José Luis Piñar Mañas *

El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro

Sumario: I. LOS ORÍGENES. "THE RIGHT TO BE LET ALONE".—II. DE LA TENSIÓN ENTRE INTIMIDAD E INFORMÁTICA AL DERECHO FUNDAMENTAL AUTÓNOMO A LA PROTECCIÓN DE DATOS, PASANDO POR EL VALOR ECONÓMICO DEL DATO PERSONAL.—III. EL CONTENIDO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.—3.1. Principios que configuran el contenido esencial del derecho fundamental a la protección de datos.—3.2. El principio de control independiente. En particular, la posición de la Agencia Española de Protección de Datos en el marco constitucional del derecho a la protección de datos personales.—IV. RETOS O TENSIONES A QUE ESTÁ SOMETIDO EL DERECHO A LA PROTECCIÓN DE DATOS.—V. ¿HACIA UN MODELO GLOBAL DE PROTECCIÓN DE DATOS? EN ESPECIAL, LA POSICIÓN DE LA DIRECTIVA 95/46/CE.—VI. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y SU NECESARIO DESARROLLO REGLAMENTARIO.—VII. UNA MIRADA AL FUTURO.

No es exageración afirmar que el derecho fundamental a la protección de datos personales es uno de los más importantes en la sociedad actual. Y no sólo en los países desarrollados, con democracias consolidadas, sino también en los que están en proceso de desarrollo, en los que la sociedad de la información es tan sólo una utopía, pero en los que ya es posible acumular y tratar información sin apenas control y garantías, con graves implicaciones para los ciudadanos. Teniendo en cuenta, además, que el tratamiento de datos personales no conoce fronteras, es un fenómeno transnacional y requiere, por tanto, una respuesta lo más uniforme y armonizada posible. El reto no es menor y merece una reflexión pausada y crítica. Pues, como ha señalado Rodota, la protección de datos, como «diritto di mantenere il con-

* Catedrático de Derecho Administrativo. Director de la Agencia Española de Protección de Datos.

trollo sulle proprie informazione», se presenta como una «dimensione della libertà esistenziale, costitutiva non solo della sfera privata, ma pure di quella pubblica» [1].

I. LOS ORÍGENES. «THE RIGHT TO BE LET ALONE»

Como he tenido ocasión de señalar recientemente [2], el Tratado por el que se instituye una Constitución para Europa recoge en dos ocasiones el Derecho fundamental a la Protección de Datos de Carácter Personal. Por un lado, en el artículo I-51, dentro del Título VI («De la vida democrática de la Unión») de la Parte Primera [3]. Por otro, en el artículo II-68, dentro del Título II («Libertades») de la Parte Segunda, «Carta de los Derechos Fundamentales de la Unión» [4]. Pese a que los avatares de la Constitución Europea todavía pueden darnos alguna sorpresa, es evidente que, si no con la Constitución, ya de por sí con la Carta de los Derechos Fundamentales de la Unión Europea, aprobada en Niza en 2000, se ha producido un cambio sustancial en la consideración que ha de darse al derecho fundamental a la protección de datos de carácter personal. Éste es el punto de partida que hoy debemos tener en cuenta de forma innegable.

En 1888 Thomas Cooley habló ya de «the right to be let alone» [5]. En 1890 Samuel Warren y Louis Brandeis publican en la *Harvard Law Review* [6] su famoso artículo *The Right to Privacy,* al que no hace mucho volvía a referirse Stefano Rodota [7]. En aquel entonces Warren y Brandeis hablaron de un nuevo derecho: *Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of*

---

[1] *Repertorio di fine secolo*, 2.ª ed., Editori Laterza, Roma-Bari, 1999, pp. 201-202.

[2] «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas», en *Cuadernos de Derecho Público*, núm. 19-20, monográfico sobre *Protección de Datos,* pp. 45 y ss. Asimismo, no pocas consideraciones que ahora expongo ya las he apuntado en «Reflexiones sobre el derecho fundamental a la protección de datos personales», en *Actualidad Jurídica. Uría Menéndez*, núm. 12, 2005, pp. 7 y ss.

[3] *Artículo I-51: Protección de datos de carácter personal.*

Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

La ley o ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

[4] *Artículo II-68: Protección de datos de carácter personal.*

Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen.

Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

El respeto de estas normas quedará sujeto al control de una autoridad independiente.

[5] *A Treatise on the Law of Torts or the Wrongs which arise independent of contract*, Callaghan, 2.ª ed., Chicago, 1888, p. 29.

[6] Vol. IV, núm. 5, 15 de diciembre de 1890.

[7] *Intervista su Privacy e Libertà*, a cargo de Paolo Conti, Editori Laterza, Roma-Bari, 2005, pp. 7 y ss.

society… Now the right to life has come to mean the right to enjoy life, the right to be let alone. La evolución que desde entonces se ha producido ha sido imparable. La lucha por la privacidad ha sido clave, sin duda, en la evolución de las sociedades democráticas. Evitar cualquier posibilidad de «Gran Hermano», de control intolerable de nuestra vida privada por los sectores público o privado era el gran reto. En este marco, la posibilidad de llevar a cabo tratamientos automatizados de datos personales supuso un punto de inflexión esencial, que ha condicionado todo el proceso a partir de entonces. Fue a partir de los años sesenta y setenta del pasado siglo cuando comenzó a generalizarse paulatinamente el uso de nuevas tecnologías que, en efecto, no sólo permitían obtener y almacenar un gran número de datos, sino, lo que seguramente es más importante y definitivo, someterlos a tratamiento. La posibilidad de ingerencias en la intimidad se incrementaba así de forma espectacular, y el legislador no podía ser ajeno a la nueva realidad que emergía de modo irrefrenable.

II. DE LA TENSIÓN ENTRE INTIMIDAD E INFORMÁTICA AL DERECHO FUNDAMENTAL AUTÓNOMO A LA PROTECCIÓN DE DATOS, PASANDO POR EL VALOR ECONÓMICO DEL DATO PERSONAL

Ya en 1967 [8] se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a no sufrir ingerencias en la vida privada (derecho éste que se había ya recogido en la Declaración Universal de Derechos Humanos [9] o el Pacto Internacional de Derechos Civiles y Políticos de 1966 [10]). De tal Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre *«los Derechos humanos y los nuevos logros científicos y técnicos»*, que respondía a una inquietud existente en toda Europa. Suele decirse, no sin razón, que en tal Resolución se encuentra el verdadero origen del movimiento legislativo que desde entonces recorrerá Europa en materia de protección de datos.

Es lugar común citar la conocida Ley del Land de Hesse, pionera en la materia, así como la Ley Federal alemana de 1977. También la Ley francesa de Informática, Ficheros y Libertades de 1978, sustancialmente modificada,

---

[8] Las reflexiones que siguen ya las he adelantado en «El derecho a la protección de datos de carácter personal en la jurisprudencia....», *op. cit.,* p. 47 y ss.

[9] El artículo 12 dispone: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.»

[10] En términos prácticamente iguales, el art. 17 del Pacto dispone:

«1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.»

al objeto de adaptarla a la Directiva 95/46/CEE, por la Ley núm. 2004-801, de 6 de agosto de 2004, relativa a la protección de las personas físicas en relación con el tratamiento de datos de carácter personal [11]. El 8 de mayo de 1979 el Parlamento Europeo aprueba una Resolución sobre *«La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática»*. En junio de 1978 se aprobaron en Dinamarca dos leyes, una sobre registros privados y otra sobre registros públicos. En 1978 se aprueba en Austria la Ley de Protección de Datos, que consagra el Derecho fundamental de todo ciudadano a exigir la confidencialidad del tratamiento y comunicación de los datos que le conciernan, y en marzo de 1979 se aprueba en Luxemburgo la Ley sobre utilización de datos en tratamientos informáticos.

En los años ochenta, desde el Consejo de Europa se dará un respaldo definitivo a la protección de la intimidad frente a la informática mediante el Convenio núm. 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal (1981). Este Convenio establece los principios y derechos que cualquier legislación estatal debe recoger a la hora proteger los datos de carácter personal.

El Convenio núm. 108 intenta conciliar el derecho al respeto de la vida privada de las personas con la libertad de información, facilitando la cooperación internacional en el ámbito de la protección de datos y limitando los riesgos de desviaciones en las legislaciones nacionales. En el capítulo II del Convenio se recogen los principios básicos de calidad de los datos, principio de especial protección y principio de garantía de la seguridad de los datos. Asimismo el Convenio reconoce, en su artículo 8, el derecho a conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad que controla del fichero.

En fin, también la OCDE publica dos importantes recomendaciones en esta materia: la recomendación sobre *«Circulación internacional de datos personales para la protección de la intimidad»* y la recomendación relativa a la *«Seguridad de los sistemas de información»*.

La perspectiva que en las normas, instrumentos internacionales y documentos que hasta aquí he simplemente enumerado es clara: se pretende resolver la tensión existente entre el uso cada vez más generalizado de la informática y el riesgo que el mismo puede suponer para la vida privada. Informática *versus* intimidad: éste es el gran dilema. Ésta es también la perspectiva de la Constitución de 1978 en su artículo 18.4.

En la década de los noventa se incorpora un elemento fundamental al debate. La construcción europea, que requiere ineludiblemente la constitución del mercado interior, exige que se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales, sobre todo en el marco de una economía cada vez más globalizada y transfronteriza. En este escenario se mueve la Directiva

[11] Sobre dicha ley véase Alex Türk, «La ley francesa de protección de datos de carácter personal», en www.agpd.es. El texto de la ley puede encontrarse en www.cnil.fr, así como en www.agpd.es.

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. Los tres primeros considerandos de la Directiva son de una importancia capital y centran perfectamente el sentido de la norma [12].

Al par de conceptos intimidad-informática, se añade ahora uno más: valor económico de los datos personales-respeto a los derechos y en particular al derecho a la intimidad. La construcción europea pasa por la creación del mercado interior en el respeto a los derechos fundamentales, y en este marco la libre circulación de los datos con respeto al derecho a la intimidad se considera de primera importancia. A ese fin responde la Directiva 95/46/CEE, de la que deriva la legislación de los países europeos en materia de protección de datos, y en particular la Ley Orgánica 15/1999, de 13 de diciembre [13].

En el año 2000 la situación experimenta un giro copernicano tanto en la Unión Europea como en España. Se abre una nueva etapa, en la que nos encontramos, que se basa en la consideración de la protección de datos de carácter personal como un verdadero derecho fundamental autónomo e independiente del derecho a la intimidad. Tan radical innovación deriva fundamentalmente de la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en la Cumbre de Niza de 7 de diciembre de 2000, que de forma lacónica, pero tajante, dispone en su artículo 8, dentro del capítulo relativo a las libertades, que *«Toda persona tiene Derecho a la protección de los datos de carácter personal que la conciernan.»* Ninguna referencia a la intimidad o privacidad; ninguna a la informática. Sí una previsión expresa, de suma importancia, al hecho de que «*El respeto de estas normas* [sobre protección de datos]

---

[12] *«(1) Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como quedó modificado por el Tratado de la Unión Europea, consisten en lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el progreso económico y social, eliminando las barreras que dividen Europa, fomentar la continua mejora de las condiciones de vida de sus pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales;*

(2) Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos;

(3) Considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas.»

[13] La protección de datos es tomada en consideración, además de en la citada Directiva 95/46, en otras tales como la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, también conocida como «Directiva sobre la privacidad y las comunicaciones electrónicas», que ha sustituido a la Directiva 97/66/CE, relativa al tratamiento de los datos personales y protección de la intimidad en el sector de las telecomunicaciones. Además de las normas sobre protección de datos existen otras dos directivas que complementan a las anteriores en el campo del comercio electrónico, a saber, la Directiva 2000/31/CE, de Comercio Electrónico, y la 1999/93/CE, sobre Firma Electrónica, aunque en ningún caso sustituyen a aquéllas en lo relativo a la protección de datos personales.

quedará sujeto al control de una autoridad independiente.» Además, en el artículo 7.º, de forma separada, se recoge el derecho a la vida privada y familiar. Hay, pues, una clara diferenciación entre ambos derechos, el derecho a la privacidad y el derecho a la protección de datos, que merecen, en consecuencia, dos preceptos distintos.

En España, ese cambio hacia la consideración del derecho a la protección de datos como un verdadero derecho autónomo e independiente viene de la mano de dos importantísimas sentencias del Tribunal Constitucional: las números 290 y 292 de 2000, ambas de 30 de noviembre. La primera ratifica la constitucionalidad de la existencia de la Agencia Española de Protección de Datos, con competencias en todo el territorio nacional, en cuanto garante de un derecho fundamental que debe tener un contenido homogéneo para todas las personas (físicas) [14]. La segunda consolida una evolución juris-

---

[14] En un momento en que está discutiéndose la reforma de algunos Estatutos de Autonomía, merece la pena recordar la doctrina del Tribunal Constitucional en relación con el reparto competencial entre Estado y Comunidades Autónomas en materia de protección de datos. El Tribunal, en la citada Sentencia 290/2000, centra su análisis en el estudio de las normas referidas a la existencia o inexistencia de una infracción del reparto competencial establecido en nuestra Constitución. En cuanto a este análisis, su fundamento jurídico 7 considera necesario *«que el examen de la presente disputa competencial se lleve a cabo partiendo de dos presupuestos, a saber: el contenido del derecho fundamental a la protección de datos personales y, en segundo término, los rasgos generales que caracterizan a la Agencia de Protección de Datos dado que la función general de este órgano es la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación»,* como se expresaba en el primer inciso del apartado a) del art. 36 LORTAD.

En relación con la segunda de las cuestiones apuntadas, el fundamento jurídico 8 de la Sentencia señala que *«en lo que respecta a las funciones y potestades atribuidas a la Agencia de Protección Datos, el apartado a) del art. 36 LORTAD ofrece una caracterización general de las primeras al encomendar a la Agencia la función general de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación de datos».* Y en cuanto especificación de esta función de carácter tuitivo en orden a la protección de datos personales, *«los restantes apartados del citado precepto le atribuyen tanto funciones de intervención o control respecto a ciertos sujetos y actividades como funciones registrales y consultivas».*

Se alegaba por las Comunidades Autónomas *«que las actividades relativas a los ficheros automatizados de carácter personal no son en sí mismas el objeto de una materia competencial, sino que constituyen una actividad instrumental al servicio de otras actividades encuadrables dentro de otras materias sobre las que las Comunidades Autónomas pueden ostentar títulos competenciales según el orden constitucional de reparto de competencias».* Sin embargo, el Tribunal Constitucional considera que tal argumento no resulta admisible por cuanto, con su planteamiento, *«se está desvirtuando cuál es el bien jurídico constitucionalmente relevante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales de los ciudadanos o afecta al pleno ejercicio de sus derechos, como claramente se desprende del tenor de dicho precepto constitucional».*

Por último, en su fundamento jurídico 14, la Sentencia recuerda que *«la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales».*

«A este fin —prosigue la Sentencia— *la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros.»*

prudencial constitucional que ha ido configurando el derecho a la protección de datos, desde el reconocimiento del derecho a la intimidad y privacidad, pasando por el llamado derecho a la autodeterminación informática o informativa [15]. Merece la pena recordar ahora las Sentencias constitucionales 110/1984, 254/1993, 143/1994, 94/1998, 11/1998, 144/1999 y 202/1999 [16]. En particular, la STC 254/1993 [17] señala que la Constitución de 1978 ha incorporado el «derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos». Añade que no es posible aceptar que «el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados... son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos».

Pero es la STC 292/2000, de 30 de noviembre, como decía, la que definitivamente ha reconocido que el derecho fundamental a la protección de datos personales deriva directamente de la Constitución y debe considerarse como un derecho autónomo e independiente. El Fundamento Jurídico Séptimo es sin duda esencial, por lo que creo oportuno transcribirlo:

> *«7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que*

En consecuencia, concluye la Sentencia, *«es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el presente caso justifica que la Agencia de Protección de Datos puede ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada»,* por lo que las normas discutidas son consideradas por el Tribunal como conformes a la Constitución.

[15] Recientemente ha llevado a cabo un completo análisis de la jurisprudencia del Tribunal Constitucional en la materia E. Guichot, *Datos personales y Administración Pública*, Thomson-Civitas, 2005, pp. 68 y ss.

[16] Las sentencias resuelven básicamente recursos de amparo, frente a tratamientos ilícitos, contrarios al principio de «autodeterminación informativa», que se traduce en el derecho de control sobre los datos relativos a la propia persona o, lo que es lo mismo, el derecho a controlar el uso de los mismos datos personales por parte de su titular. Así, las Sentencias 144/99 y 202/1999, dictadas frente a la utilización por RENFE de los datos de diversos trabajadores relativos a su afiliación sindical (Las Sentencias relacionadas con el uso de datos por parte de RENFE son numerosas. Véase Guichot, *Datos personales…, op. cit.,* p. 71). Resoluciones anteriores relacionan el derecho a la protección de datos de carácter personal con el derecho a la intimidad (SSTC 143/1944, 254/1993 y 110/1984), proclamando con carácter general *«el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque su defensa frente las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida».*

[17] Sobre esta Sentencia ver E. Guichot, *Datos personales y Administración Pública*, o*p. cit.,* pp. 69 y ss.; L. M. Arroyoyanes, «El derecho de autodeterminación informativa frente a las Administraciones Públicas (Comentario a la STC 254/93, de 20 de julio)», en *Revista Andaluza de Administración Pública*, 1993; Aspas Aspas, «La libertad informática, un nuevo derecho fundamental desvelado por el Tribunal Constitucional (STC 254/1993, de 20 de julio), en *Revista Aragonesa de Administración Pública*, núm. 4, 1994; González Murúa, «Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales», en *Revista Vasca de Administración Pública*, núm. 37, 1993; Lucas Murillo de la Cueva, «La construcción del derecho a la autodeterminación informativa», *Revista de Estudios Políticos*, núm. 104, 1999.

faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del Derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.»

No es necesario recalcar la importancia de la sentencia, que es sencillamente capital. Reconoce la existencia del derecho a la protección de datos como derecho autónomo e independiente del derecho a la intimidad; determina su contenido esencial; lo relaciona no sólo con el artículo 18.4 de la Constitución, sino también con el 10.2. Además, en el Fundamento Jurídico 8.º cita de forma expresa diversos instrumentos internacionales y en particular, pese a no estar todavía en vigor (apenas había sido adoptada), la Carta Europea de Derechos Fundamentales. Es, junto con la LORTAD de 1992 y la Ley Orgánica de Protección de Datos de 1999, el hito más importante en materia de protección de datos que se ha producido entre nosotros.

Se consolida así el concepto de derecho a la protección de datos, frente a la noción de derecho a la autodeterminación informativa, cuya construcción tanto debe al Tribunal Constitucional alemán a través de su conocida Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo.

El cambio radical que han supuesto las Sentencias 290 y 292/2000 tiene su correspondencia, a nivel europeo, en la tantas veces repetida Carta Europea de Derechos Fundamentales y en la Constitución Europea, cuyos preceptos esenciales sobre protección de datos transcribía al principio de este trabajo. De este modo, el ciclo de la protección de datos, en cuanto a su evolución, se cierra por el momento con su consideración como derecho fundamental autónomo.

III. EL CONTENIDO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

3.1. Principios que configuran el contenido esencial del derecho fundamental a la protección de datos

La cuestión estriba entonces en determinar cuál es el contenido esencial de tal derecho; los principios y características que lo definen y que no pueden ser desconocidos so pena de desconocer y, en consecuencia, violentar el propio derecho. En la XXVII Conferencia Internacional de Autoridades de Protección de Datos celebrada en Montreux, Suiza, los días 13 a 15 de septiembre de 2005 se aprobó una Declaración Final sobre *The protection of personal data and privacy in a globalised world: a universal right respecting diversities,* en la que se hace una referencia expresa a los principios del derecho a la protección de datos:

> «16. *Recognising that the principles of data protection derive from international legal binding and non binding instruments such as the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the United Nations Guidelines concerning Computerized Personal Data Files, the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data and the Asia Pacific Economic Cooperation Privacy Framework,*
>
> 17. *Recalling that these principles are in particular the following:*
> — *Principle of lawful and fair data collection and processing,*
> — *Principle of accuracy,*
> — *Principle of purpose-specification and -limitation,*
> — *Principle of proportionality,*
> — *Principle of transparency,*
> — *Principle of individual participation and in particular the guarantee of the right of access of the person concerned,*
> — *Principle of non-discrimination,*
> — *Principle of data security,*
> — *Principle of responsibility,*
> — *Principle of independent supervision and legal sanction,*
> — *Principle of adequate level of protection in case of transborder flows of personal data.»*

Creo, sin embargo, que tales principios pueden reconducirse a los que quizá son más nucleares en la configuración del derecho: consentimiento, información, finalidad, calidad de los datos, con especial referencia a la proporcionalidad, seguridad. Principios todos ellos recogidos en la LOPD, artículos 4 y ss., a los que puede añadirse el de utilización leal de los datos y el de minimización en el uso de los datos (éste, por cierto, reconducible, tam-

bién, en mi opinión, al de proporcionalidad). Principios que para ser efectivos requieren el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición (regulados, en nuestro caso, en los artículos 15 y ss. de la LOPD).

3.2. El principio de control independiente. En particular, la posición de la Agencia Española de Protección de Datos en el marco constitucional del derecho a la protección de datos personales

Además, la Carta Europea de Derechos Humanos, siguiendo ya la tónica de textos anteriores, da un paso capital a favor de otro de los principios que ya son inherentes a la protección de datos: el principio que podría denominarse de control independiente. En efecto, al disponer que «*El respeto de estas normas [de protección de datos] quedará sujeto al control de una autoridad independiente*» está exigiendo la existencia de tal autoridad como requisito para considerar que el derecho a la protección de datos está suficientemente garantizado. De modo que se presume que, faltando esa autoridad, no es posible en ningún caso considerar aceptable el marco jurídico regulador del derecho. Precisamente uno de los puntos esenciales de las decisiones de adecuación que hasta ahora ha aprobado la Comisión Europea en relación con la protección ofrecida por terceros países es la de la existencia de una autoridad independiente de control [18].

La previsión de la Carta Europea no es en absoluto nueva, aunque sí lo es el hecho de recogerla en documento de tanta trascendencia. La Resolución 45/95 de la Asamblea General de Naciones Unidas, de 14 de diciembre de 1990, por la que se establecen las directrices de protección de datos, dispone

---

[18] Tales decisiones son las siguientes:

Decisión de la Comisión de 26 julio 2000 con arreglo a la Directiva 95/46 relativa al nivel de protección adecuado de los datos personales en Suiza.

Decisión de la Comisión de 26 julio 2000, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicada por el Departamento de Comercio de EEUU de América.

Decisión de la Comisión de 20 diciembre 2001 sobre la adecuación de protección de los datos personales conferida por la ley canadiense *Information and Electronic Documents Act*.

Decisión de la Comisión de 30 junio 2003, sobre la adecuación de protección de los datos personales en Argentina.

Decisión de la Comisión de 21 de noviembre de 2003, relativa al carácter adecuado de protección de los datos personales en Guernsey.

Decisión de la Comisión de 28 abril de 2004 relativa al carácter adecuado de protección de los datos personales en la Isla de Man.

Decisión de la Comisión de 14 mayo 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de Aduanas y Protección de fronteras de los EEUU (*Bureau of Customs and Border Protection*). Esta Decisión ha sido recurrida por el Parlamento Europeo ante el Tribunal de Justicia (Asunto C-318/04). El abogado general Léger ha hecho ya públicas sus Conclusiones (22 de noviembre de 2005) en las que propone anular la Decisión. Más adelante me referiré a ello en el texto.

en su punto 8 que «el derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios [de protección de datos]. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica». Por su parte, el Protocolo Adicional al Convenio 108 del Consejo de Europa, relativo a las autoridades de Supervisión y a las Transferencias internacionales de datos, de 8 de noviembre de 2001, señala en su preámbulo que «*supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data*». En esta línea, el artículo 1.3 dispone que «*The supervisory authorities shall exercise their functions in complete independence»,* y el punto 4 del mismo artículo añade que «*Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts*». Y, por supuesto, la Directiva 95/46/CE, cuyo artículo 28.1 dispone claramente que «los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que le son atribuidas con total independencia».

En definitiva, pues, el principio de tutela del derecho a través de una autoridad independiente se ha constituido ya como verdadero principio del derecho a la protección de datos.

Y nuestro Tribunal Constitucional ya se ha pronunciado, con tanta claridad como contundencia, sobre la posición que en el sistema de garantías del derecho fundamental a la protección de datos ocupa la Agencia Española de Protección de Datos. Ha sido, como es de sobra conocido, en la Sentencia 290/2000, de 30 de noviembre, en relación con el recurso interpuesto por la Generalidad y el Parlamento de Cataluña contra los preceptos de la LORTAD de 1992 que regulaban la posición y competencias de la Agencia de Protección de Datos, por considerar que se infringía el sistema constitucional de reparto de competencias. Y el Tribunal es, como digo, meridianamente claro. Permítaseme transcribir íntegras las reflexiones y conclusiones del Tribunal Constitucional, pues merece la pena que sean recordadas en este momento [19]:

> *«8. En lo que respecta en segundo término a la Agencia de Protección de Datos que ha creado el Título VI de la LORTAD, ha de comenzarse señalando que en las regulaciones legales adoptadas antes de la entrada en vigor de nuestra Constitución por varios Estados europeos con la finalidad de proteger los datos personales frente a los peligros de la informática (Ley sueca de 11 de mayo de 1973, Ley de la República Federal de Alemania de 22 de enero de 1977, Ley francesa de 6 de enero de 1978, Ley noruega de 8 de junio de 1978), también está presente un elemento institucional. Pues dichas regulaciones,*

[19] Y ruego al lector que lea íntegramente y con detenimiento las consideraciones del Tribunal, pues son de una importancia capital.

pese a las diversas denominaciones y dependencias orgánicas que establecen, tienen en común el haber creado instituciones especializadas de Derecho público, a las que se atribuyen diversas funciones de control sobre los ficheros de datos personales susceptibles de tratamiento automatizado, tanto de titularidad pública como privada.

Pues bien, la LORTAD ha establecido un «régimen de protección de datos de carácter personal» respecto de los que figuren en ficheros automatizados, tanto de titularidad pública como privada, así como las modalidades de su uso posterior (art. 2).Y en dicho régimen su dimensión institucional es la referida a la Agencia de Protección de Datos y a los órganos que en ella se integran, tanto de dirección (Director y Consejo Consultivo, arts. 35 y 37 LORTAD) como operativos (Registro General de Protección de Datos e Inspección de Protección de Datos, arts. 38 de la Ley y 11 del Estatuto de la Agencia de Protección de Datos). Habiendo configurado el legislador a esta Agencia con unos rasgos específicos, pues se trata de «un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones» (art. 34.2 LORTAD).

En lo que respecta a las funciones y potestades atribuidas a la Agencia de Protección de Datos, el apartado a) del art. 36 LORTAD ofrece una caracterización general de las primeras al encomendar a la Agencia la función general de "Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación de datos".Y en cuanto especificación de esta función de carácter tuitivo en orden a la protección de datos personales, los restantes apartados del citado precepto le atribuyen tanto funciones de intervención o control respecto a ciertos sujetos y actividades como funciones registrales y consultivas. Siendo de destacar, en cuanto a las primeras, la de emitir las preceptivas autorizaciones previstas en la Ley o en las disposiciones de desarrollo de ésta (apartado b); la de ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de ficheros cuando no se ajusten a lo previsto en la LORTAD (apartado f); la de velar por la publicidad de la existencia de los ficheros, a cuyo efecto publicará periódicamente una relación periódica de los mismos (apartado j); la de ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos y las de cooperación internacional en esta materia (art. 36, apartado 1) y las relativas a la recogida y secreto de datos estadísticos, dictando instrucciones sobre las condiciones de seguridad de los ficheros [art. 36, apartado m)]. Se trata, pues, de un conjunto de funciones especializadas en cuanto a su objeto, la protección de los datos personales y, además, de funciones de carácter público, como se expresa en el art. 34.1 LORTAD al determinar que la Agencia de Protección de Datos actuará de conformidad con la Ley de Procedimiento Administrativo, sin perjuicio de que sus adquisiciones patrimoniales y contratación estén sometidas al Derecho privado.

En correspondencia con el carácter público de sus funciones, la Agencia de Protección de Datos dispone de potestades administrativas expresamente atribuidas por dicha Ley. En primer lugar, la potestad de investigación o de inspección que le reconoce el art. 39 para obtener información y, en su caso, pruebas sobre los hechos que contravengan lo dispuesto en la LORTAD. En segundo término, la potestad sancionadora, que la Agencia de Protección de Datos ha de ejercer en los términos previstos en el Título VII [art. 36, apartado g)], con la particularidad, cuando se trate de infracciones de una Administración Pública, que tal potestad queda limitada a la facultad de dictar una resolución indicando las medidas que han de adoptarse para corregir el incumplimiento de las previsiones legales en

esta materia (art. 45). En tercer lugar, una potestad de resolución de las reclamaciones de los afectados por incumplimiento de las previsiones de dicha Ley [art. 36, apartado d)] en relación con el art. 17.1, con sujeción al procedimiento establecido por el Real Decreto 1332/1994, de 20 de julio.Y, por último, una potestad normativa, ceñida en lo esencial a dictar las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la LORTAD [art. 36, apartados c) y m) in fine*], con miras a su debida aplicación en ámbitos determinados de actividad.*

9. Por último, de lo que se acaba de exponer se desprende un rasgo significativo de la Agencia de Protección de Datos: el carácter básicamente preventivo de sus funciones en orden a la protección de datos personales. Un rasgo caracterizador que es común a las instituciones especializadas existentes en los países de nuestro entorno y al que ha hecho referencia la Exposición de Motivos de la LORTAD al afirmar que esta disposición está guiada "por la idea de implantar mecanismos cautelares que prevengan las violaciones" de los derechos fundamentales.

En efecto, al dar cumplimiento al mandato contenido en el art. 18.4 CE, el legislador, sin excluir en modo alguno el recurso último a los órganos jurisdiccionales para la tutela de los derechos individuales, como se determina en los apartados 2 a 5 del art. 17 LORTAD, no ha querido, sin embargo, que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental. Por el contrario, ha querido que dicha protección se lleve a cabo mediante el ejercicio por la Agencia de Protección de Datos, con carácter básicamente preventivo, de las funciones de control de los ficheros tanto de titularidad pública como privada que la LORTAD le atribuye y, en su caso, a través de las reclamaciones de los afectados ante la Agencia de Protección de Datos (art. 17.1), las que provocarán la posterior actuación de este órgano. Por lo que cabe estimar que existe una correspondencia entre las funciones y potestades que la LORTAD ha atribuido a la Agencia de Protección de Datos y el carácter preventivo de sus actuaciones. Pues es este carácter tuitivo o preventivo el que, en última instancia, justifica la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada.

10. Pasando ya desde estos presupuestos al examen de las pretensiones de las partes y de los títulos competenciales que respectivamente han invocado ha de tenerse presente que el Consejo Ejecutivo de la Generalidad de Cataluña y el Parlamento de Cataluña no han cuestionado que el Estado posea un título competencial válido para dictar la LORTAD. Ni tampoco han impugnado la creación de la Agencia de Protección de Datos por dicha Ley estatal. Lo que los recurrentes reprochan al art. 40.1 y 2 LORTAD en relación con los restantes preceptos impugnados es el que sólo hayan atribuido a las Comunidades Autónomas un ejercicio de potestades de ejecución de dicha Ley limitado a los ficheros automatizados de datos de carácter personal creados o gestionados por dichos entes, así como la creación y mantenimiento de registros de ficheros públicos para el ejercicio de las competencias que se les reconocen sobre los mismos.

A juicio de los recurrentes, la consecuencia de esta limitación es que corresponde en exclusiva a un órgano estatal, la Agencia de Protección de Datos, la ejecución de la LORTAD y el ejercicio de las funciones interventoras y sancionadoras en ella previstas respecto

a los restantes ficheros automatizados. De manera que dicho precepto, según han alegado, priva a las Comunidades Autónomas del ejercicio por sus propios órganos de las funciones y potestades de ejecución de la LORTAD respecto de los ficheros automatizados de titularidad privada radicados en su territorio y que se hayan creado en el marco de actividades relativas a materias sobre las que las Comunidades Autónomas tengan atribuida competencia.

Esta conclusión se fundamenta según los recurrentes en que el tratamiento automatizado de datos de carácter personal no es una materia competencial específica, sino una actividad instrumental de otras actividades que sí son subsumibles en materias competenciales. De manera que habrá de estarse al reparto competencial de éstas entre el Estado y las Comunidades Autónomas de conformidad con las normas del bloque de constitucionalidad para determinar quién es el competente para ejecutar la LORTAD en lo que respecta a los mencionados ficheros informatizados de titularidad privada. Y al no ser la protección de datos una materia competencial, la consecuencia según los recurrentes es que el Estado no puede asumirla por no estar expresamente atribuida a las Comunidades Autónomas en sus Estatutos (art. 149.3 CE). Ni tampoco la competencia de ejecución de la LORTAD puede sustentarse en lo dispuesto en el art. 149.1.1 CE, pues el Estado no puede pretender erigirse en el garante último de la libertad e igualdad de los individuos ni esa garantía de las condiciones básicas puede desconocer el orden constitucional de reparto de competencias. Sin que tampoco pueda aceptarse que una norma meramente organizativa como la que crea la Agencia de Protección de Datos pueda ser considerada en modo alguno como la regulación de una "condición básica" a los fines del art. 149.1.1 CE.

En definitiva, lo expuesto justifica, a juicio de los recurrentes, que las potestades de ejecución de la LORTAD correspondan a las Comunidades Autónomas, así como la de tutela administrativa sobre aquellos ficheros privados que versen sobre materias respecto a las cuales una Comunidad Autónoma tenga atribuida, cuando menos, competencias ejecutivas. Conclusión a la que se ha opuesto el Abogado del Estado, para quien, en esencia, se trata de una materia competencial que corresponde al Estado ex art. 149.3 CE, dado que, en atención al desarrollo legislativo en esta materia, al adoptarse la Constitución ya poseía autonomía y, por tanto, pudo haberse incluido en los primeros Estatutos de Autonomía y no se hizo. Y aun si se estimase que la protección de datos es una actividad instrumental de otras materias competenciales, al mismo resultado se llega a su entender con base en el art. 149.1.1 CE, pues con la creación de la Agencia de Protección de Datos y las funciones que a este ente le atribuye la LORTAD se ha querido preservar la igualdad de los españoles en la protección de sus datos personales, creando condiciones institucionales que permitan excluir ejecuciones plurales y divergentes por las diferentes Comunidades Autónomas. A cuyo fin la LORTAD ha centralizado las funciones encaminadas a la protección de datos personales en una entidad estatal de Derecho público, la Agencia de Protección de Datos.

11. De lo anterior se desprende que, a diferencia de otros muchos conflictos de los que ha conocido este Tribunal, en el presente caso los recurrentes no fundamentan su reivindicación en un título competencial específico del Estatuto de Autonomía de Cataluña. Y la razón es que toda su argumentación está basada en el presupuesto que antes se ha expuesto, a saber: que las actividades relativas a los ficheros automatizados de carácter personal no son en sí mismas el objeto de una materia competencial, sino que constituyen una actividad instrumental al servicio de otras actividades encuadrables dentro de otras materias sobre las que las Comunidades Autónomas pueden ostentar títulos competenciales según el

orden constitucional de reparto de competencias. De suerte que una Comunidad Autónoma, al ejercer su competencia sobre estas materias podrá extenderla a la actividad instrumental relativa a los ficheros de datos personales.

De este modo, las distintas potestades de ejecución de la LORTAD, como son las de inscripción de los ficheros automatizados en el Registro General de Datos como acto habilitante de la creación de aquéllos, los de investigación y de sanción, quedan vinculadas a las competencias de ejecución que la Comunidad Autónoma ha asumido en distintas materias, según la Constitución y su Estatuto de Autonomía. De lo que se desprende, a juicio de los recurrentes, que poco importa que un fichero automatizado de datos de carácter personal radicado en Cataluña sea de titularidad pública o privada, que es el criterio que la LORTAD utiliza en su art. 40, pues lo determinante es la titularidad competencial que en cada caso le venga atribuida a la Comunidad Autónoma en atención a la materia principal de la que dicho fichero sólo es un instrumento técnico.

Ahora bien, en relación con este planteamiento cabe observar, en primer lugar, que aunque este Tribunal ha admitido el carácter instrumental de una determinada actividad respecto a una materia objeto de un título competencial en virtud de la conexión existente entre aquélla y ésta, tal actividad accesoria era llevada a cabo por poderes públicos. Como es el caso, por ejemplo, de la actividad cartográfica respecto a las competencias de ordenación del territorio y urbanismo (STC 76/1984, de 29 de junio, FJ 1). Mientras que en el presente caso la conexión se establece, sin la debida justificación, a partir de una actividad de los particulares, pues se trata de la relativa al tratamiento de datos personales por ficheros de titularidad privada. En segundo término, los ficheros automatizados de datos de carácter personal sólo son el soporte material sobre el que se lleva a cabo la actividad que la LORTAD regula, la recogida y el posterior uso de dichos datos. Por lo que es preciso justificar también la conexión lógica existente entre tal actividad y las concretas materias sobre las que se ha atribuido competencia a una Comunidad Autónoma, lo que no se ha llevado a cabo.

Por último, y más fundamentalmente, el planteamiento de los recurrentes no puede ser acogido, pues soslaya la función que nuestra Constitución ha atribuido a los derechos fundamentales y, en correspondencia, la necesidad de que sean protegidos, incluso en el ámbito del reparto competencial (art. 149.1.1 CE). La LORTAD, en efecto, ha sido dictada en cumplimiento del mandato contenido en el art. 18.4 CE de limitar el uso de la informática para garantizar ciertos derechos fundamentales y el pleno ejercicio de los derechos de los ciudadanos, de manera que si se considera la actividad aquí examinada como meramente instrumental o accesoria de otras materias competenciales, es claro que con este planteamiento se está desvirtuando cuál es el bien jurídico constitucionalmente relevante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales de los ciudadanos o afectar al pleno ejercicio de sus derechos, como claramente se desprende del tenor de dicho precepto constitucional. Lo que guarda entera correspondencia, además, con el objeto de dicha Ley, que no es otro, según se ha dicho, que el de establecer un régimen legal para "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de datos de carácter personal" que permita garantizar el respeto o el pleno ejercicio de tales derechos (art. 1). A lo que cabe agregar que la LORTAD también es la Ley que ha desarrollado un derecho fundamental específico, el derecho a la protección de los datos personales frente al uso de la informática, como antes se ha expuesto.

De lo que se desprende, en definitiva, que el objeto de la Ley cuyos preceptos se han impugnado no es el uso de la informática, sino la protección de los datos personales. De suerte que esta protección mal puede estar al servicio de otros fines que los constitucionales en relación con la salvaguardia de los derechos fundamentales, ni tampoco puede ser medio o instrumento de actividad alguna.

12. La conclusión negativa a la que se ha llegado en el fundamento jurídico precedente no excluye en modo alguno que, como segundo paso de nuestro enjuiciamiento, examinemos el título competencial que pueda habilitar al Estado para atribuir a la Agencia de Protección de Datos, en orden a la adecuada protección de datos personales, potestades de información, inspección y sanción en relación con los ficheros de titularidad privada radicados en el territorio de la Comunidad Autónoma de Cataluña, tal y como se desprende del art. 40 LORTAD y de los demás preceptos que se impugnan. A este Tribunal corresponde, en efecto, la salvaguardia de las normas del bloque de constitucionalidad atributivas de competencias y, por tanto, declarar si se ha producido o no la invasión competencial que los recurrentes denuncian (SSTC 167/1993, de 27 de mayo, 329/1993, de 12 de noviembre, 196/1997, de 13 de noviembre, entre otras).

13. Pues bien, si antes se han puesto de relieve los presupuestos que han de ser tenidos en cuenta para nuestro enjuiciamiento del presente caso, ha de agregarse ahora que el segundo, la creación por la LORTAD de la Agencia de Protección de Datos para velar por el cumplimiento de dicha ley y controlar su aplicación, se halla estrechamente relacionado no sólo con el mandato del art. 18.4 CE, sino con el primero de dichos presupuestos, el derecho fundamental a la protección de datos personales frente al uso de la informática. Una relación que resulta evidente si se advierte que la creación de dicho ente de Derecho público y las funciones atribuidas al mismo permiten garantizar, como se dijo en la STC 254/1993, el ejercicio por los ciudadanos del haz de facultades que integra el contenido del derecho fundamental.

En efecto, la LORTAD es la ley dictada en cumplimiento del mandato del art. 18.4 CE de limitar el uso de la informática. Como así se aprecia en su Título II sobre los principios de la protección de datos y en la parte de su Título IV relativa a la creación, modificación o supresión de ficheros. Pero es también, por el contenido en particular de su Título III, relativo a los derechos de las personas, la ley que ha desarrollado el derecho fundamental a la protección de datos personales. Y si nos situamos ante el Título VI, que ha creado la Agencia de Protección de Datos y el Registro General de Protección de Datos integrado en aquélla, es suficiente reparar en las funciones que se les han encomendado para poder apreciar que mediante este marco institucional no sólo se ha querido velar por la puntual observancia de los límites al uso de la informática que la LORTAD establece para los responsables de los ficheros de datos personales, sino también garantizar el ejercicio por los ciudadanos del derecho fundamental a la protección de dichos datos mediante la actuación preventiva por parte de los citados órganos.

14. Si se proyectan estas consideraciones sobre el conflicto competencial subyacente al presente proceso cabe estimar, en primer lugar, que cuando la LORTAD establece límites al uso de la informática en cumplimiento del mandato del art. 18.4 CE, tales límites han de ser los mismos en todo el territorio nacional ex art. 81 CE. Pues si los derechos fundamentales y las libertades públicas que nuestra Constitución reconoce son "fundamento del orden político" (art. 10.1 CE) y, por tanto, constituyen el estatuto jurídico básico de los ciudadanos, sólo mediante esa proyección general es posible garantizar la protección de los

derechos a que se refiere el art. 18.4 CE, con independencia de que tales límites a la informática también contribuyen a la salvaguardia del específico derecho fundamental a la protección de datos personales.

De igual modo, es significativo que el constituyente haya querido introducir mediante la cláusula del art. 149.1.1 CE la garantía de los derechos fundamentales en el pórtico del reparto competencial y, a este fin, que haya apoderado al Estado para asegurar su respeto en todo el territorio nacional mediante el establecimiento de aquellas "condiciones básicas" que hagan posible que el disfrute de tales derechos sea igual para todos los españoles. Imponiendo así un límite a las potestades de las Comunidades Autónomas en aquellas materias donde éstas ostenten un título competencial.Y si bien el alcance del art. 149.1.1 CE es "esencialmente normativo", como hemos dicho en la reciente STC 208/1999, de 15 de noviembre, FJ 6, por referirse a "la regulación" de esas condiciones básicas, cabe observar, sin embargo, que ninguna calificación adicional se ha agregado por el constituyente respecto a la naturaleza de tales condiciones que pueda restringir su alcance.

De lo que se desprende, en definitiva, que junto a la normación como aspecto esencial del art. 149.1.1 CE las regulaciones estatales dictadas al amparo de este precepto también pueden contener, cuando sea imprescindible para garantizar la eficacia del derecho fundamental o la igualdad de todos los españoles en su disfrute, una dimensión institucional. Como hemos reconocido tempranamente en la STC 154/1988, de 21 de julio, FJ 3, respecto a la regulación del censo electoral y las funciones de la Oficina del Censo Electoral, al declarar que mediante esta regulación el Estado había pretendido ejercer la competencia que en esta materia "se deriva del art. 149.1.1 de la Constitución, en relación con el art. 23 de la misma". A lo que cabe agregar que no es infrecuente que la Ley Orgánica que lo ha llevado a cabo haya establecido un órgano al que encomienda la ejecución de sus preceptos, como es el caso, por ejemplo, respecto al derecho fundamental del art. 30.2 CE, de la creación por la Ley 48/1984, de 26 de diciembre, Reguladora de la Objeción de Conciencia y de la Prestación Social Sustitutoria, de un Consejo Nacional de Objeción de Conciencia al que corresponde, entre otras funciones, resolver sobre las solicitudes de declaración de dicha objeción (STC 160/1987, de 27 de octubre, FJ 5).

De lo anterior se desprende, pues, que la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas ex art. 149.1.1 CE para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales.

A este fin la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados.Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros.

15. En definitiva, es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el pre-

sente caso justifica que la Agencia de Protección de Datos y el Registro Central de Protección de Datos puede ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada radicados en Cataluña. Y, por ello han de decaer los reproches de inconstitucionalidad que los recurrentes han imputado al art. 40.1 y 2 LORTAD y, por consecuencia, los que se extendieron a los arts. 24 y 31 de dicha Ley.»

IV. RETOS O TENSIONES A QUE ESTA SOMETIDO EL DERECHO A LA PROTECCIÓN DE DATOS

El derecho así configurado, que supone, por tanto, el reconocimiento a las personas de un verdadero y efectivo poder de disposición sobre sus datos personales, está, sin embargo, siendo sometido a diversos retos o tensiones que conviene tener muy en cuenta. Creo que tales tensiones [20] pueden reconducirse a las siguientes: protección de datos *versus* a) libertad de expresión; b) transparencia y acceso a la información; c) intereses y evolución del mercado; y d) lucha contra el terrorismo y garantía de la seguridad pública.

Ante todo debe afirmarse de inmediato y sin género de dudas que en absoluto existe una contradicción entre tales derechos o situaciones y la protección de datos. Así lo ha señalado, en relación con la transparencia y acceso a la información, por ejemplo, el Tribunal de Justicia de la Unión Europea en su conocida Sentencia de 20 de mayo de 2003, *Rundfunk y otros*, Asuntos C-465/00, C-138/01 y C-139/01; y en lo que respecta a la libertad de expresión en su no menos conocida Sentencia de 6 de noviembre de 2003, *Linqvist*, Asunto C-101/01 [21]. Más bien al contrario: sólo respetando el derecho fundamental de todos a la protección de sus datos personales se conseguirá un marco adecuado de respeto a la libertad de expresión y al derecho de acceso a la información, un correcto desarrollo del mercado y una eficaz lucha contra el terrorismo.

Pero sin duda la situación más aparentemente conflictiva es la que deriva de la relación que se da entre protección de datos y seguridad. Sobre todo tras los brutales atentados de Nueva York, Madrid y Londres.

Desde luego nadie puede cuestionar el hecho irrefutable de que es imprescindible adoptar medidas eficaces en la lucha contra el terrorismo. Pero del mismo modo es imprescindible afirmar y reafirmar que tales medidas deben ser respetuosas con los derechos fundamentales, pues de lo contrario se estaría produciendo ya la primera y capital victoria de los terroristas: restringir el marco de libertades y derechos que, afortunadamente, caracterizan a las sociedades occidentales. Y uno de esos derechos es el de protección de datos de carácter personal. Cualquier medida que se adopte para acabar con el terrorismo y

---

[20] Que he tenido ocasión de exponer en la XXVII Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Montreux los pasados días 13 a 15 de septiembre de 2005.

[21] Sobre estas Sentencias puede verse mi estudio antes citado «El derecho a la protección de datos de carácter personal en la jurisprudencia....», *op. cit.,* pp. 16 y ss.

las formas graves de delincuencia organizada debe respetar el contenido esencial del derecho, integrado por los principios a los que antes me refería.

Y es en este escenario donde se sitúa la necesidad de contar con un modelo global de protección de datos, que permita tener claras las reglas del juego a nivel internacional. Modelo en el que sin duda desempeña un papel protagonista la Directiva 95/46/CE, de protección de datos.

V. ¿HACIA UN MODELO GLOBAL DE PROTECCIÓN DE DATOS? EN ESPECIAL, LA POSICIÓN DE LA DIRECTIVA 95/46/CE

Ésta es, por lo demás, una tendencia cada vez más generalizada. El derecho fundamental a la protección de datos está hoy experimentando una expansión internacional extraordinaria. Puede perfectamente decirse que en el marco de la globalización va alcanzando un protagonismo hasta ahora desconocido. Además, con una fuerte presencia del modelo europeo, no sólo a través de la influencia que ejerce la Directiva 95/46/CEE y los documentos elaborados por el llamado Grupo del Artículo 29 [22], sino por la puesta en marcha de iniciativas como la Red Iberoamericana de Protección de Datos, integrada ya por representantes de la gran mayoría de los países de la Comunidad Iberoamericana. De hecho, en la declaración final de la ya referida Conferencia Internacional de Montreux se ha incluido una mención expresa a las iniciativas transnacionales [23], al señalar que los responsables de protección de datos instan a los «*Heads of States and Governments that will join in Tunis for the World Summit on the Information Society (16-18 November 2005) to include in their final declaration a commitment to develop or reinforce a legal framework that ensures the rights to privacy and data protection to all citizens within the Information Society in me of the commitment taken in the Summit of Santa Cruz (Bolivia) by the lberoamerican Heads of Government and States (November 2003) and in the summit of Ougadougou by the Heads of Government and States of Countries which share French language (November 2004)*». La declaración de Santa Cruz de la Sierra, en su artículo 45 incluye, en efecto, una referencia expresa al derecho fundamental a la protección de datos, a la Red Iberoamericana de Protección de Datos y a las iniciativas normativas que en materia de protección de datos están desarrollándose ya en numerosos países de Iberoamérica [24].

Cierto que todavía subsisten notables diferencias entre el modelo estadounidense y el europeo [25], basadas fundamentalmente en el hecho de que

---

[22] Grupo de Autoridades Europeas de Protección de Datos, previsto en el artículo 29 de la Directiva.

[23] Texto debido, por cierto, a la iniciativa conjunta de las delegaciones española y francesa.

[24] «Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad.»

[25] Sobre ello puede verse Carter Manny, «La intimidad de la Unión Europea y la seguridad de los Estados Unidos: la tensión entre la ley europea de protección de datos y los esfuerzos por parte de Esta-

en el primero la protección de datos no se considera un verdadero derecho fundamental, pero, en mi opinión, la expansión del modelo europeo es hoy incuestionable.

En ese panorama internacional, la Directiva 95/46/CE desempeña un papel esencial.Y es necesario resaltar, a los diez años de su aprobación, que los principios que en ella se recogen han pasado a ser ya principios de general aplicación y reconocimiento en el ámbito de la protección de datos. En este sentido, se ha planteado la cuestión de la aplicabilidad de la Directiva a los asuntos relacionados con el III Pilar. Se afirma, con razón, que la Directiva corresponde al I Pilar, y que, en consecuencia, no es aplicable a los asuntos de Justicia e Interior. Nada puede objetarse ante ello, pero de inmediato ha de añadirse una reflexión que creo de enorme importancia. La Directiva se aprueba, en efecto, en 1995 y en el seno de lo que es la construcción sin barreras del mercado interior. No está de más recordar de nuevo que su objetivo es facilitar la libre circulación de los datos personales con pleno respeto a los derechos fundamentales y en particular el de protección de datos. Nace, pues, en el marco del mercado interior y con el objetivo de eliminar «las barreras que dividen Europa» [26]. Pero la vocación de la Directiva va ahora mucho más allá del mercado interior. La que podría llamarse su posición institucional en el ordenamiento comunitario, sobre todo tras la aprobación de la Carta Europea de Derechos Humanos, trasciende a la consecución del Mercado Interior. La Directiva es la norma comunitaria que define el contenido y los principios de la protección de datos, y lo hace, en mi opinión, extendiendo sus efectos a toda la actividad de la Unión. De modo que no sería posible alterar, excepcionar o modificar el contenido o la aplicación de los principios de protección de datos contenidos en la Directiva a través de normas sectoriales contrarias a lo en ella dispuesto. Una directiva o un reglamento sectoriales no podrían alterar para casos o supuestos concretos los principios del derecho a la protección de datos tal como están regulados en la Directiva, ni siquiera siendo posteriores a ésta. No sería posible, por ejemplo, que se estableciese que en ciertos casos no es de aplicación el principio de proporcionalidad previsto en la Directiva, pues si fuese posible podría darse el caso de que al final, a través de las excepciones, podría dejarse la Directiva sin contenido.

Que la Directiva no se ha de circunscribir exclusivamente al III Pilar es algo, por lo demás, que la propia realidad desmiente, o al menos va desmintiendo poco a poco. Así, en la Declaración de la Conferencia de Primavera de Autoridades de Protección de Datos celebrada en Cracovia los días 25 y 26 de abril de 2005, sobre la necesidad de un adecuado marco de protección de datos en el III Pilar, se señala lo siguiente:

> *«The Conference also welcomes the approach of the Commission in advocating a core set of guiding principles for the treatment of personal data under the Third Pillar, to be deve-*

---

dos Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros delitos», en *Cuadernos de Derecho Público*, núm. 19-20, monográfico sobre *Protección de Datos,* pp. 145 y ss.

[26] Considerando Primero de la Directiva.

loped in close co-operation with data protection authorities. Furthermore, the Conference is encouraged by the steps taken by the Commission towards developing a new legal framework for data protection in the Third Pillar which, it is hoped, will provide an appropriate set of rules applicable to law enforcement activities consistent with the current level of data protection in the First Pillar. When developing these detailed data protection rules, the standard of data protection in Directive 95/46/EC should serve as a basis.

The need to develop a harmonised data protection approach in the Union would suggest that when the Treaty establishing a Constitution for Europe enters into force there should be a comprehensive European Law on data protection covering all areas of processing personal data.

The new legal instrument would present the most important evolution in data protection law since the adoption of the Data Protection Directive 95/46/EC and it would have large impact on the future architecture of data protection in Europe. In order to avoid a divergence between the First and the Third Pillars which would have a negative impact on enforcement and transparency and in view of the Charter of Fundamental Rights and the forthcoming Constitution for Europe which will abolish the Pillars, the Conference calls to preserve —and where necessary to regain— the coherence, the consistency and the unity of data protection. The principles of Directive 95/46 should form the common core of a comprehensive European data protection law. In particular, as regards its legal provisions, the principle of lawfulness, the data subject's rights, and the principle of enforcement must be emphasised, and as regards its institutional provisions, stress must be put on the need for a EU Working Party composed of representatives of the national and the EU Data Protection supervisory authorities acting independently, entrusted with co-operation, monitoring and advisory missions.»

Queda patente esa posición institucional de la Directiva. Que igualmente se aprecia al comprobar que el Reglamento (CE) 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre del 2000, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales por las Instituciones y los organismos comunitarios y la libre circulación de estos datos, contiene constantes referencias a la Directiva y a los principios en ella desarrollados.

Pero es que la repetida posición queda aún más reforzada si tenemos en cuenta que en numerosos países europeos, y desde luego en España con la LOPD, los principios de la Directiva se aplican a lo que en términos de la Unión Europea sería no sólo I Pilar, sino también III Pilar. Es decir, a nivel de la normativa nacional se ha extendido ya la aplicación de la Directiva a asuntos relacionados con justicia e interior.

La anterior conclusión no queda debilitada tras las conclusiones del abogado general Philippe Léger en los asuntos acumulados C-317/04 y C-318/04, *Parlamento Europeo contra Consejo de la Unión Europea* y *Parlamento Europeo contra Comisión de las Comunidades Europeas,* de 22 de noviembre de 2005, referidas al ya conocido como asunto PNR (*Passenger Name Records*). Como es sabido, a raíz de los atentados del 11 de septiembre de 2001 Estados Unidos aprobó una norma en virtud de la cual las compañías aéreas que operasen vuelos con origen, escala o destino en su territorio debían facilitar a las autoridades americanas acceso a los datos del PNR referidos al sistema

de reserva y control de salidas. Tras largas y arduas negociaciones con la Unión Europea, finalmente la Comisión aprobó la Decisión 2004/535/CE, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de datos de pasajeros transferidos al Servicio de Aduanas y Protección de Fronteras de los Estados Unidos (CBP), y el Consejo adoptó la Decisión 2004/496/CE, de 17 de mayo de 2004, relativa a la celebración de un acuerdo entre la Comunidad Europea y los Estados Unidos sobre el tratamiento y la transferencia de los datos de los pasajeros por las compañías aéreas a las autoridades de Estados Unidos. Una y otra han sido recurridas por el Parlamento ante el Tribunal de Justicia, al que solicita su anulación. Y en sus conclusiones el abogado general propone la anulación de ambas medidas por ser contrarias al Derecho comunitario. La primera, la Decisión de Adecuación, por basarse en la Directiva 95/46, siendo así que la Decisión versa sobre materias relativas a la seguridad pública y a materia penal, que quedan fuera del ámbito de aplicación de la Directiva. La segunda, la Decisión del Consejo, por basarse en el artículo 95 del Tratado CE, que, sin embargo, sólo permite la adopción de medidas relativas a aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tengan por objeto el funcionamiento del mercado interior.

Cabría pensar que el abogado general restringe notablemente la posibilidad de aplicación extensiva de la Directiva, pero lo cierto es que sus consideraciones sobre el contenido del derecho a la protección de datos parten de lo dispuesto en el artículo 8 del Convenio Europeo de Derechos del Hombre, en el artículo 8 de la Carta Europea de Derechos y en la propia Directiva 95/46/CE. En cualquier caso habremos de esperar a la Sentencia que en su momento dicte el Tribunal de Justicia.

VI. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y SU NECESARIO DESARROLLO REGLAMENTARIO

En este punto es necesario resaltar la posición que a su vez caracteriza a la Ley Orgánica 15/1999, de protección de datos de carácter personal. Esta Ley, que en principio toma como referencia el artículo 18.4 de la Constitución y que transpone la Directiva 95/46, es la norma llamada a regular los principios, la garantía de ejercicio y la tutela del derecho fundamental a la protección de datos. Como es de sobra conocido, sustituye a la Ley orgánica 5/1992, LORTAD, que fue previa, incluso, a la Directiva. Y a decir verdad, ha sido usual considerarla como una norma compleja y de no siempre fácil aplicación. Ello se debe en gran medida a la propia complejidad de la materia: en más de una ocasión he señalado que la protección de datos no es ni tan cara ni tan compleja como por muchos se pretende, pero esto no puede hacernos olvidar que en efecto estamos ante un sector que, también por lo novedoso, es complicado. Por ello, se impone hacer un esfuerzo de simplificación, de aclaración desde la razonabilidad, pero con estricto respeto al derecho fundamental a la protección de datos. Más todavía si tenemos en cuenta que hoy está absolutamente reconocido que tanto la legislación española

como el funcionamiento de nuestro sistema, con especial referencia a la Agencia Española de Protección de Datos, es muy tenida en cuenta tanto en Europa como en Iberoamérica. Por ello es particularmente importante conseguir un marco jurídico que facilite la labor de responsables y encargados de los tratamientos y garantice con rigor los derechos de los titulares de los datos personales. Reto éste de innegable alcance para una mejor consolidación del derecho a la protección de datos.

En esta línea se mueve, por ejemplo, la reforma del artículo 37 de la LOPD, al que se ha añadido un apartado, de extraordinaria importancia para reforzar la transparencia en la actuación de la AEPD, que prevé la publicación de sus resoluciones [27].

Pero asimismo es imprescindible aprobar de una vez el reglamento de desarrollo de la LOPD, tal como establece su disposición final primera. Varios son los motivos que hacen que su aprobación no pueda demorarse más. Por un lado, el hecho de que, salvo diversas instrucciones aprobadas por la propia Agencia Española de Protección de Datos [28], las normas reglamentarias hasta ahora aprobadas lo han sido en desarrollo de la LORTAD [29] y permanecen en vigor parcialmente, en cuanto no se opongan a la Ley Orgánica 15/1999, según dispone su disposición transitoria tercera. Por otro, la necesidad de aclarar, con estricto respeto al contenido de la propia LOPD, diversos preceptos que podrían plantear, según la opinión de algunos, ciertos problemas interpretativos en relación con la Directiva 95/46.

Por ello se ha puesto en marcha ya la mecánica necesaria para poder contar con un reglamento de desarrollo de la LOPD en los próximos meses.

La iniciativa de impulsar un Reglamento de la Ley Española ha sido asumida por el Ministerio de Justicia que la ha incorporado dentro de su programa normativo para el año 2005. Para ello se ha constituido una Comisión conjunta entre el Ministerio y la AEPD que está finalizando un borrador de norma.

Tal como ya he tenido ocasión de exponer en otra ocasión [30], podría considerarse que algunos de los aspectos más destacados del borrador serían los siguientes:

La exigencia de obligaciones precisas de información a los afectados cuando se recaban o tratan sus datos personales, impulsando que el consentimiento que presten, cuando sea exigible, sea un consentimiento plenamente informado. Estas exigencias resultan especialmente importantes ante los tratamientos de datos que posibilita el desarrollo tecnológico y de la sociedad de la información.

---

[27] Reforma llevada a cabo por el artículo 82 de la Ley 62/2003, de 30 de diciembre.

[28] Instrucción 1/2000, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos, e Instrucción 1/2004, de 22 de diciembre, sobre publicación de las resoluciones de la Agencia.

[29] Reales Decretos 428/1993, 1332/1994 y 994/1999.

[30] Principalmente en el Curso de Verano que sobre el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos organizó la AEPD en la Universidad Internacional Menéndez Pelayo entre los días 27 de junio a 1 de julio de 2005.

En la misma línea de reforzar las garantías en el tratamiento de los datos la nueva norma pretende delimitar los fines determinados y explícitos para los que pueden ser objeto de tratamiento.

Una de las omisiones relevantes de la Directiva y de las normas nacionales de protección de datos es la ausencia de un concepto de datos de salud. El Reglamento supliría esta omisión con un concepto expansivo que parte de la Memoria Explicativa del Convenio 108 del Consejo de Europa, de la Recomendación núm. R(97) de su Comité de Ministros y de la STJCE de 6 de noviembre de 2004, *Lindquist*, asunto C-101/01.

Uno de los temas más debatidos en relación con la LOPD ha sido el del acceso a los datos por cuenta de terceros, regulado en el artículo 12. La intervención cada vez más frecuente e intensa en el tratamiento de los datos por parte de empresas que prestan servicios al responsable hace necesario desarrollar un régimen jurídico integral de sus relaciones contractuales que garantice un correcto acceso y tratamiento de la información personal por parte de terceros. Las relaciones entre responsable y encargado del tratamiento son, pues, objeto de atención en el borrador que en estos momentos se está preparando. Así como las que se den, en su caso, entre el encargado y un tercero subcontratista de sus servicios.

También ha sido necesario fijar las medidas de seguridad, técnicas y organizativas, que deben implantarse, revisando las que ya se exigen para tratamientos automatizados y articular las que sean apropiadas para los tratamientos manuales. Este extremo es especialmente importante, pues durante demasiado tiempo se ha considerado que el Reglamento de medidas de seguridad aprobado por Real Decreto 994/1999 no era aplicable a los tratamientos no automatizados. Pese a que la AEPD ya ha señalado en diversas ocasiones que tal Decreto también se extiende a los tratamientos manuales en lo que les sea de aplicación, conviene prever de forma expresa y clara qué medidas deben aplicarse en relación con los mismos. Algo que se pretende hacer en el nuevo Reglamento.

Por otra parte, las exigencias de seguridad son especialmente importantes en algunos tratamientos de datos como son los biométricos o los de tráfico y localización en las comunicaciones electrónicas.

Como es sabido, la Directiva 95/46 permite, en su artículo 18.2, que los Estados miembros dispongan la simplificación o incluso la omisión de la notificación a las autoridades de control de los tratamientos en ciertos casos tasados y con determinadas condiciones. También es sabido que la LOPD exige la inscripción de los ficheros de titularidad pública y de titularidad privada. En línea con los trabajos del Grupo del Artículo 29 se han revisado las obligaciones de notificación de los ficheros simplificándolas para facilitar el cumplimiento de esta obligación.

Por otra parte, se incorpora una nueva regulación de las transferencias internacionales que aclaran algunas dudas planteadas sobre el carácter vinculante de las Decisiones de Adecuación de la Comisión Europea y se apuntan soluciones para la admisión de nuevas fórmulas como son las llamadas *Binding Corporate Rules*.

Más son las novedades que se pretende incluir en la norma reglamentaria que está elaborándose. No es posible, ni seguramente oportuno, hacer ahora referencia a todas ellas. Deberá ser el Gobierno el que en su momento, tras la tramitación formal de elaboración del Reglamento, lo apruebe.

VII. UNA MIRADA AL FUTURO

Los retos de futuro de la protección de datos son interminables. La aprobación del reglamento será un paso decisivo en la consolidación de la cultura de la protección de datos en España. No podemos dejar de mirar al frente con la esperanza puesta en el uso de las nuevas tecnologías y en la implantación efectiva de las sociedad de la información, superando cualquier tipo de brecha digital, pero con respeto absoluto a los derechos fundamentales, y entre ellos el derecho a la protección de datos de carácter personal.

Hoy se considera que se envían y reciben diariamente en todo el mundo decenas de miles de millones de correos electrónicos no deseados. Más del 80 por ciento de los correos son ilegales; la invasión de la intimidad o los daños que derivan de los virus, además del trastorno y pérdida de tiempo que se ocasiona a los usuarios, son ya graves. Mediante los llamados identificadores de radiofrecuencia (RFID) es posible localizar no sólo productos, sino personas, sin que éstas sean conscientes de ello. El mal uso de datos genéticos puede condicionar, cuando no bloquear, la suscripción de una póliza de seguros o una contratación laboral. Nunca antes había sido posible saber tanto de tanta gente.

En este escenario la protección de datos adquiere un protagonismo capital. Nada se exagera si se afirma que estamos ante uno de los más importantes retos de las sociedades contemporáneas. El derecho fundamental a la protección de los datos personales es parte no sólo de la privacidad e intimidad de las personas, sino de su propia dignidad. Stefano Rodota, hasta hace unos meses presidente del *Garante* italiano de la *Privacy*, en la presentación de su *Relazione 2004* el pasado 9 de febrero de 2005, en el Senado Italiano, con la presencia del presidente de la República, Carlo Azeglio Ciampi, y a la que tuve el honor de asistir invitado por aquél, señaló que la protección de datos es un elemento fundamental de la sociedad de la igualdad, una condición esencial de la sociedad de la participación, un instrumento necesario para salvaguardar la sociedad de la libertad y un componente imprescindible de la sociedad de la dignidad.

William Faulkner, en su delicioso ensayo *On Privacy*, publicado en 1955 [31], denunció cómo el sueño americano (un nuevo mundo en el que todos tendrán derecho a la dignidad y a la libertad) se viene abajo cuando la privacidad es despreciada. No es exagerado decir que una sociedad democrática que pretenda ser avanzada no es posible sin el respeto al derecho fun-

[31] Y reeditado ahora por el Garante italiano de la Privacy, Roma, 2004.

damental a la protección de datos de carácter personal. Porque todos tenemos el derecho de disponer de nuestros propios datos personales, evitando ingerencias indeseadas.

Esta reflexión cobra más importancia si cabe en momentos en que salvajes e indiscriminados atentados terroristas golpean a las sociedades democráticas. Y en este escenario es imprescindible una vez más recordar que la victoria final de los terroristas sería acabar con la democracia, por lo que resulta imprescindible reiterar que cualquier medida que se adopte en la lucha contra el terrorismo —que todos debemos apoyar— ha de ser respetuosa con los derechos fundamentales. Ésta es precisamente la posición que las autoridades de control de protección de datos han asumido en relación con las medidas que en el seno de las instituciones europeas se están adoptando para regular la retención de datos de tráfico en el ámbito de las telecomunicaciones. La propuesta de Directiva hecha pública el 21 de septiembre de 2005, por la Comisión Europea acerca de la retención de datos de tráfico, pretende alcanzar este objetivo [32]. El Grupo de Autoridades de Protección de Datos establecido en base al artículo 29 de la Directiva 95/46/CE ha expresado ya su criterio, a través de la Opinión 113/2005, de 21 de octubre de 2005, en la que se ha mostrado muy crítico con su contenido. Parte de la base de que la retención de datos interfiere con el inviolable y fundamental derecho a la confidencialidad de las comunicaciones y que cualquier restricción a tal derecho sólo es admisible de forma excepcional y con la adopción de adecuadas medidas de seguridad. Considera que deben delimitarse las finalidades para las que se prevé la retención de tales datos, evitarse cualquier tipo de acceso ilimitado a los mismos, adoptar medidas de seguridad en el tratamiento de los datos, fijar con claridad el plazo máximo de retención (que no debería superar los doce meses; seis en caso de datos de tráfico de Internet), y un largo etcétera de observaciones. También ha sido muy crítico el Parlamento Europeo, que a través del Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior de 28 de noviembre de 2005 [33] ha resaltado los problemas que en el ámbito de la protección de datos plantea la propuesta.

En definitiva, tanto en lo que se refiere al tratamiento de los datos de pasajeros por parte de las autoridades de Estados Unidos, como a la retención de datos de tráfico, la idea capital es (no puede ser otra) la de respeto absoluto a los principios configuradores del contenido esencial del derecho fundamental a la protección de datos. Ése es sin duda el verdadero reto de presente y futuro: que este derecho, íntimamente ligado a la dignidad de la persona (y no sólo a su intimidad), sea incorporado de una vez por todas, de forma plena, a la cultura política y ciudadana. Que se normalice la cultura de la protección de datos para garantizar una sociedad más libre, democrática y segura.

---

[32] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE.

[33] http://www.europarl.eu.int/omk/sipade3?PUBREF=-//EP//TEXT+TA+P6-TA-2005-0512+0+DOC+XML+V0//ES&L=ES&LEVEL=1&NAV=S&LSTDOC=Y&LSTDOC=N