

DERECHO A LA PROTECCIÓN DE DATOS Y ACTIVIDAD ADMINISTRATIVA (1)

Emilio Guichot

SUMARIO: Introducción. I. La normativa europea sobre protección de datos y su valor en España. II. Perfiles constitucionales del derecho a la protección de datos. 1. El artículo 18.4 de la Constitución y su desarrollo legal. 2. La doctrina del Tribunal Constitucional y la necesidad de su perfeccionamiento. 3. Las relaciones entre el derecho a la protección de datos y el derecho a la intimidad. III. El régimen jurídico de los ficheros públicos. 1. La normativa sobre protección de datos y su deficiente técnica legislativa. 2. La naturaleza pública o privada de los ficheros y sus repercusiones en cuanto al régimen legal aplicable. 3. Los distintos tipos de datos personales y sus diferentes niveles de protección. 4. El contenido del derecho a la protección de datos: principios del tratamiento, derechos del afectado y garantías institucionales y organizativas. 4.1. Los principios del tratamiento y su aplicación a los ficheros públicos. 4.1.1. El principio de calidad. 4.1.2. El principio de finalidad. 4.1.3. El principio de consentimiento. 4.2. Los derechos del afectado y su aplicación a los ficheros públicos. 4.3. Garantías institucionales y organizativas. Conclusión.

Introducción

Las Administraciones públicas son las mayores detentadoras del bien que define la sociedad de comienzos de milenio, la información, una parte muy importante de la cual está relacionada con personas determinadas (datos de filiación y estado civil, sanitarios, académicos, patrimoniales...). La acumulación de datos personales por parte de sujetos públicos ha ido aumentando de forma geométrica, y se extiende a todas las modalidades de la actividad administrativa, potenciada por las posibilidades informáticas y por la creación de redes europeas o internacionales para hacer frente a nuevos retos de cooperación interadministrativa, como el terrorismo o la inmigración.

(1) Este trabajo se enmarca en el Proyecto de investigación *Derecho de las tecnologías de la información y las comunicaciones*, SEC 2001-3696, dirigido por Javier Barnés Vázquez, y financiado por el Ministerio de Ciencia y Tecnología.

El derecho a la protección de datos se enfrenta a una curiosa paradoja. Nacido como barrera a la acumulación de datos personales de los ciudadanos por los poderes públicos, bien puede decirse que en la actualidad, los mayores riesgos para su efectividad provienen de los tratamientos privados (piénsese, p. ej., en los ficheros de solvencia). Ello explica que la normativa que lo desarrolla parezca ideada, principalmente, para regular este segundo tipo de tratamientos, que dista enormemente en sus presupuestos de los efectuados por Administraciones Públicas que están al servicio del ciudadano, y, respecto de las cuales, un flujo informativo de información personal es presupuesto para la eficaz persecución de los intereses generales. Por ello, los principios y facultades que integran el contenido del derecho a la protección de datos cuentan necesariamente con un alto número de excepciones y matizaciones que hacen poco significativo hablar, a la postre, de un único «derecho»; en realidad, si se nos permite la expresión, habría más bien que hablar de «los derechos a la protección de datos», en función del carácter público o no de los fines perseguidos por los tratamientos, de modo que elementos claves como el consentimiento, la cancelación o el propio régimen sancionador tendrán un juego muy reducido en el caso de los ficheros públicos.

El objeto de este estudio se encuentra aún en una primera fase de definición, tanto en el plano legislativo, como el jurisprudencial y el doctrinal (2). Precisa de un análisis específico respecto del tratamiento adminis-

(2) No obstante lo cual, la bibliografía, con ilustres precursores como los profesores A.E. Pérez Luno o P. Lucas Murillo de la Cueva, comienza a ser destacable. Por citar algunos de los más destacados, APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 2.ª ed., Aranzadi, Cizur Menor, 2002; CASTELLS ARTECHE, J.M., «Derecho a la privacidad y procesos informáticos: análisis de la Ley orgánica 5/1992», de 29 de octubre (LORTAD), *Revista Vasca de Administración Pública*, n.º 39, 1994; «La limitación informática», en *Estudios sobre la Constitución española, Libro homenaje al profesor Eduardo García de Enterría*, Ed. Civitas, Madrid, 1991, tomo II; FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas*, Civitas, Madrid, 2003; FREIXAS GUTIÉRREZ, G., *La protección de los datos de carácter personal en el Derecho español*, Bosch, Barcelona, 2001; GAY FUENTES, C., *Intimidad y tratamiento de datos en las Administraciones Públicas*, Complutense, Madrid, 1995; GRIMALT SERVERA, P., *La responsabilidad civil en el tratamiento automatizado de los datos*, Comares, Granada, 1999; HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*, Tecnos, Madrid, 1996; *La Directiva comunitaria de protección de los datos de carácter personal*, Aranzadi, Pamplona, 1997; *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos personales*, Dykinson, Madrid, 2002; HURTADO GONZÁLEZ, J.F., *El deber de colaboración con la Administración tributaria facilitando información sobre terceros*, Lex Nova, Valladolid, 2001; LEGUINA VILLA, J., «Libertad informática y datos accesibles al público», *Justicia Administrativa*, n.º 4, 1998, y en SOSA WAGNER, F. (coord.), *El Derecho Administrativo en el umbral del siglo XXI. Homenaje al Profesor Martín Mateo*, Tomo I, Tirant lo Blanch, Valencia, 2000; LINDE PANIAGUA, E., «Presupuestos constitucionales de la protección de datos personales», en SOSA WAGNER, F. (coordinador), *El Derecho Administrativo en el umbral del siglo XXI. Homenaje al Profesor Martín Mateo*, Tomo I, Tirant lo Blanch, Valencia, 2000; LOSANO, M.G., PÉREZ LUÑO, A.E. y GUERRERO MATEUS, M.F., «Libertad informática y protección de datos personales», *Cuadernos y Debates*, n.º 21, 1989; LUCAS MURILLO DE LA CUEVA, P. L., *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990; *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter*

trativo de datos que ha de integrar esta nueva dogmática en el conjunto del Derecho Administrativo de forma armónica, sin que quepan soluciones maximalistas que pugnen, bien por un derecho absoluto a la reserva de los datos personales, bien por un despojo al ciudadano de cualquier posibilidad de control del flujo informativo de información sobre su persona.

I. La normativa europea sobre protección de datos y su valor en España

En el ámbito europeo, la normativa pionera de referencia la constituye el Convenio n.º 108, de 28 de enero de 1981, para la protección de los individuos respecto al procesamiento automático de datos personales, ratificado por España (3), que ha inspirado a su vez la normativa comunitaria, y constituye un referente permanente para la jurisprudencia comunitaria y nacional, habiendo servido a esta última como auténtico bastón interpretativo del art. 18.4 CE, ante la falta de normativa de desarrollo hasta 1992.

personal), Centro de Estudios Constitucionales, Madrid, 1993; «La construcción del derecho a la autodeterminación informativa», *Revista de Estudios Políticos*, n.º 104, 1999, pp. 35-60; «Las vicisitudes del derecho de la protección de datos personales», *Revista Vasca de Administración Pública*, n.º 58-II, 2000; *El derecho a la autodeterminación informativa*, Ed. Tecnos, Madrid, 1990; «La protección de los datos personales ante el uso de la informática (I y II)», *Estudios de Jurisprudencia, Colex*, n.º 3, 1992 y n.º 4, 1993; «La protección de los datos personales ante el uso de la informática (I y II)», *Estudios de Jurisprudencia, Colex*, n.º 3, 1992 y n.º 4, 1993; MESSIA DE LA CERDA, J.A., *La cesión de datos de carácter personal*, Civitas, Madrid, 2003; ORTI VALLEJO, A., *Derecho a la intimidad e informática*, Comares, Granada, 1994; PÉREZ LUÑO, A.E., «La defensa del ciudadano y la protección de datos», *Revista Vasca de Administración Pública*, n.º 14, 1986; «La incorporación del Convenio Europeo sobre protección de datos personales al ordenamiento jurídico español», en M. LOSANO, A.E. PÉREZ LUÑO y M.F. GUERRERO MATEUS, *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989; «La tutela de la libertad informática en la sociedad globalizada», *Isegoría*, n.º 22, 2000; *Derechos humanos, Estado de Derecho y Constitución*, séptima edición, ed. Tecnos, Madrid, 2001; SÁNCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea*, Secretariado de Publicaciones de la Universidad de Sevilla, Sevilla, 1998; SERRANO PÉREZ, M.M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, 2003; SOUVIRÓN MORENILLA, J.M., «En torno a la juridificación del poder informativo del Estado y el control de datos por la Administración», *Revista Vasca de Administración Pública*, n.º 40, 1994; TÉLLEZ AGUILERA, A., *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002; *Nuevas tecnologías. Intimidad y protección de datos*, Edisofer, Madrid, 2001; TONIATTI, R., «Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada», *Revista Vasca de Administración Pública*, n.º 29, 1991; VALERO TORRIJOS, J. y LÓPEZ PELLICER, J.A., «Algunas consideraciones sobre el derecho a la protección de los datos personales en la actividad administrativa», *Revista Vasca de Administración Pública*, n.º 59, 2001; VALERO TORRIJOS, J., «El uso de cookies por las Administraciones Públicas: ¿una vulneración de la normativa sobre protección de los datos personales?», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 3, 2003; VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001. Nosotros mismos hemos realizado una monografía sobre el tema, *Datos personales y Administración Pública*, Civitas, Madrid, 2005 (en prensa).

(3) Instrumento de ratificación de 17 de enero de 1984 (BOE, n.º 274, de 15 de noviembre de 1985).

Por su parte, los Estados han ido aprobando sus respectivas leyes de protección de datos, a partir de los principios de mínimos sentados en el Convenio de 1981, y de los más detallados establecidos en la Directiva 95/46/CE (4), a cuya transposición estaban obligados en tanto que Derecho vinculante y con primacía respecto del nacional. Se ha formado, de este modo, una suerte de *ius commune* de la protección de datos, tanto en general, como en concreto respecto a los datos personales en poder de la Administración, en el que observamos un triple escalón, una «normación en cascada»: un *Derecho de mínimos del Consejo de Europa* (integrado en este caso por el Convenio de 1981 y por la jurisprudencia en torno al art. 8 del Convenio Europeo de Derechos Humanos —en adelante, CEDH—); un *Derecho comunitario más detallado* (Directiva 95/46/CE); y un *Derecho pormenorizado* (Reglamento 45/2001/CE, respecto a las Instituciones (5); las respectivas Leyes nacionales, en relación con los Estados). A ello se ha unido el reconocimiento de la naturaleza iusfundamental del derecho a la protección de datos en todos las escalas: en el CEDH (integrado en el derecho a la vida privada de su art. 8 (6), aunque con proyectos de consagración como derecho autónomo); en la Carta de los Derechos Fundamentales, llamada a integrar, con pleno valor jurídico, la futura Constitución europea (en su art. 8, ésta vez como derecho autónomo respecto del derecho a la intimidad (7)); y en las diferentes Constituciones nacionales (extraído del derecho al libre desarrollo de la personalidad, del derecho a la intimidad, o afirmado como derecho autónomo a la vez que instrumental, como en España, a partir de la vaga referencia del art. 18.4 CE). Ello no quiere decir, entiéndase bien, que las Instituciones y Agencias comunitarias y cada uno de los Estados miembros compartan un idéntico modelo

(4) Directiva n.º 46/1995 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.

(5) Reglamento n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

(6) «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás». Como pronunciamientos señeros pueden citarse las SSTEDH *Leander*, de 26 de marzo de 1987; *Gaskin*, de 7 de julio de 1989; *Guerra* y otros, de 19 de febrero de 1998; *Fressoz y Roire*, de 21 de enero de 1999; *Amann*, de 16 de febrero de 2000; *Rotaru*, de 4 de mayo de 2000; o *Odievre*, de 13 de febrero de 2003.

(7) «1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. 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 su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.»

de protección de datos, puesto que el Convenio de 1981, desde luego, pero también la Directiva, permiten un cierto margen de elección a la hora de desarrollar sus principios en el Derecho nacional. Pero sí puede afirmarse que buena parte de la regulación es común a los Estados del Consejo de Europa, y, con mayor grado de concreción, de la Unión Europea.

No obstante, aún cabe esperar una mayor uniformización por vía interpretativa o, en su caso, a través de una más profunda armonización por vía de una futura reforma de la Directiva, puesto que el primer Informe sobre su aplicación considera que las divergencias entre las regulaciones nacionales son aún demasiado grandes para la buena marcha del mercado interior, aunque se muestra reticente, por el momento, a reformar la Directiva y darle mayor grado de detalle, optando por apurar los mecanismos de interpretación y coordinación (8). Sobre el particular, cobra especial relevancia el pronunciamiento del Tribunal de Justicia de las Comunidades Europeas (en adelante, TJCE) en su Sentencia *Lindqvist* (9). En la cuestión prejudicial, el órgano jurisdiccional nacional preguntaba, entre otras, si los Estados miembros pueden establecer una protección más rigurosa de los datos personales o un ámbito de protección más amplio que los que resultan de la Directiva 95/46, cuestión que había suscitado respuestas diversas de los Gobiernos nacionales y de la propia Comisión. Para el TJCE, la Directiva lleva a cabo una armonización completa, no de mínimos, pese a que reconozca a los Estados un margen de apreciación en ciertos aspectos y en gran número de sus disposiciones les permita mantener o establecer regímenes particulares para situaciones específicas. No obstante, dichas posibilidades deben emplearse tal y como dispone la Directiva y de conformidad con su objetivo, que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad.

En todo caso, ha de reseñarse que la base competencial comunitaria para legislar sobre protección de datos es controvertida, así como la extensión de su aplicación. La Directiva de 1995 se aprobó sobre la base del artículo 95 CE, entendiendo que la armonización de legislaciones era presupuesto para un flujo de datos que permitiera los intercambios económicos y las actividades administrativas relacionadas con aquéllos; en definitiva, se conectaba con la realización del mercado interior, dentro del cual está garantizada la libre circulación de mercancías, personas, servicios y capitales. No obstante, a nuestro juicio, la normativa en realidad demuestra tener vocación «universal», en la medida en que regula tratamientos sin relación con actividad económica alguna (p. ej., con fines religiosos,

(8) COM (2003) 265 final, de 15 de mayo de 2003. Disponible en el portal www.europa.eu.int.

(9) STJCE de 6 de noviembre de 2003, Asunto C-101/01.

filosóficos, etc.), lo que plantea una cuestión capital, cual es la de determinar si la Directiva (y, cuando la Carta de Derechos Fundamentales se dote de eficacia jurídica, el derecho fundamental a la protección de datos), cubren cualquier tratamiento de datos, o sólo aquél que puede considerarse incluido en el ámbito de aplicación del Derecho comunitario, por cuanto pueda afectar de algún modo al funcionamiento del mercado interior. La polémica ha llegado al TJCE, que, frente a la postura de diferentes Estados miembros y de su propio Abogado General, ha sido extraordinariamente «expansivo» en su extensión del ámbito de cobertura de la Directiva, y ha venido a considerar que no empece para la aplicación de la misma que el tratamiento no guarde relación con el flujo informativo intracomunitario o con actividad económica alguna, sin que quepa distinguir respecto de *cada* tratamiento según su vinculación con el ejercicio de las libertades fundamentales garantizadas por el Derecho comunitario (10). No podemos compartir esta interpretación, por mucho que facilite la integración jurídica y la resolución de problemas interpretativos, ya que supone una lectura injustificadamente extensiva del ámbito de aplicación del Derecho comunitario sin apoyatura en los Tratados. Cuestión distinta, evidentemente, es que los legisladores nacionales, como el español, hayan decidido extender la aplicación de sus leyes de protección de datos a cualquier tratamiento de datos personales (en ámbitos regidos o no por el Derecho comunitario; provoquen o no un flujo informativo entre los Estados miembros), sin distinciones de regímenes en función de que se den o no en ámbitos comunitarizados. En ese caso, las leyes nacionales serán de aplicación a todo tratamiento, pero sólo habrán de ser interpretadas a la luz del Derecho comunitario cuando se trate de tratamientos que caigan en su ámbito de aplicación. Por lo demás, esta misma tendencia a ampliar el campo de aplicación de la Directiva podemos encontrarla en la jurisprudencia de nuestro Tribunal Constitucional, que atiende a dicha Directiva, junto a los Tratados suscritos en el seno del Consejo de Europa, como instrumentos de interpretación del art. 18.4 CE *ex* art. 10.2 CE (11). En realidad, ello no es del todo correcto, ya que las Directivas, como ha afirmado la propia jurisprudencia constitucional, no son Tratados o acuerdos internacionales, y su valor como parámetro interpretativo lo es no del precepto constitucional *ex* art. 10.2 CE, sino de la normativa nacional, en virtud del principio de interpretación conforme acuñado por el Tribunal de Justicia de las Comunidades Europeas (12).

(10) STJCE de 20 de mayo de 2003, *Österreichischer Rundfunk*, Asuntos acumulados C-465/00, C-138 y 139/01.

(11) Por todas, STC 292/2000, de 30 de noviembre.

(12) Tal y como defendía el Abogado del Estado en el recurso que dio origen a la Sentencia citada en nota anterior, apelando a las SSTC 28/1991, de 14 de febrero, y 128/1999, de 1 de julio.

II. Perfiles constitucionales del derecho a la protección de datos

1. El artículo 18.4 de la Constitución y su desarrollo legal

La Constitución española de 1978 fue una de las primeras de nuestro entorno jurídico en dedicar un precepto a las relaciones entre informática y derechos fundamentales. Se trata del párrafo cuarto del artículo 18, de acuerdo con el cual «(l) a Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». El desarrollo legislativo de este precepto fue ciertamente tardío. Hasta la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal (en adelante, LORTAD), no existía ningún texto legal que regulara con carácter general la protección de datos personales, con la sola excepción de la disposición transitoria primera de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. El 24 de octubre de 1995 se aprobó, tras un largo iter legislativo, la Directiva 95/46/CE. De esta forma, se hizo necesario adecuar la normativa española a dicha Directiva (a pesar de que la LORTAD había tenido en cuenta el proyecto inicial), y, en consecuencia, se procedió a su transposición (de nuevo con retraso, esta vez respecto al plazo de tres años a partir de su publicación), mediante la Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), que, respetando el grueso de la LORTAD, se limitó a adaptar el texto a las diferencias existentes con la Directiva y a introducir algunas otras modificaciones. Datos todo ellos que revelan una auténtica desidia de legislador nacional, y que han generado gravísimos defectos de técnica legislativa, que conducen a la cuasi ininteligibilidad de la norma, y con ello, a una peligrosa quiebra del principio de seguridad jurídica.

2. La doctrina del Tribunal Constitucional y la necesidad de su perfeccionamiento

El Tribunal Constitucional ha considerado que la LORTAD y la LOPD son las leyes que dan cumplimiento al mandato del art. 18.4 CE (13). Sin embargo, a diferencia de su predecesora, la segunda extiende su objeto a los tratamientos no automatizados de datos personales, lo que contrasta con la referencia exclusiva a la informática del art. 18.4 CE. El Tribunal Constitucional, no obstante, ha pasado por alto esta contradicción, estimando desde su primera sentencia que el precepto recoge un derecho funda-

(13) STC 292/2000, de 30 de noviembre.

mental autónomo (en especial, respeto del derecho a la intimidad) a la par que instrumental para la efectividad de los demás derechos fundamentales (14). En su aproximación a este «derecho nuevo», el Tribunal Constitucional ha realizado un inhabitual esfuerzo dogmático para poner de manifiesto cuáles son sus puntos en común y sus elementos diferenciales respecto del derecho a la intimidad, en especial, en las Sentencias 290 y 292/2000, por referencia a una notable multiplicidad de nociones jurídicas: «objetivo» (garantizar la vida privada personal y familiar); «función» (otorgar al titular del derecho un poder de control sobre los datos personales, y no sólo la posibilidad de evitar injerencias de terceros); «objeto» (cualquier dato personal, y no sólo los «íntimos»); «contenido» (todas las facultades que permiten el control sobre los datos, y no sólo el derecho a exigir una abstención de un tercero), y «límites» (los mismos que el derecho a la intimidad). Algunas de ellas resultan un tanto indefinidas y reiterativas, y no responden en todos los casos a categorías suficientemente decantadas en la doctrina constitucional (en especial, la «función» y el «objetivo» del derecho; o la noción de «objetivo», que está, o debiera estar, directamente imbricada con la de «objeto») (15). Por ello, creemos que habrá de avanzarse aún mucho en la construcción dogmática del derecho a la protección de datos y en su delimitación (si es que cabe) respecto al derecho a la intimidad, ya que el pronunciamiento suscita diversos interrogantes, entre los cuales podemos ahora destacar los siguientes:

—El *objetivo* del derecho es la protección de la vida privada, sin embargo su *objeto* son todos datos personales, no sólo los íntimos, lo que se viene interpretando, finalmente, como equivalente a cualquier información que contenga el nombre de una persona, aunque se refiera a su vida pública o relacional, a sus actividades profesionales o económicas. Sin

(14) STC 254/1993, de 20 de julio.

(15) Véanse, entre otros, BARNÉS, J., *La propiedad constitucional. El estatuto jurídico del suelo agrario*, Civitas, Madrid, 1988, pp. 165-283; «El principio de proporcionalidad. Estudio preliminar», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 15-49; «Introducción al principio de proporcionalidad en el Derecho comparado y comunitario», *Revista de Administración Pública*, n.º 135, 1994, pp. 495-535; CRUZ VILLALÓN, P., «Derechos fundamentales y legislación», pp. 233-245; «Nota: los derechos fundamentales», pp. 247-252, ambos recogidos en *La curiosidad del jurista persa, y otros estudios sobre la Constitución*, Centro de Estudios Políticos y Constitucionales, Madrid, 1999; MARTÍN-RETORTILLO, L. y DE OTTO Y PARDO, I., *Derechos fundamentales y Constitución*, Civitas, Madrid, 1988; MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Ed. McGrawHill, Madrid, 1996; «El principio de proporcionalidad y el legislador de los derechos fundamentales», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 119-141; REQUEJO PAGÉS, J.L., *Derechos de configuración legal*, Enciclopedia Jurídica Básica, Civitas, pp. 2385-2387; RODRÍGUEZ DE SANTIAGO, J.M., *La ponderación de bienes e intereses en el Derecho administrativo*, Marcial Pons, Madrid, 2000; VILLAVERDE, I., «Concepto, contenido, objeto y límites de los derechos fundamentales», en *La democracia constitucional, Estudios en homenaje al profesor Rubio Llorente*, Congreso de los Diputados/Tribunal constitucional/Universidad Complutense/Fundación Ortega y Gasset/Centro de Estudios Políticos y Constitucionales, Madrid, 2002, pp. 317-363.

embargo, cabe plantearse si ello no supone una expansión excesiva, desproporcionada con el objetivo mismo del derecho. Por limitarnos a un aspecto de sus repercusiones en la actividad administrativa, y como veremos al analizar la relaciones entre privacidad y publicidad de la actividad administrativa, comienzan a escucharse voces de alerta hacia los efectos que una interpretación tan amplia tiene para la efectividad del principio de transparencia, anudado al principio democrático. En todo caso, e insistiremos en ello más adelante, la naturaleza de los datos habrá de ser tenida en cuenta a la hora de ponderar este nuevo derecho con otros derechos y bienes constitucionales.

—Conforme a la doctrina del TC, acerca del *contenido* del derecho a la protección de datos, formarían parte del mismo los principios de consentimiento, finalidad y exactitud, y los derechos a ser informado de los datos en poder de terceros, a acceder a ellos y a obtener su rectificación y cancelación en caso de incumplimiento de los principios antes señalados. Ahora bien, se hace necesario precisar que ese contenido constituye lo que podríamos llamar el contenido «amplio» del derecho, pues, en realidad, admite amplísimas limitaciones, en especial, respecto a los tratamientos administrativos. Hasta el punto de que, como se verá, todos ellos pueden ser, en determinadas circunstancias, excepcionados, salvo los referentes a la veracidad de los datos, y la obligación de rectificarlos en caso contrario.

—En su formulación general contenida en las referidas sentencias, el Tribunal Constitucional ha determinado de forma exhaustiva cuáles son los *posibles límites al derecho*, operando una suerte de «constitucionalización» de la normativa europea, a la par que identificando los mismos con los límites al derecho de acceso contemplados en el art. 105 b) CE. Pero una limitación tal, con pretendido alcance de cierre del sistema, resulta muy delicada. Baste pensar que dicho precepto no considera la protección de los intereses financieros del Estado como un límite al derecho de acceso, pero sí su normativa de desarrollo (art. 37 Ley 30/1992, en adelante LRJAP-PAC). Y que, asimismo, en la propia jurisprudencia constitucional, la protección de las finanzas públicas sirve de fundamento a la exigencia de comunicar datos personales a la Administración, con base en el art. 31.1 CE, pese a suponer una restricción al derecho a la intimidad (16). O que, finalmente, la propia Directiva de 1995 (17), al igual que el Convenio de 1981 (18), contempla la salvaguarda de los intereses económicos y monetarios de los Estados como susceptible de justificar una limitación al derecho. Es el problema de intentar «enjaular» los posibles límites de un derecho, en un

(16) Por todas, STC 110/1984, de 26 de noviembre.

(17) Art. 13.1.e).

(18) Art. 9.2.a).

sistema iusfundamental en el que éstos derivan de una interpretación sistemática y global de la Constitución, que llama a compatibilizar *todos* los derechos y bienes constitucionales, y de la indeterminación de cuáles hayan de ser éstos, puesto que, dado que la Administración sirve intereses generales, no es difícil conectar una función administrativa y un bien constitucional. La voluntad del Tribunal Constitucional, a nuestro juicio, ha sido la de excluir el principio de eficacia de la actividad administrativa del art. 103 CE como continente de una «cláusula de comunidad», o, si se quiere, de una «cláusula de Administración», cualquiera que sea el sector donde ésta actúe, que pudiera legitimar cualquier restricción del derecho a la protección de datos. Sin embargo, nos parece que en esta materia han de evitarse pronunciamientos generales. De hecho, la jurisprudencia del propio TC en torno al derecho a la intimidad ha identificado otros límites en diferentes preceptos constitucionales, y en ocasiones ha venido a apuntar, de forma más o menos expresa, al principio de competencia y eficacia como justificativos de la injerencia (19). Es más, en coherencia con esta doctrina, tampoco las excepciones generales contempladas en la propia LOPD satisfacen estos requisitos (aparte de carecer del rango orgánico necesario), en la medida en que restringen sustancialmente el contenido del derecho (el principio de consentimiento) siempre que los datos se recojan y utilicen en el ejercicio de las funciones de cada órgano administrativo (20), fundamento éste insuficiente desde una dogmática constitucional como la acogida en los pronunciamientos antes reseñados, y que, sin embargo, se contempla en la normativa europea sobre protección de datos (21).

—Otro tema polémico, en directa conexión con las dos anteriores, es la de determinar el *rango (de ley orgánica u ordinaria) exigido a la normativa sobre protección de datos*, cuestión sobre la que el Tribunal Constitucional ha pasado de puntillas. La normativa nacional ha otorgado rango de Ley Orgánica a las disposiciones generales, los principios de la protección de datos y los derechos de las personas, considerando, así, que se trata de un desarrollo directo del derecho a la protección de datos. A ello ha sumado la regulación de una serie de garantías institucionales como son las relativas a la Agencia de Protección de Datos y las infracciones y sanciones, a las que ha dotado de rango de ley ordinaria. A esta regulación general, de aplicación tanto a los ficheros de titularidad pública como privada, ha unido una regulación específica sobre cada uno de ellos, que, en el caso de los ficheros públicos, establece importantísimas excepcio-

(19) Una referencia a esta cuestión en RODRÍGUEZ DE SANTIAGO, J.M., *La ponderación de bienes e intereses en el Derecho administrativo*, Marcial Pons, Madrid, 2000, p. 61 nota 106.

(20) Art. 6.2.

(21) Art. 7.e) Directiva 95/46/CE; art. 7 Reglamento 45/2001/CE.

nes generales a los principios y derechos establecidos en la regulación general (22). Ello plantea, a nuestro juicio, serios problemas de constitucionalidad, ya que, conforme a la doctrina constitucional, la regulación general en negativo de los principios y derechos que conforman la arquitectura del derecho (y que, por ende, constituye su desarrollo directo) debiera, en buena lógica, tener el mismo rango que su regulación en positivo. Sólo cuando las limitaciones no son generales, sino modalizaciones al tiempo, lugar o forma de ejercicio del derecho, cabría entenderlas comprendidas en la regulación del ejercicio, y, por ello, reservadas a ley ordinaria.

—Otra cuestión relevante que queda abierta es, a nuestro juicio, la de determinar si existe una parte de dicho contenido que pueda identificarse con la noción de «*contenido esencial*», noción ésta por lo demás objeto de aproximaciones doctrinales diversas en la doctrina iuspublicista y en la propia doctrina del Tribunal Constitucional. La jurisprudencia en esto no es lo suficientemente precisa, ya que la literalidad de la argumentación del Tribunal Constitucional parece concluir que todos estos principios y derechos son indispensables para la efectividad del derecho (*ergo*, a contrario, cualquier privación de los mismos supone no una limitación, sino una desaparición del derecho a la protección de datos). Sin embargo, el Tribunal Constitucional admite a continuación la compatibilidad de la garantía del derecho con su limitación, siempre que tenga fundamento constitucional, previsión legal y resulte proporcionada, sin que ello le lleve a concluir que cualquier restricción a los principios y derechos por él mismo enunciados como indispensables, aunque cumpla estos requisitos, implique una vulneración del «*contenido esencial*» (aproximación ésta que, por lo demás, no es infrecuente en la dogmática iusfundamental del Tribunal Constitucional). A nuestro juicio, un análisis de la configuración del derecho a la protección de datos en el Derecho europeo y comparado lleva a concluir que el derecho a la protección de datos, cuando se ostenta frente a los poderes públicos, no prohíbe que se le puedan imponer cargas informativas (salvo, en este caso, que la posibilidad esté prohibida con carácter absoluto respecto de cierto tipos de datos, como aquellos que revelan las ideologías o creencias por el art. 16.2 CE), ni otorga al interesado un derecho a consentir en todo caso el flujo de sus datos personales. La sustancia de este derecho, incluso cuando es objeto de limitaciones, es más bien el derecho a que los poderes públicos no posean más datos personales que los estrictamente necesarios para el ejercicio de sus competencias legales, a que éstos sean veraces, y a conocer

(22) La LORTAD diferenciaba, dentro del régimen de los ficheros públicos, el carácter de orgánico u ordinario de cada uno de los preceptos, a veces de forma discutible, pero en el aparente entendimiento de que toda limitación o exclusión general de los principios y derechos precisaba de rango de Ley orgánica. En la LOPD, sin embargo, el Legislador ha optado por dotar a todas las disposiciones sectoriales del rango de ley ordinaria.

la identidad de los responsables de los ficheros y de los datos personales que poseen, en este último caso con posibilidad de restricciones en el modo, tiempo y forma, siempre que haya un fundamento constitucional y guardando una relación de proporcionalidad con el derecho del interesado.

Asistimos así al nacimiento de un derecho fundamental «ex novo», esto es, que se «deriva» del art. 18.4 CE pero en el que no tiene una formulación expresa, ya que la limitación de la informática es sólo un medio de hacerlo efectivo. De esta forma, el derecho a la protección de datos se «independiza» de su referencia exclusiva a los datos automatizados. Formulación ésta, por lo demás, que supone una «evolución adaptativa» a la ampliación del objeto de las sucesivas leyes de protección de datos por parte de una jurisprudencia constitucional que, a la vez y de forma no del todo coherente, ha conectado la *ratio* del derecho con los peligros que supone la acumulación de datos merced a las posibilidades informáticas.

3. Las relaciones entre el derecho a la protección de datos y el derecho a la intimidad

Un tema nuclear es el de las relaciones entre derecho a la intimidad y derecho a la protección de datos, que juzgamos aún irresuelto, pese a la voluntad del Tribunal Constitucional por marcar dogmáticamente sus diferencias, dado que hay una notoria contradicción entre la enfática proclamación de la autonomía del primero, y la recurrente intercambiabilidad de ambos en la argumentación *ad casum*.

En efecto, sintetizando las similitudes y diferencias entre el derecho a la intimidad y el derecho a la protección de datos apuntadas por el TC, puede decirse que las *similitudes* estriban en que ambos buscan un mismo objetivo, garantizar la vida privada, y tienen los mismos límites. Las *diferencias* radicarían en que el derecho a la intimidad es insuficiente para alcanzar este objetivo frente al flujo automatizado de datos personales, ya que no se extiende a toda información sobre una persona, sino sólo a la relativa a determinados aspectos de su vida, los que tengan la consideración de íntimos, ni implica facultades positivas, esto es, derecho a obtener prestaciones de terceros, sino que se limita a una vertiente negativa, consistente en la facultad del titular del derecho de imponer a terceros una abstención de intromisión o injerencia en la parcela de realidad protegida por el derecho. Sin embargo, garantizar la vida privada, hoy, precisa del reconocimiento al individuo de un poder de control sobre todos sus datos personales, consistente en prohibiciones (de obtención, uso y comunicación sin consentimiento) y derechos o facultades (de información, acceso, rectificación y cancelación). Ese *plus* respecto al derecho a la intimidad lo otorga un nuevo derecho, el derecho a la protección de datos

personales, cuyo reconocimiento, de forma desde luego original, no se extrae del 18.1 CE.

Sin embargo, un análisis exhaustivo de la jurisprudencia constitucional muestra que las diferencias enfáticamente resaltadas por la STC 292/2000 no se compadecen bien con lo que es el estadio evolutivo actual del derecho a la intimidad informacional en la jurisprudencia constitucional. Ésta tiende a extender lo que el TC califica de su objeto hacia datos que no siempre se habían considerado íntimos, como determinados datos económicos o, cuando menos, su jurisprudencia es ambigua en este punto, rehuendo una afirmación tajante sobre su pertenencia o no al círculo de lo íntimo, y entrando invariablemente a conocer del fondo de las demandas (23). Además, su contenido no es un derecho incondicionado de exclusión del conocimiento ajeno, sino más bien un poder de control sobre la información propia que se resuelve en un derecho a que la información personal no salga de la esfera reservada sin consentimiento, salvo que medie una justificación constitucional y con las debidas garantías de que la información comunicada será utilizada para dicho fin constitucional, lo que incluye medidas posteriores de seguridad y secreto (24). A la vez, en la jurisprudencia constitucional, el derecho a la protección de datos se extiende también a esta fase de recogida y comunicación de datos, esto es, al tránsito de la reserva a la publicidad, a resultas de todo lo cual las diferencias parecen diluirse. Desde el punto de vista procesal, la elección del fundamento constitucional invocado (párrafo primero frente a párrafo cuarto del art. 18), ha dependido, en la práctica, de la fase del proceso informativo en juego, de modo que la *obtención* de datos personales sin el consentimiento de su titular ha sido enfocada normalmente desde el prisma de su conformidad con el *derecho a la intimidad*, considerándose invariablemente que la injerencia que ello supone en este derecho puede encontrar justificación en principios constitucionales (destacadamente, en el necesidad de garantizar el cumplimiento del deber de contribuir a los gastos públicos), y que la injerencia será proporcionada en la medida en que el posterior tratamiento de la información se limite a la satisfacción de dicho objetivo, y se realice con todas las garantías que recoge la normativa sobre *protección de datos*. Cuando el recurso se ha centrado en una irregularidad ya no en la fase de obtención, sino en la de *tratamiento* de datos, entonces ha sido cuando los demandantes han apelado directamente a los principios y derechos que les brinda la normativa sobre protección de datos, y es entonces cuando el TC ha apelado al derecho a la protección de datos como derecho autónomo, a la par que instrumental.

(23) Véanse el ATC 642/1986, de 23 de julio, o las SSTC 143/1994, de 9 de mayo, y 233/1999, de 13 de diciembre.

(24) STC 143/1994, de 9 de mayo.

Entre la doctrina, las posiciones se encuentran divididas. P. LUCAS MURILLO DE LA CUEVA, uno de los autores con una contribución más temprana y decisiva al análisis constitucional del derecho en cuestión, se pronuncia por una conceptualización como derecho autónomo fundado en el art. 18.4 CE, por contraposición con una noción clásica, defensiva y acotada en su objeto del derecho a la intimidad (25). Por el contrario, otros autores, como J.M. CASTELLS ARTECHE (26), C. GAY FUENTES (27), L. PAREJO ALFONSO (28), o I. VILLAVARDE MENÉNDEZ (29) ponen de relieve la evolución del derecho a la intimidad que, en la sociedad informacional, y, precisamente por obra de la combinación de la acumulación de información personal y medios técnicos, viene a identificarse con un poder de autodisposición del propio ámbito personal reservado. De este modo, en una sociedad tecnificada en que los datos personales se hallan en poder de diversos sujetos públicos y privados, que pueden utilizarlos y cruzarlos, el derecho a la intimidad ha ampliado su alcance (para referirse a cualquier dato cuya utilización por terceros puede determinar las posibilidades de desarrollo del individuo en sociedad) y su contenido (para integrar facultades positivas que garanticen la efectividad del poder de autodisposición del individuo sobre la información que le concierne). La argumenta-

(25) En *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990, pp. 120-121. Tras la aprobación de la LORTAD, en su autocalificada continuación *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993, pp. 27-36. Más recientemente, ha defendido la misma postura en «La construcción del derecho a la autodeterminación informativa», *Revista de Estudios Políticos*, n.º 104, 1999, pp. 35-60, o *Las vicisitudes del derecho de la protección de datos personales, La democracia constitucional, Estudios en homenaje al profesor Rubio Llorente*, Congreso de los Diputados/Tribunal constitucional/Universidad Complutense/Fundación Ortega y Gasset/Centro de Estudios Políticos y Constitucionales, Madrid, 2002, pp. 509-537; o en el Tema dedicado a este derecho fundamental, en *Manual de Derecho constitucional*, ed. IUSTEL-Portal Derecho, www.iustel.com. ARROYO YANES, L.M., «El derecho de autodeterminación informativa frente a las Administraciones públicas (Comentario a la STC 254/93, de 20 de julio)», *Revista Andaluza de Administración Pública*, 1993, pp. 119-139, p. 122, consideraba, en esa fecha, que era ésa la doctrina dominante. Suscribe esta teoría GONZÁLEZ MURUA, A.R., «Comentario a la S.T.C. 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales», *Revista Vasca de Administración pública*, n.º 37, 1993, pp. 227-270, p. 270. Niega, asimismo, la subsunción del derecho a la protección de datos en el derecho a la intimidad M. FERNÁNDEZ SALMERÓN, *La protección de los datos personales en las Administraciones Públicas*, Civitas, 2003, Madrid, p. 60.

(26) «Derecho a la privacidad y procesos informáticos: análisis de la Ley orgánica 5/1992», de 29 de octubre (LORTAD), *Revista Vasca de Administración Pública*, n.º 39, 1994, pp. 249-278, p. 253.

(27) *Intimidad y tratamiento de datos en las Administraciones Públicas*, Complutense, Madrid, 1995, pp. 29-30.

(28) «El derecho fundamental a la intimidad y sus restricciones», en LÓPEZ ORTEGA, J.J. (dir.), *Perfiles del derecho constitucional en la vida privada y familiar*, Consejo General del Poder Judicial, Madrid, 1996, pp. 22 y ss., en pp. 41-42.

(29) VILLAVARDE MENÉNDEZ, I., «Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993», *Revista Española de Derecho Constitucional*, n.º 41, 1994, pp. 187-224.

ción de un especialista en la materia, el profesor A.E. PÉREZ LUÑO, parece igualmente inscribirse en esta línea de pensamiento (30). Como hemos notado, la jurisprudencia del Tribunal Constitucional revela la tensión entre ambas posturas, al fin y al cabo no tan diferentes como aparentan.

Llegados a este punto, cabe cuestionarse si acaso no resulta más coherente con la ubicación del art. 18.4 (en el precepto que consagra el derecho a la intimidad y sus manifestaciones), y con el conjunto de la jurisprudencia constitucional (en que se camina hacia un concepto subjetivo del derecho a la intimidad (31), y se afirma que su contenido no sólo cuenta con una faceta negativa o de exclusión sino también con una positiva o de control (32)) sostener que el derecho a la intimidad comprende, dentro de su con-

(30) PÉREZ LUÑO, A.-E., *Manual de informática y Derecho*, Ariel, Barcelona, 1996, p. 44; PÉREZ LUÑO, A.-E., *Derechos humanos, Estado de Derecho y Constitución*, séptima edición, ed. Tecnos, Madrid, 2001, pp. 318-335.

(31) Véase LÓPEZ BOFILL, H., «Hacia un concepto formal del derecho a la intimidad y sus consecuencias (Reciente jurisprudencia del TC en materia de derecho a comunicar libremente información veraz y derecho a la intimidad personal y familiar como límite al mismo: SSTC 115/2000, de 5 de mayo; 187/1999, de 25 de octubre, y 134/1999, de 15 de julio, RTC, 11/2000)», *Revista Aranzadi*, Estudio, 2000, pp. 15-27.

(32) STC 144/1999, de 22 de julio: «El derecho a la intimidad salvaguardado en el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simples particulares, que está ligado al respeto de su dignidad [...]. El derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida. *Es cierto que inicialmente pueden quedar excluidos de ese poder de disposición aquellos datos o informaciones producidos y destinados al tráfico jurídico con terceros o sometidos a fórmulas específicas de publicidad (SSTC 110/1984 y 143/1994), pero no lo es menos que esta circunstancia no obsta para que el individuo esgrima un interés legítimo en sustraerlos del conocimiento de los demás*, como del mismo modo lo puede haber para que esos aspectos de la vida individual sean públicos y conocidos, o puedan serlo [...]. Y ello es así porque el art. 18.1 CE no garantiza sin más la "intimidad", sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Es el legislador el llamado a precisar todas estas circunstancias en desarrollo del derecho a la intimidad, estableciendo justamente los límites a unos y otros intereses, pero con escrupuloso respeto del contenido esencial de este derecho, que no ha de ser otro que el derivado de la abstracta definición que del mismo hace el art. 18.1 CE. Del precepto constitucional se deduce, de un lado, que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o a su familia, pudiendo imponer a terceros, sean éstos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida. Lo que ha de encontrar sus límites, como es obvio, en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos [...]. De otro lado, el derecho a la intimidad impone a los poderes públicos la obligación de adoptar cuantas medidas fuesen necesarias para hacer efectivo aquel poder de disposición, y preservar de potenciales agresiones a ese ámbito reservado de la vida personal y familiar, no accesible a los demás; en especial, cuando la protección de otros derechos fundamentales o bienes constitucionalmente protegidos pueden justificar que ciertas informaciones relativas a una persona o su familia sean registradas y archivadas por un poder público, como es el caso del Registro Central de Penados y Rebeldes (STC 254/1993; AATC 642/1986 y 600/1989, Sentencias del TEDH. Caso X e Y, de 26 de marzo de 1985; Caso Leander, de 26 de marzo de 1987; Caso Gaskin, de 7 de julio de 1989; Caso Costello-Roberts, de 25 de marzo de 1993; Caso Z,

tenido, los principios, derechos y garantías a los que alude la STC 292/2000, que serían el nuevo contenido del derecho a la intimidad de la información personal, y no un «nuevo» derecho a la protección de datos cuyo anclaje constitucional sería más que incierto, ya que el art. 18.4 no parece formular un derecho fundamental autónomo, sino un mandato al legislador de regular la informática para proteger los derechos fundamentales; debilidad del fundamento que se acrecienta cuando el propio TC (al igual que la legislación europea y española) ha referido el derecho a la protección de datos a los tratamientos, *automatizados o no*. En una sociedad tecnificada y global como la actual, el derecho a la intimidad tiene que integrar facultades positivas y garantías institucionales que hagan efectivo el poder de cada persona de controlar la información sobre su persona, un poder de autodeterminación, que implica necesariamente ir más allá de una concepción defensiva o pasiva para integrar una faceta activa que permita dicho control. Esto es, sería precisamente la nueva realidad la que ha hecho evolucionar el contenido del derecho a la intimidad, lo que es consecuente con la interpretación histórica de los derechos fundamentales. Ello no es óbice para reconocer que el derecho a la intimidad, así concebido, conecta con los valores de libertad e igualdad, acogidos en el art. 1 CE, y con la dignidad humana y el libre desarrollo de la personalidad contemplados en el art. 10 CE, y se convierte en presupuesto para el pleno ejercicio de los demás derechos fundamentales, dado que los derechos fundamentales constituyen un sistema, en que la efectividad de unos hace posible la de los otros. En este sentido, el derecho a la intimidad es, en efecto, un derecho instrumental a la vez que autónomo.

No obstante, es de justicia reconocer que esta integración de la protección de datos en el contenido del derecho a la intimidad presenta algunas dificultades:

—En primer lugar, parece situarse fuera de la tendencia a destacar su autonomía manifestada por el Tribunal Constitucional (aun con las contradicciones expuestas), por el propio Legislador orgánico de la LORTAD, e,

de 25 de febrero de 1997). [...] Todas estas precauciones derivadas del contenido constitucional del derecho a la intimidad y, en particular, del deber positivo de protección de este derecho, que pesa sobre los poderes públicos, son, justamente, la razón que justifica las medidas legales restrictivas del acceso a esa información sensible, constituyendo una ilegítima intromisión en la intimidad individual, lesiva del art. 18.1 CE la infracción de las normas sobre acceso a la información relativa a una persona o su familia, *con independencia de que esa información sea objetivamente considerada de las íntimas o de que su conocimiento o divulgación pueda ser pernicioso para la integridad moral o la reputación de aquel o de aquellos a quienes se refiere. Pues, de no ser así, atribuiríamos a los poderes públicos el poder de determinar qué es íntimo y qué no lo es, cuando lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los linderos de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio.*» (Las cursivas son nuestras).

incluso, con la Carta Europea de Derechos Fundamentales, que, como vimos, consagra dos preceptos distintos (aunque consecutivos, como muestra al menos de su inexorable relación) al derecho a la intimidad y al derecho a la protección de datos.

—En segundo lugar, la jurisprudencia constitucional se debate entre un concepto objetivo y otro subjetivo de intimidad, y es el primero el acogido, como veremos, en Leyes que forman un conjunto normativo con las dedicadas a la protección de datos, en especial, por la LRJAP-PAC, en su regulación del derecho de acceso, que distingue, a la hora de delimitar las restricciones al derecho de acceso, entre «documentos que contengan datos referentes a la intimidad de las personas», y «documentos de carácter nominativo que no incluyan *otros* datos pertenecientes a la intimidad de las personas».

—En tercer lugar, ha que destacarse que la normativa europea y española distingue una serie de datos «especialmente protegidos» o «sensibles», entre los que se encuentran los referidos a las convicciones ideológicas, religiosas, políticas o sindicales, el origen racial, la salud y vida sexual, o las condenas penales sufridas (33). Se trata de datos que sólo con el consentimiento del individuo o, en su caso, por razones de interés público superior, pueden salir de la esfera de lo reservado, dado que la información sobre estos aspectos condiciona las posibilidades de la persona de participación en la vida económica y social. Cabría, entonces, cuestionarse si lo que califica de «datos especialmente protegidos» o «datos sensibles» coincide con lo que han de calificarse de «datos referentes a la intimidad». La idea es tentadora, pero sin embargo tampoco parece que pueda identificarse plenamente estos datos y el círculo de lo «materialmente íntimo», principalmente por omisión (piénsese, por ejemplo, que no se incluyen los datos sobre filiación o fecha de nacimiento, reconocidos socialmente como íntimos y declarados secretos por la legislación del Registro Civil). En realidad, la respuesta a por qué el legislador europeo y nacional otorga una garantía más férrea a los datos «sensibles» se encuentra en que se trata de datos directamente conectados con derechos fundamentales, como los del art. 14 (datos raciales); 16 (datos sobre ideología, religión, creencias, sindicales, en este último caso, además, con el art. 28); 18, (datos relativos a la salud y la vida sexual); y 25 (datos

(33) Arts. 6 Convenio del Consejo de Europa de 1981, 8 Directiva de 1995 y 7 LOPD. Hay una diferencia en la regulación del nivel de protección de los datos relativos a infracciones administrativas. El Convenio sólo concede una protección reforzada a los datos relativos a condenas penales. La Directiva prevé sólo como opción que queda abierta a la decisión estatal el conceder una protección especial a los datos relativos a sanciones administrativas o procesos civiles, consistente, en su caso, en que los tratamientos se realicen bajo el control de los poderes públicos. Finalmente, la LOPD ha dispuesto que: «Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras».

sobre condenas penales e infracciones administrativas). Finalmente, puede encontrarse un fundamento común, que además resulta esclarecedor en cuanto a la naturaleza y razón de ser del derecho a la protección de datos, y que radica en la necesidad de otorgar la máxima protección frente a aquellos tratamientos que pueden comprometer en mayor medida el respeto a la dignidad y al libre desarrollo de la persona consagrados en el art. 10 CE. Por ello, sólo con el consentimiento del individuo o, en su caso, por razones de interés público superior establecidas por ley, estos datos pueden ser objeto de recogida, almacenamiento, utilización y cesión, o, en el caso de los relativos a infracciones penales o administrativas, ser tratados por las autoridades públicas. Ciertamente, es posible identificar estos datos con los íntimos, lo que resulta tentador, sobre todo en cuanto que una equiparación tal, en la práctica, tiene además unos sensibles efectos clarificadores para la aplicación práctica del derecho (entre otros sectores, respecto u en lo que más nos interesa, respecto a las normas que disciplinan la publicidad de las actuaciones administrativas). No obstante, también sería posible establecer su relación con el principio de no discriminación. Al cabo, ambas perspectivas confluyen en la caracterización de ambos derechos como presupuesto para el ejercicio de los demás derechos fundamentales, como presupuestos del libre desarrollo de la persona en sociedad.

III. El régimen jurídico de los ficheros públicos

El alcance del derecho a la protección de datos varía en función de la naturaleza pública o privada del responsable del tratamiento. En la práctica, puede decirse que los ciudadanos sólo gozan de un poder de disposición cuasipleno sobre sus datos, con el contenido y las facultades afirmados por nuestro Tribunal Constitucional, respecto a las demás personas privadas, mientras que, frente al poder público, y, en particular, frente a la Administración, los intereses generales a los que ésta sirve, que tienen un referente más o menos próximos en los principios, bienes y valores constitucionales, exigen de un recorte radical en los principios y facultades que conforman el contenido del derecho, tal y como ha sido descrito por el Tribunal Constitucional. Se llega así a la paradoja de que un derecho calificado como fundamental (y, por tanto, ante todo, derecho subjetivo del ciudadano frente al poder público) sólo despliega toda su efectividad en las relaciones horizontales, relaciones a las que ni la normativa ni la jurisprudencia ha dudado en entender la vigencia del derecho a la protección de datos (34).

(34) Se trata de una apasionante cuestión, hasta el punto de que K.H. FEZER ha calificado esta pregunta como el problema del siglo y ha afirmado, parafraseando al Fausto de Goethe, que la situa-

1. La normativa sobre protección de datos y su deficiente técnica legislativa

La normativa europea (Convenio n.º 108, Directiva de 1995) ha optado por regular de forma unitaria el régimen aplicable tanto a los ficheros públicos como privados, bien que contemplando la posibilidad de los Estados de establecer excepciones amparadas en la necesidad de salvaguardar intereses públicos (de aplicación, como puede seguirse y aunque la normativa europea no lo haga expreso, a los ficheros públicos). En el Derecho comparado, se observan soluciones de todos los géneros. Por su parte, tanto la LORTAD como su sustituta, la LOPD, destacan por su mala sistemática, ya que establecen unas disposiciones comunes aplicables a todo género de ficheros, y otras específicas atinentes en exclusiva a los públicos o a los privados; pero, la vez, en las supuestas disposiciones comunes se contemplan especificidades aplicables sólo a unos o a otros. Ello obliga a un considerable esfuerzo para analizar en particular el régimen de los ficheros públicos, que constituye nuestro objeto de estudio.

En cuanto a la *normativa aplicable*, la LOPD (y antes la LORTAD) constituye la «normativa general» en dos sentidos: en cuanto autoriza a lo largo de todo su articulado a leyes sectoriales (ordinarias) a establecer excepciones a los principios y facultades que integran el contenido del derecho; y por cuanto no diseña un régimen común de protección de datos aplicable a todos los sectores de la realidad. En este segundo sentido, se distingue entre ficheros a los que no se aplica la normativa sobre protección de datos (35), y ficheros que se rigen por lo establecido por su normativa es-

ción actual plantea una pregunta crucial y embarazosa a todo jurista: ¿cuál es tu posición sobre la relación entre Constitución y Derecho privado? (en «Diskriminierende Werbung. Das Menschenbild der Verfassung im Wettbewerbsrecht», *Juristen Zeitung*, n.º 6, 1998, p. 267, citado por A.J. GÓMEZ MONTORO en *La titularidad de derechos fundamentales por personas jurídicas: un intento de fundamentación*, Libro homenaje al profesor Rubio Llorente, pp. 387-438, p. 418, que a su vez lo recoge de C.W. CANARIS). *Vid.*, al respecto, en nuestra doctrina, BILBAO USEROS, J.M., *La eficacia de los derechos fundamentales frente a los particulares. Análisis de la jurisprudencia del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 1997; CRUZ VILLALÓN, P., «Derechos fundamentales y derecho privado», en *Anales de la Academia Sevillana del Notariado*, Sevilla, 1987, pp. 97-114, recogido en *La curiosidad del jurista persa, y otros estudios sobre la Constitución*, Centro de Estudios Políticos y Constitucionales, Madrid, 1999, pp. 217-232; DE LA QUADRA-SALCEDO, T., *El recurso de amparo y los derechos fundamentales en las relaciones entre particulares*, Civitas, Madrid, 1981; GARCÍA TORRES, J. y JIMÉNEZ BLANCO, A., *Derechos fundamentales y relaciones entre particulares: la Drittwirkung en la jurisprudencia del Tribunal Constitucional*, ed. Civitas, Madrid, 1986, JIMÉNEZ CAMPOS, J., en su «prólogo» al libro de BILBAO USEROS, J.M., *La eficacia de los derechos fundamentales frente a los particulares. Análisis de la jurisprudencia del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 1997, p. 24; PÉREZ LUÑO, A.E., *Derechos humanos, Estado de Derecho y Constitución*, séptima edición, ed. Tecnos, Madrid, 2001, pp. 312-314.

(35) Art. 2.2 LOPD: «El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. b) A los ficheros sometidos a la

pecífica y por lo especialmente previsto, en su caso, por dicha normativa general (36). Con estas exclusiones y matizaciones, es de aplicación a todos los ficheros, públicos y privados, que contengan datos personales, y se complementa con Reglamentos de desarrollo, con Instrucciones y Recomendaciones emanadas de la Agencia de Protección de Datos, y con la posibilidad de elaboración de autorregulaciones que complementen y adapten la regulación legal en determinados sectores, y que pueden referirse tanto a ficheros privados como públicos, supuesto éste último que suscita las dudas que despierta, en general, el recurso por parte de la Administración a este género de *soft law*. A todo ello hay que sumar la existencia de *normativa autonómica* reguladora de las Agencias autonómicas y del régimen de creación de ficheros públicos y de ejercicio de los derechos del interesado sobre sus datos en ellos contenidos, respecto los ficheros públicos de ámbito autonómico o inferior, al portillo abierto por el art. 41 LOPD. Hasta el presente, sólo tres Comunidades Autónomas han legislado sobre la materia y creado su propia Autoridad independiente de control: la Comunidad Autónoma de Madrid, la de Cataluña y la del País Vasco (37).

2. La naturaleza pública o privada de los ficheros y sus repercusiones en cuanto al régimen legal aplicable

El derecho a la protección de datos lo ostenta cualquier persona física cuyos datos obren en poder de un sujeto sea público o privado. Al respecto, resulta crucial la consideración de la *naturaleza del fichero* como público o privado, pues a esta determinación se anuda un régimen muy diverso, merced a las numerosas excepciones con que cuentan los princi-

normativa sobre protección de materias clasificadas. c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.»

(36) Art. 2.3 LOPD: «Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: a) Los ficheros regulados por la legislación de régimen electoral; b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública; c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas; d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes; e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.»

(37) Ley madrileña 8/2001, de 13 de julio, de protección de datos de carácter personal en la Comunidad de Madrid y por el Decreto madrileño 22/1998, de 12 de febrero, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid; y, en el caso de Cataluña, por la Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos, y por el Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos. Recientemente, la Ley vasca 2/2004, de 25 de febrero.

pios y derechos del interesado respecto de los datos obrantes en ficheros públicos. La Ley utiliza los conceptos de «ficheros de titularidad pública», «ficheros de las Administraciones públicas» y «sector público» de forma indistinta y poco rigurosa. En la práctica, los ficheros son objeto de una clasificación de públicos o privados en el Registro General de la Agencia española de Protección de Datos (en adelante APD), que no atiende a criterios ciertos, sino, aparentemente, al formulario seleccionado por el propio encargado de notificar el fichero a la Agencia. Resulta, pues, particularmente útil asomarse a la normativa comparada y a la autonómica (38), así como a los planteamientos doctrinales sobre la materia (39), se decantan, con matices, por una concepción funcional que nos parece la solución más acorde con la razón que lleva a establecer un régimen diferenciado, en que los principios y facultades que integran el derecho a la protección de datos se modalizan precisamente en función de la necesidad de salva-

(38) «Del Derecho comparado se extrae como directriz que el régimen de los ficheros públicos se aplica a todo sujeto, público o privado, que ejerce funciones públicas, con exclusión, por tanto, de las empresas de capital público que concurren con los particulares en pie de igualdad en el mercado. Por su parte, la normativa autonómica ha optado, en el caso madrileño, aparentemente, por un criterio formal, que atiende a la personalidad jurídico pública o privada del ente que crea o gestiona el fichero. Los ficheros de las Corporaciones de Derecho Público sólo entran en el concepto de ficheros públicos en la medida en que se trate de ficheros creados o gestionados para el ejercicio de potestades de derecho público; la catalana, por su parte, extiende expresamente su competencia a los ficheros creados por las personas jurídico-públicas y gestionados por personas privadas, lo que es de gran importancia en dicha Comunidad, en especial, a la vista del modo de gestión concertada de su servicio de salud. A ello la Ley Catalana ha sumado la competencia sobre los ficheros de las Universidades radicadas en Cataluña, sin distinguir según su naturaleza pública o privada, lo que tiene ya más difícil encaje en el reparto de competencias Estado/Comunidades Autónomas en esta materia. La Ley vasca incluye en su ámbito de aplicación los ficheros creados o gestionados, para el ejercicio de potestades de derecho público, por: La Administración General de la Comunidad Autónoma, los órganos forales de los Territorios Históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público; b) El Parlamento Vasco; c) El Tribunal Vasco de Cuentas Públicas; d) El Ararteko; e) El Consejo de Relaciones Laborales; f) El Consejo Económico y Social; g) El Consejo Superior de Cooperativas; h) La Agencia Vasca de Protección de Datos; i) La Comisión Arbitral; j) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco; k) Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario.»

(39) La doctrina iuspublicista se decanta, mayoritariamente, hacia un criterio funcional, el que atiende a la conexión del fichero y el tratamiento con el ejercicio de funciones públicas, sea por sujetos públicos o privados. En este sentido, FERNÁNDEZ SALMERÓN, M. (*La protección de los datos personales en las Administraciones Públicas*, Civitas, 2003, Madrid), pp. 110-128, que insiste, en todo caso, en la necesidad de aplicar algunos preceptos relacionados con los ficheros privados (en particular, el régimen sancionador) a los sujetos privados que gestionan ficheros públicos; GAY FUENTES, C., *Intimidad y tratamiento de datos en las Administraciones Públicas*, Complutense, Madrid, 1995, p. 89; HERNÁNDEZ GONZÁLEZ, FL., «El concepto de “ficheros de titularidad pública” en la Ley de Protección de Datos», *Actualidad Administrativa*, n.º 23/2-8 de julio de 1997, pp. 413-425; VALERO TORRIJOS, J. y LÓPEZ PELLICER, «Algunas consideraciones sobre el derecho a la protección de los datos personales en la actividad administrativa», *Revista Vasca de Administración Pública*, n.º 59, 2001, pp. 268-271.

guarda de intereses públicos dignos de protección, a cuya efectividad, precisamente, sirve la Administración pública, por sí misma o a través de terceros, y en vista de los cuáles se les atribuyen potestades exorbitantes. Ahora bien, este entendimiento parece presuponer que, en el caso de los concesionarios de servicios públicos, el fichero deba entonces ser creado por la Administración a la que se considerará responsable del mismo, mientras que el sujeto privado tendrá la consideración del encargado del tratamiento, y que la creación deberá preverse en una disposición general objeto de publicación oficial. Asimismo, hace surgir la duda acerca de cuál sea el régimen sancionador aplicable, y, en concreto, si cabe que las Agencias de protección de datos impongan sanciones pecuniarias a los sujetos privados que infringen la normativa en relación de ficheros conectados con el ejercicio de funciones públicas, lo que nos parece que debe obtener una respuesta afirmativa, so pena de crear ámbitos de impunidad.

3. Los distintos tipos de datos personales y sus diferentes niveles de protección

La LOPD, como antes hiciera la LORTAD, traza lo que podríamos considerar tres círculos concéntricos de protección, en función de la *naturaleza de los datos*, que llevan asociados un diferente régimen en la verificación del principio del consentimiento y del régimen de medidas de seguridad y sanciones. Podríamos así distinguir tres categorías de datos: un círculo externo, integrado por los datos contenidos en «fuentes accesibles al público» (se sigue un sistema de lista cerrada, que incluye los datos que han sido objeto de publicidad oficial) (40); un círculo interno, al que pertenecen los llamados «datos especialmente protegidos» (41); y un círculo medio, en el que se integran el resto de datos personales. De este modo, el contenido del derecho a la protección de datos se modula en función del objeto, esto es, del tipo de datos de que se trate y la repercusión que pueda tener en la vida social y económica su flujo informativo: en unos casos, constituye un presupuesto de la misma (datos contenidos en fuentes accesibles al público), mientras que en el polo opuesto pueden constituir un obstáculo para el libre desarrollo de la personalidad del individuo y del ejercicio de sus derechos fundamentales (datos especialmente protegidos). No obstante, en todos los casos conserva su configuración como derecho de libre disposición de los datos, puesto que es el consentimiento

(40) Art. 3.j) LOPD.

(41) Art. 7 LOPD.

del afectado, prestado en formas diversas en función de género de datos de que se trate, el que va a decidir qué datos y para qué finalidades son objeto de tráfico informativo, conservando, como veremos a continuación, sus facultades de control sobre los mismos. Sin embargo, como veremos inmediatamente, dicho poder de decisión es muy limitado en relación con los tratamientos de datos personales por la Administración pública.

4. El contenido del derecho a la protección de datos: principios del tratamiento, derechos del afectado y garantías institucionales y organizativas

La LOPD dedica sus Títulos II y III a los «*principios de la protección de datos*» y a los «*derechos de las personas*», respectivamente, y los regula con rango de ley orgánica, entendiendo que constituyen el desarrollo directo del derecho a la protección de datos. Como idea general, debe partirse de la propia razón de ser del derecho, que, como vimos en el capítulo anterior, consiste en asegurar al afectado un poder de control sobre su información personal. Para ello el sujeto debe poder decidir qué información está dispuesto a poner a disposición de terceros (*principio de consentimiento*) a la vista de los fines para los que ésta puede ser utilizada (*principio de finalidad*), y asegurarse de que dicha información sea en todo caso cierta y adecuada a la finalidad pretendida (*principios de veracidad y adecuación*). Para hacer efectivo estos principios se requiere que el ciudadano pueda conocer en todo momento quién posee qué información sobre su persona, a qué se destina, y retirarla del conocimiento ajeno en caso de que sea información inexacta o innecesaria (*derechos de consulta al registro, y de información, acceso, rectificación y cancelación*), impugnando, en su caso, las decisiones basadas exclusivamente en el tratamiento efectuado (*derecho de impugnación de valoraciones*), y exigiendo la compensación por los daños sufridos (*derecho a ser indemnizado*). A este juego de principios y derechos (con los consiguientes deberes), se le unen unas garantías institucionales que persiguen la efectividad de estos principios y derechos (*medidas de seguridad para garantizar el secreto, existencia de un registro general de protección de datos, establecimiento de un sistema de sanciones*, todos ellos bajo el control y tutela de las *Agencias de Protección de Datos*, estatal y autonómicas).

Los principios del tratamiento, los derechos de los afectados y las garantías institucionales y organizativas se restringen, desaparecen o se modalizan en el caso de los ficheros públicos, como consecuencia de la necesidad de compatibilizar el derecho a la protección de datos con los intereses generales a los que sirve la Administración pública. Veamos, resumidamente, de qué modo.

4.1. LOS PRINCIPIOS DEL TRATAMIENTO Y SU APLICACIÓN A LOS FICHEROS PÚBLICOS

4.1.1. *El principio de calidad*

En relación a las exigencias de veracidad y adecuación de los datos íntitas a la idea de «calidad», cabe plantearse, en el ámbito de los ficheros públicos, a quién corresponde garantizar su respeto. Parece que, en el caso de datos suministrados por los interesados en cumplimiento de una obligación legal, ésta se extiende a la comunicación de los posibles errores o cambios en los mismos, como por lo demás prevén diversas leyes, y, más en general, como exige el cabal cumplimiento por el ciudadano de sus deberes con la Administración. A su vez, las Administraciones están obligadas a hacer constar cualquier error o cambio en los datos personales del que tengan conocimiento, como de nuevo prevén diversas leyes sectoriales, y, más globalmente, en aplicación del principio de legalidad. En todo caso, la obligación de rectificación de datos personales deriva directamente del art. 4 LOPD, y encuentra su trasunto, ya general y no referido sólo a éstos, en el art. 105.2 Ley 30/1992. Sin embargo, cuando se trata de datos generados por la propia Administración (piénsese, p. ej., en Registros policiales), la obligación de garantizar la exactitud pesa exclusivamente sobre ella, bien que pueda ser instada por el afectado. En cuanto a la conservación y cancelación, hay que advertir que el tema enlaza directamente con la regulación de la documentación administrativa y el régimen de los archivos que constituye, bien puede decirse, una de las mayores fallas de nuestro ordenamiento jurídico-público, con una regulación desubicada, confusa y obsoleta; en que materias cruciales como el expurgo y los tiempos de conservación en los diferentes archivos (de gestión, central, general, histórico) carecen del mínimo rigor regulatorio exigible; y en que las Comisiones Calificadoras de Documentos Administrativos apenas han echado a rodar. Se trata, sin embargo, de una cuestión clave para la localización de los ficheros y para el ejercicio de los derechos de acceso, rectificación y cancelación del interesado. Y ello pese a que, en lo que respecta a los datos personales, la LOPD contiene un mandato específico, englobado bajo el rótulo de la «calidad», según el cual los datos de carácter personal han de ser almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados, previendo así una medida organizativa. En este sentido, la obligación de inscripción de ficheros en el Registro General de Protección de Datos, que afecta asimismo a los manuales una vez pasado el período transitorio, puede contribuir a mejorar y racionalizar la organización interna de las diversas Administraciones. Por lo demás, hay que señalar que la vigencia del principio de adecuación de los datos a la finalidad para la que fueron recabados ha sido destacada de forma insistente por la doctrina del Tribunal Constitucional y Supremo como uno de los pará-

metros para juzgar la proporcionalidad de la injerencia en la esfera de intimidad informacional de la persona.

4.1.2. *El principio de finalidad*

Cuál sea el alcance del principio de finalidad constituye, junto con el propio concepto de dato personal, el segundo punto crucial de la dogmática del derecho fundamental que se encuentra en proceso de redefinición. La doctrina del Tribunal Constitucional parte del principio conforme al cual se proscribía toda utilización de datos para fines *diferentes* a los que motivaron su recogida (42), lo que explica, además, la declaración de inconstitucionalidad del precepto que permitía la autorización reglamentaria de la comunicación de datos interadministrativa para fines diferentes a los que motivaron la recogida, dado que cualquier excepción al principio ha de ser establecida por ley. El Tribunal Constitucional se situaba en línea con lo que establecía la LORTAD. Sin embargo, paradójicamente, en dicha Sentencia la Ley enjuiciaba no era ésta sino la LOPD, que cambió el enunciado del principio de finalidad. De este modo, lo que la LOPD prohíbe ahora es el tratamiento posterior para finalidades *incompatibles* con la que motivó la recogida. El cambio es fruto de una enmienda presentada en su trámite de aprobación por el P.N.V. y justificada en la pertinencia de no limitar en extremo ciertos tratamientos privados conexos, pero diferentes a aquél que motivó la recogida, pero se ha formulado con alcance general. La doctrina se muestra enfrentada sobre el alcance de dicho cambio (43). Ciertamente, el cambio de redacción no ha ido acompañado de una modificación sistemática del resto del articulado, que ha permanecido inalterado. El TC parece haber seguido esta vía de hacer caso omiso de la alteración del precepto, sin plantearse su posible inconstitucionalidad, y construyendo su doctrina a partir del principio de finalidad en su entendimiento clásico, conforme al cual emplear datos para una finalidad diferente de aquella para la que fueron recabados significaría un desconocimiento de la misma esencia del derecho, imposibilitando el conocimiento del ciudadano del posible destino final de sus datos. Sin embargo, lo cierto es que resulta incuestionable la diferencia en la redacción, que no

(42) STC 292/2000, de 30 de noviembre: «la llamada “libertad informática” es así derecho a controlar el uso de los mismos datos insertos en un programa informático (“habeas data”) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención».

(43) No dan trascendencia al cambio de redacción VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001, pp. 93-95; o LUCAS MURILLO DE LA CUEVA, P., «Las vicisitudes del derecho de la protección de datos personales, Las vicisitudes del derecho de la protección de datos personales», *Revista Vasca de Administración Pública*, n.º 58-II, 2000, pp. 523-527. En contra, APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 2.ª ed., Aranzadi, Cizur Menor, 2002, p. 111.

ha pasado desapercibida a la APD, que ha interpretado que existe un cambio en la perspectiva (44). Se trata, pues, de una cuestión abierta de trascendencia suma para la dogmática del derecho, en general, y para el régimen de los ficheros públicos, puesto que difícilmente puede entenderse que las diversas finalidades públicas son incompatibles entre sí, por lo que, de consagrarse este entendimiento, se daría vía libre a un flujo libre de datos personales intra e interadministrativo sin necesidad de obtener el consentimiento del interesado.

4.1.3. *El principio de consentimiento*

La tercera pieza maestra del derecho a la protección de datos es el principio de *consentimiento* (no por casualidad el derecho a la protección de datos ha sido llamado, como sabemos, derecho a la «autodeterminación informativa»). Es decir, cada persona puede determinar, a la vista de la finalidad a que se pretenden destinar sus datos, qué información personal da a conocer a otra y en qué condiciones podrá ser o no comunicada a un tercero. En esta medida, la persona es «dueña de sus datos» y determina las posibilidades de su tráfico. Ahora bien, este principio cuenta con importantes excepciones, establecidas en la propia LOPD, que además permite adicionar otras por ley. La mayoría de ellas se aplican a los tratamientos administrativos. En efecto:

A) La necesidad o no de consentimiento para la *recogida de datos por la Administración* no se prevé en la LOPD. Es más, la LOPD da por supuesto que los ciudadanos pueden tener la obligación de suministrar datos personales, propios o de terceros, obligación que por lo demás imponen numerosas leyes (valga el ejemplo de las de naturaleza policial, tributaria o de seguridad social). Pueden plantearse dos cuestiones principales sobre el consentimiento en la fase de recogida. En primer lugar, si la Administración tiene una obligación de tratar de recabar los datos personales del propio interesado, y no de un tercero. La Sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983 (45), y así lo consagra

(44) Memoria APD 2002: «[...] (d)ado que la Ley no identifica qué ha de entenderse por “fin compatible”, debe analizarse la existencia de dicha compatibilidad en cada supuesto de hecho que se plantee, determinando si a la luz de las disposiciones aplicables a cada caso y de las circunstancias del mismo cabe considerar que esa finalidad que se alega como compatible resulta lícita a la luz de las normas aplicables y si la misma guarda una adecuada relación con la finalidad que justificó el tratamiento de los datos».

(45) Sentencia que giró sobre la constitucionalidad de la Ley sobre Censo de la población, las profesiones, las viviendas y los centros de trabajo, que constituyó, en expresión de la doctrina alemana, el «Sermón de la montaña» en materia de protección de datos (PÉREZ-LUÑO, A.-E., *Derechos humanos, Estado de Derecho y Constitución*, séptima edición, ed. Tecnos, Madrid, 2001, p. 367, nota 23).

la Ley alemana de protección de datos (46), y en este sentido puede leerse también algún pronunciamiento judicial de nuestro Tribunal Supremo, que apunta a que, al menos, el interesado siempre debe contar con la opción de suministro personal de información, prescindiendo de intermediarios (47), lo que resulta coherente con el principio de proporcionalidad que debe presidir toda injerencia en el derecho de toda persona a la libre disposición de sus datos. En segundo lugar, cabe cuestionarse qué rango ha de tener una norma que imponga cargas informativas. Como vimos, la jurisprudencia constitucional ha afirmado que toda restricción al derecho a la intimidad informacional (la principal de las cuales es, precisamente, la imposición de este género de obligaciones) tiene que tener una base legal, lo que no impide no obstante la colaboración reglamentaria para la identificación detallada de la información requerida. Diferente será en los casos en que no se trata de la imposición de cargas informativas, sino en la determinación, en los procedimientos iniciados a instancia de parte, de los datos personales que hayan de consignarse, en cuyo caso la ausencia de obligatoriedad hará que no exista reserva de ley, en la medida en que no hay injerencia, sino ha de considerarse una carga de quien pretende obtener un beneficio.

B) El consentimiento para el *tratamiento de datos dentro de una misma Administración* (en sentido estricto, esto es, su utilización por la Administración que los posee) no es necesario cuando los datos se recogen para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias (48). La Ley no regula de forma expresa la comunicación de datos de un órgano administrativo responsable de un fichero a otro de la misma Administración. A falta de una clarificación, y conforme a una interpretación coherente y sistemática de la Ley, ha de entenderse que ésta cabe siempre que se respete el principio de finalidad, en el entendimiento que éste haya de tener.

C) El consentimiento para la *comunicación de datos entre Administraciones públicas* no es preciso cuando los datos hayan sido obtenidos o elaborados por una Administración con destino a otra, o tenga lugar para el ejercicio de las mismas competencias o de competencias que versen sobre las mismas materias (49). El primero de estos supuestos se caracteriza por la instrumentalidad en la actividad de la Administración cedente.

(46) Art. 4.2 *Bundesdatenschutzgesetz* de 20 de diciembre de 1990: «Los datos personales se recogerán del afectado, salvo que una previsión legal lo disponga; o la naturaleza de la tarea administrativa exige que se recoja de un tercero o exigiría un esfuerzo desproporcionado y, en ambos casos, no hay indicios de que los intereses legítimos superiores del afectado sean afectados por ello».

(47) STS de 20 de mayo de 2000, Ar. 4497.

(48) Art. 6.2 LOPD.

(49) Art. 21 LOPD.

En estos casos, y conforme a las definiciones legales, habría de entenderse que no se produce en realidad una cesión, en la medida en que la Administración cedente actúa como encargada del tratamiento, y la cesionaria es la auténtica responsable del fichero o tratamiento. En él se encuadran los casos de colaboración interadministrativa, articulada a menudo como encomienda de gestión, o como delegación de competencias. Un supuesto destacado sería la elaboración por las Diputaciones de los Padrones de pequeños municipios. También los casos de presentación de escritos en Registros de una Administración con destino a otra, acogidos en el art. 38.4 Ley 30/1992. Por su parte, el régimen general de la comunicación interadministrativa se caracteriza por una absoluta oscuridad, que trae su causa tanto del dictado de la Ley, que utiliza una formulación en negativo y unos conceptos de difícil encaje en la sistemática legal, como en que la redacción inicial del precepto ha quedado alterada tras la declaración de inconstitucional llevada a cabo por la STC 292/2000 (50). Conforme a esta jurisprudencia constitucional, habría que distinguir, pues, dos supuestos: *cuando la comunicación de datos tiene como destino su empleo por otra Administración para la misma finalidad para la que han sido recabados y tratados*, no se precisa el consentimiento del interesado, si bien la comunicación ha de preverse en la disposición de creación del fichero (51). En este caso, no se requiere consentimiento del afectado (como no lo requiere la normativa europea), y la explicación sería que la efectividad de los fines públicos, que han legitimado previamente la obtención de los datos requiere que el reparto territorial de competencias no sea óbice para su efectividad y para una actuación coordinada entre los órganos de las diversas Administraciones con competencia sobre la materia. Por el contrario, cuando la comunicación de datos tiene como destino su empleo por otra Administración para una finalidad distinta de aquélla para la que han sido recabados y tratados, conforme al dictado de

(50) El precepto disponía que: «Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, *salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso*, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos». Esta dicción abría la posibilidad de previsión reglamentaria de comunicación de datos para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas (que podía llevarse a cabo en la propia disposición de creación del fichero), de modo que lo resaltado en cursiva fue considerado inconstitucional en la STC 292/2000.

(51) Hacemos referencia al principio de finalidad, siendo así que el art. 21 alude al criterio de las «competencias diferentes» y las «competencias que versen sobre materias distintas». Los términos utilizados conllevan una gran dificultad hermenéutica, y ha dado lugar a interpretaciones doctrinales muy diversas. Entendemos que la Ley ha querido asegurar la libre circulación de datos entre Administraciones siempre que se mantenga una identidad de destino, lo que vendría a coincidir con el concepto de «materia» (medio ambiente, seguridad, tributos, etc.).

la STC 292/2000, es precisa una previsión legal expresa, en cuyo caso puede llevarse a cabo sin consentimiento del afectado.

Ahora bien, en lo que se refiere a la necesidad de consentimiento o de previsión legal expresa para la comunicación de datos, cuando se pretenden destinar a una finalidad distinta a la que motivó la recogida, nos parece posible argumentar que, frente a la actividad administrativa, ningún riesgo corre el ciudadano por el hecho de que sus datos personales sean trasvasados libremente en el interior de una misma Administración o de una Administración a otra para el ejercicio de las competencias respectivas de cada órgano de cada Administración en sus diversos ámbitos competenciales. Se trata ésta de una afirmación aparentemente herética (52). Pero entendemos que el control frente a los posibles abusos radicaría, precisamente, en la combinación de los principios de legalidad de la actuación administrativa y calidad de los datos, que impediría a cualquier órgano administrativo acumular más datos de los estrictamente necesarios para el cumplimiento de sus funciones. Cualquier desviación sería contraria a estos principios, y, por ende, ilegal, mientras que el ciudadano no debería sentir amenaza alguna por el correcto ejercicio de sus competencias por parte de las Administraciones a partir de datos personales veraces, y conservaría en todo caso sus facultades de información, acceso, rectificación y cancelación para controlar el cumplimiento de estos presupuestos. De este modo, el principio de eficacia administrativa (que, dependiendo del sector, puede ponerse en relación con el derecho a la salud, a la seguridad, al sostenimiento equitativo de las cargas públicas, etc.) unido, en el caso de las cesiones interadministrativas al deber de cooperación hoy expresado en el art. 4 LRJAP-PAC, pugnaría por un flujo sin limitaciones de datos entre Administraciones públicas para el ejercicio de sus respectivas competencias (53). A fin de cuentas, el único límite añadido por el TC consiste en someter este libre tráfico a los requisitos generales de toda limitación a un derecho fundamental, lo que en la práctica

(52) Si bien, parece apuntar también este sentido, A. TRONCOSO REIGADA (en su «prólogo» al libro de FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas*, Civitas, 2003, Madrid) que defiende que «impedir a una Administración Pública utilizar ese fichero para una finalidad parcialmente distinta no tiene en ocasiones sentido al tener ésta la facultad de tratar datos personales sin consentimiento del interesado. La solución de pedirle el consentimiento sería contradictoria con el art. 6.2 LOPD» (p. 39, nota 41).

(53) En definitiva, ¿por qué no facilitar este trasvase de datos, cuando la Administración es una entidad de naturaleza vicarial al servicio de los intereses generales? ¿acaso no originaría ello un mejor funcionamiento de las diferentes Administraciones y un mejor reparto de las cargas públicas (controlando, por ejemplo, que los ingresos consignados a efectos de solicitar una subvención coinciden con los declarados ante la Administración tributaria? ¿qué interés digno de protección puede esgrimir el ciudadano para oponerse a este flujo informativo?). No parece que haya en nuestro Estado democrático un riesgo cierto de acumulación silente de datos para formar perfiles individuales por parte de las Administraciones públicas (lo cual, por lo demás, estaría abiertamente proscrito por los principios de legalidad y calidad).

viene a significar, fundamental y casi exclusivamente, someterlo a reserva de ley, reserva podría argumentarse si no puede considerarse cubierta por la obligación de colaboración interadministrativa prevista en el art. 4 LRJAP-PAC (54). Aún más, el análisis de la normativa sectorial muestra que las leyes especiales que autorizan la comunicación de datos inconsciente intra o interadministrativas, discriminando supuestos en que cabe y otros en que no, lo hacen atendiendo a criterios carentes de motivación y de elementos ponderativos, a menudo del modo más amplio la cesión interadministrativa de datos personales sin consentimiento en sectores claves de la actividad administrativa, como Hacienda o la Seguridad Social, y declaran inaplicable el régimen de la comunicación de datos diseñado en el art. 21.1 LOPD (a efectos de eliminar la limitación de la identidad de finalidades) (55). Además, ha de tenerse en cuenta que los datos esenciales de las personas (nombre, apellidos, domicilio, sexo, fecha y lugar de nacimiento, DNI, nivel de estudios) están a disposición de todas las Administraciones públicas para el ejercicio de sus respectivas competencias, a través del padrón municipal y el fichero o registro de población creado por la LOPD (56). Lo mismo cabe decir de los datos catastrales, también los reservados, que se consideran a disposición de todas las Ad-

(54) Ciertamente, puede argüirse que la declaración de inconstitucional parcial del art. 21 LOPD llevada a cabo por la STC 292/2000 presupone una respuesta negativa, pero lo cierto es que otros preceptos de la misma LOPD tienen un alcance igualmente general y que una reserva de ley especial carece de la necesaria flexibilidad que puede exigir la colaboración administrativa en supuestos imprevistos (piénsese, por ejemplo, en una solicitud de información sobre los empresarios que producen determinado producto exigida a la Administración estatal tributaria por una Administración autonómica que la precisa para adoptar medidas sanitarias).

(55) Así, p. ej., en materia tributaria (arts. 93 a 95 Ley General Tributaria); o de recaudación de derechos de la seguridad social (art. 36 Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social).

(56) En efecto, por una parte, la normativa reguladora del padrón municipal (en el que los ciudadanos han obligatoriamente de inscribirse) prevé la cesión de datos del padrón a otras Administraciones públicas es obligatoria para los Ayuntamientos y no requiere el consentimiento previo, si bien debe limitarse a aquellos casos en que sea necesario *para el ejercicio de sus respectivas competencias*, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. Dichos datos son muy relevantes (nombre, apellidos, domicilio, sexo y fecha y lugar de nacimiento, D.N.I. —o equivalente para extranjeros— y el nivel de estudios —arts. 16 y 17 LRBRRL). Por su parte, con base en el padrón y del censo electoral que se forma a partir del mismo la LOPD ha previsto la creación de los llamados ficheros o registros de población, previendo su cesión interadministrativa inconsciente para *cualquier finalidad que se encuentre dentro del ámbito competencial de cada Administración* (disposición adicional segunda: «1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. 2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas de las Administraciones públicas»).

ministraciones «con las limitaciones derivadas de los principios de competencia, idoneidad y proporcionalidad» (57). O de los datos del Registro de la Propiedad, cuya comunicación se prevé, genéricamente, a instancias de cualquier autoridad administrativa (58). De esta suerte, podría decirse que a la postre las Administraciones se comunican con práctica libertad los datos personales de los ciudadanos que le son necesarios para el ejercicio de sus competencias, sin el consentimiento de los interesados. Como único contenido auténticamente garantizado está que toda comunicación se supedita a la necesidad y adecuación de los datos para el desempeño de sus funciones en la materia específica sobre la que cada Administración, y dentro de ella, cada órgano, es competente. Es más, debe tenerse en cuenta que en ocasiones, en dichas disposiciones se prevé que un fichero cumpla más de una finalidad, integrándose cada una de ellas en el marco competencial de diferentes órganos administrativos. En este caso, el órgano responsable del fichero podrá ceder al que no lo sea los datos necesarios para alcanzar la finalidad prevista. El TS ha entendido que la inconstitucionalidad de la previsión de la LOPD que permitía autorizar por reglamento la cesión de datos personales se refiere a la cesión para finalidad diferente a la contemplada en la norma de creación, y no para una de las finalidades ya inicialmente previstas. Sin embargo, lo cierto es que en todos los casos antes mencionados, en que se contemplan supuestos absolutamente generales de comunicación inconstitucional, el particular desconoce *de facto* cuáles serán los posibles destinos de sus datos, pese a que la normativa exige que las disposiciones reglamentarias de creación de cada fichero hagan constar las posibles cesiones, por lo que su previsión legal no se antoja una garantía de peso. Como argumento comparativo, ha de reseñarse que la autorización de cualquier comunicación intra e interadministrativa de datos para el ejercicio de las respectivas competencias está prevista en la propia normativa comunitaria que regula el tratamiento de datos por las Instituciones, y puede derivarse de la Directiva de 1995, que no regula de forma específica la comunicación, sino que la integra dentro del concepto de tratamiento, y éste se legitima, sin necesidad de consentimiento del interesado, siempre que es necesario para el cumplimiento de una misión pública o de una obligación legal. Creemos, pues, que el legislador español ha sido corto de miras, y que el Tribunal constitucional ha ido probablemente demasiado lejos en su aplicación mimética de la dogmática general de los límites de los derechos fundamentales. Por último, obsérvese que, de consagrarse la trascendencia del cambio de dicción (de finalidades «diferentes» a «incompa-

(57) Arts. 51 a 53 Real Decreto Legislativo 1/2004, de 5 de marzo.

(58) Art. 332.6 Reglamento Hipotecario.

tibles»), a lo que parece apuntar hoy el derecho a la protección de datos, difícilmente podrían considerarse incompatibles entre sí cualesquiera finalidades públicas atribuidas a cualesquiera Administraciones Públicas de acuerdo con la ley. Como puede comprobarse, estas reflexiones se adentran, a nuestro juicio, en la línea de flotación de todo el sistema, y requiere una reflexión dogmática del mayor calado que vaya de la mano de un aproximación profunda (incluidos sus componentes extrajurídicos) acerca del entendimiento de cuál es la naturaleza de la relación Administración-ciudadanos (59).

D) Finalmente, el tema del consentimiento para la *comunicación a terceros de datos personales en poder de la Administración*, llama al necesario equilibrio entre publicidad y reserva, y precisa de un análisis detallado y monográfico del que aquí sólo podemos trazar alguna pincelada, a modo conclusivo. Por sorprendente que pueda parecer, se trata de una cuestión jurídica aún irresuelta, legislativa, jurisprudencial y doctrinalmente. A nuestro juicio, no caben, desde luego, maximizaciones de un derecho que lleve al sacrificio de su opuesto. La publicidad de datos personales no sólo tiene lugar a través del ejercicio del derecho de acceso. Los registros públicos, las publicaciones oficiales, la publicidad de actos administrativos y de sanciones por diversas vías, desde tablones hasta medios de comunicación, e incluso la más reciente fórmula de la reutilización para fines comerciales de información pública requieren una interpretación armónica con la normativa sobre protección de datos personales cuando los incorporan. En todos los casos, se requiere una ponderación de derechos y un análisis al caso que, en nuestra opinión, tiene que basarse en la efectiva vinculación del dato personal a la privacidad o vida privada, y no, tal y como en la actualidad se interpreta, con su identificación indiferenciada con toda información referible a una persona. Y arbitrar medidas de toda índole (publicidad de datos previa anonimación, medidas procedimentales que permitan tener elementos de juicio nece-

(59) Finalmente, lo dicho respecto a los datos personales «comunes» ha de complementarse con una reflexión acerca de la vigencia del principio de consentimiento en el caso de los datos especialmente protegidos. El art. 7 establece la prohibición absoluta de tratamiento de datos que revelen la ideología, afiliación sindical, religión y creencias sin consentimiento. Respecto a los relativos al origen racial, a la salud y a la vida sexual admite, además, que sean recabados, tratados y cedidos cuando por razones de interés general así lo disponga una ley. Este régimen se aplica aparentemente (la sistemática de la LOPD resulta realmente diabólica, y es útil acudir a la normativa comunitaria y comparada) tanto a los ficheros públicos como a los privados, en cuyo caso habría de concluirse que en estos casos es preciso que, o bien la propia LOPD, o bien una ley sectorial específica prevea el tratamiento (en sentido amplio) in consentido. Ello se hallaría en línea con la idea de que, al estar particularmente en juego en el manejo de estos datos la dignidad de la persona (en relación con el principio de no discriminación y al derecho a la intimidad), toda posible afección (bajo la forma de tratamiento in consentido) precisa de cobertura legal específica, justificada en la protección de un derecho o bien constitucional, sin que baste al respecto una mera norma reglamentaria general o la propia disposición de creación del fichero.

sarios para la ponderación, medidas técnicas y de seguridad para evitar acceso a información personal para finalidades que no tengan relación con la eficacia y transparencia de la actividad pública, etc.). Estos principios son extensibles al acceso a registros públicos que contengan datos personales, respecto a los cuales, como síntesis, puede decirse que, en nuestra opinión, la clave radica en la aplicación del principio de finalidad, entendiendo que ha de prevalecer el interés del solicitante de información cuando responda a la finalidad para la que se instituyó el Registro. Se trata de acompasar un sistema de publicidad con el rechazo de un uso desviado de la finalidad que los mueve, cuando normalmente a la información se accede mediante la mera presentación de la solicitud acompañada de los datos identificativos del demandante y, en su caso, de la expresión de la causa genérica de la solicitud.

Una reflexión final acerca de las relaciones publicidad/reserva y la necesaria extrapolación de las directrices a otros ámbitos. La LOPD exige una previsión legal para la comunicación incontestada de datos. Ello conlleva que, al margen ya del ejercicio del derecho de acceso, regulado en nuestro derecho en una fuente legal, la LRJAP-PAC, cualquier modalidad de publicidad diferente haya de tener una cobertura legal, so pena de vulnerar la LOPD. Si partimos de un concepto extensísimo (que, a nuestro juicio, está llamado a su restricción) de «datos personales», ello supone que, por ejemplo, una iniciativa consistente en facilitar datos de licenciados por parte de una Universidad pública a un Colegio profesional o a una gran empresa con fines de ocupación laboral, o cualesquiera otra iniciativa que se nos ocurra estará vedada en la medida en que carezca de cobertura legal, sin que baste para ello, pues, una norma reglamentaria (aprobada, por ejemplo, por la respectiva universidad). En definitiva, toda posibilidad de difusión se somete a la Ley, sin que ni el reglamento ni, menos aún, la propia iniciativa de la autoridad pública, cualquiera que sea la modalidad de publicidad de los datos (incluidos los tableros de anuncios) y por mucho que busque perseguir el interés general al que se enderezan las competencias que les han sido atribuidas pueda servir de base suficiente (60). A nuestro juicio, de esta forma, el legislador español, por un empeño inadecuado en regular de forma autónoma la comunicación respecto de las demás operaciones de tratamiento, ha creado un sistema a la vez rígido e indeterminado.

(60) Un ejemplo de este entendimiento por la propia APD lo encontramos en la Memoria de 1995, en que se le planteó por parte del Instituto Nacional de Empleo de exhibir un listado de las personas que en una determinada localidad cobran prestaciones o subsidios, con el fin de controlar el fraude en el ámbito de las prestaciones por desempleo. La APD estimó que en un supuesto como éste no es de aplicación la normativa sobre acceso del art. 37 LRJAP-PAC, y por tanto, no existe ninguna Ley que autorice la publicación de esta información, siendo la publicación en consecuencia contraria a la Ley Orgánica.

En nuestro Derecho administrativo sí contamos con algunos preceptos legales que se refieren a aspectos parciales de la actividad administrativa, como los arts. 59.6 y 60 LRJAP-PAC, que habilitan genéricamente a la publicación en determinados supuestos, con la cláusula moderadora del art. 61 conforme a la cual si el órgano competente apreciase que la notificación por medio de anuncios o la publicación de un acto lesiona derechos o intereses legítimos, se limitará a publicar en el diario oficial que corresponda una somera indicación del contenido del acto y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para conocimiento del contenido íntegro del mencionado acto y constancia de tal conocimiento. Como puede apreciarse, esta previsión (referido sólo a la publicación de *actos* administrativos) manifiesta una preocupación por compatibilizar la necesaria difusión de los mismos y la protección de los derechos. A ello debe añadirse que, a la hora de elegir el medio de publicidad de los actos, incluso en los casos en que la norma procedimental la dote de la suficiente cobertura, habrán de tenerse en cuenta todas aquellas consideraciones que hemos venido poniendo de relieve, y que llaman a una ponderación caso por caso de los riesgos reales que un determinado tipo de publicidad puede generar, y las posibilidades de uso posterior incompatible con la finalidad misma de la publicidad o generador de riesgo para los derechos e intereses de los afectados (61). Lo mismo puede decirse del régimen de publicidad de determinadas sanciones, previsto en numerosas normas sectoriales estatales y autonómicas disponen la posibilidad de dar publicidad a las sanciones firmes, bien sea en tabloneros de anuncios, boletines oficiales o medios de comunicación, en casos de especial gravedad, en muy diversas materias como la salud humana o el medio ambiente, a la represión del narcotráfico o el blanqueo de capitales (62), o en materia de consumidores y usuarios (63). El cumplimiento de la mera cobertura legal exigida por la LOPD para la comunicación incontestada no excusa de la aplicación del resto de los principios de dicha norma, en especial, los de adecuación y proporcionalidad, y la prohibición de posterior tratamiento para fines incompatibles de aquéllos para los que los datos fueron recogidos (esto es, en este caso, sancionadores). En es-

(61) Piénsese, por ejemplo, en la publicación de datos personales, o el sólo nombre, de funcionarios de prisiones; o la publicidad por Internet sin clave de acceso de aprobados de una oposición que puede ser empleada sin posibilidad de control para fines comerciales, etc.).

(62) Así, p. ej., véase, en materia de espectáculos taurinos, el art. 21 de la Ley 10/1991, de 4 de abril, de potestades administrativas en espectáculos taurinos y el art. 96 del Real Decreto 145/1996, de 2 febrero, que lo desarrolla; el art. 8 del Reglamento del procedimiento sancionador de las infracciones en el ámbito de la Marina Civil establecidas en la Ley 27/1992, de 24 de noviembre, de Puertos del Estado y de la Marina Mercante...

(63) Art. 44.4 Ley del País Vasco; art. 70.3 Ley de Andalucía; art. 51.6 de la Ley de la Comunidad Valenciana; art. 58.4 Ley de Aragón; art. 52.1 Ley de Canarias; art. 49.2 Ley de Murcia; art. 23 de la Ley de Cataluña 1/1990, de 8 de enero, de Disciplina del mercado y Defensa de los Consumidores y Usuarios.

tos casos, a nuestro juicio, sí se justifica especialmente la necesaria cobertura legal, puesto que se trata de datos sensibles conforme a la normativa sobre protección de datos.

4.2. LOS DERECHOS DEL AFECTADO Y SU APLICACIÓN A LOS FICHEROS PÚBLICOS

Sólo atribuyendo al afectado una serie de derechos a ejercitar frente al responsable del fichero, y que consisten en obtener información sobre quién y para qué posee sus datos, y qué datos en concreto posee, puede hacerse efectivo el poder de control sobre los propios datos en que consiste el derecho. Y sólo pudiendo exigir de forma inmediata la rectificación y cancelación de los datos en caso de incumplimiento de los principios de finalidad, consentimiento y calidad (o, en su caso, si no se obtiene inmediata satisfacción, a través de la APD), puede hacerse real el derecho, lo que, por el contrario, difícilmente puede lograrse *a posteriori* a través de los mecanismos clásicos de control judiciales, por su lentitud, difícilmente pueden satisfacer. Estos derechos instrumentales del propio derecho a la protección de datos rigen respecto a cualquier tipo de datos. De nuevo, las excepciones las encontraremos principalmente en el campo de los ficheros públicos. No podemos extendernos en ellas en este trabajo (64), sino tan sólo reseñar como la regulación común del ejercicio de estos derechos es de clara inspiración administrativa, con la garantía del recurso a la autoridad de control en caso de denegación total o parcial, que, no obstante, tampoco se ha regulado con la claridad necesaria que despeje las dudas acerca de la ejecutividad de sus pronunciamientos. No obstante, entendemos, como hemos consignado, que los términos del art. 18.2, según el cual la Autoridad de control debe comprobar la procedencia o no de la denegación, regulándose con detalle el procedimiento en el RD 1332/1994, y previéndose la posibilidad de interponer recurso contencioso-administrativo contra sus resoluciones, hace notorio que se trata de una decisión administrativa ejecutiva a todos los efectos (que, en el caso de los ficheros públicos, actúa a modo de resolución de recurso administrativo).

Las especialidades del ejercicio de estos derechos respecto de los datos obrantes en ficheros públicos se encuentran reguladas en el art. 23 Se refiere al tratamiento con fines policiales y hacendísticos, que conectan con valores constitucionales, y goza de una cierta concreción, si bien presentan indefiniciones y flancos a la crítica (65). Junto a estas especialida-

(64) Nos remitimos, como para el resto de las cuestiones, a nuestra monografía, de pronta aparición.

(65) Lo que no resulta evidente de la regulación actual es: a) El motivo por el que, junto al derecho de acceso, se exceptiona el derecho de rectificación y cancelación, en la medida en que, respecto a datos de aportación obligatoria, éstos sólo pueden ejercerse si se conculcan los principios de la LOPD (calidad —incluida la pertinencia y la adecuación— finalidad). De lo contrario, el particular no podrá exigir su rectificación o cancelación. Si, por el contrario, no responden a dichos principios, di-

des sectoriales, el art. 24 LOPD preveía otras genéricas, que fueron declaradas inconstitucionales por la Sentencia 292/2000, de 30 de noviembre (66). Finalmente, cabe al menos reseñar que, en materia de responsabilidad por daños es de aplicación el régimen, procesal y material, de responsabilidad administrativa, como expresamente prevé el art. 19.1 LOPD (67).

4.3. GARANTÍAS INSTITUCIONALES Y ORGANIZATIVAS

La normativa de protección contiene, además, una serie de previsiones encaminadas a asegurar su cumplimiento. En concreto, la necesaria adopción por los responsables de los ficheros de medidas de seguridad,

fácilmente la cancelación puede causar perjuicio alguno a bienes públicos o a derechos y libertades de terceros. b) La necesidad o no de motivar la denegación del acceso, rectificación y cancelación, y la naturaleza de la intervención de la Autoridad independiente, ya que el art. 23 no se refiere a ella (en contraste con el art. 24.1, declarado inconstitucional, que sí especificaba que el responsable debía dictar resolución motivada, en caso de denegación del ejercicio de los derechos). A nuestro juicio, en tanto que acto desfavorable, habrá de ser motivado, si bien podrá serlo de una forma genérica, aludiendo precisamente a la concurrencia de uno de los supuestos del art. 23 LOPD y de una forma tal que no pueda suponer un peligro para la salvaguarda de los mismos. c) Por último, creemos que debe concederse un acceso parcial, siempre que no se frustren los objetivos que permiten limitar el derecho. Nos parece que la única solución coherente con la dogmática iusfundamental expuesta en el capítulo segundo, que, además, encaja sin problemas en la literalidad de la norma.

(66) El TC consideró que la previsión del art. 24.1 LOPD conforme a la cual el interesado se ve privado de su derecho a la información en la recogida de datos cuando impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas, es inconstitucional en lo que se refiere a «las funciones de control y verificación de las Administraciones públicas» y a la «persecución de infracciones administrativas». Argumenta que, teniendo en cuenta que la Administración ha de verificar en todas sus relaciones con los ciudadanos el cumplimiento por éstos de la normativa que las regule, la amplitud de la referencia a las «funciones de control y verificación» es tal que supone, en la práctica, una ausencia de regulación legal, dejando la efectividad del derecho a ser informado a la pura discrecionalidad de la Administración. Por su parte, el interés público en sancionar «infracciones administrativas» resulta insuficiente, al carecer de fundamento constitucional. En ambos casos, el TC parece afirmar rotundamente la incapacidad del principio de eficacia administrativa para constituirse en fundamento de la limitación de una de las facultades integrantes del derecho fundamental a la protección de datos, que, además, en el caso de los procedimientos sancionadores, puede llevar a una merma de las posibilidades de defensa del ciudadano. El TC, pese a poner el acento en el grado de necesaria determinación que debe contener la Ley limitadora del contenido del derecho, basa en realidad su control en la correspondencia de los fundamentos de las posibles restricciones al derecho con algunos de los bienes constitucionales que, en un aparente *numerus clausus* inspirado en el Derecho europeo, justifican la limitación del derecho a la protección de datos. Finalmente, el TC considera inconstitucional la habilitación legal por el art. 24.2 LOPD al órgano administrativo responsable del fichero para denegar los derechos de acceso, rectificación y cancelación de sus datos «ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección.» El TC considera que ambos preceptos atribuyen a la Administración un amplísimo a la hora de privar al ciudadano de las facultades (derechos de información, de acceso, de rectificación y cancelación) que integran el contenido del derecho, con la sola previsión legal de los objetivos, algunos de ellos sin fundamento directo constitucional en que puede ampararse.

(67) «Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.»

que garanticen el secreto y la integridad en el tratamiento de los datos; el establecimiento de un régimen sancionador por vulneración de sus determinaciones; y la creación de una Autoridad independiente encargada de vigilar la correcta observancia de la ley, dotada para ello de facultades de resolución de reclamaciones, inspectoras y sancionadoras, y encargada a un tiempo de la gestión de un Registro General de protección de datos, donde han de inscribirse todos los ficheros existentes. No podemos entrar en el detalle de esta regulación en un trabajo de esta envergadura, pero al menos creemos de interés resaltar las dos particularidades principales del régimen de los ficheros públicos en este ámbito.

El régimen de *creación de ficheros públicos* arbitrados por la LOPD consiste en el establecimiento de la obligación del responsable del fichero de aprobar por disposición general la creación de ficheros, con especificación de una serie de datos que permiten conocer sus características e identificar a sus responsables, y notificar al Registro la creación, modificación y cancelación de los ficheros públicos y privados, en vistas a su inscripción en el Registro. Algún autor ha estimado que para la aprobación de estas disposiciones es necesaria al menos una habilitación legal específica (68). No podemos compartir esta interpretación, que obligaría a la intervención legal para la creación de cualquier fichero (de nóminas, de alumnos, de control de accesos, etc.), y creemos que la regulación legal contenida en la LOPD actúa de cobertura suficiente. Un sistema distinto carecería de flexibilidad, y supondría, entre otros, negar la capacidad de crear ficheros en el ámbito local, o a las Universidades Públicas. Lo que sí debe cumplirse, evidentemente, es la conexión entre la finalidad del fichero y el ámbito de competencia del órgano administrativo responsable del mismo, competencia, ésta sí, que será de atribución legal. En cuanto al órgano competente para su aprobación, deberá contar consiguientemente con potestad reglamentaria. A ello debe añadirse que la inscripción de todos los ficheros, cualquiera sea su naturaleza, pública o privada, o entidad, puede advenirse un carga excesiva, máxime teniendo en cuenta la extensión a los ficheros manuales (sometida, respecto a los ya existentes a la entrada en vigor de la LOPD, a una prórroga hasta el 2007) (69). El deber de notificar cualquier fichero de nóminas, en una empresa familiar (en este caso, agravado por incluir datos sindicales a efectos de descuento de cuotas, con las consiguientes exigencias de seguridad); o de las propias fichas de alumnos, en una Universidad, parece a todas luces excesivo. El Derecho europeo permite eximir este deber cuando el

(68) LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993, p. 92.

(69) Disposición Adicional Primera.

riesgo sea reducido o cuando el responsable designe un encargado de la protección de datos, excepciones que han sido desarrolladas en el Derecho comparado, pero no así en el nuestro, lo que no impide constatar cómo el cumplimiento de esta obligación sigue siendo parcial, sobre todo, precisamente, respecto de los ficheros de menor «entidad».

En cuanto al régimen sancionador, ha de notarse que las Agencias no pueden imponer sanciones económicas por infracciones cometidas en ficheros públicos, sino sólo la intimación al cumplimiento y las medidas disciplinarias contra los responsables (personas físicas) del incumplimiento (70). La LOPD, como ya hiciera la LORTAD, ha querido excluir el fenómeno de las sanciones interadministrativas, entendiéndolo, al parecer, que carece de sentido un trasvase de fondos tal, cuando se hace con cargo a los ciudadanos, que son los que financian los presupuestos de las diferentes Administraciones públicas. Sin embargo, hay que advertir que el Derecho Administrativo conoce de este fenómeno, que tiene aplicación diaria (71), y que, en este caso la independencia funcional de las Agencias de control podría garantizar un correcto funcionamiento del sistema (72). Se plantea entonces cuál haya de ser el proceder de la Agencia cuando detecte una posible infracción y cuál sea el grado de vinculación que ejerce sobre el superior jerárquico del órgano responsable de la infracción de la instancia del Director de la Agencia a ejercer la potestad disciplinaria. Desde luego, se echa en falta una clarificación en un aspecto relevante como éste. Tampoco se regula si los requerimientos de cese del incumplimiento son de obligado acatamiento por el responsable del fichero, si bien una interpretación sistemática, la contemplación de los casos de negativa al cumplimiento como supuestos sancionables y la lógica de la propia institución de la Agencia parecen conducir a esta conclusión (73), ni siquiera si lo es una propuesta de inicio de procedimiento disciplinario, lo que nos parecería deseable, pero no creemos que pueda deducirse de la regulación legal. Tampoco se establece con claridad *cómo ha de ejercerse en estos casos la potestad disciplinaria*. Entendemos que el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de los agentes públicos de cada Administración (74).

(70) Art. 46 LOPD.

(71) Sobre el tema, véase VERA JURADO, D., «Las sanciones entre Administraciones públicas, en Infracciones, sanciones y procedimiento administrativo sancionador», *Justicia Administrativa*, Número extraordinario 2001, pp. 53-74.

(72) En este sentido, M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001, 508-509.

(73) En este sentido se manifiesta P. LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993, p. 150.

(74) Como dispone el apartado segundo del art. 46 LOPD.

Ahora bien, la cuestión más delicada es determinar si el elenco de infracciones es el genérico contemplado en dicha legislación, o el específico contenido en la LOPD. Creemos que la solución más conforme con el principio de tipicidad es ésta segunda. Una vez subsumido el incumplimiento en uno de los tipos de la LOPD, y determinada consiguientemente la gravedad del mismo, correspondería aplicar las sanciones previstas en la legislación de régimen disciplinario para faltas de dicha gravedad (75). Por último, una cuestión sin despejar es *cuál sea el régimen sancionador aplicable a los incumplimientos imputables a sujetos privados encargados de tratamientos en ficheros públicos*. Parece indudable que, en el supuesto de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, contemplado en el art. 12.4 LOPD, se le aplicará de lleno el régimen sancionador, ya que, como dice la Ley, en estos casos «será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente». Más polémico es qué ocurre cuando el incumplimiento es de otro género (p. ej., el incumplimiento de las medidas de seguridad). El art. 46 no es concluyente, en la medida en que se rotula «infracciones de las Administraciones públicas» pero refiere su régimen excepcional a las infracciones cometidas «en ficheros de los que sean responsables las Administraciones públicas». Creemos que la solución correcta debe ser la aplicación, también en este caso, del régimen sancionador, so pena de generar en estos casos un auténtico círculo de impunidad total, al no poder ejercerse la potestad disciplinaria.

Conclusión

El tratamiento de datos personales por la Administración pública plantea múltiples cuestiones irresueltas. La importancia del tema contrasta con la relativa escasa atención prestada por la doctrina administrativista (que, no obstante, comienza a volver hacia el mismo su atención), y con el injustificable descuido y desacierto de la legislación española, de extraordinaria parquedad e indefinición en temas claves como el propio concepto de dato personal o el sentido del principio de finalidad. Cierto es que se trata de cuestiones sobre las que el Derecho europeo y comparado se en-

(75) En este mismo sentido, M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001, p. 514. La Ley vasca 2/2004 prevé en su art. 24 que «el procedimiento y las sanciones a aplicar serán los establecidos en la legislación reguladora del régimen disciplinario de los funcionarios y personal al servicio de las administraciones públicas, instituciones y corporaciones a las que se refiere el artículo 2.1 de esta ley. *A estos efectos, las infracciones tipificadas en esta ley completarán el régimen disciplinario que sea de aplicación*» (la cursiva es nuestra).

cuentra aún en proceso de definición, pero forzoso es constatar que dicho proceso se encuentra más avanzado. Pese a haber sido una de las primeras Constituciones en hacer referencia (bien que imprecisa y parcial) a la relación entre informática y derechos fundamentales, el legislador español sólo ha cumplido el mandato constitucional con un gran retraso y a remolque de sus obligaciones comunitarias. El Tribunal Constitucional, por su parte, ha realizado un considerable esfuerzo por trazar una dogmática del derecho fundamental a la protección de datos, llevado por la necesidad de dibujar nítidamente su contenido, a falta de una definición constitucional, siquiera mínima. No obstante, el haberlo llevado a cabo a falta de una noción bien perfilada en la doctrina, su caracterización como derecho autónomo respecto del derecho a la intimidad, las supuestas notas diferenciales respecto de éste, y la complitud del contenido que le ha atribuido, plantean aspectos polémicos. La doctrina constitucional, en fin, está llamada muy probablemente a ser progresivamente perfilada. Frente a la Administración Pública, los principios, derechos y garantías del derecho a la protección de datos se encuentran fuertemente modalizados, lo que resulta coherente con la diferencia en los presupuestos de la acción administrativa respecto a la actividad económica de los sujetos privados (76).

(76) Como ha señalado un experto conocedor del tema, el profesor y Director de la Agencia de Protección de Datos de Madrid A. TRONCOSO REIGADA (en su «prólogo» al libro de FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas*, Civitas, 2003, Madrid): «El estatuto constitucional de la Administración Pública, incluido el estatuto de la función pública, suponen una garantía en razón del sujeto» (p. 33), constatando que «No hay reclamaciones abundantes frente a tratamientos de datos por la Administración pública» (p. 34), y que es necesaria una adaptación de los principios de la protección de datos para que sean compatibles con las funciones desarrolladas dentro de la reserva de Administración Pública (p. 36). «Se puede concluir que existe un mayor derecho fundamental a la protección de datos de carácter personal frente a ficheros privados; en cambio, existe un menor derecho fundamental a la protección de datos de carácter personal frente a los ficheros públicos, ya que en este caso es necesario hacer un *balancing* constitucional entre este derecho y la vertiente objetiva de otros derechos fundamentales. O dicho al revés, existe una mayor vinculación de los particulares —de los responsables privados— al derecho a la autodeterminación informativa y una menor vinculación a este derecho fundamental de los poderes públicos.» (p. 45).