de cooperación internacional entre todas ellas para salvaguardar en todo momento los derechos del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita (sobre todo, en el Estado de destino).

El establecimiento de cauces de cooperación entre autoridades se muestra como uno de los retos para la liberalización del tráfico de datos de carácter personal y para garantizar la efectividad de las medidas que puedan imponer, salvaguardando, p. ej., el deber recíproco de informarse sobre las actuaciones de protección de destino que no garanticen el cumplimiento de la normativa de protección en ese lugar, o la obligación que pesa sobre la autoridad nacional del Estado parte de informar a la Comisión Europea cuando haga uso de la facultad de suspender la transferencia internacional de datos personales a ese lugar[32].

---

30 *Vid.* Troncoso Reigada, A.: *Memoria 2004 de la Agencia de Protección de Datos de la Comunidad de Madrid*, Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, 2005, pág. 11.

31 Quizás, hoy día, *ad intra*, se podría plantear la configuración de un órgano que facilite la comunicación, coordinación y cooperación entre las AEPD y las agencias autonómicas. *Vid.*, en el mismo sentido, Troncoso Reigada, A.: «Introducción y Presentación» a Agencia de Protección de Datos de la Comunidad de Madrid, *Repertorio de…*, *op. cit.*, pág. 96.

32 La institucionalización de la cooperación entre autoridades de protección de datos se ordena también en el contexto de diversos foros internacionales: p. ej., en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, o en la Recomendación de la OCDE sobre los Principios rectores de la protección de la vida privada y de las transferencias internacionales de datos personales.

17. El *problema jurídico* de las transferencias internacionales de datos de carácter personal no ha sido la ausencia de normas y de usos prácticos sino más bien lo contrario: la existencia de una fragmentaria regulación, dispersa y, en gran medida, obsoleta. Ciertamente se echa en falta a estas alturas un enfoque global y actualizado, que atienda a los dos intereses en juego: la libre circulación de datos y los derechos del titular del derecho a la protección de datos derivada de una transferencia internacional de sus datos de carácter personal.

18. Debemos apostar por un enfoque común por el diálogo transatlántico entre la conjunción privacidad-seguridad, optando por el establecimiento de unos estándares comunes. Más aún en una sociedad como la actual, en la que el desarrollo de las herramientas que proporciona la sociedad de la información y las tecnologías de la información y la comunicación dan lugar a un marco enteramente globalizado, en el que son comunes los flujos de datos entre los distintos Estados, siendo dichos flujos necesarios para el funcionamiento de la sociedad tal y como es hoy concebida.

Eso sí, hasta tanto se desarrollen estas iniciativas es preciso atender con especial sensibilidad a los flujos internacionales de datos, con el fin de que se permita su transferencia desde entornos geográficos con niveles de protección adecuados a otros que carezcan de ellos, garantizándose la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita.

19. Sin duda alguna, en este ámbito la colaboración y cooperación entre las autoridades de control, nacionales, autonómicas/regionales, públicas o privadas será fundamental para garantizar el derecho a la protección de datos en el marco de una transferencia internacional[33]. A tal efecto, a nuestro modo de ver dichas autoridades deberían colaborar y cooperar a un triple nivel:

- **1.er nivel**: garantizando un marco lo más armonizado posible de la protección de la privacidad.
- **2.º nivel**: intercambiando la información que resulte necesaria para resolver las reclamaciones o cuestiones concretas planteadas a cada una de ellas y que exijan dicha transmisión de información.
- **3er nivel**: garantizando que podrá producirse una persecución de las conductas contrarias a la privacidad de las personas con independencia de la nacionalidad del autor o del perjudicado o del lugar o lugares en que se encuentren los datos, evitando así la creación de «paraísos de datos» (*data havens*) o zonas de impunidad o de desprotección del derecho[34].

---

33 *Vid.* artículo 23 de la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal, elaborada por la AEPD, de 24 de abril de 2009, disponible en *http://www.agpd.es*

34 El peligro de fomentar siquiera indirectamente la existencia de *data havens* lleva a que las transferencias internacionales de datos solo puedan efectuarse cuando se garantice un «nivel de protección adecuado». Sin duda, para evitar los *data*

Dichas autoridades deberían realizar, particularmente, los mayores esfuerzos para, entre otras funciones:

a) Compartir estudios, técnicas de investigación, estrategias de regulación y demás información que resulte de utilidad para el más eficaz ejercicio de sus funciones, en especial tras recibir una petición de apoyo en el desarrollo de una investigación o intervención.

b) Realizar investigaciones o intervenciones coordinadas, tanto a nivel nacional como internacional, en asuntos en los que concurra el interés de dos o más autoridades de supervisión.

c) Participar en asociaciones, grupos de trabajo y foros conjuntos, así como en seminarios, talleres o cursos que contribuyan a adoptar posturas comunes o a mejorar la cualificación técnica del personal que preste sus servicios a dichas autoridades de supervisión.

d) Mantener los niveles apropiados de confidencialidad con respecto a la información intercambiada en cumplimiento del presente apartado.

20. La elaboración de unos estándares internacionales en materia de transferencias internacionales de datos de carácter personal, a modo de instrumento jurídico vinculante de alcance global, no resultaría completa si no se tratase de dar respuesta a una cuestión que reviste especial trascendencia en su aplicación, cual es la resolución de controversias y la determinación de la ley nacional aplicable ante un litigio derivado de una internacional de datos de carácter personal ilícita.

Tal respuesta puede resolverse acudiendo a distintos criterios tales como el lugar de recogida de los datos, el domicilio del interesado cuyos datos son tratados o el lugar del tratamiento de datos. No obstante, las legislaciones comunitarias, convencionales y estatales que han dado respuesta a esta cuestión han partido en su gran mayoría de considerar como punto de conexión el lugar del establecimiento[35] de la persona o entidad responsable en relación con cuyo marco de actividad se llevan a cabo las distintas operaciones de tratamiento de datos de carácter personal[36].

---

havens las transferencias internacionales de datos, en la práctica, deben ser auditadas, inspeccionadas y controladas, bien mediante la actuación directa de las autoridades de control de los países de origen o de los países de destino de los datos (auditorías públicas), o bien mediante la intervención de operadores privados externos (auditorías privadas), sobre todo, cuando se realizan transferencias de datos a terceros Estados, a los efectos de verificar el cumplimiento de las obligaciones asumidas por exportador e importador de los datos (contrato de transferencia internacional de datos).

35 Se puede entender por «establecimiento» cualquier instalación estable que permita el ejercicio efectivo y real de una actividad, con independencia de su forma jurídica.

36 Se deberían articular los criterios de determinación de la competencia judicial internacional en litigios derivados de los tratamientos de datos de carácter personal (jurisdicción), tales como, p. ej., la sumisión expresa o tácita, el domicilio del demandado, el lugar de celebración/ejecución de un contrato cuyo objeto sean datos de carácter personal, o el lugar de tratamiento de los datos, residencia del afectado por el tratamiento de datos. Se podrían establecer otras

Sin embargo, esta regla debe completarse atendiendo a las especiales circunstancias promovidas por el desarrollo de las tecnologías de la información y la comunicación y por la utilización generalizada de herramientas de uso potencialmente global por los sujetos obligados y por los interesados titulares del derecho a la privacidad.

En el marco de estas herramientas no es poco común el supuesto en que una persona o entidad responsable dirija su actividad a un colectivo delimitado por su situación geográfica, con independencia del lugar en que ese responsable se encuentre ubicado y del hecho de que establezca físicamente o no en el mismo su actividad, evitando soluciones forzadas en la delimitación de la regla del establecimiento y aclarando que en estos supuestos el criterio delimitador de la legislación aplicable no será el lugar del establecimiento del responsable sino aquel al que dirija específicamente su actividad[37]. De este modo, cuando una actividad tenga por objeto recoger datos de los nacionales de un Estado concreto o de Estados determinados será la legislación de dichos Estados la aplicable al tratamiento con independencia del lugar en que se encuentre el establecimiento de quien recaba los datos personales.

21. Pero, ¿no hay ya demasiados instrumentos normativos? ¿Para qué otro? ¿De verdad son necesarios unos estándares internacionales comunes para garantizar la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal? La razón, a mi modo de ver, es que los marcos internacionales han sido muy sobrepasados en su implementación práctica por la Directiva 95/46/CE, que no entendería que el cumplimiento de los anteriores implicara el cumplimiento de la misma. En este sentido, un instrumento internacional que sí cumpliera con los requisitos de la normativa europea sería entendido por el régimen europeo como «adecuado» en términos de su normativa.

La superación de fronteras físicas y temporales requiere, ineludiblemente, de un instrumento normativo común con el que se logre el mayor consenso posible internacional. No se trata de abandonar los sistemas jurídicos tradicionales ni la fuerza de las leyes sino de adaptar el sistema para que su aplicación y control sea lo más inmediato y factible posible. Es, por tanto, una adaptación multirregional y multidisciplinar del Derecho en materia de transferencia internacional de datos.

Es necesaria, pues, cierta coordinación en el ámbito mundial en materia de transferencia internacional de datos personales, con el fin último de garantizar la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal.

---

soluciones de ley aplicable para dar respuesta a los conflictos derivados de los tratamientos de datos de carácter personal, tales como, p. ej., la ley libremente elegida por las partes, la ley del Estado de la residencia habitual común del responsable y de la víctima, la ley del lugar donde se ha producido el daño, la ley de residencia o domicilio habitual del afectado, la ley del país de origen/destino de la transferencia internacional de datos, la ley del Estado donde suceden los elementos más significativos de la pérdida o el daño, la ley que más vinculada esté con el supuesto, por ser la más previsible para las partes, la ley de residencia del afectado, etc.

37 Sería recomendable también definir algunos conceptos que se puedan manejar y que, en la práctica, pueden inducir a error o confusión, tales como: «persona responsable» y «dirija específicamente una actividad a su territorio».

Se necesitan acuerdos internacionales que pongan fin a las disparidades legales existentes y configuren escenarios previsibles y adecuados, donde los intercambios de datos personales queden garantizados. Se debe trabajar en *pro* de la aprobación de un instrumento internacional vinculante en materia de protección de datos, con vocación universal, que permita el establecimiento de un marco jurídico seguro y estable[38]. Mientras tanto, en el periodo de transición, la implementación de la solución contractual, si bien no soluciona el problema, nos brinda una elegante salida que nuestros legisladores deberían considerar.

IV. COOPERACIÓN INTERNACIONAL ENTRE AUTORIDADES DE CONTROL Y CONVENIENCIA O NO DE CREAR UNA AUTORIDAD SUPRANACIONAL PARA LA PROTECCIÓN DEL TITULAR DEL DERECHO A LA PROTECCIÓN DE DATOS ANTE EL TRATAMIENTO ILÍCITO INTERNACIONAL DE SUS DATOS DE CARÁCTER PERSONAL

22. Como hemos tenido ocasión de señalar, confluyen en materia de control de las transferencias internacionales de datos una pluralidad de entidades: las autoridades de protección estatales (públicas y/o privadas), los órganos jurisdiccionales estatales, las autoridades de protección autonómicas/regionales, la Comisión Europea (y hasta el Grupo de Trabajo del artículo 29 o el Supervisor Europeo de Protección de Datos), lo que, en la práctica, puede provocar desajustes: ausencia de control, sobreprotección o problemas relativos a la efectividad de las medidas que puedan imponer en aras de la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita.

En la medida en que las transferencias internacionales de datos se supeditan al aseguramiento de los derechos de los interesados en el Estado de recepción de los datos, el establecimiento de vías de cooperación entre las autoridades de control (públicas y/o privadas) de los Estados intervinientes (origen y destino de los datos personales) viene a convertirse en un verdadero reto para asegurar la libre circulación de datos de carácter personal[39].

23. Tras la armonización legislativa entre los Estados miembros de la UE sobre la normativa en materia de protección de datos de carácter personal (Directiva 95/46/CE), sí queremos establecer un marco uniforme para la regulación de los flujos internacionales de datos y presumir *iuris tantum* de que existe un «nivel de protección adecuado» en todo Estado que tenga leyes específicas sobre la materia, con mecanismos de aplicación efectivos; se debería, en un primer momento,

---

38 *Vid.*, en el mismo sentido, Aced Félez, E. «Transferencias internacionales de datos», en Piñar Mañas, J. L. (dir.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos)*, La Antigua-Guatemala, 2-6 de junio de 2003), Valencia: Tirant lo Blanch, 2005, pág. 127.

39 *Vid.* Sancho Villa, D.: *Transferencia internacional de datos personales*, Madrid: Agencia de Protección de Datos, 2003, págs. 213-214.

exportar este estándar único dentro de la UE al resto de países europeos[40] y no europeos[41] para evitar la existencia de disposiciones contrapuestas entre la normativa comunitaria y convencional; y, en un segundo momento, lanzarse decididamente hacia la articulación de unos estándares internacionales comunes en materia de transferencia internacional de datos de carácter personal.

La idea última, en definitiva, es apostar por una sola voz sobre la protección de datos personales, lo que, sin duda, contribuiría a difundir la preocupación por la protección de datos entre países que aún no poseen legislación al respecto, velando para que exista un verdadero equilibrio entre intereses económicos (libre flujo de datos personales) e individuales (protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal) y actuando como interlocutor con aquellos países donde no exista un «nivel adecuado o equivalente» de protección de datos.

24. El control relativo a las transferencias internacionales de datos no debe recaer exclusivamente en el ámbito del control interno de los Estados. La nueva realidad nos introduce en un ciberespacio transversal, que es *tierra de nadie*, que nos obliga a articular mecanismos de resolución de controversias basados en técnicas de cooperación entre todos los entes participantes, sobre la base del contexto normativo en que se han construido:

- **Mecanismos de cooperación entre autoridades comunitarias**: la Comisión Europea debería auxiliarse del Grupo de Trabajo del artículo 29 a la hora de evaluar si el nivel de protección de un tercer Estado es o no adecuado y dictar la correspondiente decisión, vinculante para todos los Estados miembros; y el Supervisor Europeo de Protección de Datos debería colaborar con las autoridades de control nacionales u otros organismos de control.
- **Mecanismos de cooperación entre autoridades de control estatales**: las Autoridades nacionales de protección están obligadas a prestarse asistencia mutua y a informar al resto de Estados de las autorizaciones concedidas para transferir datos a terceros Estados, amparados en un contrato con cláusulas tipo o una ***binding corporate rule (BCR)***.
- **Mecanismos de cooperación entre autoridades comunitarias y autoridades de control estatales**: existe un deber recíproco de información entre los Estados

40 P. ej., en el seno del Consejo de Europa, a través de la reforma del mencionado Convenio 108/81/CE, p. ej., en el seno del Consejo de Europa, a través de la reforma del mencionado Convenio 108/81/CE.

41 P. ej., bajo el paraguas de la Organización de Naciones Unidas –ONU– sobre la base de las *Directrices sobre los principios rectores para la reglamentación de los ficheros computadorizados de datos personales*; o, en el marco de la Organización para la Cooperación y el Desarrollo Económicos –OCDE–, con las *Líneas directrices sobre la protección de la intimidad y los flujos internacionales de datos*, o de la Organización Mundial del Comercio –OMC–, mediante la adopción de un *Acuerdo General sobre Privacidad de la Información*, considerando en su totalidad el valor económico de los datos personales y el impacto de su regulación en el comercio internacional.

miembros y la Comisión Europea: a) en los casos en que entiendan que un tercer Estado no ofrece un nivel de protección adecuado, que obliga, en la práctica, a que los Estados miembros adopten las medidas oportunas para impedir la transferencia y a la Comisión a entablar negociaciones con dicho Estado; b) sobre las actuaciones de las autoridades del Estado de destino que no garanticen el cumplimiento de la normativa de protección en ese lugar; o c) la obligación que pesa sobre la autoridad de control del Estado de origen de informar a la Comisión cuando haga uso de la facultad de suspender el flujo de datos a ese Estado.

- **Mecanismos de cooperación con terceros Estados**: el instrumento es el mecanismo de cooperación entre las partes contratantes articulado por el Convenio 108/81/CE, 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[42], que les obliga a la designación por cada una de ellas de una o varias autoridades, con funciones de información recíproca sobre el Derecho y la práctica administrativa sobre protección de datos: el «Comité Consultivo» (T-PD), que puede auxiliarse por el denominado «Comité de Expertos en Protección de Datos» (*Project Group on Data Protection*, CJ-PD), creado por el Consejo de Europa en 1976, a modo de reunión de expertos en protección de datos personales de cada uno de los Estados miembros.

25. En consecuencia, el panorama descrito requiere de elevados índices de desarrollo normativo en aras de una mayor y mejor cooperación en materia de protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita, ya que son únicamente las funciones de investigación o integración las que presentan un desarrollo más significativo. La cooperación entre autoridades vinculada al ejercicio de facultades punitivas o sancionadoras, como hemos visto, tienen una escasa proyección[43].

26. Llegados a este punto cabe preguntarse si, en el contexto actual, caracterizado por la ausencia de una autoridad común y la diversidad de actitudes entre las autoridades nacionales existentes, creando problemas a las empresas que operan en diferentes países cuando deben presentar solicitudes de transferencias internacionales de datos personales y no asegurando la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos

---

42 BOE núm. 274, de 15 de noviembre de 1985. Han ratificado el convenio: Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Irlanda, Islandia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido y Suecia. Otros países han procedido solo a la firma del convenio, sin ratificarlo: Chipre, Eslovenia, Grecia, Hungría, Italia y Turquía.

43 Así, p. ej., podría manifestarse dicha cooperación con fines explícitos punitivos y sancionadores, en el contexto contractual, cuando el destinatario de los datos se someta expresamente a la competencia de la autoridad de protección del Estado de origen o de la autoridad en quien delegue. *Vid.* Sancho Villa, D.: *Transferencia internacional...*, *op. cit*., págs. 220-221.

de carácter personal ilícita, sería conveniente que existiera algún tipo de autoridad supranacional con funciones más o menos específicas para resolver los conflictos que pudieran derivarse de las transferencias internacionales de datos, pero sin que disminuyan las competencias de las autoridades de protección estatales[44].

27. La garantía del cumplimiento de los comentados estándares internacionales quedaría sujeta al establecimiento de un sistema de supervisión externa en forma de autoridad independiente: al control de esa nueva autoridad supranacional, que debería actuar con plena independencia e imparcialidad, no pudiendo estar sometida en el ejercicio de sus funciones al mandato de ninguna autoridad pública.

Esta nueva autoridad supranacional debería ser un órgano especializado y cualificado (especialmente preparado en la materia) e independiente (sin admitir la intervención de las autoridades de control estatales), que asumiera, como mínimo, las siguientes competencias:

a) Competencias de control, supervisión, asesoramiento e inspección:

- Resolución de los conflictos que puedan plantearse con ocasión de una transferencia internacional de datos de carácter personal entre varios Estados, y así evitar que la falta de acuerdo produzca una merma de la «libre circulación de datos de carácter personal».
- Ofrecer vías adecuadas de recurso a quienes resulten perjudicados por una transferencia internacional de datos.
- Controlar el establecimiento de barreras estatales protectoras sobre el flujo internacional de información.
- Autorizar, cuando sea preciso, las transferencias internacionales de datos a Estados con un nivel de protección no adecuado.
- Promover el uso de mecanismos de autorregulación como instrumentos complementarios de protección de datos personales en materia de transferencias internacionales de datos que: (a) representen un valor añadido en su contenido respecto de lo dispuesto en las leyes, (b) contengan o estén acompañados de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales y (c) consagren medidas efectivas en caso de su incumplimiento.

---

44 *Vid.* Estadella Yuste, O.: *La protección de la intimidad...*, *op. cit*., págs. 147-148; y, en relación con las BCR y la adopción del concepto de *lead regulator* o *leading authority*, Blas, F.: «Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales», *Revista Derecho del Estado*, n.º 23, diciembre de 2009, págs. 58-60.

b) Competencias relacionadas con la inscripción y registro.

- Mantener un registro público de las transferencias internacionales de datos realizadas y llevadas a cabo por los sectores público y privado, al que puedan acceder los interesados.

c) Competencias normativas.

- Armonizar las legislaciones nacionales de protección de datos, incluyendo el tema de las transferencias internacionales de datos.
- Homogeneizar los criterios estatales en las transferencias internacionales de datos.
- Emisión de dictámenes o pronunciamientos específicos, con el objeto de hacer frente a la obsolescencia normativa resultante de las permanentes innovaciones introducidas en el sector.
- Dictaminar los proyectos de disposiciones normativas estatales que puedan afectar al derecho fundamental a la protección de datos personales impidiendo la puesta de los datos de carácter personal en circulación internacional.

d) Competencias de asesoramiento y cooperación.

- Practicar acciones de cooperación internacional en materia de tratamiento de datos dirigidas, bien hacia titulares de datos personales y entidades tratantes de datos con residencia en el extranjero, bien hacia organismos internacionales o autoridades de control de otros países.
- Cooperar con las autoridades de control estatales para el cumplimiento de sus competencias y generar los mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse el debido auxilio mutuo cuando se requiera.
- Compartir estudios, técnicas de investigación, estrategias de regulación y demás información que resulte de utilidad para el más eficaz ejercicio de sus funciones, en especial tras recibir una petición de apoyo en el desarrollo de una investigación o intervención.
- Realizar investigaciones o intervenciones coordinadas, tanto a nivel nacional como internacional, en asuntos en los que concurra el interés de dos o más autoridades de supervisión.
- Participar en asociaciones, grupos de trabajo y foros conjuntos, así como en seminarios, talleres o cursos que contribuyan a adoptar posturas comunes o a mejorar la cualificación técnica del personal que preste sus servicios a dichas autoridades de supervisión.

- Mantener los niveles apropiados de confidencialidad con respecto a la información intercambiada en cumplimiento del presente apartado.

e) Competencias en relación con la potestad sancionadora y la adopción de decisiones.

- Requerimiento de informes y antecedentes de los responsables de datos, así como el ingreso y registro de los establecimientos y equipos en que se realizan las operaciones de transferencias internacionales de datos.
- Adopción de las medidas que resulten necesarias para evitar la persistencia en el incumplimiento de la normativa en materia de transferencia internacional de datos, tales como multas y restricciones temporales para la transferencia internacional de datos, cada vez que se cerciora de la ocurrencia de actos u omisiones que importen una infracción a las disposiciones legales y reglamentarias vigentes, sin perjuicio de su reclamación judicial.

f) Otras competencias.

- Promover las transferencias internacionales de datos, divulgando entre los individuos y a los poderes públicos el contenido del derecho fundamental a la protección de datos personales.
- Difundir las disposiciones legales y reglamentarias aplicables a las transferencias internacionales de datos personales, ya que la mayoría de las veces la infracción de sus preceptos encuentra su explicación en una falta de conciencia de antijuridicidad del comportamiento por parte del responsable de los datos personales.
- Prestar asistencia a los más diversos sectores de la comunidad: a los titulares de datos, acogiendo sus denuncias y dándoles curso, a través de un procedimiento de resolución alternativa de las controversias suscitadas entre estos y las entidades que tratamos sus datos; a los responsables de los datos, asistiéndolos en la formulación de códigos deontológicos, en la adopción de políticas de seguridad, etc.; o a los organismos públicos, informándoles de las decisiones que recaigan sobre materias de su competencia.
- Promover el establecimiento de nuevos mecanismos que faciliten las transferencias internacionales de datos: a) la definición de criterios que permitan distinguir categorías de transferencias que puedan suponer una amenaza para la vida privada; b) el establecimiento de cláusulas contractuales-tipo; y c) el establecimiento de «listas blancas» provisionales de Estados que puedan presumirse que garantizan un nivel de protección adecuado.
- Investigar y estudiar los problemas que para la «libre circulación de datos de carácter personal» se derivan del desarrollo de las nuevas tecnologías de la información.

En definitiva, debería tratarse de una autoridad independiente con funciones de cooperación internacional en materia de transferencia internacional de datos personales, con potestad de vigilancia y sancionadora en lo que se refiere a la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal.

28. De lo expuesto hasta el momento, la conclusión parece evidente: o apostamos por una autoridad supranacional *de nuevo cuño* o, por el contrario, nos apoyamos en las autoridades existentes, y en concreto por una de ellas, revistiéndola autoridad supranacional.

Si optamos por alguna de las autoridades en materia de protección de datos de carácter personal ya existentes:

a) **En el ámbito de la UE**, la apuesta pasaría, siempre *de lege ferenda*, por la asunción de esas nuevas competencias administrativas por parte del propio **Comité del artículo 31 de la Directiva 95/46/CE** («Comité de protección de datos personales»), del **Grupo de Trabajo del artículo 29** (el «G 29»), o del **Supervisor Europeo de Protección de Datos**[45].

b) **Fuera del ámbito de la UE**, por la creación de una autoridad administrativa de control-órgano jurisdiccional en el seno del Convenio 108/81/CE, del Consejo de Europa, asumiendo, p. ej., competencias el mencionado **Comité Consultivo del Convenio 108/81/CE**; o, finalmente, en su caso, optar por la cooperación sectorial, apostando por una «**autoridad privada de protección**» con competencia y potestad sancionadora en materia de transferencias internacionales de datos de carácter personal.

No obstante, si al final «el gato al agua» se lo lleva la UE, esa autoridad supranacional podría ser la **Agencia de los Derechos Fundamentales de la UE**, creada en virtud del Reglamento 168/2007 del Consejo, de 15 de febrero de 2007, que tiene como objetivos principales la lucha contra el racismo, la xenofobia y la intolerancia asociada a los mismos, y que, para el periodo 2007-2012, por Decisión de 28 de febrero de 2008[46], estableció como ámbitos temáticos de actividad de la Agencia: «h) la sociedad de la información y, en particular, el respeto a la intimidad y la protección de datos personales...».

Una u otra autoridad, lo que está claro es que en materia de transferencia internacional de datos de carácter personal debemos apostar por la cooperación internacional a través de la creación de una autoridad central, punto de encuentro para la colaboración entre Estados y motor

---

45 Merece la pena destacar que, sin perjuicio de eventuales recursos ante el Tribunal de Justicia de la UE, todo afectado por una transferencia internacional de datos está facultado a presentar una reclamación ante el supervisor si considera violados los derechos que reconoce el artículo 286 del Tratado de la Comunidad Europea (protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos). Las decisiones del supervisor son susceptibles de recurso ante el Tribunal de Justicia de la UE.

46 DOUE L 93/14, de 7 de marzo de 2008, artículo 2.

para evitar los conflictos entre empresarios, garantizar la confianza de los usuarios y permitir el cumplimiento de la normativa en protección de datos para, en definitiva, evitar y/o remover los obstáculos a las transferencias internacionales de datos de carácter personal.

Además, con el objeto último de garantizar la tutela del afectado ante un tratamiento ilícito internacional de sus datos de carácter personal sería interesante **también la constitución de un tribunal especializado en materia de protección de datos personales adscrito al Tribunal de Justicia de las Comunidades Europeas**[47].

La idea sería que, en virtud del artículo 257 del Tratado de Funcionamiento de la UE (*ex* artículo 225 A del Tratado de la Comunidad Europea) que el Parlamento Europeo y el Consejo, con arreglo al procedimiento legislativo ordinario, creara un tribunal especializado adjunto al Tribunal General, encargado de conocer en primera instancia de determinadas categorías de recursos interpuestos en materia de tutela del derecho a la protección de datos de carácter personal.

El Parlamento Europeo y el Consejo se pronunciarían mediante reglamentos, bien a propuesta de la Comisión y previa consulta al Tribunal de Justicia, bien a instancia del Tribunal de Justicia y previa consulta a la Comisión.

El reglamento por el que se pudiera crear este tribunal especializado fijaría las normas relativas a la composición de dicho tribunal y precisaría el alcance de las competencias que se le atribuyan.

---

47 Se podría *aprovechar* la experiencia del ya creado Tribunal de la Función Pública de la UE. El Tribunal de la Función Pública es, dentro de la institución jurisdiccional de la Unión, el órgano especializado en el ámbito del contencioso de la función pública de la UE, competencia que ejerció anteriormente el Tribunal de Justicia y posteriormente, a partir de su creación en 1989, el Tribunal de Primera Instancia. Es competente para conocer en primera instancia de los litigios entre la UE y sus agentes en virtud de lo dispuesto en el artículo 270 del Tratado de Funcionamiento de la UE, lo que representa, en consecuencia, aproximadamente 120 asuntos al año; el personal de las instituciones de la Unión está compuesto por unas 35.000 personas. Dichos litigios se refieren no solamente a las cuestiones relativas a las relaciones laborales propiamente dichas (retribuciones, desarrollo de la carrera, contratación, medidas disciplinarias, etc.), sino también al régimen de seguridad social (enfermedad, vejez, invalidez, accidentes laborales, complementos familiares, etc.). Es también competente para conocer de los litigios entre cualquier órgano u organismo y su personal, para los que se haya atribuido la competencia al Tribunal de Justicia de la UE [por ejemplo, los litigios entre Europol, la Oficina de Armonización del Mercado Interior (OAMI) o el Banco Europeo de Inversiones y sus agentes]. En cambio, no puede conocer de los litigios entre las Administraciones nacionales y sus agentes. Las resoluciones dictadas por el Tribunal de la Función Pública pueden ser objeto, en un plazo de dos meses, de un recurso de casación ante el Tribunal General limitado a las cuestiones de Derecho.

El Tribunal de la Función Pública de la UE está compuesto por siete jueces nombrados por el Consejo, por un periodo de seis años renovable, previas la convocatoria de candidaturas y la consulta a un comité compuesto por siete personalidades elegidas entre antiguos miembros del Tribunal de Justicia y del Tribunal General y juristas de reconocida competencia. El Tribunal de la Función Pública actúa en salas compuestas por tres jueces. No obstante, cuando la dificultad o la importancia de las cuestiones jurídicas lo justifiquen, un asunto podrá atribuirse al tribunal en pleno. Además, en los casos que determina su Reglamento de Procedimiento, puede actuar en salas compuestas por cinco jueces o en formación de juez único. Los jueces nombran a un secretario por un periodo de seis años. El Tribunal de la Función Pública dispone de su propia secretaría, pero utiliza los servicios del Tribunal de Justicia para cubrir sus demás necesidades administrativas y lingüísticas.

Contra las resoluciones dictadas por este tribunal especializado se podría interponer ante el Tribunal General recurso de casación limitado a las cuestiones de Derecho o, cuando el reglamento relativo a la creación de dicho tribunal especializado así lo contemplase, recurso de apelación referente también a las cuestiones de hecho.

Los miembros de dicho tribunal especializado serían elegidos entre personas que pudieran ofrecer absolutas garantías de independencia y que tuvieran la capacidad necesaria para el ejercicio de funciones jurisdiccionales. Serían designados por el Consejo por unanimidad.

En definitiva, este mecanismo judicial pondría fin a una práctica ilegal (las transferencias internacionales de datos de carácter personal ilícitas) y facilitaría a la parte perjudicada (titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal) el acceso uniforme a la justicia ante la violación de un derecho reconocido por el Derecho de la UE, permitiéndole incluso, en su caso, reclamar una indemnización por daños y perjuicios.

V. REFLEXIONES FINALES

29. En aras de garantizar la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita pensamos que la solución aportada por el artículo 25 de la Directiva 95/46/CE no es la más adecuada. El legislador comunitario debería haber optado por la solución prevista en el artículo 12 del Convenio 108/81/CE, esto es, enjuiciar la existencia de un «nivel de protección equivalente» sobre la base de una reglamentación técnica establecida al efecto, que garantizara la protección de datos en ese país tercero, objeto de la transferencia de datos de carácter personal.

30. Sin obviar los avances normativos acaecidos en los últimos años y las propuestas «anacionales» comentadas, la diversidad de sistemas de protección de datos y la privacidad o, en algunos casos, la ausencia de ellos, la elaboración de unas directrices o estándares internacionales (aunque sean mínimos) que faciliten con garantías los flujos de datos en un mundo globalizado, garantizándose así la «libre circulación de datos de carácter personal» y la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal, se ha convertido en una tarea cada vez más urgente.

Los Estados deben superar los prejuicios que las transferencias internacionales de datos de carácter personal provocan, con el fin de eliminar obstáculos injustificados en los movimientos internacionales de datos personales, implementados en nombre de la protección de la intimidad personal[48]. Ha llegado la hora: «un sistema realista de estándares debe emerger. Es absolutamen-

48 *Vid.* Herrán Ortiz, A. I.: «Problemas jurídicos del flujo internacional de datos personales en la legislación española», en Davara Rodríguez, M. Á. (coord.), *XIII Encuentros sobre Informática y Derecho 1999-2000*, Elcano (Navarra): Aranzadi, 2000, pág. 92.

te 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»[49]. Los estándares deben responder a tres valores: técnica, organizativa y semántica y deberían tener como objeto el asegurar, a través de la fijación de unos criterios comunes de protección, el libre flujo de los datos de carácter personal derivado de su cumplimiento. Es decir, deberán tratar de garantizar, a través de la adopción de los estándares, que ningún Estado pueda limitar el flujo de datos de carácter personal desde sus fronteras amparándose en la deficiente protección de la privacidad de sus nacionales o residentes.

El carácter universal del que debe dotarse a los estándares resulta clave: se trataría de trabajar en *pro* del establecimiento de unos principios y requisitos básicos que garanticen una protección uniforme de la privacidad de los individuos, en relación con el tratamiento de sus datos a nivel mundial.

31. La articulación de unos estándares internacionales en materia de protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita no vendría, en ningún caso, a suplantar a las legislaciones nacionales (o autonómicas/regionales) en aquellas áreas en las que existe una tradición reguladora del derecho a la privacidad en relación con el tratamiento de los datos; pero, eso sí, evitaría los conflictos de leyes, puesto que pasaríamos de un entorno territorial a un entorno internacional. En estos ámbitos podrán existir normativas que impongan, en su ámbito interno, exigencias superiores a las contenidas en los estándares, tanto en su contenido como en su concreto ámbito de aplicación[50].

Pero, en todo caso, esa regulación no debería suponer una limitación a la transferencia internacional de datos de carácter personal, siempre y cuando en el lugar de destino de los mismos se cumplan los requisitos mínimos establecidos en los estándares. De este modo, los estándares se configurarían como un mínimo común de protección de la privacidad cuyo cumplimiento sería requisito suficiente para considerar posible la transferencia de datos a los Estados que cumplan con aquellos. No debe dejar de tenerse en cuenta lo ya dicho al delimitar el objeto de los estándares, en lo referido a su finalidad de establecer un marco armonizado que garantice el libre flujo de datos personales, garantizando que lo heterogéneo de los distintos marcos legislativos nacionales o autonómicos/regionales aplicables pueda dificultar esos movimientos.

32. La propuesta debe ser clara: un instrumento que sea aceptado y seguido internacionalmente, que no tenga límite de aplicación sectorial o por objetivos, sino un alcance general, y que contenga mecanismos adecuados y coercitivos, nacionales e internacionales. Se trataría de un modelo para la protección de los intereses de los consumidores que cumpla con el nivel adecuado de

---

49 *Vid.* Blas, F.: «Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales», *Revista Derecho del Estado*, n.º 23, diciembre de 2009, pág. 58.

50 Por ejemplo, en dichos ámbitos podrá ser posible la extensión de la protección a las personas jurídicas o a los tratamientos no automatizados de datos personales.

protección, que facilite las transferencias internacionales de datos, que aliente el cumplimiento internacional y que, en definitiva, complemente la regulación.

La posibilidad de alcanzar resultados efectivos en torno a unos estándares internacionales en la protección del titular del derecho a la protección de datos, derivada de una transferencia internacional de datos de carácter personal ilícita, permitiría a todos los sujetos implicados que dispusieran de un marco estable poder tratar los datos internacionalmente sin temor a estar en un entorno demasiado regulado, jurídicamente hablando, o que sus competidores sean desleales y se vayan a «paraísos de datos», donde el desequilibrio entre los sujetos implicados sea eludible. De lo anterior deriva la necesidad, no solo teórica sino eminentemente práctica, de zanjar las diferencias entre la tradición europea en general (y, española en particular), caracterizada por un galantismo formal y rígido, frente a la concepción normativa adoptada, p. ej., por los Estados Unidos, mucho más laxa, y en sintonía con la fuerza de su economía y potencial mercado, puesto que no son dos posturas irreconciliables.

33. El establecimiento de un marco uniforme para la regulación de los flujos internacionales de datos y la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal, a modo de *corpus* de principios básicos, ha de ser considerado como uno de los aspectos esenciales en la fijación de los estándares internacionales[51].

La protección del derecho a la protección de datos constituye hoy en una necesidad, en una actuación ineludible de los Estados. Ahora bien, el contexto actual nos lleva a una ruptura de conceptos clásicos, como el de limitación territorial del Estado y de su ordenamiento jurídico. Ahora no es únicamente necesaria la intervención del Estado, y sí una normativa de carácter internacional. Se deben superar las divergencias normativas estatales actuales, romper la dicotomía UE *vs.* Estados Unidos y apostar decididamente por un ordenamiento jurídico internacional eficaz, donde no solo se reconozca el derecho a la protección de datos y se establezca un adecuado marco para el desarrollo de las transferencias internacionales de datos sino que también que se establezcan los medios de garantía adecuados para lograr tal fin.

34. La cesión internacional de datos personales ha sido, y sigue siendo, uno de los aspectos en que parece necesaria la coordinación estatal. Esta materia, en buena lógica jurídica, ha de ser regulada por una norma de ámbito supranacional; de lo contrario, se entraría en un sistema anárquico de cesión de datos a Estados que no tengan un nivel de garantía acorde con el Derecho nacional del Estado de origen.

Teniendo en cuenta la finalidad perseguida con los estándares, resulta coherente con su planteamiento que el criterio para delimitar la procedencia o improcedencia, en términos generales,

---

51 *Vid.* artículo 14 de la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal, elaborada por la AEPD, de 24 de abril de 2009, disponible en *http://www.agpd.es*

de la realización de una transferencia internacional de datos sea, precisamente, el establecimiento de un modelo normativo de mínimos, universal y vinculante en materia de transferencia internacional de datos. Con ello se garantizaría, en todo caso, que los principios, derechos y garantías previstos en un Estado respetuoso con este modelo se mantendrían en el Estado de destino y que, en particular, no sería posible la transferencia ulterior de los datos a Estados que no respetasen dichos principios, derechos y garantías.

35. La instauración de una autoridad supranacional con competencia en materia de transferencia internacional de datos resulta, sin duda alguna, novedosa; y, sobre todo, ambiciosa, aunque entendemos necesaria, en aras de la construcción de la «libre circulación de datos de carácter personal», sin que el derecho fundamental a la protección de datos de carácter personal que toda persona física tiene se vea perjudicado.

En cuanto al ámbito de actuación de la «nueva autoridad de control», lo ideal sería que fuera de carácter internacional y que se pudiera incluir dentro del marco de la ONU[52], si buscamos un grado de vinculación «total» por parte de los Estados. Sin embargo, eso sería demasiado ambicioso debido a la falta de experiencia y de tradición legal de muchos países no europeos en materia de protección de datos. Aunque, eso sí, sería más conveniente que, antes de instaurar una autoridad supranacional cuasiuniversal, todos los países contasen con su propia normativa de protección de datos[53].

36. Los Estados tienen un interés común en prevenir la creación de lugares donde la regulación nacional del tratamiento de datos de carácter personal pueda fácilmente realizarse, fuera de los límites legalmente establecidos. Quizás este hecho, y una comprensiva regulación aceptada a nivel internacional, podría permitir, a nuestro juicio, la articulación de una autoridad supranacional para juzgar los litigios internacionales derivados de la vulneración del derecho a la protección de datos, otorgando una protección internacional adecuada al titular del derecho a la protección de datos de carácter personal.

Así las cosas, debemos apostar de forma decidida, completa, clara, eficaz y eficiente por la expansión del principio de territorialidad *stricto sensu* para garantizar los intercambios globalizados de datos personales; esto es, por la creación de una autoridad supranacional y por la extraterritorialidad de la jurisdicción. Causar un impacto extraterritorial significa que la legislación debe poseer un ámbito extraterritorial. Los problemas globales, como son las transferencias internacionales de datos, exigen soluciones globales. En esta época de globalización, la soberanía se reconstruye. La reconstrucción parte de los mismos estándares originales en cuanto al tema que

---

52 En nuestra opinión podría ser UNCITRAL la entidad adecuada para llevar a cabo esta función. Podría, en un primer momento, encargarse de resolver los problemas que, como hemos visto, las transferencias internacionales de datos de carácter personal generan en los mercados internacionales para, en un segundo momento, desarrollar una ley modelo, antesala de una futura Convención de Naciones Unidas sobre Privacidad.

53 *Vid*. Estadella Yuste, O.: *La protección de la intimidad...*, *op. cit*., pág. 148.

estamos examinando, pues en esta materia es de interés de los Estados que afirman que su nivel de protección es «adecuado» entender la jurisdicción soberana desde el punto de vista clásico replanteado, con el fin de evitar la multiplicación de las autoridades/los tribunales competentes, eliminar obstáculos a la libre circulación de datos de carácter personal y dotar de protección al titular del derecho a la protección de datos de carácter personal ante un tratamiento ilícito internacional. En definitiva, ***one World, one Privacy, one Authority*** (un Mundo, un Sistema de Protección de Datos, una Autoridad).