La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional[1]

Antonio Troncoso Reigada
Profesor Titular de Derecho Constitucional
Director de la APDCM

SUMARIO 1. La configuración constitucional de un derecho fundamental a la protección de datos personales y su desarrollo por el legislador: a) *El reconocimiento de este derecho fundamental en las Constituciones de los países europeos.* b) *El Convenio 108, de 28 de enero de 1981, del Consejo de Europa y la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995.* c) *El artículo 18.4 de la Constitución española.* d) *El desarrollo legislativo: la LORTAD y la LOPD.*— 2. El Tribunal Constitucional en la definición del contenido del derecho fundamental a la protección de datos personales: análisis crítico de la jurisprudencia constitucional: a) *Criterios de interpretación constitucional del artículo 18.4.* b) *La definición del contenido del derecho fundamental a la protección de datos personales a través de la resolución de recursos de amparo.* c) *La definición del contenido del derecho fundamental a la protección de datos personales a través de la resolución de recursos de inconstitucionalidad.*—3. Reflexión final.

---

[1] Este artículo es una primera versión de un trabajo más amplio sobre *El derecho fundamental a la protección de datos personales en las Administraciones Públicas,* que espero poder publicar el próximo año. Sus conclusiones están todavía sometidas a revisión y me remito desde este momento al texto definitivo. En cualquier caso, deseo aclarar que estas páginas están escritas para un público universitario y desde una vertiente académica, que tiene que ser necesariamente crítica y que debe estudiar la *constitutione lata* y las propuestas de *lege ferenda*. Por ello, las objeciones que se plantean a la legislación y a la jurisprudencia constitucional —especialmente en el *apartado 2.c)*— no reflejan, como es lógico, el parecer de la Agencia de Protección de Datos de la Comunidad de Madrid, sino el mío propio. Para conocer la posición de la Agencia, que actúa siempre con estricto sometimiento al ordenamiento jurídico y a la jurisprudencia en este ámbito, me remito a las Memorias anuales, a los informes jurídicos y a las consultas, así como a los proyectos de disposiciones que afectan a la protección de datos, a la resolución de los procedimientos de inspección y de tutela de derechos y a las distintas Recomendaciones.

1. LA CONFIGURACIÓN CONSTITUCIONAL DE UN DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES Y SU DESARROLLO POR EL LEGISLADOR

En las últimas décadas se ha producido un intenso desarrollo de las tecnologías de la información tanto en la sociedad como en la Administración Pública[2]. Los modernos sistemas de información y comunicación han permitido mejorar el funcionamiento de los mercados, al mismo tiempo que su utilización por parte de los poderes públicos ha mejorado la actividad administrativa, incrementando la satisfacción de los ciudadanos por los servicios públicos que reciben y materializando de esta forma el principio constitucional de eficacia administrativa —art. 103.1 CE—[3].

No obstante, este desarrollo de las tecnologías de la información presenta también algunos aspectos de incertidumbre y riesgo. Son distintos los derechos fundamentales que pueden verse amenazados o vulnerados por un uso indebido de las tecnologías de la información. Especialmente, existe el peligro de que las tecnologías de la información entren en conflicto con el derecho a la intimidad. Como ya hemos señalado en alguna otra ocasión, la informática facilita ilimitadas posibilidades para recoger datos personales, tratarlos, conservarlos y transmitirlos. La tecnología es capaz de mover un gran volumen de información y de ponerla en relación, de manera que se construyan perfiles de nuestra personalidad, que pueden llegar a justificar decisiones públicas o privadas y que puedan limitar nuestra libertad o condicionar nuestro modo de actuar. A través de tratamientos de datos se puede llegar a saber si tengo una enfermedad grave, si estoy afiliado a un sindicato, si tengo algún hijo con alguna minusvalía, cuál es mi nivel de renta, mi situación familiar o mis hábitos de conducta[4].

---

[2] Existe un conjunto de trabajos interesantes que abordan el estudio de la sociedad de la información desde la sociología o la ciencia política. Cfr., especialmente, J. B. TERCEIRO, *Sociedad digital. Del homo sapiens al homo digitalis,* Alianza Editorial, Madrid, 1996, págs. 179-193; J. B. TERCEIRO y G. MATÍAS, *Digitalismo. El nuevo horizonte sociocultural*, Taurus, Madrid, 2001, págs. 115-122. Uno de los autores más citados es CASTELLS, por su pretensión enciclopédica, a pesar de los déficits de su método periodístico. Cfr. M. CASTELLS, *La sociedad red, El poder de la identidad* y *El fin del milenio*, que componen la trilogía sobre *La era de la información*, Alianza Editorial, Madrid, 1997 y 1998, págs. 35-43, págs. 457-467, págs. 377-431, respectivamente. Más interés tiene M. CASTELLS, *La galaxia Internet*, Debolsillo, Barcelona, 2001, págs. 217-239. Entre nosotros, cfr. S. MUÑOZ MACHADO, *La regulación de la red. Poder y derecho en Internet*, Taurus, Madrid, 2000, págs. 151-186.

[3] Cfr. AA.VV., *Administración electrónica y procedimiento administrativo,* Ministerio de Economía, 2004, esp. págs. 73-89; AA.VV., *Libro blanco para la mejora de los servicios públicos. Una nueva Administración al servicio de los ciudadanos,* MAP, Madrid, 2000; AA.VV., *Las Tecnologías de la Información en las Administraciones Públicas,* MAP, Madrid, 2000; J. VALERO, *El régimen jurídico de la e-Administración*, Comares, Granada, 2004, esp. págs. 1-14; L. PAREJO, *Eficacia y Administración. Tres estudios*, Madrid, INAP, 1995; J. CHIAS, *Marketing Público. Por un Gobierno y una Administración al servicio del público*, McGraw-Hill, Madrid, 1995, págs. 31-48. Cfr. *Informatization developments and the public sector*, IOS, Washington DC, págs. 49-81.

[4] Cfr., más ampliamente, A. TRONCOSO REIGADA, «Introducción», en *Manual de Protección de Datos para las Administraciones Públicas*, Civitas-APDCM, Madrid, 2003, págs. 5-9.

a) *El reconocimiento de este derecho fundamental en las Constituciones de los países europeos*

Con anterioridad al establecimiento de un derecho específico a la protección de datos de carácter personal, la tutela de este bien jurídico tenía que ser desarrollada a través de la invocación de un derecho más amplio a la intimidad y a la privacidad personal, recogido en los textos internacionales y constitucionales. Así, la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948, proclama en el artículo 12 que «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques»[5]. El Convenio de Roma, de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales tiene la virtud de ser el primer texto europeo que consagra la tutela de la vida privada, afirmando en su artículo 8: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencias de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por 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». El contenido efectivo de este precepto ha sido precisado a través de la jurisprudencia del Tribunal Europeo de Derechos Humanos[6]. Nuestro Tribunal Constitucional ha tenido en cuenta frecuentemente la normativa emanada del Consejo de Europa y la jurisprudencia del Tribunal de Estrasburgo, a partir de la cláusula del artículo 10.2 CE.

En nuestro país, la Constitución española de 1978 reconoce en el artículo 18 el derecho al honor, a la intimidad personal y familiar, a la propia imagen, el derecho a la inviolabilidad del domicilio y al secreto de las comunicaciones. El principal desarrollo legislativo que se ha producido hasta ahora del derecho a la intimidad, reconocido en el artículo 18.1 de la Constitución, ha sido 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. Esta Ley, básicamente, desarrolla el contenido de este derecho como límite a la libertad de expresión y al derecho a la información, en los términos previstos en el artículo 20.4 CE. La principal doctrina y jurisprudencia constitucional so-

---

[5] Con posterioridad se ha aprobado la Resolución 45/1995 de la Asamblea General de las Naciones Unidas, donde se recogen los Principios Rectores aplicables a los Ficheros Computarizados de Datos Personales.

[6] Cfr. C. Ruiz Miguel, *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos,* Civitas, Madrid, 1994; A. Queralt Jiménez, *El Tribunal de Estrasburgo: una jusrisdicción internacional para la protección de los derechos fundamentales,* Tirant lo Blanch, Valencia, 2003, págs. 71-122.

bre el derecho a la intimidad ha tratado sobre todo de deslindar estos dos derechos enfrentados[7].

La Constitución portuguesa de 1976 y la Constitución española de 1978 fueron las primeras en hacer una referencia específica a la protección de datos personales en sus textos. La Constitución portuguesa de 1976 afirma, por un lado, de manera más genérica en el artículo 26.2, que «[l]a ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones referentes a las personas y a las familias»[8]. Pero, por otro lado, dedica un precepto expreso a esta cuestión, el artículo 35, que señala: «1. Todo ciudadano tendrá derecho a tener conocimiento de lo que conste en forma de registros informáticos acerca de él y de la finalidad a que se destinan esos datos, y podrá exigir su rectificación, así como su actualización, sin perjuicio de lo dispuesto en la ley sobre secretos de Estado y secreto de actuaciones judiciales. 2. Se prohíbe el acceso a ficheros y registros informáticos para el conocimiento de datos personales referentes a terceros y la respectiva interconexión, salvo en casos excepcionales previstos por ley. 3. No podrá utilizarse la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliación a partidos o a sindicatos, fe religiosa o vida privada, salvo cuando se trata del tratamiento de datos estadísticos no identificables individualmente. 4. La ley definirá el concepto de datos personales para fines de registro informático, así como de bases y bancos de datos y las respectivas condiciones de acceso, constitución y utilización por entes públicos y privados. 5. Se prohíbe la asignación de un número nacional único a los ciudadanos. 6. La Ley determinará el régimen aplicable a los flujos de datos allende las fronteras, estableciendo formas adecuadas de protección de los datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional»[9].

---

[7] Cfr. SSTTC 117/1994, 231/1998, 76/1990; C. RUIZ MIGUEL, *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995; F. HERRERO-TEJEDOR, *Honor, intimidad y propia imagen*, Colex, Madrid, 1984; P. A. MUNAR, «Derecho a la intimidad», *en Enciclopedia Jurídica Básica*, Civitas, Madrid, 1995, III, págs. 3725-3728; J. VIDAL MARTÍNEZ, *El derecho a la intimidad en la Ley Orgánica de 5 de mayo de 1982*, Madrid, 1984; L. M. FARIÑAS MANTONI, *El derecho a la intimidad,* Madrid, 1983; D. ORTEGA, *Derecho a la información versus derecho al honor*, CEPC, Madrid, 1999.

[8] Cfr. J. J. GOMES CANOTILHO, *Dereito Constitucional*, Almedina, Coimbra, 1996, pág. 665. GOMES CANOTILHO habla de un nuevo peligro para los ciudadanos, «la digitalización de los derechos fundamentales». Frente a él afirma la existencia de un derecho fundamental a la autodeterminación informativa que se traduce, fundamentalmente, en la facultad de un particular de determinar y controlar la utilización de sus datos personales. Este autor cita también el derecho de *habeas data*, consagrado en la Constitución brasileña de 1988. Cfr., más ampliamente, A. EIRAS, *Segredo de justica e controlo de dados pessoais informatizados*, Almedina, Coimbra, 1992.

[9] En su primera redacción, la Constitución portuguesa de 1976 había incluido un artículo 35 que afirmaba: «1) Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones, y podrán exigir la rectificación de los datos, así como su actualización; 2) No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos, y 3) Se prohíbe atribuir un número nacional único a los ciudadanos». Con posterioridad a 1976, este artículo 35 ha recibido distintas reformas constitucionales. En 1982 se añadió un nuevo apartado que señalaba: «La Ley definirá el concepto de datos personales para fines de registro informático, así como de bases y bancos de datos y las respectivas condiciones de acceso, constitución y utilización por entes públicos y privados». La reforma de 1989 añade

Más recientemente, las reformas de las Constituciones en los países europeos están incluyendo preceptos que garantizan la protección de los datos personales. Así, la Ley Fundamental del Reino de los Países Bajos, revisada en 1983, ha señalado que «[l]a ley establecerá las normas de protección de la intimidad personal en relación con la indagación y difusión de datos personales» —art. 10.2— y que «[l]a ley dictará normas sobre el derecho de toda persona a que se le dé conocimiento de los datos recogidos sobre ella y del uso que se hiciere de los mismos, así como al perfeccionamiento de dichos datos» —art. 10.3—. La Constitución de Finlandia de 1919 —a partir de la reforma de 1980— señala —art. 8— que «[l]a ley establecerá normas de detalle sobre la salvaguardia de los datos de carácter personal». La Constitución de Suecia de 1994 afirma en el artículo 3 que «[t]odo ciudadano quedará protegido, en la medida que se disponga en detalle por la ley, contra la violación de la integridad de su persona resultante del registro de información sobre él mediante tratamiento electrónico de datos». En cambio, Bélgica, con un texto refundido de 1994 de la Constitución originaria de 1831, sigue limitándose en el artículo 22 a afirmar que «[t]odos tendrán derecho al respeto de su vida privada y familiar, excepto en los casos y en las condiciones que establezca la ley»[10].

Otros países como Italia y Alemania, cuyas Constituciones en vigor fueron aprobadas después de la II Guerra Mundial, y que, por ello, no podían prever el fenómeno de la informática, han configurado un derecho a la protección de datos personales a partir de la interpretación constitucional de otros preceptos desarrollada por sus Tribunales Constitucionales. Además, ambos países carecían de un reconocimiento constitucional del derecho a la intimidad. Así, la doctrina italiana ha analizado el *diritto a la riservatezza* como un componente de la propia libertad personal[11]. Así se ha calificado la

---

un nuevo inciso al primer apartado del precepto con el siguiente contenido: «... sin perjuicio de lo dispuesto en la ley sobre secretos de Estado y secreto de actuaciones judiciales»; y un nuevo apartado segundo que reestructura el orden del precepto: «Se prohíbe el acceso a ficheros y registros informáticos para el conocimiento de datos personales referentes a terceros y la respectiva interconexión, salvo en casos excepcionales previstos por la ley».

[10] Los últimos textos constitucionales de los países europeos se pueden ver en G. GÓMEZ ORFANEL, *Las Constituciones de los Estados de la Unión Europea*, CEC, Madrid, 1996.

[11] La Constitución italiana no reconoce un derecho a la intimidad —«a ser dejado solo»—. Por ello, entre los autores italianos existen dudas sobre la tutela constitucional de la *riservatezza*. Unos lo afirman a partir de la interpretación de distintos preceptos constitucionales —secreto de la correspondencia, inviolabilidad del domicilio—; otros lo califican como un principio no escrito; por último, otros autores lo consideran una consecuencia de los derechos de libertad personal. La doctrina clásica está explicada en A. PIZZORUSSO, «Sul diritto alla riservatezza nella Constituzione italiana», *Prassi e teoria*, 1976. Para MARTINES, la Constitución italiana contiene dos principios, estrechamente unidos, que pueden valer para la tutela de la privacidad: la garantía de los derechos inviolables de la persona, ya como individuo, ya en las formaciones sociales donde se desarrolla su personalidad —art. 2 CI—, y el pleno desarrollo de la persona humana —art. 3 CI—. Cfr. T. MARTINES, *Diritto Costituzionale*, Giuffrè, Milano, 1990, págs. 709-712 y 689. En todo caso, este autor sitúa la protección de datos dentro del derecho a la intimidad: «Nella c.d. società tecnologica in cui viviano, esistono invece strumenti che non consentono all'uomo di godere appieno della propria sfera di intimità. Il telefono, la radio, la televisione, i mass media in genere, gli elaboratori ed i *congegni elettronici —archivi elettronici—* le sofisticate apparecchiature fotografiche sono altrettanti strumenti per mezzo dei quali l'intimità può essere penetrata e violata. […] Se riflettiamo sui modi in cui la sfera privata dell'individuo può essere compressa e violata nelle moderne società di massa —e si

posición de los individuos frente a los tratamientos automatizados de datos personales como un tipo de libertad, como un auténtico derecho de defensa del ciudadano frente a las tecnologías de la información[12]. Se habla así de «libertad informática» como una nueva clase de libertad personal, incardinada dentro del derecho de libertad reconocido en el artículo 13 de la Constitución italiana y que puede ser definida como la facultad de la persona para controlar las informaciones que sobre ella se almacenan en un ordenador, lo que implica el acceso, la rectificación y la cancelación de esta información. Si la libertad personal tradicional es el derecho a disponer libremente del propio cuerpo, la libertad informática no es ya una libertad física, sino moral, que evita que se condicione la actuación de la persona a través de la información que otros tengan sobre ella. Esta libertad informática, como todas las libertades, trata de garantizar al ciudadano un espacio para la libre actuación. Así, si la institución del *habeas corpus* surgió en el Derecho anglosajón como garantía de la libertad personal, de su integridad física —«tener el propio cuerpo»—, se habla de un *habeas data* como un conjunto de instrumentos procesales —acceso, rectificación y cancelación— que garantiza que la persona dispone de un control sobre sus datos personales y, por tanto, una protección sobre su identidad personal. Otros autores han entendido que este derecho fundamental a la protección de datos personales está vinculado no sólo a los derechos de libertad, sino a todos los derechos fundamentales. Por ello, se ha acudido al artículo 2 de la Constitución italiana, que alude a los derechos inviolables y al desarrollo de la personalidad. Este artículo 2 ha sido considerado por la jurisprudencia constitucional italiana como una cláusula abierta —*open clause*—, un valor que permite la tutela de intereses jurídicos y de derechos subjetivos que no han tenido acogida expresa en el texto constitucional[13].

---

pensi soltando alle banche dei dati utilizzate dai poteri pubblici e privati—, allora dobbiamo constatare che non esistono se non deboli barriere a difusa dell'intimità».

[12] Un autor clásico al respecto en la doctrina italiana es Vittorio FROSINI. Cfr. V. FROSINI, *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981; íd., «Banco de datos y tutela de la persona», *REP*, n.º 30, 1982; íd., «Los derechos humanos en la era tecnológica», en A. E. PÉREZ LUÑO, *Derechos humanos y constitucionalismo ante el tercer milenio,* Marcial Pons, Madrid, 1996; AA.VV., *Il diritto alla riservatezza in Italia e in Francia*, Padova, 1988. Cfr., más recientemente, G. P. CIRILLO, *La tutela della privacy nel sistema del nuevo codice sulla protezione dei dati personali*, Cedam, Padova, 2004, especialmente lo relativo a la tutela administrativa, págs. 130-170.

[13] Merece destacarse especialmente la posición de ARENA, de defensa de la integridad personal en un sentido dinámico, como sujeto activo y partícipe de la vida de la sociedad. Este autor vincula el derecho a la protección de datos *(riservatezza)* como un instrumento de autonomía, entendiendo ésta «no solamente en el sentido tradicional que se ha dado hasta tiempos recientes al término *privacy*, esto es, como clausura de cada individuo en sí mismo, sino también en sentido relacional, esto es, como posibilidad de relaciones entre sujetos, cada uno de los cuales, a pesar de estar inserto en una densísima red de comunicaciones, puede sin embargo continuar siendo él mismo y desarrollar su propia personalidad gracias a las protecciones ofrecidas a su esfera privada; y por tanto, en tal modo, la tutela de los datos deviene condición para la existencia misma de una sociedad de la comunicación basada en intercambios de pensamientos potencialmente originales, en cualquier caso no todos uniformes y homogéneos». Cfr. G. ARENA, «La tutela de la riservatezza nella società dell'informazione», en *Scritti in onore di Pietro Virga*, t. I, Giuffrè, Milano, 1994, págs. 92-93. Esta última cita la tomamos de M. FERNÁNDEZ SALMERÓN, *op. cit.* Cfr. el interesante estudio doctrinal que lleva a cabo este autor en *La protección de los datos personales en las Administraciones Públicas*, Civitas, Madrid, 2003, págs. 51-68.

La elaboración en Alemania de una construcción doctrinal para sustentar el nuevo derecho a la protección de datos personales ha encontrado, como en el caso italiano, la dificultad de carecer de un precepto constitucional expreso que reconociera no sólo un derecho fundamental a la protección de datos personales, sino un derecho fundamental a la intimidad[14]. Por ello, la doctrina alemana ha optado por ubicar este nuevo derecho fundamental a la protección de datos personales dentro del reconocimiento constitucional de la dignidad de la persona —art. 1.1— y del libre desarrollo de la personalidad —art. 2.1 *Persönlichkeitsrecht*—[15]. El Tribunal Constitucional Federal alemán construyó toda su argumentación sobre el derecho general de la personalidad y la dignidad de la persona, afirmando que en «la clave de bóveda del ordenamiento de la Ley Fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre», y a cuya protección se encamina este derecho de la personalidad[16]. La jurisprudencia alemana afirma las limitaciones del derecho a la intimidad para tutelar a la persona frente a las tecnologías de la información y ha optado por volver al propio principio del libre desarrollo de la personalidad, donde nacen tanto el derecho a la intimidad como el derecho a la autodeterminación informativa[17]. De esta forma, el Tribunal Constitucional Fe-

---

[14] El autor de referencia es K. VOGELSANG, *Grundrechte auf informationelle Selbtsbestimmung*, Baden-Baden, 1987. Una reflexión más breve y sencilla, en T. MAUNZ y R. ZIPPELIUS, *Deutsches Staatsrecht*, 29.ª ed, C. H. Beck, München, 1994, págs. 167-168. Cfr. H. HORSTKOTTE, *La protección de datos en Alemania*, Internationes, Bonn, 2001. Cfr., entre nosotros, R. MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, Civitas, Madrid, 2004, págs. 237-244; A. PÉREZ LUÑO, «Libertad informática y derecho a la autodeterminación informativa», en *I Congreso sobre Derecho Informático*, Facultad de Derecho de la Universidad de Zaragoza, 1989, págs. 359-375.

[15] El artículo 1.1 señala: «1. La dignidad del ser humano es inviolable y es obligación de todos los poderes estatales respetarla y protegerla». El artículo 2.1 dice: «1. Todos tienen derecho al libre desarrollo de su personalidad, en tanto en cuanto no lesione los derechos ajenos y no contravenga el orden constitucional o las buenas costumbres».

[16] BENDA señala que la afirmación de la dignidad de la persona contempla al individuo estáticamente «tal cual es» y la afirmación del libre desarrollo de la personalidad «tal cual actúa». Cfr. E. BENDA, «Dignidad humana y derechos de la personalidad», en A. LÓPEZ PINA (coord.), *Manual de Derecho Constitucional,* Marcial Pons-IVAP, Madrid, 1996, pág. 123. La concepción abierta y dinámica del libre desarrollo de la personalidad ha permitido, para PÉREZ LUÑO, «ir incorporando al sistema de los derechos fundamentales y, consiguientemente, a su esfera de tutela, aquellas necesidades y exigencias que se han manifestado más relevantes en el devenir de la experiencia constitucional alemana. Existe, por tanto, una arraigada actitud metodológica, en la dogmática germana de los derechos fundamentales, que se muestra más proclive a ampliar sucesivamente la incidencia de determinados valores constitucionales, como la dignidad humana y el libre desarrollo de la personalidad, que a multiplicar, por vía jurisprudencial, derechos no expresamente reconocidos en la *Grundgesetz*». Cfr. A. PÉREZ LUÑO, «El derecho a la autodeterminación informativa», en *II Jornadas de Estudio sobre Protección de Datos y Derechos Fundamentales. Anuario de Jornadas*, Servicios de Estudios del IVAP, Oñati, 1991, pág. 323.

[17] Cfr. E. DENNINGER, «El derecho a la autodeterminación informativa», en *Problemas actuales de la documentación y la informática jurídica*, Tecnos, 1987, pág. 273. Para este autor, ni el objeto ni la denominación del derecho a la autodeterminación informativa pueden considerarse como un invento del Tribunal Constitucional Federal alemán. En lo que atañe al objeto, porque se trata del resultado de una larga evolución jurisprudencial dirigida al reconocimiento y elaboración del derecho general de la personalidad; y en lo tocante a la terminología, porque esta expresión había sido utilizada por la doctrina jurídica alemana a partir del año 1971. Cfr. también A. E. PÉREZ LUÑO, «La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo», en *Anuario de Derechos Humanos*, n.º 4, 1986-1987, pág. 264. La discusión tanto en Alemania como en Italia se encuentra muy bien analizada en M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, 2003, págs. 33-72.

deral alemán ha establecido las bases del derecho a la autodeterminación informativa —*informationelle Selbstbestimmungsrecht*—, que fue proclamado en la Sentencia, de 15 de diciembre de 1983, que declaraba inconstitucionales algunos preceptos de la Ley del Censo, de 4 de marzo de 1982[18]. Este derecho trata de proteger el ámbito de la personalidad que asegure al individuo su plena libertad y capacidad de decisión frente al abuso de quien maneja bases de datos personales.

b) *El Convenio 108, de 28 de enero de 1981, del Consejo de Europa y la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995*

Al reconocimiento de este derecho han contribuido, sin duda, la normativa del Consejo de Europa y el Derecho de la Unión Europea. Especial mención merece el Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, los principios de los derechos y libertades[19]. Como es sabido, este Convenio, como el resto de los Tratados inter-

---

[18] Esta Sentencia se puede ver en *BJC,* n.º 33, enero de 1984, págs. 126-170. Véase M. HEREDERO HIGUERAS, «La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983», *Documentación Administrativa*, n.º 198, 1983, págs. 139-158. Cfr. los comentarios a esta Sentencia de P. LUCAS MURILLO, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990, págs. 122-123; L. REBOLLO DELGADO, «Derechos de la personalidad y datos personales», *Revista de Derecho Político,* n.º 44, 1998, págs. 161-162; A. E. PÉREZ LUÑO, «Libertad informática y derecho a la autodeterminación informativa», en *I Congreso sobre Derecho Informático,* Universidad de Zaragoza, 1989, págs. 359-375; íd., «La defensa del ciudadano y la protección de datos», *Revista Vasca de Administración Pública,* n.º 14, 1986, págs. 44-47.

[19] El desarrollo de la informática en todos los países europeos exigía una normativa que facilitara el intercambio de datos y las relaciones institucionales y comerciales entre los distintos países, evitando los paraísos de datos. Por ello, el Consejo de Europa trabajó a través de un conjunto de Resoluciones para proteger los derechos de las personas frente a la amenaza de la informática. Así, en primer lugar aprobó en 1968 la Resolución 509 de la Asamblea del Consejo, sobre «los derechos humanos y los nuevos logros científicos y técnicos». El Comité de Ministros del Consejo de Europa estableció una Comisión de Expertos con la finalidad de alumbrar una serie de proyectos orientados a la tutela de las libertades ante el desarrollo tecnológico. Los resultados de estas reuniones culminaron en 1973 y 1974, con la elaboración de dos Resoluciones del Comité de Ministros del Consejo de Europa: la Resolución (73) 22, de 26 de septiembre, relativa a la «protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado», y la Resolución (74) 29, de 20 de septiembre, respecto a «la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público». Estas dos Resoluciones afirman ya principios que se encuentran vigentes en la actualidad, como el de calidad de los datos, información sobre la finalidad, seguridad de los datos, derecho de acceso y cancelación, etc. Estas resoluciones, sin ser textos jurídicos vinculantes —como el Convenio 108 del Consejo de Europa—, constituyen los primeros textos a nivel internacional que contienen directrices dirigidas a los Estados, lo que influyó decisivamente en la legislación de esa época y permitió inicialmente la armonización paulatina y flexible de los textos legales europeos sobre protección de datos. Sin embargo, el Comité de Ministros del Consejo de Europa fue pronto consciente de la necesidad de tener un texto jurídico vinculante para los Estados, con un carácter más amplio. Por ello, en la Resolución (76) 3 encarga a un nuevo Comité de Expertos en protección de datos el inicio de los trabajos preparatorios para la elaboración de un Convenio. Se aprueba así el 28 de enero de 1981 el primer texto a nivel europeo regulador de la materia, el Convenio 108, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que entra en vigor el 1 de octubre de 1985, tres meses después de la ratificación del quinto país europeo, Alemania. Cfr., especialmente, M. HEREDERO HIGUERAS —que fue uno de los intervi-

nacionales, tiene una doble funcionalidad: por una parte, es una norma incorporada al Derecho español por la vía prevista en el artículo 96 CE; por otra, sirve como criterio de interpretación de los derechos fundamentales a la luz de lo dispuesto por el artículo 10.2 CE. La Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, que es la primera que reconoce un derecho fundamental autónomo en el artículo 18.4 CE, fue ocasión para un debate doctrinal sobre el Convenio 108 del Consejo de Europa y su aplicación directa sin desarrollo legislativo previo[20].

En el ámbito de la Unión Europea hay que destacar la Directiva

---

nientes en su preparación en representación de España—, «Ante la ratificación del Convenio de protección de datos del Consejo de Europa», *Documentación Administrativa*, n.º 199, 1983, págs. 753-764; A. A. SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática*, Universidad de Sevilla, Sevilla, 1998, pág. 78; A. E. PÉREZ LUÑO, «La incorporación del Convenio europeo sobre protección de datos personales al ordenamiento jurídico español», *ICADE. Revista de las Facultades de Derecho y Ciencias Económicas*, Madrid, 1989, pág. 28-29; G. GARZÓN CLARIANA, «La protección de los datos personales y la función normativa del Consejo de Europa», *Revista de Instituciones Europeas*, n.º 1, 1981, págs. 9 a 25. Cfr., más ampliamente, M. SERRANO, *El derecho fundamental a la protección de datos*, cit., págs. 89-93.

[20] El Magistrado Rodríguez-Piñeiro y Bravo-Ferrer, en su voto particular a esta Sentencia, afirma que la estimación del recurso de amparo supone la utilización del Convenio 108 del Consejo de Europa no como un elemento de interpretación de la Constitución a través de Tratados internacionales, lo que permite el artículo 10.2 CE, sino la integración de este Convenio dentro del ordenamiento jurídico interno, como auténtico canon de constitucionalidad de las leyes. En este caso, lo que sucede es «que el Convenio no se utiliza meramente, frente a lo que se dice, como una fuente interpretativa que contribuye a la mejor interpretación del contenido de los derechos [STC 64/1991, fundamento jurídico 4.º.a)], sino como un elemento de integración ante la demora del desarrollo legislativo del precepto constitucional». Para este Magistrado, el Convenio «no puede implicar un efecto directo e inmediato que obligue a los poderes públicos a su ejecución prescindiendo de la necesaria intermediación legislativa, como efectivamente ha hecho la Ley Orgánica 5/1992, de 29 de octubre. A partir de este momento, los derechos reconocidos en dicha Ley, en cuanto desarrollo del derecho a la intimidad, pueden ser objeto de tutela y protección a través del recurso de amparo, pero no antes, por lo que legítimamente el órgano judicial pudo confirmar el acto denegatorio de la Administración».

Es indudable que los Tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, forman parte del ordenamiento jurídico interno —art. 96.1 CE—, sin necesidad de *interpositio legislatoris*. No hay que olvidar, en todo caso, que el propio artículo 4 del Convenio 108 recoge un compromiso de los Estados miembros de adaptación de la normativa interna al mismo, sin perjuicio de exigir la aplicación directa de sus preceptos y principios. Cfr. J. BERMEJO VERA, «Premisas jurídicas de la intimidad personal y de la protección de datos en el derecho español», en R. GÓMEZ-FERRER MORANT, *Libro homenaje al Profesor José Luis Villar Palasí,* Civitas, Madrid, 1989, pág. 160. También SERRANO ALBERCA mantiene la aplicación directa de los derechos reconocidos en el Convenio sin desarrollo legislativo. Cfr. J. M. SERRANO ALBERCA, «Comentario al artículo 18 de la Constitución», en M. GARRIDO FALLA, *Comentarios a la Constitución,* Civitas, Madrid, 1985, págs. 380-381. RUIZ MIGUEL señala que los preceptos constitucionales que reconozcan derechos fundamentales se interpretarán de forma que *no sólo* sea conforme con las demás normas constitucionales, *sino también* con esos convenios internacionales, de suerte que si existiera una interpretación de estas normas conforme con los demás preceptos constitucionales, pero disconforme con esos convenios, dicha interpretación deberá ser rechazada en beneficio de otra que también sea conforme con esos tratados. Los convenios no permiten una interpretación *contra constitutionem.* Cfr. C. RUIZ MIGUEL, *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Civitas, Madrid, 1994. Lógicamente, esta posición no permite atribuir rango constitucional al Convenio 108, para justificar un recurso de amparo al Tribunal Constitucional. No obstante, la propia doctrina del contenido esencial de los derechos fundamentales, establecida por el Tribunal Constitucional en la Sentencia 11/1981, de 8 de abril, puede servir para definir el contenido constitucional del artículo 18.4 a partir de los intereses jurídicos dignos de protección —en este caso el derecho de acceso—, que en caso contrario quedarían desprotegidos, y del tipo abstracto o de la noción comúnmente admitida de lo que un derecho significa, que puede ser establecida a partir del contenido del propio Convenio 108 del Consejo de Europa. No creemos que la única facultad que se deriva del artículo 18.4 CE sea el derecho de oposición al tratamiento de datos que, según el Magistrado, se extraería del artículo 18.1 CE.

95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[21]. Con anterioridad a la aprobación de la Directiva 95/46/CE, muchos países europeos habían ido progresivamente aprobando leyes de protección de datos teniendo en cuenta lo fijado en el Convenio 108 del Consejo de Europa[22]. Sin embargo, la Unión Europea, que se apoya en la libre circulación económica dentro de los países miembros y, por tanto, en la libre circulación de los datos, demanda una protección igual de este derecho fundamental en los países de la Unión, lo que no era posible con la sola aplicación del Convenio 108[23]. Esto es así especialmente después del reforzamiento de la cooperación en asuntos de justicia e interior, que ha llevado a la celebración de distintos acuerdos entre los Estados miembros, como el Convenio de *Schengen* —causa motora principal de la LORTAD—, y que obliga a la transmisión de datos personales entre las Administraciones de los Estados miembros[24]. Se hizo necesaria la aprobación de la primera norma comunitaria en esta materia, la Directiva 95/46/CE, que tuvo una intensa tramitación, con el doble objetivo de tutelar la intimidad a la vez que se garantiza el mercado interior y la libre circulación de datos personales entre los Estados miembros.

Con posterioridad, la normativa comunitaria sobre las telecomunicaciones y sobre la sociedad de la información ha hecho mención expresa a la necesidad de respetar en las comunicaciones electrónicas y en el comercio electrónico este derecho fundamental a la protección de datos personales[25]. Así,

---

[21] Sobre la Directiva, cfr. R. MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, cit., págs. 226-232; J. J. MARTÍN CASALLO, «Implicaciones de la Directiva sobre protección de datos en la normativa española», en *X años de Encuentros sobre Informática y Derecho*, Aranzadi, Pamplona, 1997, págs. 75-86; M. HEREDERO HIGUERAS, *La Directiva Comunitaria de protección de los datos de carácter personal*, Tecnos, Madrid, 1998; A. SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, Sevilla, 1998; D. ALONSO BLAS, «La aplicación de la Directiva europea de protección de datos en España. Reformas necesarias en la LORTAD», en *X años de Encuentros sobre Informática y Derecho*, Aranzadi, Pamplona, 1997, págs. 141-149. Un análisis de los primeros pasos sobre la cuestión en el ámbito europeo, sobre la distinta protección de datos en los diferentes Estados de la Unión Europea y, más en concreto, sobre la Directiva 95/46/CE se puede ver en M. A. DAVARA, *La protección de datos en Europa*, Universidad de Comillas ICAI-ICADE, Madrid, 1998, págs. 41-59. Un estudio sistemático de las legislaciones de protección de datos de los países de la Unión Europea, centrándose en las divergencias normativas, se puede ver en A. TÉLLEZ AGUILERA, *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, págs. 329-349.

[22] La propia Unión Europea ha reconocido como antecedente de su derecho derivado el Convenio 108. Así, la Recomendación de la Comisión de 29 de julio de 1981 instó a los Estados miembros de la Comunidad a firmar y ratificar lo antes posible el Convenio 108 del Consejo de Europa. De hecho, el propio texto de la Directiva 95/46/CE se basa en los principios enunciados en el Convenio del Consejo de Europa.

[23] Como señala la Exposición de Motivos de la Directiva, es necesario impedir que «las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales» afecten al ordenado funcionamiento del mercado único.

[24] El Acuerdo de Schengen imponía a los firmantes la exigencia de adecuar su normativa de protección de datos, lo que llevó en nuestro país a la aprobación de la LORTAD. Cfr. también la Recomendación R (87), de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa, sobre uso de los datos de carácter personal en el sector policial.

[25] Cfr. A. ALABAU, *La Unión Europea y su política para la sociedad de la información: en el umbral de una nueva gobernanza europea,* Ariel, Madrid, 2001.

la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[26], contiene una remisión expresa a la Directiva 95/46/CE en lo que afecta a la tutela de la intimidad y a la regulación del tratamiento de datos personales en el ámbito de las comunicaciones, atribuyendo a esta Directiva carácter supletorio. La Directiva 97/66/CE pretende hacer compatible el desarrollo del sector de las telecomunicaciones, que supone el tratamiento y almacenamiento masivo de datos de abonados y usuarios, y la protección de los derechos y las libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas. La Directiva 97/66/CE ha sido derogada por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Esa Directiva, a diferencia de la 95/46/CE y de la 97/66/CE, sí hace ya una referencia expresa no sólo a la necesidad de proteger la intimidad y la vida privada de los ciudadanos, sino el derecho fundamental a la protección de datos personales como derecho autónomo[27]. Otra Directiva a la que hay que hacer mención es la 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior[28]. Esta Directiva ha sido transpuesta en nuestro país a través de la Ley 34/2002, de 11 de julio, de servicios de sociedad de la información y de comercio electrónico. Esta Directiva hace una mención expresa a la Directiva 95/46/ CE en relación al tratamiento de datos personales y, por tanto, no supone ninguna innovación en este ámbito.

No obstante, la Unión Europea contenía hasta ahora sólo una breve mención a la protección de datos personales dentro del Derecho comunitario originario. Al no ser la hasta ahora Unión Europea competente en materia de derechos fundamentales, los preceptos comunitarios se referían solamente a la vigencia de este derecho en relación con los actos de las instituciones comunitarias y a su vigilancia por una Comisión independiente[29]. Hasta ahora, la ausencia de un reconocimiento de derechos fundamen-

---

[26] *DOCE,* Serie L, n.º 24, de 30 de enero.

[27] *DOCE,* Serie L, n.º 201, de 31 de julio. Sobre la Directiva, cfr. S. SORIANO MALDONADO, «Un marco comunitario para la privacidad en las comunicaciones electrónicas», *Datos Personales. Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n.º 1, marzo 2003. Cfr. también A. PRIETO ANDRÉS, «La nueva directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones», *La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía*, n.º 5, 2002, págs. 1710-1713.

[28] *DOCE,* Serie L, n.º 178/1, de 17 de julio.

[29] Así, el artículo 286 del TUE —versión consolidada, antiguo art. 213B— afirmaba que: «1. A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo. 2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251,

tales en los Tratados constitutivos de la Unión Europea se ha superado de diversas maneras[30]. Por una parte, se mantenía que los derechos fundamentales reconocidos en los textos constitucionales de los Estados miembros eran parte de los principios generales del Derecho comunitario y del acervo comunitario[31]. Esto permitía la afirmación a nivel de la Unión Europea de este derecho fundamental a la protección de datos personales, al estar reconocido en las Constituciones de los Estados miembros. Por otro lado, la consideración del Convenio de Roma para la Protección de los Derechos Humanos y de las Libertades Fundamentales como auténtica Carta europea de derechos fundamentales facilitaba fácilmente la remisión al Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, los principios de los derechos y libertades[32]. Con la entrada en vigor del Tratado de la Unión Europea —antiguo art. F— se establece que: «1. La Unión se basa en los principios de libertad, democracia, respeto de los derechos humanos y de las libertades fundamentales y el Estado de Derecho, principios que son comunes a los Estados miembros. 2. La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950, y tal y como resultan de las tradiciones constitucionales comunes a los Estados miembros como principios generales del Derecho comunitario». Existe, además, en menor medida, una jurisprudencia del Tribunal de Justicia de las Comunidades Europeas que ha analizado de manera indirecta este derecho fundamental[33].

---

un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes». Posteriormente se ha aprobado el Reglamento (CE) 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. Cfr. *Diario Oficial de las Comunidades Europeas*, Serie L, n.º 8, de 12 de enero de 2002. Existe, además, otra mención en el artículo 30 del Tratado de la Unión Europea —antiguo art. K.2)— referente a la actuación de la Europol: «1. La acción en común en el ámbito de la cooperación policial incluirá: ... b) la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente, en particular mediante Europol, incluida la correspondiente a informes sobre operaciones financieras sospechosas que obre en poder de servicios con funciones coercitivas, con sujeción a las disposiciones correspondientes en materia de protección de datos personales».

[30] Cfr. M. PI I LLORENS, *Los derechos fundamentales en el ordenamiento comunitario*, Ariel, Barcelona, 1996; A. CHUECA SANCHO, *Los derechos fundamentales en la Unión Europea*, Bosch, Barcelona, 1999.

[31] El Tribunal de Justicia de las Comunidades Europeas ha afirmado —asunto *Stauder*, 1969— que los derechos fundamentales se hallaban comprendidos «en los principios generales del derecho comunitario que el Tribunal garantiza», de manera que «el respeto a los derechos fundamentales forma parte integrante de los principios generales del derecho que el Tribunal de Justicia salvaguarda», salvaguardia que se inspira en «las tradiciones constitucionales comunes a los Estados miembros». Cfr., más ampliamente, R. ALONSO GARCÍA, *Derecho Comunitario. Sistema constitucional y administrativo de la Comunidad Europea*, Ceura, Madrid, 1994, págs. 600-665.

[32] El Tribunal de Justicia señaló la imposibilidad de la adhesión de la Comunidad Europea al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de Roma, de 1950, señalando que la Comunidad carecía de competencias en esta materia —Dictamen 2/1994, de 28 de marzo de 1996—.

[33] Así, en el asunto *X contra la Comisión*, el Tribunal reconoció el derecho a mantener la reserva so-

En los últimos años se ha avanzado, primero, con la aprobación en el Tratado de Niza de 2000 de una Carta de Derechos Fundamentales de la Unión Europea[34] y, finalmente, con los trabajos de la Convención que preparó una Constitución europea, aprobada por el Tratado de Roma el 29 de octubre de 2004 y pendiente de ratificación por los Estados. En ambos textos se reconoce el derecho fundamental a la protección de datos personales como derecho fundamental autónomo.

La Carta de Derechos Fundamentales de la Unión Europea afirma la necesaria adaptación al progreso en el campo de los derechos fundamentales y proclama en su Preámbulo que «[p]ara ello es necesario, dotándolos de mayor presencia en una Carta, reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos». Así, dentro del Capítulo II, que se titula «Libertades», afirma en el artículo 7 el respeto a la vida privada y familiar: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones». No obstante, el derecho a la protección de los datos personales no se configura en el mismo ámbito que el derecho a la intimidad. Así, el artículo 8 de la Carta, que se titula «Protección de datos de carácter personal», establece que: «1. Toda persona tiene derecho a la protección de 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»[35].

---

bre el estado de salud. No obstante, este derecho puede sufrir limitaciones, como señala el propio artículo 8 del Convenio, lo que implica que si los servicios de contratación de las instituciones comunitarias exigen a un candidato que se someta a un examen médico y éste se niega, la Comisión no está obligada a soportar los riesgos derivados de su contratación. En este caso se estudió la protección de la vida privada en el contexto de las relaciones laborales, al amparo de la jurisprudencia del Tribunal Europeo de Derechos Humanos y de los principios derivados de las tradiciones constitucionales comunes a los Estados miembros —As. C-404/92, *X contre Commission des Communautés européennes*, Recueil 1994, I, págs. 4737 y ss.—. En el asunto *Fisher* se analizó la divulgación de datos de carácter personal contenidos en un fichero, resolviéndolo a partir de los criterios generales establecidos en la Directiva 95/46/CE, que, si bien no había entrado en vigor todavía en el momento en el que se planteó el asunto, remitía en su Exposición de Motivos a los principios comunes a los Estados miembros en esta materia —As. C-369/98, *The Queen contre Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher*, Recueil 2000, I, págs. 6751 y ss.—. Cfr., más ampliamente, R. MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, cit., págs. 211-233.

[34] *DOCE* de 18 de diciembre de 2000 (2000/C 364/01). Sobre la Carta de los Derechos Fundamentales, cfr. R. ALONSO GARCÍA, «El triple marco de protección de los derechos fundamentales en la Unión Europea», y A. SAIZ ARNÁIZ, «La Carta de los Derechos Fundamentales de la Unión Europea y los ordenamientos nacionales: ¿qué hay de nuevo?», *Cuadernos de Derecho Público,* n.º 13, 2001, págs. 13 y ss. y 153 y ss. Cfr. también A. WEBER, «La Carta de los Derechos Fundamentales de la Unión Europea», *Revista Española de Derecho Constitucional,* n.º 64, 2002, págs. 79 y ss.; A. RODRÍGUEZ BEREIJO, «La Carta de Derechos Fundamentales», y R. VICIANO PASTOR, «El largo camino hacia una constitución europea», ambos en *Revista de Derecho de la Unión Europea,* monográfico *¿Quo Vadis Europa?*, n.º 1, 2.º semestre de 2002, págs. 45-57 y 105-123, respectivamente; A. FERNÁNDEZ TOMÁS, *La Carta de Derechos Fundamentales de la Unión Europea*, Tirant lo Blanch, Valencia, 2001, págs. 84 y ss.

[35] Cfr. C. RUIZ MIGUEL, «El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico», *Revista de Derecho Comunitario Europeo*, n.º 14, 2003.

En la misma dirección, la propuesta de Tratado para establecer una Constitución para Europa establece un precepto específico para la protección de datos personales. Así, el artículo I-51 señala que: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. La Ley o ley marco europea establecerá las normas sobre sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes». Una referencia semejante se encuentra también el el artículo II-68.

c) *El artículo 18.4 de la Constitución española*

Nos corresponde ahora abordar la situación en España. Como hemos señalado antes, la Constitución de 1978 ha regulado de manera específica esta cuestión. Así, en el mismo precepto donde se reconoce el derecho al honor, a la intimidad personal y familiar, a la propia imagen y se salvaguarda la inviolabilidad del domicilio y el secreto de las comunicaciones, se establece que «[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» —art. 18.4 CE—[36]. Llama la atención que la única vez que la Constitución habla de la informática lo haga para limitar su uso. Se trata de que un elemento provechoso no sea utilizado para recortar derechos y, especialmente, la privacidad de las personas. Esta regulación es, por tanto, una respuesta constitucional ante una amenaza concreta. Así, frente al riesgo que suponen los tratamientos de datos personales por medios informáticos, se ha reconocido un derecho específico de protección de datos personales, como ha afirmado claramente la jurisprudencia constitucional, en especial la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

La antigua proclamación del derecho a la intimidad no era una protección bastante frente a la nueva realidad del progreso tecnológico. El Tribunal Constitucional, en su Sentencia 292/2000, de 30 de noviembre, ha afirmado la existencia de un derecho fundamental a la protección de datos personales, definiendo su contenido como el «[p]oder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos

[36] Uno de los primeros autores que analizó este precepto entre nosotros fue LUCAS MURILLO DE LA CUEVA. Cfr. P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa,* Tecnos, Madrid, 1990; P. LUCAS MURILLO DE LA CUEVA, *Informática y Protección de Datos Personales*, CEC, Madrid, 1993; más recientemente, cfr. M. CARRILLO, *El derecho a no ser molestado. Información y vida privada*, Aranzadi, Navarra, 2003, págs. 91-100.

datos personales y para qué, pudiendo oponerse a esa posesión o uso» —FJ 7.º—. Como señalaremos más adelante, el derecho fundamental a la protección de datos es, por una parte, un *derecho autónomo nuevo* que protege a la persona —en especial, la propia información personal— frente a las tecnologías de la información y que, de alguna manera, representa una concretización del derecho a la intimidad en los tratamientos de datos personales, un derecho más específico dentro del más general derecho de privacidad personal; por otra, es un *instrumento de garantía* de otros derechos fundamentales, en especial del derecho a la intimidad, pero no sólo de este derecho. Es importante señalar que este derecho fundamental a la protección de datos personales no tiene un carácter abstracto o genérico. Atribuye a su titular un haz de facultades que consiste en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos. Dentro del contenido de este derecho fundamental se encontrarían los principios de calidad de los datos, información en la recogida de los mismos, consentimiento del afectado para su tratamiento y para la cesión, seguridad informática y deber de secreto. También los derechos de acceso, oposición, rectificación y cancelación sobre los datos de carácter personal sometidos a tratamiento.

La Constitución española de 1978 es, como hemos señalado antes, después de la Constitución portuguesa de 1976, el segundo texto constitucional que reconoce un derecho fundamental a la protección de los ciudadanos frente a las tecnologías de la información. No obstante, el precepto constitucional español es más breve que el portugués y que aquellos otros artículos que se han introducido posteriormente a través de reformas constitucionales o en la Constitución europea. Así, la Constitución portuguesa no se circunscribe, como hace el texto español, a limitar el uso de la informática para garantizar los derechos de las personas, sino que establece un contenido positivo que posibilite el control de los ciudadanos de su propia información personal, englobando en un solo artículo los problemas más acuciantes que suscitan las relaciones entre intimidad e informática[37].

El texto constitucional español no ha aprovechado, por ello, la experiencia del texto constitucional portugués, sino que se ha centrado únicamente en el aspecto defensivo; no ha proclamado de manera clara un derecho fundamental a la protección de datos personales, sino que ha establecido únicamente un mandato al legislador para que limite la informática en garantía del derecho al honor y a la intimidad personal y familiar y del pleno ejercicio de los derechos. El artículo 18.4 CE es un precepto poco concreto, que no delimita claramente el bien jurídico objeto de protección. De una simple lectura se advierte únicamente una preocupación acerca de la potencial amenaza que la informática representa para el derecho a la intimidad, al honor y para el resto de los derechos fundamentales. Es, por tanto, un precepto que presenta insuficiencias, al centrarse únicamente en el aspecto defensivo y res-

[37] La comparación entre el texto portugués y el español se puede ver en A. E. PÉREZ LUÑO, *Derechos humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1991, pág. 338.

trictivo[38]. En relación con otros preceptos constitucionales que tienen fórmulas lingüísticas donde abiertamente se reconocen derechos fundamentales —«garantizará», «regulará»—, el tenor literal del artículo 18.4 recoge únicamente de manera expresa la obligación del legislador de limitar el fenómeno de la informática[39].

Haciendo un análisis propio de teoría de la norma y del lenguaje constitucional, el precepto representa un ejemplo de cláusula abierta, no de cláusula cerrada; de valor, no de regla constitucional. Es un precepto con muy poca densidad normativa. Por tanto, el contenido necesario y positivo de este derecho fundamental —las facultades que conforman su contenido esencial— se tiene que dibujar con una construcción indirecta: las garantías de este derecho fundamental se alcanzan limitando el fenómeno de la informática. Posiblemente, el constituyente español, a pesar del modelo portugués, no fue en ese momento consciente de la importancia de la informática, de su desarrollo futuro y de los peligros que ésta podía suponer para los derechos de las personas. La existencia de una previsión constitucional expresa —lo que no ha ocurrido en Italia y Alemania, como ya hemos señalado— no ha evitado la necesidad de desarrollar una labor interpretativa. Ha sido necesario, por tanto, desarrollar una intensa exégesis constitucional para afirmar un derecho fundamental a la protección de datos personales, a partir del tenor literal del artículo 18.4 CE, y para establecer, aunque sea de manera mínima, su núcleo a partir de la doctrina del contenido esencial de los derechos fundamentales[40]. En su momento, el Convenio 108 del Consejo de Europa —y, en la actualidad, la propia Directiva 95/46/CE y, especialmente, los preceptos relativos al derecho fundamental a la protección de datos personales de la Constitución europea— facilitó la determinación de este contenido, ya que las normas relativas a los derechos fundamentales que la Constitución reconoce «se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas ratificados por España» —art. 10.2 CE—.

En todo caso, la propia existencia de este precepto constitucional supu-

---

[38] Cfr. J. BERMEJO, «Premisas jurídicas de la intimidad personal y de la protección de los datos en el Derecho español», en el *Libro Homenaje al Profesor José Luis Villar Palasí*, Civitas, Madrid 1989, pág. 144; J. M. CASTELLS ARTECHE, «La limitación informática», en *Estudios sobre la Constitución Española. Homenaje al Profesor Eduardo García de Enterría,* II, Civitas, Madrid, 1991.

[39] Lógicamente, parece claro que limitar el fenómeno de la informática obliga a regularlo, lo que implica no sólo el establecimiento de frenos a los tratamientos de datos personales que deben respetar unos principios y unos derechos en este ámbito, sino también la posibilidad de facilitar la utilización de la informática bajo ciertas condiciones. Sin embargo, para LÓPEZ-MUÑIZ GOÑI, aunque el artículo 18.4 prefiere el verbo «limitar» sobre el término «regular», un análisis de la LORTAD —tanto de las excepciones al principio de consentimiento del interesado como de la amplitud de posibilidades para los responsables de los ficheros— muestra que lo que ha llevado a cabo el legislador es una regulación, no una mera limitación. Cfr. M. LÓPEZ-MUÑIZ GOÑI, «La ley de regulación del tratamiento automatizado de datos de carácter personal», en V. CARRASCOSA LÓPEZ, *Informática y Derecho*, n.os 6 y 7, UNED, Mérida, 1994, pág. 94.

[40] Cfr. STC 11/1981, de 8 de abril. Para la noción de contenido esencial, cfr. L. MARTÍN-RETORTILLO e I. DE OTTO, *Derechos fundamentales y Constitución*, Civitas, Madrid, 1988, y L. LÓPEZ GUERRA, *Introducción al Derecho Constitucional*, Tirant lo Blanch, Valencia, 1994, págs. 112-113.

so, sin duda, un elemento positivo. Difícilmente se puede criticar la parquedad del constituyente, vista la falta de sensibilidad del legislador, que esperó al año 1992 para aprobar la LORTAD y desarrollar este precepto. Es necesario destacar, además, que este artículo constitucional se incluye dentro de la Sección 1.ª del Capítulo II del Título I. Es decir, este derecho ha sido situado en un lugar de máxima relevancia constitucional. Si clasificáramos los derechos fundamentales en virtud de las garantías de protección, tanto genéricas como específicas —art. 53 CE—, hay que señalar que el grupo de derechos reconocidos en la Sección 1.ª del Capítulo II del Título I disponen de un conjunto de garantías específicas o jurisdiccionales como la protección a través de los procedimientos preferentes y sumarios —amparo judicial o amparo ordinario— y a través del recurso de amparo ante el Tribunal Constitucional.

El derecho fundamental a la protección de datos personales es, por una parte, un derecho autónomo, con un contenido específico que atribuye a la persona un control de sus datos personales, sean o no íntimos. Esto se manifiesta claramente tanto en la Carta de Derechos Fundamentales de la Unión Europea como en la Constitución europea, antes citadas, donde se reconoce este derecho en preceptos distintos al derecho a la protección de la vida privada. Pero, al mismo tiempo, este derecho fundamental a la protección de datos se encuentra muy relacionado con el derecho a la intimidad. El artículo 18.4 CE se encuentra incluido dentro del precepto constitucional que reconoce y proclama distintos derechos relativos a la privacidad de las personas. Así, sin desconocer que este precepto proclama un derecho nuevo a controlar la propia información personal (sea íntima o no lo sea), un derecho general frente a las tecnologías de la información, hay que señalar que de su ubicación en el artículo 18 se desprende que la limitación de la informática y el derecho a la protección de datos personales no debe ser visto como un derecho absolutamente independiente, sino dentro de la esfera amplia del derecho a la intimidad, como una especie de manifestación más de la protección de la vida privada, aunque tutele también el ejercicio de otros derechos fundamentales, como, por otra parte, también le ocurre al propio derecho a la intimidad. Así, la ubicación dentro del artículo 18 CE de este precepto que exige la limitación del uso de la informática equivale a una cierta actualización del derecho a la privacidad, a una modalidad nueva frente al desarrollo de las nuevas técnicas de la información[41]. De hecho, otros países como Italia y Alemania han buscado otros preceptos constitucionales como los dere-

[41] Sin embargo, para VILARIÑO PINTOS, «[...] no resulta correcta la utilización del término intimidad para referirse a la protección de los datos personales, lo que desgraciadamente ocurre no sólo en el lenguaje ordinario, sino también en organismos oficiales y en disposiciones normativas, pero que hace ya un buen número de años, tal identificación, es rechazada por la mejor doctrina. Tal error, en castellano, se produce por la mala traducción del término *privacy* por intimidad en lugar de dato personal o, cuando menos, vida privada, que es a lo que corresponde el concepto inglés». Cfr. E. VILARIÑO PINTOS, «Los derechos de la persona en el ámbito de las tecnologías de la información», en D. BELLO JANEIRO y M. HEREDERO HIGUERAS, *El derecho a la intimidad y a la privacidad y las Administraciones Públicas*, EGAP, Santiago de Compostela, 1999, pág. 20.

chos de libertad, el libre desarrollo de la personalidad o el reconocimiento de la dignidad de la persona para fundamentar el derecho a la protección de datos personales porque carecían de un precepto constitucional específico que reconociera el derecho a la intimidad. De este modo, parece que la informática está concebida en nuestra Norma Fundamental, no únicamente pero sí señaladamente, como una garantía adicional de protección de la intimidad, como un mecanismo de tutela que pretende adecuar este derecho a las nuevas técnicas de la información. Esta concepción de la relación de la limitación del uso de la informática respecto de la intimidad no suprime ni atenúa su carácter de derecho autónomo. Sencillamente, resalta su carácter mixto o bifronte.

Parece clara la intensa relación existente entre la intimidad personal y familiar y la protección de datos personales. El artículo 1 de la LOPD establece como objeto de esta Ley «garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y *especialmente* de su honor, intimidad personal y familiar». El legislador es consciente de que el tratamiento de datos personales, especialmente a través de las tecnologías de la información, afecta principalmente a la intimidad —o la privacidad, por utilizar un término empleado por la Exposición de Motivos de la LORTAD—. El principio de calidad —art. 4 LOPD— que limita la recogida de datos personales a aquellos adecuados y pertinentes en relación con la finalidad, y que prohíbe la acumulación de datos excesivos o su utilización para finalidades distintas, frena el conocimiento excesivo sobre nuestra persona. El derecho de acceso a los datos personales —art. 15 LOPD— y el principio de información antes de la recogida de los datos —art. 5 LOPD— están encaminados a proporcionar al ciudadano un conocimiento sobre quién tiene o quién puede llegar a tener información acerca de uno mismo, sobre qué información personal se maneja exactamente y para qué finalidad[42]. La exigencia de consentimiento para el tratamiento y la cesión de sus datos personales —arts. 6 y 11 LOPD— o el derecho de oposición buscan preservar una esfera personal del sujeto al margen del conocimiento y del tratamiento automatizado por los demás. El derecho de rectificación y cancelación —art. 16 LOPD— de los datos personales supone facilitar al titular de los datos unas facultades que le permiten suprimir sus referencias personales y evitar aquellas que dan una imagen errónea de sí mismo. Igualmente, la calificación de los datos de ideología, afiliación sindical, religión, creencias, salud, raza o vida sexual como datos «especialmente protegidos» —art. 7 LOPD— se hace en virtud de su especial sensibilidad y de la mayor proximidad a la intimidad del sujeto, sin perjuicio de que también proteja el ejercicio de otros derechos como la libertad ideológica y religiosa —art. 16 CE—. De esta forma, el derecho a la protección de datos personales conecta con el clásico concepto de intimidad

[42] Cfr. A. I. Herrán Ortiz, *El derecho a la intimidad en la nueva Ley de Protección de Datos Personales,* Dykinson, Madrid, 2002, pág. 86.

personal y familiar, que exige un reducto al margen del conocimiento de los demás que opera, lógicamente, también en materia de protección de datos[43]. Nuestros datos personales materializan muchas veces informaciones que ya son conocidas —que han dejado de ser de dominio exclusivamente privado o personal—, pero esto no suprime que estos datos personales automatizados manifiesten y materialicen nuestra intimidad personal. Que un dato personal llegue a ser conocido no elimina su vinculación con nuestra vida privada.

No obstante, este planteamiento no debe excluir el carácter autónomo del derecho fundamental a la protección de datos, dado también su carácter instrumental en relación con otros derechos fundamentales. Como veremos posteriormente en el análisis de la jurisprudencia constitucional, un tratamiento indebido del dato relativo a la cuota sindical de un trabajador supone una vulneración de la libertad sindical —art. 28 CE—. Así, la protección especial de los datos de ideología, afiliación sindical, religión o creencias —art. 7 LOPD— es una exigencia de otros derechos fundamentales como la libertad ideológica y religiosa. No olvidemos que el artículo 16.2 CE señala que «[n]adie podrá ser obligado a declarar sobre su ideología, religión o creencias», lo que demuestra que esta libertad requiere un respeto a la propia información personal. Así, el hecho de que las vulneraciones de la libertad sindical, de la libertad ideológica y religiosa por tratamientos informáticos ilegítimos tienen también tutela en sus propios derechos específicos no debe suprimir la garantía que presta en este caso el propio derecho fundamental a la protección de datos personales y la limitación al uso de la informática para garantizar «el pleno ejercicio de los derechos» previsto en el artículo 18.4 CE[44].

Así, el constituyente ha establecido en el propio artículo 18.4 CE que la limitación del uso de la informática no es sólo para garantizar el honor y la intimidad de las personas, sino también *el libre ejercicio de sus derechos*. Así, la limitación de algunas manifestaciones de las tecnologías de la información sirve para proteger otros derechos fundamentales distintos del derecho a la intimidad. No se puede excluir, por tanto, la relación entre el derecho fundamental a la protección de datos personales y otros derechos fundamentales. Como ha recordado PÉREZ LUÑO, «todos los derechos fundamentales son interdependientes y su conexión no depende del dato formal de su positivación en un determinado sector del texto constitucional, sino de su interrelación material»[45]. La relación material y expresa de la informática, según el propio artículo 18.4, se establece con el honor, la intimidad personal y fami-

---

[43] Una muestra clara de la vinculación entre estos dos derechos es que la Disposición Transitoria 1.ª 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, señalaba que en tanto no se promulgara la normativa prevista en el artículo 18.4 CE, «la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente Ley».

[44] Cfr. un planteamiento contrario en P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento de datos personales,* Comares, Granada, 1999, págs. 22 y ss.

[45] Cfr. A. E. PÉREZ LUÑO, «La protección de la intimidad frente a la informática en la Constitución Española de 1978», *REP*, n.º 9, 1979, pág. 70.

liar, pero también con el resto de derechos fundamentales. De hecho, la informática puede ser utilizada para limitar el «*pleno ejercicio de* [otros] *derechos*», distintos del derecho a la intimidad. Imagínese la utilización de Internet para la difusión de mensajes racistas o las limitaciones a la libertad de expresión y acceso a la información de los ciudadanos mediante el bloqueo de determinadas áreas de Internet[46]. De esta forma, el derecho a la protección de datos personales del artículo 18.4 CE protege frente a cualquier uso de las tecnologías de la información que vulnere el pleno ejercicio de los derechos fundamentales.

Este debate sobre la vinculación de la protección de datos personales al derecho a la intimidad o sobre su carácter autónomo también se produjo en sede constituyente. El Anteproyecto constitucional mencionaba exclusivamente la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos. En los debates parlamentarios se manifestaban tres posturas contradictorias: aquellos que se inclinaban por la supresión del apartado, considerándolo una reiteración ya que la protección de la intimidad y del honor quedaba asegurada frente a cualquier agresión con el artículo 18.1 CE; otros que defendían el texto de la ponencia que limitaba la informática para proteger la intimidad; y, por último, quienes consideraban la necesidad de mantener el precepto y proponían una redacción más amplia que hiciera referencia a que la limitación de la informática fuese encaminada también a facilitar el pleno ejercicio de todos los derechos fundamentales[47]. Ésta fue, obviamente, la posición que se terminó imponiendo.

El artículo 18.4 CE contiene principalmente un mandato al legislador para que establezca los límites necesarios en la utilización de la informática, con el fin de garantizar y proteger los derechos de los ciudadanos. Se establece, por tanto, una remisión al legislador para que desarrolle la normativa que establezca y ordene un desarrollo de la informática que sea compatible con los derechos de las personas. Si todos los derechos tienen que ser desarrollados por ley —arts. 53.1 y 81 CE—, este derecho dispone de una reserva de ley específica. Esto podría haber conducido a dos interpretaciones alternativas: por una parte, podría justificar una regulación general que limite el uso de la informática para garantizar los derechos de los ciudadanos, como han hecho la LORTAD y la LOPD; por otra, podría exigir al legislador que tuviera en cuenta la necesidad de limitar la informática cuando desarrolle los derechos constitucionales, regulando indirectamente la informática en distintas leyes sectoriales. Este último planteamiento limitaría el artículo 18.4 CE a una dimensión meramente instrumental y atenuaría en gran medida su carácter de derecho autónomo, perdiendo en gran medida su eficacia.

---

[46] Cfr., más ampliamente, R. MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, cit. Así, como señala este autor, la garantía de la vida privada es un presupuesto del propio funcionamiento del sistema democrático. Cfr. R. RUIZ, «The Right to Privacy: A Discourse-Theoretical Approach», *Ratio Juris,* vol. 11, n.º 2, junio 1998, págs. 155-167.

[47] Ésta fue una propuesta de Minoría Catalana, defendida por su portavoz, Miguel Roca. Cfr. A. E. PÉREZ LUÑO, *Derechos Humanos, Estado de Derecho y Constitución*, cit., págs. 361 y ss.

Lógicamente, al limitar la informática en beneficio de los derechos de los ciudadanos, el constituyente ha situado a la primera no en plano de igualdad, sino subordinado a la segunda. Por tanto, el uso de la informática está subordinado al derecho a la intimidad y al resto de los derechos fundamentales. El empleo del verbo limitar manifiesta una postura de recelo por parte del legislador frente a la informática. Sin embargo, como después han señalado la Exposición de Motivos de la LORTAD y el propio Tribunal Constitucional, es necesario también permitir y promover la implantación y utilización de los distintos medios informáticos, como instrumentos decisivos tanto para el desarrollo económico como para el buen funcionamiento de la Administración, que, en ambos casos, van encaminados al interés general. Si cualquier labor de interpretación constitucional exige llevar a cabo un *balancing* constitucional entre diversos derechos enfrentados —derecho al honor y libertad de expresión— o entre derechos y otros intereses jurídicos o bienes constitucionales —derecho a la libertad y a la inviolabilidad del domicilio, por una parte, y seguridad pública e interés general, por otra—, esto no es una excepción en el caso del artículo 18.4 CE. Así, la legislación que ha desarrollado este precepto ha buscado siempre una posición de equilibrio entre los distintos intereses en juego. A diferencia de lo que ocurre con la regulación del derecho a la intimidad —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—, que establece el concepto de intromisión ilegítima y fija la prohibición de inmiscuirse en la esfera íntima de las personas, tanto la LORTAD como la LOPD han establecido un régimen no de prohibición de la informática, sino de utilización de ésta de manera respetuosa con los derechos de los afectados. Así, el título de la LORTAD resultaba elocuente al respecto: Ley Orgánica reguladora del *tratamiento automatizado* de datos de carácter personal. No es una Ley que prohíbe, sino una Ley que regula y ordena —organiza— los tratamientos automatizados. La vigente Ley Orgánica de Protección de Datos de Carácter Personal, como señala su artículo 1, pretende proteger los derechos fundamentales en los tratamientos de datos personales. Se trata de tutelar los derechos fundamentales no prohibiendo el recurso a la informática y la acumulación de información personal en bases de datos, sino, partiendo de la realidad y de la necesidad de su utilización, regular y someter estos tratamientos de datos personales al respeto a unos principios y a unos derechos de las personas.

Al precisar el artículo 18.4 CE que la ley limitará el uso de la *informática*, parece que este derecho fundamental a la protección de datos sólo existe frente a los tratamientos automatizados y no frente a los no automatizados, ya que la informática se refiere a tratamientos mecanizados. De esta forma, el ámbito de protección del artículo 18.4 CE es más restringido que el de la Directiva 95/46/CE y el de la LOPD, ya que ambas incluyen la protección de los datos personales frente a tratamientos no automatizados. Sólo la LORTAD regulaba únicamente los tratamientos automatizados de datos personales, como exigía el artículo 18.4 CE y el propio Convenio 108 del

Consejo de Europa. Sin pretender restar importancia a los riesgos de los modernos sistemas de información y a la necesidad de tutelar los derechos fundamentales frente al incremento de las bases de datos personales, no obstante, en la elaboración de nuestra Constitución se perdió la oportunidad de reconocer expresamente un derecho fundamental a la protección de datos personales, no limitando la tutela a los tratamientos automatizados, sino abarcando también a los no automatizados. Eso no era obstáculo para que se hubiera establecido también una protección clara de los derechos frente al desarrollo de las nuevas tecnologías —no sólo de la informática—, que en ese momento no se podía precisar pero tal vez sí se podía intuir. Nos estamos refiriendo, obviamente, a Internet y a las inmensas posibilidades de las tecnologías de la comunicación y de los multimedia para afectar gravemente a los derechos fundamentales. Es decir, se echa en falta un reconocimiento más claro tanto del derecho fundamental a la protección de datos personales, estén o no automatizados, como de la protección de los derechos frente a las nuevas tecnologías.

Es imprescindible desarrollar un análisis constitucional intenso del artículo 18.4 CE, especialmente de su contenido, porque éste es el límite frente a los poderes públicos, especialmente frente al legislador. Hasta ahora, el esfuerzo tanto doctrinal como jurisprudencial se ha limitado básicamente a debatir si el artículo 18.4 reconoce la existencia de un derecho fundamental autónomo o si, por el contrario, únicamente introduce un instrumento más de protección del derecho a la intimidad del artículo 18.1 CE. No obstante, como señalaremos más adelante, este debate, frecuentemente presente en nuestra jurisprudencia y doctrina constitucional, se caracteriza principalmente por su inutilidad. Ambas posibilidades tienen la tutela constitucional reforzada de los derechos fundamentales de la Sección 1.ª del Capítulo II del Título I. Considerar el derecho a la protección de datos personales o derecho a la autodeterminación informativa como un derecho autónomo o instrumental del derecho a la intimidad no debe hacernos olvidar que ambos derechos poseen el mismo origen: la dignidad de la persona[48].

d) *El desarrollo legislativo: la LORTAD y la LOPD*

Los legisladores de los distintos países, a la hora de ir aprobando normas que desarrollan este derecho fundamental a la protección de datos personales, han tenido que adoptar una postura ante la realidad de las tecnologías de la información, bien positiva o bien de recelo frente a las mismas[49].

---

[48] Cfr. X. O'CALLAGHAN MUÑOZ, *Libertad de expresión y sus límites: honor, intimidad y propia imagen*, Edersa, Madrid, 1991, pág. 36.

[49] Cfr., más ampliamente, el estudio que hace M. SERRANO, *El derecho fundamental a la protección de datos*, cit., págs. 96-103. Cfr. también A. E. PÉREZ LUÑO, «El derecho a la autodeterminación...», págs. 310 y ss.; íd., *Libertad informática*, cit., pág. 152; A. A. SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, 1998, págs. 75-78; M. HEREDERO HIGUE-

Así, se podía adoptar una posición negativa, de desconfianza, hacia el nuevo fenómeno de las tecnologías de la información, que resultaba imparable. Este modelo, que ha sido calificado como *preventivo* pero que debería considerarse como *represivo* —porque reprime y dificulta la extensión de estas nuevas tecnologías—, se caracterizaba por la prohibición *a priori* de todos los tratamientos de datos personales, salvo autorización expresa. Esta visión de tolerancia forzada parte del rechazo general al tratamiento de datos, que se admite sólo en supuestos específicos. Este sistema presentaba en la práctica la dificultad de habilitar un órgano que pudiese autorizar los tratamientos de datos.

Existía también la posibilidad de adoptar una posición más positiva hacia los tratamientos de datos, estableciendo no un control previo para la creación del fichero, sino un control en su utilización posterior. Este modelo, que ha sido definido como *represivo* aunque tenga realmente un carácter *permisivo,* afirma, a diferencia del modelo anterior, el principio de libertad de tratamientos de datos, siendo la ley una norma no de presupuesto, sino de límite y prohibición para algunas actuaciones, cuyo incumplimiento conllevaría la sanción *a posteriori* por las infracciones cometidas. Estas leyes se caracterizan por establecer garantías de los ciudadanos frente a los tratamientos de datos personales.

El legislador de la mayoría de los países ha optado por modelos mixtos, con una cierta preferencia hacia uno u otro modelo[50]. La opción por un modelo represivo o permisivo ha dependido, en ocasiones, del ámbito sectorial donde se establece el tratamiento de datos, diferenciando, a estos efectos, entre ficheros públicos y ficheros privados. Otras leyes han valorado los tratamientos a partir de los bienes jurídicos en presencia y de los posibles riesgos de los tratamientos —distinguiéndose así los supuestos de ficheros sanitarios o de solvencia patrimonial y de crédito, etc.—, lo que puede llevar a acentuar o a suavizar los instrumentos de control. Así, se puede mantener con carácter general un sistema permisivo al facilitar la libre creación de ficheros con una mera notificación a la Autoridad reguladora que garantice la publicidad de los mismos, pero para los casos en los que el tratamiento implique un riesgo particular para los individuos, como es el supuesto de los datos de ideología, no puede llevarse a cabo el tratamiento hasta que exista una autorización del órgano de control. De esta forma, el tipo de fichero condiciona y presiona sobre el modelo de control.

A partir de estos criterios, la doctrina ha mantenido la existencia de tres generaciones en las leyes de protección de datos, clasificación que se ha establecido, lógicamente, no a partir de la fecha de aprobación, sino del tipo de

---

RAS, «La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal», *Boletín del Ministerio de Justicia,* n.º 1669; íd., «La protección de los datos personales registrados en soporte informático», *Actualidad Jurídica Aranzadi*, enero 1992.

[50] El Convenio 108 del Consejo de Europa, en primera instancia, y, principalmente, la Directiva 95/46/CE han hecho un esfuerzo por clarificar y homogeneizar la normativa nacional reguladora de los tratamientos de datos personales en los distintos países europeos.

respuesta que cada país ha dado ante el desarrollo de las tecnologías de la información.

La primera generación albergaría las leyes que tienen un carácter represivo de las tecnología de la información porque exigían una autorización previa para la creación y funcionamiento de ficheros con datos personales[51]. Estas leyes tratan de regular un fenómeno poco extendido, con una visión negativa frente a la informática, que se visualiza como una amenaza que es necesario limitar y controlar. Entre las leyes de la primera generación destacan la *Datenschutz* alemana, de 1977; la legislación de la década del setenta de los *Länder* alemanes como Hesse (1970) y Renania-Palatinado (1974), o la *Data Lag* sueca, de 11 de mayo de 1973.

Las leyes de la segunda generación serían aquellas que permitían los tratamientos personales pero controlando más aquellos que implicaran un mayor peligro hacia los derechos de las personas. Dentro de esta segunda generación se incluirían la *Privacy Act* americana, de 31 de diciembre de 1974; la Ley francesa n.º 78-17, de 6 de enero de 1978, sobre informática, ficheros y libertades; la *Privacy Act* de Gran Bretaña, de 12 de julio de 1984, y la *Privacy Act* de Irlanda, n.º 25 de 1988. Estas leyes empiezan a garantizar los principios de calidad, información, consentimiento y datos especialmente protegidos y los derechos de acceso, rectificación y cancelación[52].

Por último, las leyes de tercera generación han tenido que hacer frente al desarrollo intenso de las tecnologías de la información tanto en la Administración Pública como en la sociedad civil. El incremento de los ficheros de datos personales hace que los planteamientos basados en la autorización previa no sean operativos. Se opta por desarrollar los principios y derechos de protección de datos de las personas, al mismo tiempo que se admiten los elementos positivos que la informática aporta a la sociedad y a la Administración Pública. Estas leyes están menos centradas en la informática —abandonan así los aspectos técnicos, que son estructuralmente cambiantes— y más en las garantías para la protección de los individuos. Entre las leyes de la tercera generación podemos destacar la Ley alemana de 1990; la Ley portuguesa n.º 10/91, de 29 de abril, sobre protección de datos personales frente a la informática; la Ley Federal suiza de Protección de Datos, de 19 de junio de 1992, o la Ley belga de 1992.

Las diferencias que pueden apreciarse entre las características propias de las primeras leyes de protección de datos y las últimas revelan un cambio general en la orientación de las mismas. Mientras que las primeras leyes centraban su atención en el control de la informática como técnica que hay que dominar para evitar abusos, pasando la persona y sus derechos a un segundo plano, las leyes de la tercera generación relegan los aspectos técnicos a unas

---

[51] Lógicamente, la doctrina define estas leyes como preventivas porque establecen un control de los ficheros *a priori.* No obstante, a nuestro parecer, en la calificación de estas leyes debe primar su cualidad sustancial de reprimir los tratamientos de datos personales, frente a otras clases de leyes.

[52] Cfr., recientemente, T. GARCÍA-BERRIO HERNÁNDEZ, *Informática y libertades. La protección de datos personales y su regulación en Francia y España,* Universidad de Murcia, 2003, págs. 163-203.

pautas generales y se orientan hacia la protección del individuo frente a la acumulación de datos personales. No se fija la atención en la informática como fenómeno, sino en el individuo del que se recaban datos personales y que puede ver lesionados sus derechos como consecuencia de un mal uso de los mismos. El ordenamiento jurídico de protección de datos se vuelca así en la garantía de las personas[53].

En nuestro país, después de la aprobación de la Constitución española de 1978, a pesar de que el artículo 18.4 CE obligaba a la ley a limitar «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», no existió hasta 1992 una normativa específica en este ámbito. Únicamente la Ley Orgánica 1/1982, de 5 de mayo, reguladora de la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, establecía que las intromisiones que la informática generase en la esfera de la intimidad serían objeto de protección en el ámbito de aplicación de esta Ley. Señala la Disposición Transitoria 1.ª: «*En tanto no se promulgue la normativa prevista en el artículo 18, ap. 4 de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente Ley*». Así, en los artículos 7 y 8 de la Ley Orgánica 1/1982, de 5 de mayo, que analizan las intromisiones ilícitas, además de las formas tradicionales de vulneración de la vida privada —revelación de secretos, difamación, uso indebido o no autorizado de la imagen—, aparece también el recurso a nuevas tecnologías, como la captación, grabación, registro, reproducción, a las que se consideran también intromisiones ilegítimas. Así, el artículo 1.1 de la Ley Orgánica 1/1982, de 5 de mayo, señala que el derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo 18 de la Constitución, será protegido civilmente «frente a todo género de intromisiones ilegítimas», entre las que habría que incluir, lógicamente, la informática. Hasta 1992, ésta fue la única norma vigente con carácter de Ley Orgánica que regulara la utilización de la informática.

Obviamente, la Ley Orgánica 1/1982, de 5 de mayo, otorgaba una tutela insuficiente a la protección de datos personales, ya que esta Ley está destinada principalmente a garantizar el derecho al honor, a la intimidad personal y familiar y a la propia imagen, especialmente frente a la libertad de expresión y de información. Además, esta Ley extiende su aplicación a las intromisiones provocadas por el uso de la informática cuando las mismas afecten *al honor, la intimidad y la propia imagen*, excluyendo los demás derechos. Sin embargo, como hemos señalado anteriormente, el derecho a la protección de datos personales, como establece el artículo 18.4 *in fine*, trata de limitar la informática para garantizar el pleno ejercicio de todos los derechos constitucionales, y no únicamente del derecho al honor y a la intimi-

[53] Cfr. M. Heredero Higueras, «La nueva Ley Alemana Federal de Protección de Datos», *Boletín del Ministerio de Justicia*, n.º 1630, pág. 127.

dad personal y familiar. Así, la Ley Orgánica 1/1982, de 5 de mayo, no representaba un cumplimiento del mandato constitucional del artículo 18.4 CE, que exigía una ley que limite expresamente el uso de la informática para garantizar los derechos de las personas.

Con posterioridad, nuestro país ha aprobado dos leyes que han desarrollado adecuadamente la previsión del artículo 18.4 CE. En primer lugar, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal —LORTAD—. En segundo lugar, y derogando la anterior, la Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal —LOPD—. Ambas normas han estado claramente inspiradas en las legislaciones de los países europeos y, especialmente, en la normativa internacional: la LORTAD se inspiró en el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; la LOPD es transposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Al ser un desarrollo de un derecho fundamental, ambas normas tenían el carácter de Ley Orgánica.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, es, como ya hemos señalado, la primera norma de desarrollo del artículo 18.4 CE y, por ello, representa un hito en la legislación española sobre tecnologías de la información[54]. Antes del Anteproyecto final del Gobierno, hubo distintas iniciativas legislativas[55]. Fue una norma intensamente criticada durante su proceso de tramitación, que fue objeto de gran número de enmiendas[56]. Su elaboración suscitó una gran polémica, especialmente en los foros más sensibilizados en protección de datos, que la consideraban insuficiente, y fue objeto de diversos recursos de inconstitucionalidad: los que afectaban al reparto competencial entre el Estado y las CC.AA. fueron resueltos por el Tribunal Constitucional en la Sentencia 290/2000, de 30 de noviembre; los recursos que planteaban la vulneración del contenido del derecho fundamental fueron resueltos por el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre, que analizó la constitucionalidad de distintos preceptos de la LOPD, que eran reproducción de otros artículos de la LORTAD, que habían sido previamente

---

[54] Cfr. M. HEREDERO HIGUERAS, *La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal: comentarios y textos*, Tecnos, Madrid, 1996. Uno de los primeros trabajos, de carácter más expositivo, fue el de E. DEL PESO NAVARRO y M. A. RAMOS, *Lortad. Análisis de la Ley*, Díaz de Santos, 1994, págs. 169-180.

[55] Cfr. su análisis en P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, cit., págs. 165-172. Cfr. los distintos borradores del texto en «Protección de datos personales» —documentación preparada para la tramitación del Proyecto de Ley Orgánica de regularización del tratamiento de los datos de carácter personal—, *BOCG Congreso,* Serie A, n.º 59, de 24 de julio de 1991, págs. 105 y ss.

[56] Cfr. D. LÓPEZ GARRIDO, «Aspectos de inconstitucionalidad de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal», *RDP,* n.º 38, 1993; J. C. NAVARRO RUIZ, «Algunas consideraciones sobre la tramitación de la LORTAD», *Cuadernos de la Cátedra de Fadrique Furió Ceriol*, n.º 1, págs. 98-107.

impugnados ante el Tribunal Constitucional pero que no fueron resueltos por el Alto Tribunal al derogarse la LORTAD por la LOPD con anterioridad a su resolución[57]. En todo caso, la LORTAD puede calificarse ya como una ley de la tercera generación, al establecer un modelo no represivo, sino permisivo; que reconoce la libertad de tratamientos; no estando centrada en la informática como fenómeno, sino en la protección de los derechos de las personas frente a la informática, estableciendo unos principios de protección de datos y unos derechos y garantías de los ciudadanos en este ámbito[58].

La LORTAD, como ya hemos señalado, fue una norma ampliamente influida por el Convenio 108 del Consejo de Europa y por el Proyecto de Directiva comunitaria relativa a la protección de datos personales y a la libre circulación de esos datos. Sin embargo, el empuje definitivo para su aprobación fue la necesidad de ratificar el Acuerdo de *Schengen*, que establecía la transmisión de información policial entre los países europeos que lo ratificaron, suprimiendo los controles interiores pero reforzando, al mismo tiempo, los mecanismos de información sobre sospechosos. Además, no puede olvidarse la necesidad de desarrollar expresamente el mandato constitucional del artículo 18.4, que obligaba al legislador a regular el uso de la informática para garantizar los derechos de las personas. Igualmente, la LORTAD también ha estado influida por las legislaciones de los países europeos que ya habían aprobado hace años normas de estas características[59].

La LORTAD tiene, por una parte, una visión estática, ya que tiene en cuenta al dato en sí mismo, desarrollando una protección distinta dependiendo del carácter más o menos sensible de los datos —art. 7 LORTAD—, aunque el principio de calidad sea predicable para todos —art. 4 LORTAD—. Pero, por otra, lleva a cabo una protección dinámica orientada a controlar los datos en la medida en que aparecen insertos en un programa informático,

---

[57] Esto se encuentra muy bien expuesto en los Antecedentes de la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre. Así, los recursos de inconstitucionalidad acumulados n.os 201/1993, 219/1993, 226/1993 y 236/1993 fueron interpuestos, respectivamente, por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y el Grupo Parlamentario Popular, contra los artículos 6.2, 19.1, 20.3, 22.1 y 2.1, 24, 31, 39.1 y 2, 40.1 y 2, y disposición final tercera de la LORTAD. No obstante, la derogación formal de la LORTAD por la LOPD dejó en parte vacíos de contenido estos recursos de inconstitucionalidad, especialmente el de cincuenta diputados del Grupo Parlamentario Popular, ya que fue este Grupo el que apoyó la aprobación de la LOPD con algunos de los preceptos que habían impugnado previamente en la LORTAD. Únicamente se mantuvo frente a la LORTAD el recurso interpuesto por la Generalitat de Cataluña, que se refería a materias competenciales y que es el origen de la STC 290/2000, de 30 de noviembre. Otros preceptos de la LORTAD que habían sido impugnados y que se mantuvieron en la LOPD fueron nuevamente impugnados por el Defensor del Pueblo, lo que fue origen de la STC 292/2000, de 30 de noviembre. Sobre la cuestión, cfr. P. LUCAS MURILLO DE LA CUEVA, «Las vicisitudes del Derecho de protección de datos personales», *RVAP*, n.º 58, 2000, págs. 217 y ss.

[58] Cfr. A. E. PÉREZ LUÑO, «Comentario legislativo: La LORTAD y los derechos fundamentales», *Derechos y Libertades*, n.º 1, 1993, pág. 409; íd., *Manual de informática y derecho*, Ariel, Barcelona, 1996, págs. 61 y ss., así como la bibliografía que cita sobre la LORTAD.

[59] De los distintos modelos, realmente, nuestro legislador no optó claramente por ninguno de ellos. Ello ha llevado a criticar la falta de aprovechamiento por parte de nuestro legislador de la legislación comparada. Cfr. J. A. MARTÍN PALLÍN, «La Ley Orgánica de Regulación del tratamiento automatizado de datos de carácter personal. Una visión crítica», en *Informática Judicial y Protección de Datos Personales*, Gobierno Vasco, Vitoria, 1994, pág. 81.

estableciendo unos principios de protección de datos, atribuyendo a toda persona un conjunto de derechos con respecto a su información personal y creando un órgano independiente para la tutela específica de la vigencia de este ordenamiento jurídico. Este sistema mixto es el asumido por los países de forma mayoritaria en las leyes de protección de datos de tercera generación[60]. También lleva a cabo una distinción en el régimen jurídico entre ficheros públicos o ficheros privados, que no va referida al tipo de dato, sino a la cualidad pública o privada del responsable del fichero —arts. 18 y 23 LORTAD—.

Así, la LORTAD se ha inclinado por un sistema permisivo, que facilita la creación de los ficheros *a priori*, siempre que cumplan unas exigencias en la solicitud de inscripción que supervisa la autoridad de control —arts. 18 y 24 LORTAD—. Como señala la Exposición de Motivos, con la pretensión de «evitar una perniciosa burocratización, la Ley ha desechado el establecimiento de supuestos como la autorización previa o la inscripción constitutiva en un registro. Simultáneamente, ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que el de aquellos de titularidad pública». Existe una excepción a la libre creación de ficheros, que es la prohibición de «los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual» —art. 7.4 LOPD—. La Ley, no obstante, diferencia el régimen para la creación de los ficheros públicos y de los privados.

Con la aprobación de la LORTAD, nuestro legislador ha optado por disponer de una norma general sobre protección de datos, sin perjuicio de que existan diversas regulaciones sectoriales a las que la propia LORTAD se remite[61]. Una ley general de protección de datos tiene la ventaja de facilitar la configuración de un ordenamiento jurídico de protección de datos, que permite una interpretación uniforme y reduce el riesgo de incoherencias. Sin embargo, otros países habían optado inicialmente por regulaciones sectoriales o parciales[62], lo que obedecía, por una parte, a una toma de conciencia

---

[60] Sin embargo, la Ley alemana de 1990 ha optado por un modelo dinámico, que se centra en el control del uso de los datos en general, sin hacer ninguna alusión a datos especialmente protegidos. Cfr. A. E. PÉREZ LUÑO, «La protección de datos personales en España: presente y futuro», *Informática y Derecho*, n.º 4, UNED, Mérida, 1994, pág. 239

[61] Dentro de éstas podemos destacar: la Ley 12/1989, de 9 de mayo, de la función estadística pública; la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional, que establece en el artículo 68 los informes personales de las Fuerzas Armadas; la Ley 230/1963, de 28 de diciembre, General Tributaria, modificada por las Leyes 10/1985, de 26 de abril, y 4/1990, de 29 de junio, en lo que respecta a sus artículos 111 y 112, que regulan una cesión obligatoria de datos y limitan el uso de los mismos a las finalidades tributarias; la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas, que en sus artículos 13 y 14 reconoce la utilización de los datos en función de su finalidad; la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, que prohíbe recoger datos sensibles e incluirlos en los ficheros de personal, etc.

[62] El ejemplo más claro de leyes sectoriales lo constituye el caso americano, que ha optado por un modelo legislativo de protección de datos basado en un conjunto de leyes sectoriales *(sector by sector)*, antes que en una única ley general *(omnibus Act)*. Cfr. A. PÉREZ LUÑO, «El derecho a la autodeterminación

progresiva de cómo la informática podía afectar a la vida de las personas, además de a una forma de responder al problema de manera prematura y desintegrada, lo que favorecía el surgimiento de regulaciones parciales en detrimento de una norma general que llegaría más tarde[63]. No obstante, las normas sectoriales presentaban la ventaja de su mayor facilidad para aproximarse a cada uno de los sectores. La complejidad técnica de muchas materias y la propia tendencia a la superproducción normativa en el Estado contemporáneo hacen difícil que una sola norma regulase la informática y las tecnologías de la información. El propio fenómeno de la informática, que va afectando a otros derechos, y la propia dinamicidad de las tecnologías de la información hacen difícil un modelo de norma única general. Por ello se ha optado por modelos mixtos, donde la ley general no deroga toda la normativa sectorial precedente, sino que también puede respetarla en ocasiones, quedando como norma general subsidiaria[64].

Esta solución mixta, adoptada por el legislador español, presenta algunas ventajas[65]. Así, la normativa general de protección de datos facilita la coherencia y la seguridad jurídicas. En cambio, una regulación de la protección de datos sin ley general y dependiendo de una pluralidad de normas sectoriales podría restar seguridad jurídica y hacer inefectivos los instrumentos de protección. La normativa sectorial se adapta mejor a las especificidades y a las necesidades concretas, ya que una ley general difícilmente da respuesta a los problemas existentes y a los potenciales[66]. El modelo mixto de norma general y remisión a normas sectoriales precedentes permite, además, abreviar las normas generales, que así no tienen la necesidad de reproducir ni derogar la normativa sectorial precedente y que pueden diferir en la regulación sectorial futura aspectos nuevos sobre informática y protección de da-

---

informativa», en *II Jornadas de Estudio sobre Protección de Datos y Derechos Fundamentales*, IVAP, Oñate, 1991, pág. 313. M. G. LOSANO califica las normas sectoriales como *normae fugitivae* que son una fuente de problemas legislativos graves («Los Proyectos de Ley italianos sobre la protección de los datos personales», en *Problemas actuales de la documentación y la informática jurídica*, Tecnos, Madrid, 1987, pág. 127).

[63] Para DAVARA, la normativa sectorial que regula aspectos parciales de la informática son «normas prematuras», en el sentido de adelantadas a la regulación unitaria del fenómeno informático. Cfr. M. A. DAVARA RODRÍGUEZ, *Derecho Informático*, Aranzadi, Pamplona, 1993, pág. 4.

[64] PEREZ LUÑO habla de «elección entre un modelo de ley única y global, o por una serie de leyes particulares sectoriales para distintos aspectos de la tecnología de la información y de la comunicación que requieren una reglamentación peculiar. Si bien parece más oportuna una solución mixta tendente a conjugar una disciplina unitaria con un marco jurídico adaptado a las exigencias de determinados aspectos tecnológicos». Cfr. A. E. PÉREZ LUÑO, «El derecho a la autodeterminación informativa», cit., pág. 319. HEREDERO HIGUERAS habla también de dos posibles soluciones: «la consistente en codificar los principios contenidos en dichas disposiciones preexistentes, al modo de los códigos clásicos, con una generalidad tal que pudieran ser aplicados a cualquier contexto específico... Otra alternativa consistía en una ley de una concepción parecida, pero que dejara subsistentes las disposiciones anteriores que incidían en la protección de los datos y regular *ex novo* los demás ficheros automatizados extrapolando los principios que estaban expresados o en germen en las disposiciones preexistentes e integrar éstas en un sistema del cual fueran regulaciones específicas y a las cuales fuera aplicable subsidiariamente la regulación general». Cfr. M. HEREDERO HIGUERAS, «La Ley Orgánica...», cit., pág. 46.

[65] Para PÉREZ LUÑO, la LORTAD optaba por un sistema mixto a caballo entre las regulaciones sectoriales y la regulación única y global que no resuelve todas las concordancias, reiteraciones y antinomias, «Comentario legislativo...». Cfr. A. E. PÉREZ LUÑO, «El derecho a la autodeterminación», cit., pág. 411.

[66] Cfr. A. E. PÉREZ LUÑO, *Manual,* cit., pág. 54.

tos. De hecho, la propia ley general llama a la aprobación de otras leyes cuando justifica como excepción del consentimiento del afectado para el tratamiento de sus datos la existencia de una habilitación legal —art. 6.1 LORTAD—. Esto lleva a un modelo de coexistencia de ley general y leyes sectoriales, que presenta como principal inconveniente que el sistema jurídico de protección de datos se pueble de reenvíos y de excepciones, que dificultan no sólo la seguridad jurídica, sino su propia lectura, y matizan en parte su unidad jurídica.

La opción de legislaciones sectoriales sin ley general de protección de datos era difícilmente compatible con el mandato del artículo 18.4 CE, que obliga, a nuestro parecer, al legislador a aprobar una ley general. En cambio, no se extrae del precepto constitucional el rechazo a la presencia de leyes sectoriales, que, por otra parte, ya existían con anterioridad y que conformaban un conjunto heterogéneo, de rango normativo diverso, que se limitaba a proteger de manera genérica la intimidad[67]. De esta forma, se puede afirmar que el modelo mixto no constituyó tanto una opción del legislador como una aceptación de una realidad preexistente, que no se quiso modificar. La LORTAD permitió la coexistencia de la regulación general y sectorial, al optar por no derogar estas últimas. El mantenimiento de la legislación sectorial podía haber sido limitado algo más por la LORTAD, ya que su carácter de norma general en desarrollo del artículo 18.4 CE le convertía en el instrumento jurídico adecuado para ordenar esta materia[68]. Sin embargo, finalmente, la relación entre la informática y los derechos de los ciudadanos ha estado regulada no sólo en la LORTAD, sino también en todo nuestro ordenamiento jurídico, y no siempre ha existido una coordinación adecuada, ya que muchas de estas normas, lógicamente, se han ido aprobando posteriormente. Así, la LORTAD, como después hará la LOPD, enumeraba un conjunto de normas que desarrollan una regulación específica al margen de la ley, pero hay otras muchas regulaciones sectoriales que no aparecen mencionadas en la LORTAD. Así, por ejemplo, la LORTAD no contenía ninguna remisión al régimen de conductas delictivas reguladas ya por el Código Penal, lo que significaba una importante omisión de la normativa precedente[69].

Este modelo mixto fue también el adoptado por el Consejo de Europa, que, con posterioridad al Convenio 108, de 1981, aprobó distintas recomendaciones relativas a la protección de datos personales en algunos sectores,

---

[67] Cfr. M. HEREDERO HIGUERAS, «La Ley Orgánica...», cit., pág. 87.

[68] A. E. PÉREZ LUÑO, piensa, al igual que HEREDERO HIGUERAS, que la LORTAD al decantarse por este modelo mixto no acaba de resolver todos los problemas que pueden surgir en nuestro ordenamiento. CASTELLS ARTECHE entiende que la LORTAD estaba llamada a «establecer, por imperativos de seguridad jurídica, una ordenación armonizadora de toda esa normativa sectorial en materia de protección de datos que sirviera de guía y trazara la dirección a seguir». Cfr. J. M. CASTELLS ARTECHE, «Derecho a la privacidad y procesos informáticos: análisis de la Ley Orgánica 5/1992, de 29 de octubre (LORTAD)», *RVAP,* n.º 39, 1994, pág. 250. Tampoco parece ser éste el papel que desempeña la LOPD.

[69] Cfr. A. E. PÉREZ LUÑO, «Comentario legislativo: la LORTAD y los derechos fundamentales», *Derechos y Libertades*, n.º 1, 1993, pág. 413. Cfr. A. RUIZ CARRILLO, *La protección de los datos de carácter personal*, Bosch, Barcelona, 2001, págs. 239-261.

como los bancos de datos electrónicos en el sector privado y en el sector público, los datos médicos automatizados, los servicios de *marketing* directo, los servicios telefónicos, la seguridad social, la policía, etc.[70]. De igual forma, la Unión Europea, después de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, aprobó distintas Directivas sectoriales como la ya citada Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, ya derogada por la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, o la Directiva 2000/31/CE, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. De hecho, la propia Directiva 95/46/CE aconseja la existencia de un modelo mixto en el considerando 28, al afirmar que «los Estados miembros están facultados para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas respecto del tratamiento de los datos de carácter personal como mediante leyes sectoriales, como las relativas a los institutos estadísticos».

La LORTAD fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal —LOPD—[71]. La LOPD ha tenido la virtualidad de extender el derecho a la protección de datos personales a los tratamientos no automatizados y sustentados sobre un soporte-papel, en consonancia con la Directiva 95/46/CE del Parlamento y el Consejo, relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales y a la libre circulación de esos datos. El artículo 1 de la LOPD señala como objeto «garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor, intimidad personal y familiar». El artículo 2 de la LOPD establece como ámbito de aplicación «los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento». Por último, la LOPD define como tratamiento de datos las «operaciones y procedimientos técnicos de carácter automatizado o no» —art. 3.c)—[72].

---

[70] Estas Recomendaciones se encuentran recogidas en *El Consejo de Europa y la Protección de Datos Personales*, APD, Madrid, 1997.

[71] Cfr., especialmente, J. APARICIO, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Navarra, 2002; M. VIZCAÍNO, *Comentarios a la Ley Orgánica de protección de datos de carácter personal*, Civitas, Madrid, 2001. Cfr., para un comentario general, A. RUIZ CARRILLO, *La protección de datos de carácter personal*, Bosch, Barcelona, 2001; A. TÉLLEZ AGUILERA, *Nuevas tecnologías, intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Edisofer, Madrid, 2001, págs. 107-164. Cfr. también J. J. MARTÍN CASALLO y J. A. MARTÍN PALLÍN, «Intimidad, privacidad y protección en la nueva Ley Orgánica 15/1999», en M. A. DAVARA, *XIV Encuentros sobre Informática y Derecho 2000-2001,* Aranzadi, Navarra, 2001, págs. 51-53 y 55-59. Cfr., como referencias más generales, A. E. PÉREZ LUÑO, *Manual de Informática y Derecho*, Ariel, Barcelona, 1996; J. M. ÁLVAREZ CIENFUEGOS, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona, 1999; H. CAMPUZANO, *Vida privada y datos personales*, Tecnos, Madrid, 2000.

[72] Todo ello sin perjuicio de la Disposición Adicional Primera, segundo párrafo, que difiere al año 2007 la aplicación de parte de la normativa de protección de datos a los ficheros manuales. Cfr. A. TRON-

La LOPD representa esencialmente una continuación de la LORTAD. Así, la LOPD reproduce la mayoría de preceptos de la LORTAD y de la Directiva, incluidos algunos artículos sobre los que habían versado diversos recursos de inconstitucionalidad[73]. No se repitió en la tramitación de la LOPD el debate intenso que tuvo la LORTAD, ni en el Parlamento —ya que fue aprobada con cierto consenso— ni en la sociedad, sin perjuicio de que esta Ley mantuviera muchos de los preceptos que habían sido antes cuestionados. Sin embargo, son muchos los defectos de la LOPD. Por una parte, hay que reconocer que la LOPD ha sido redactada con una técnica legislativa deficiente. Así, no tiene Exposición de Motivos —algo completamente inusual en los textos normativos—, por lo que no conocemos la *voluntas legislatoris*, uno de los criterios de interpretación para determinar el sentido de las normas jurídicas[74]. Además, carece de una sistemática razonable, especialmente en lo relativo a la regulación de los tratamientos realizados por las Administraciones Públicas[75]. Estas dificultades traen causa de su azarosa tramitación parlamentaria. Lo que inicialmente era un Proyecto de Ley de reforma de algunos preceptos de la LORTAD para adecuarla a la Directiva 95/46/CE, sobre la base de un Anteproyecto elaborado por el Gobierno, en el que había intervenido decisivamente la Agencia Española de Protección de Datos, se transformó en un nuevo texto completo de Proyecto de Ley Orgánica de Protección de Datos Personales, elaborado por la Comisión Constitucional del Congreso de los Diputados, que se sintió con la voluntad y la capacidad de hacer una reforma global de la LORTAD a todas luces innecesaria[76]. En todo caso, la preparación de un texto nuevo en sede parlamentaria que no había recibido un estudio adecuado a través del Poder Ejecutivo —de las distintas Secretarías Generales Técnicas y Subdirecciones Generales de Normativa de los distintos Ministerios, de la Abogacía del Estado y del Consejo de Estado— ha favorecido la aprobación de una Ley menos cuidada y con defectos graves de carácter sistemático[77].

COSO REIGADA, «Introducción», en *Guía de Protección de Datos Personales para Universidades*, Civitas, Madrid, 2004, págs. 13-17.

[73] Como hemos señalado antes, la LOPD fue impugnada por el Defensor del Pueblo —repitiendo argumentos utilizados en los recursos de inconstitucionalidad de la LORTAD—, lo que fue origen de la STC 292/2000, de 30 de noviembre.

[74] El Proyecto de Ley, que era una mera modificación de algunos preceptos de la LORTAD para adecuarlos a la Directiva 95/46/CE, sí incluía una Exposición de Motivos.

[75] Por ejemplo, los supuestos de comunicación de datos entre Administraciones Públicas sin consentimiento del interesado no están regulados en el artículo 11, sino en el artículo 21.

[76] El Proyecto de Ley Orgánica de reforma de la LORTAD tenía como objetivos, principalmente, proteger los tratamientos de datos personales no automatizados, como exigencia de la Directiva, así como incluir la regulación del acceso a los datos por cuenta de terceros. Sin embargo, la ponente, Bernarda Barrio, planteó la elaboración de un texto nuevo, para lo que se crea una Comisión extraparlamentaria. El texto que sale de esta Comisión contiene defectos importantes, que tienen que ser modificados, a propuesta de la Agencia Española de Protección de Datos, a través de enmiendas en el Senado.

[77] Buen ejemplo de ello es la defectuosa regulación de los tratamientos de datos de salud —arts. 7.6 y 8—. El artículo 11 LOPD autoriza la comunicación de datos personales sin consentimiento del interesado a los comisionados del Parlamento y no al Parlamento, por lo que hay que acudir a la propia Constitución y a los Estatutos de las Cortes Generales y de los Parlamentos autonómicos. A esto hay que añadir, lógicamente, las dificultades intrínsecas de la propia materia de protección de datos personales, que pre-

Además, la LOPD no ha sido objeto hasta ahora de desarrollo reglamentario, estando todavía vigente la normativa de rango infralegal de desarrollo de la LORTAD[78]. Esto es lo que ocurre con el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal; el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal; o el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos[79]. Por tanto, todavía no se dispone de una normativa que haya tratado de dar coherencia y sistemática a la LOPD. Así, la Disposición Transitoria Tercera de la LOPD —«Subsistencia de normas preexistentes»— señala que «[h]asta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes, y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley». No existe, por tanto, un ordenamiento jurídico de protección de datos, dotado de un conjunto de normas que atribuyan seguridad jurídica a este sector de la actividad social y administrativa, lo que permite la existencia de zonas de incertidumbre, como, por ejemplo, en lo relativo a la aplicación de las medidas de seguridad a los ficheros manuales posteriores a la LOPD[80].

La LOPD ha seguido manteniendo la opción de la LORTAD por un sistema permisivo, que facilita la creación de ficheros y sólo actúa *a posteriori,* sin perjuicio del trámite de inscripción de los ficheros en el Registro General

---

senta una cierta complejidad. Es una legislación muy técnica, con un vocabulario propio. Esto ha hecho que tanto la Directiva 95/46/CE como la LORTAD y la LOPD contengan un grupo de definiciones de qué se entiende por datos de carácter personal, fichero, tratamiento de datos, responsable del fichero o del tratamiento, afectado o interesado, procedimiento de disociación, encargado del tratamiento, consentimiento del interesado, cesión o comunicación y fuentes accesibles al público —art. 3 LOPD—.

[78] El retraso en el desarrollo reglamentario de la Ley vino motivado por la voluntad de esperar la experiencia práctica en la ejecución de la LOPD. No obstante, uno de los retos principales para el futuro de la Agencia Española de Protección de Datos es acometer el desarrollo de la LOPD, a través de la aprobación de un Reglamento general de desarrollo de la Ley y de un nuevo Estatuto para la AEPD. Esto es especialmente importante en lo que hace referencia a las medidas de seguridad de los ficheros manuales.

[79] Siguen en vigor la Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a la prestación de servicios de solvencia patrimonial y crédito; la Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal; la Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios; la Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo; y la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

[80] A esta problemática nos hemos referido en A. TRONCOSO REIGADA, «Introducción y Presentación», en *Guía de protección de datos personales para Universidades*, Civitas-APDCM, Madrid, 2004, págs. 13-17, y *Guía de protección de datos personales para Servicios Sanitarios Públicos*, Civitas-APDCM, Madrid, 2004, págs. 52-58.

de Protección de Datos —art. 39—[81]. La LOPD, al igual que la normativa europea, mantiene la libertad para el establecimiento de un fichero. Esto no es óbice para que la Autoridad de Protección de Datos pueda establecer mecanismos de control para aquellos tratamientos que presentan inicialmente más amenazas para los derechos de las personas o prohíba aquellos ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual —art. 7.4—[82].

La LOPD pretende ser, como la LORTAD, una norma general de protección de datos, pero a la vez se encuentra llena de excepciones[83] en lo relativo a su ámbito de aplicación —art. 2.2 LOPD[84]— y afectada por lo previsto en otras legislaciones más específicas, como la estadística, la del régimen electoral general, la del régimen del personal de las Fuerzas Armadas, del Registro Civil, del Registro Central de Penados y Rebeldes, o la de la legislación que regula imágenes y sonidos obtenidos a través de videocámaras por las Fuerzas y Cuerpos de Seguridad —art. 2.3 LOPD—[85]. De esta forma, el legislador ha optado en la LOPD, como lo hizo en la LORTAD, por un sistema mixto. Así, junto a una ley general de protección de datos, existe una fuerte remisión a legislaciones sectoriales[86].

La LOPD no abarca todo el ordenamiento jurídico de protección de da-

---

[81] Este artículo establece como objeto de inscripción en el Registro General de Protección de Datos: «a) Los ficheros de que sean titulares las administraciones públicas. b) Los ficheros de titularidad privada. c) Las autorizaciones a que se refiere la presente ley. d) Los códigos tipo a que se refiere el artículo 32 de la presente ley. e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición».

[82] Así, por ejemplo, las inspecciones sectoriales que ha llevado a cabo la Agencia Española de Protección de Datos se han dirigido especialmente a sectores sensibles como los ficheros del SIDA, el Hospital Militar Cómez Ulla, Hospitales Psiquiátricos o los ficheros de solvencia patrimonial y de crédito —estos últimos de nivel medio—. Igualmente, la Agencia de Protección de Datos de la Comunidad de Madrid se ha centrado especialmente en ficheros especialmente protegidos, como los ficheros de historias clínicas en los Servicios Sanitarios o los ficheros de historias sociales en los Servicios Sociales.

[83] Las abundantes excepciones provenían inicialmente de la LORTAD —aunque fueron modificadas parcialmente por la LOPD— y ha sido muy criticado. Cfr. A. E. PÉREZ LUÑO, *Manual,* cit., págs. 61 y ss.; G. FREIXAS GUTIÉRREZ: «Y si algún reproche se le puede hacer a esta ley, aunque haya intentado corregir aspectos negativos de la LORTAD en el régimen de excepciones, es la indeterminación jurídica de muchos aspectos que justifican las excepciones de los derechos de los ciudadanos, con lo que la interpretación subjetiva de éstas puede perjudicarlos de una manera acusada» —*La protección de los datos de carácter personal*, Bosch, Barcelona, 2001, pág. 222—.

[84] El artículo 2.2 LOPD señala que «[e]l 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 normativa sobre protección de materias clasificadas. c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada».

[85] La LORTAD añadía a los ficheros sometidos a su legislación específica aquellos regidos por la normativa sobre materia clasificada que ahora la LOPD excluye de su ámbito de aplicación. Por otra parte, la LOPD incluye como novedad, dentro de los remitidos a su legislación específica, los tratamientos procedentes de imágenes y sonido obtenidos a través de videocámaras por las Fuerzas y Cuerpos de Seguridad.

[86] Las Leyes de protección de datos francesa y belga sí han repetido parte de la regulación sectorial, lo que les ha hecho ser mucho más detalladas y extensas. Cfr. M. HEREDERO HIGUERAS, «La Ley Orgánica», cit., pág. 47.

tos al remitirse y mantener la normativa sectorial precedente. En todo caso, una característica esencial del carácter de norma general de la LOPD es su carácter supletorio, salvo para los ficheros que han sido excluidos expresamente de su ámbito de aplicación por el artículo 2.2 LOPD. Así, el artículo 2.3 LOPD señala que los ficheros antes mencionados «[s]e regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica». Así, estos ficheros que el artículo 2.3 LOPD refiere a una regulación específica deben también respetar los criterios generales de la LOPD[87]. La LOPD se convierte así en una norma general del sistema que respeta la existencia de regulaciones específicas, pero trata de someter todos los tratamientos a la disciplina general de la Ley, por lo que se sitúa en el centro del sistema de protección de datos[88].

Los tratamientos de datos de salud son un buen ejemplo de lo que estamos explicando. Así, a pesar del carácter específico de los ficheros con datos de salud, el legislador no los ha remitido inicialmente a una legislación sectorial sanitaria, sino que ha preferido regularlos dentro del régimen general de la Ley —arts. 7.6 y 8 LOPD—. Esto no ha evitado que con posterioridad se aprobase la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que solucionase muchos problemas de adaptación de la legislación de protección de datos a las especificidades del sistema sanitario. Así, eran muchos los autores que han reclamado reiteradamente la necesidad de una ley de protección de datos sanitarios, que adecuase y adaptase la normativa en este ámbito[89]. Esta normativa sectorial no tiene que tratar siempre de excepcionar y limitar las garantías de la legislación general de protección de datos personales. De hecho, ha sido también necesario aprobar una normativa de protección de datos sanitarios para intensificar la tutela del dato de salud y de las historias clínicas en general, estableciendo, por ejemplo, un deber de tratamiento de los datos de salud, aclarando cuáles son los datos adecuados y pertinentes en una historia clínica y definiendo distintos niveles de acceso para profesionales sanitarios y personal de administración y servicios. Así, en relación con los ficheros sanitarios, es posible que haya que adaptar el principio de información en los tratamientos —art. 5 LOPD— para no burocratizar en exceso la actividad asistencial, al mismo tiempo que hay que fortalecer el principio de seguridad y el deber de custo-

---

[87] En relación con la supletoriedad, la enmienda n.º 45, presentada por el Grupo Parlamentario Socialista, a la LOPD presentaba la siguiente redacción: «Se regirán por sus disposiciones específicas y supletoriamente por la presente Ley Orgánica». Igualmente, el Consejo de Estado en su informe preceptivo recogía la posibilidad de proceder a la regulación de la protección de datos mediante una sola ley o por medio de leyes sectoriales, pero respetando siempre el régimen de garantías de la Ley. *Boletín del Congreso de los Diputados*, Serie A, n.º 135-7, pág. 29.

[88] Sin embargo, para Mercedes SERRANO, la aplicación de la LOPD a los sectores que poseen una regulación específica no es algo automático, sino que requiere una interpretación y un análisis particularizado. Para esta autora, «la ocasión para aclarar su posición y convertirse en una norma de cierre del sistema ha vuelto a ser desaprovechada por nuestro legislador». Cfr. M. SERRANO, *op. cit.*

[89] Cfr. J. SÁNCHEZ-CARO y F. ABELLÁN, *Telemedicina y protección de datos sanitarios*, Comares, Granada, 2002; C. SÁNCHEZ CARAZO, *La intimidad y el secreto médico*, Díez de Santos, Madrid, 2000.

dia. Esta normativa sectorial, en todo caso, no se sale de los principios establecidos en la LOPD[90].

Así, la realidad social sigue cambiando, lo que lleva a regular determinados tratamientos específicos, a través de leyes sectoriales, sin reformar necesariamente la LOPD. Después de las sucesivas leyes orgánicas, el legislador ha necesitado diversas regulaciones sectoriales para abordar la protección de datos en campos específicos. Además de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, tenemos que tener en cuenta lo previsto en la Ley 32/2003, General de Telecomunicaciones, o la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información. En todo caso, estas normas sí contienen una referencia expresa a la legislación de protección de datos y a su carácter supletorio, al igual que lo han hecho las Directivas de las que estas Leyes son transposición con la Directiva 95/46/CE. Este procedimiento es especialmente apropiado para materias como las tecnologías de la información y la comunicación, que se prestan a constantes cambios[91] y que pueden llegar a afectar a otros derechos. Por último, una regulación flexible de la protección de datos permite a los órganos encargados de su interpretación y aplicación, en especial a las Agencias de Protección de Datos, adaptar los principios a las situaciones que sucesivamente se presenten[92]. La adecuación de la normativa de protección de datos a los distintos sectores a través de la interpretación de la normativa general por las Autoridades de Control es una vía aún sin explorar que puede facilitar la adaptación de la normativa a determinados ámbitos sin necesidad de aprobar normas específicas.

En todo caso, sí se echa en falta alguna remisión de la LOPD a otras leyes con las que está conectada materialmente. Así, si la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, no contenía ninguna referencia a la LORTAD, tampoco la nueva LOPD se remite a la Ley 30/1992, de 26 de noviembre. Hubiera sido positiva una mayor coordinación para evitar incongruencias, especialmente entre el derecho de acceso a los datos personales —art. 15 LOPD—, facultad contenida en el derecho fundamental a la protección de datos personales del artículo 18.4 CE, y el derecho de acceso de los ciudadanos a los archivos y registros administrativos, previsto en el artículo 105.b) CE y en el artículo 37 LRJAPyPAC[93]. Esto es especialmente

---

[90] Una exposición que explica los principios de protección de datos y los derechos de los pacientes en relación con la historia clínica, que trata de integrar y complementar la LOPD y la Ley 41/2002, de 14 de noviembre, puede verse en A. TRONCOSO REIGADA, «Introducción y Presentación», en *Guía de Protección de Datos Personales para Servicios Sanitarios Públicos*, APDCM-Civitas, Madrid, 2004, págs. 11-58.

[91] Obsérvese, por ejemplo, lo obsoleto que se ha quedado el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

[92] Cfr. A. E. PÉREZ LUÑO, «Comentario legislativo...», cit., pág. 412.

[93] Cfr. J. GONZÁLEZ PÉREZ y F. GONZÁLEZ NAVARRO, *Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común*, I, 2.ª ed, Civitas, Madrid, 1999,

importante en el caso del derecho de acceso a datos personales que obran en ficheros no informatizados sino manual-estructurados, que puede prestarse a confusión con el derecho de acceso a archivos y registros administrativos. En todo caso, el derecho de acceso a archivos y registros administrativos no tienen por qué contener datos de carácter personal, y puede consistir meramente en documentación administrativa. Además, muchos archivos administrativos se encuentran ordenados por fechas, y no de manera alfabetizada o a través de cualquier otro dato personal, lo que no facilita su accesibilidad. Sí comparte la Ley 30/1992, de 26 de noviembre, con la LOPD algunas de las materias que ésta remite a sus disposiciones específicas, como es el caso de los archivos del régimen electoral general o los del Registro Civil y del Registro Central de Penados y Rebeldes.

2. EL TRIBUNAL CONSTITUCIONAL EN LA DEFINICIÓN DEL CONTENIDO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES: ANÁLISIS CRÍTICO DE LA JURISPRUDENCIA CONSTITUCIONAL

Vamos a analizar el significado de los preceptos constitucionales a partir del estudio de la jurisprudencia constitucional, que ha tratado de definir las obligaciones que la Constitución impone sobre protección de datos a particulares y a poderes públicos. El Tribunal Constitucional ha desarrollado una intensa labor de interpretación del artículo 18.4 CE para construir la existencia de un derecho fundamental a la protección de datos personales. No obstante, la jurisprudencia constitucional en este punto no ha sido uniforme, pecando sus pronunciamientos de algunas contradicciones en relación con su jurisprudencia precedente. En todo caso, antes de comenzar a estudiar la jurisprudencia constitucional, vamos a analizar los criterios de interpretación constitucional del artículo 18.4 CE, teniendo en cuenta la teoría de la norma y el tipo de actividad enjuiciada[94].

a) *Criterios de interpretación constitucional del artículo 18.4*

Las normas constitucionales pueden clasificarse, atendiendo a su mayor o menor precisión o a su mayor o menor densidad normativa, en cláusulas

---

págs. 1019-1085. Cfr. M. FERNÁNDEZ SALMERÓN, *La protección de los datos personales en las Administraciones Públicas*, cit., págs. 340 y ss.; S. FERNÁNDEZ RAMOS, *El derecho de acceso a los documentos administrativos*, Marcial Pons, Madrid, 1997, págs. 366-380; J. M. CASTELLS ARTECHE, «Derecho a la privacidad», cit., pág. 267. En todo caso, hay que señalar que la LRJAPyPAC —art. 38—, al referirse a los registros generales, obliga a su instalación en soporte informático, así como a garantizar la integración con los restantes registros de órganos administrativos.

[94] Nos remitimos a lo que hemos expuesto en A. TRONCOSO REIGADA, «Método jurídico, interpretación constitucional y principio democrático», en E. ESPÍN y F. J. DÍAZ REVORIO, *La justicia constitucional en el Estado democrático*, Tirant lo Blanch, Valencia, 2000, págs. 399-454, especialmente 450-454.

abiertas —conceptos— y cláusulas cerradas —concepciones—[95]. Dentro de las primeras habría que distinguir los valores y los principios, y dentro de las segundas, las reglas. Las reglas se caracterizan porque son normas muy precisas que no dejan libertad al intérprete. Los principios se diferencian de los valores en que los primeros tienen una mayor densidad normativa[96]. La mayoría de los preceptos constitucionales que reconocen derechos están redactados como valores. Pues bien, la afirmación contenida en el artículo 18.4 CE —«[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»— es, como hemos señalado anteriormente, una cláusula abierta, una cláusula general, no una cláusula cerrada; es un valor, no una regla constitucional. Esto no es algo excepcional ya que la Constitución se caracteriza por la abundancia de cláusulas generales. Esta ambigüedad o amplitud de la Constitución tiene indudables ventajas: facilita el consenso, permite que la Constitución informe y sea la norma principial y de cierre de todo el ordenamiento jurídico, facilita su contenido programático y transformador y permite su evolutividad y su capacidad de adaptación a las nuevas situaciones, sin necesidad de acudir a la reforma constitucional, elemento éste muy importante cuando se aborda cómo pueden afectar las tecnologías de la información a los derechos fundamentales.

Pues bien, teniendo en cuenta esta clasificación de los preceptos constitucionales a partir de la teoría de la norma, se puede afirmar que si bien sobre las reglas y los principios constitucionales es posible adoptar una decisión jurídica —claramente fundamentada sobre el parámetro constitucional—, en cambio, la jurisprudencia constitucional establecida sobre la interpretación de valores y de cláusulas generales corre serios riesgos de no ser una actividad jurídica, sino una jurisprudencia ideológica o filosófica. El método jurídico se caracteriza porque aplica no una voluntad propia, sino una voluntad ajena, la voluntad de la norma que se trata de comprender. Por ello, los razonamientos jurídicos deben estar motivados —argumentados— en base al parámetro —en este caso, la Constitución— y deben ser aceptados por su fuerza explicativa. El método jurídico puede ser calificado de «objetivo» porque empieza y acaba en el dato normativo, porque estudia un problema a la luz de un parámetro «objetivo», que el intérprete no ha creado ni puede cambiar y que es susceptible de una aplicación neutral.

El método jurídico exige aplicar sólo aquello previsto expresamente en la Constitución. Pues bien, el artículo 18.4 CE, que únicamente establece que

---

[95] Cfr. M. ARAGÓN, *Constitución y Democracia*, Tecnos, Madrid, 1990, págs. 91-97; G. ZAGREBELSKY, *La Giustizia Costituzionale*, Il Mulino, Bologna, 1988, págs. 125-130; R. DWORKIN, *Los derechos en serio*, Ariel, Barcelona, 1984, caps. II y III; A. E. PÉREZ LUÑO, *Derechos humanos, Estado de Derecho y Constitución*, cit., págs. 291-295; L. PRIETO SANCHÍS, *Ideología e interpretación jurídica*, Tecnos, Madrid, 1987, págs. 66-73.

[96] Sería una regla la previsión del artículo 15 CE: «Queda abolida la pena de muerte, salvo lo que puedan disponer las leyes penales militares para tiempos de guerra». Distintos ejemplos de principios los encontramos en el artículo 9.3 CE —por ejemplo, el de jerarquía normativa—.

«[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», no tiene una densidad normativa suficiente que facilite el análisis constitucional de la actividad del legislador a través de un método estrictamente jurídico. Por ello, la determinación del contenido del artículo 18.4 CE para poder llevar a cabo el enjuiciamiento de la actividad legislativa puede no ser tanto una decisión jurídica, sino una decisión política; o, mejor dicho, una decisión política bajo procedimiento judicial —*justizformig*—[97]. De esta forma aparece uno de los peligros de la interpretación constitucional, que es el riesgo contramayoritario; es decir, el peligro de que un órgano independiente no sometido a controles políticos vaya a aplicar normas amplias y ambiguas para desautorizar al legislador, cercenando la libertad política de éste para desarrollar la Constitución. Surge así nítidamente un conflicto entre el Poder Legislativo, que tiene legitimidad democrática —elegido por el pueblo y controlado por el pueblo a través de elecciones periódicas—, y el Tribunal Constitucional, que es un órgano independiente que no responde ante el depositario de la soberanía popular[98]. De esta manera, si bien es verdad que frecuentemente los jueces ordinarios toman decisiones no estrechamente apoyadas en la ley, hay que reseñar aquí que la gran diferencia entre el activismo de los jueces ordinarios y el del Tribunal Constitucional es que el primero no pone en riesgo el principio democrático, al no declarar inconstitucional las leyes aprobadas por la mayoría política[99].

Por ello, se hace necesario adaptar la interpretación constitucional no sólo al tipo de cláusula, distinguiendo la interpretación de cláusulas abiertas y cláusulas cerradas, sino también a la clase de actividad enjuiciada, diferenciando la actividad política —la ley, pero también los actos políticos de la Administración— de la actividad *materialmente* jurídica de los poderes públicos, prestando atención especialmente a qué actuaciones jurisdiccionales pueden llegar a amenazar el principio democrático. De esta forma, hemos defendido la necesidad de un método jurídico propio para la interpretación de la Constitución, que se adapte tanto a las peculiaridades de la norma constitucional —a la existencia de distintos tipos de preceptos constitucionales— como a los riesgos contramayoritarios que conlleva esta interpretación constitucional.

A partir de estos principios, se puede afirmar que las cláusulas abiertas —y, entre ellas, el art. 18.4 CE— son para el legislador —y para el gobierno

---

[97] Así, hay que señalar con Carl SCHMITT que «la decisión que resuelve las dudas sobre el contenido de una determinación constitucional no puede deducirse del propio contenido dudoso; por ello, esta decisión en su esencia no es una decisión judicial, la cual supone la decisión de una pretensión conflictiva sobre el fundamento de una ley, supuestamente clara e inequívoca». Cfr. C. SCHMITT, *Teoría de la Constitución*, Alianza Universidad, Madrid, 1982, y *La defensa de la Constitución*, Tecnos, Madrid, 1983.

[98] Cfr. V. FERRERES, *Justicia constitucional y democracia*, CEPC, Madrid, 1997; E. AJA (ed.), *Las tensiones entre el Tribunal Constitucional y el Legislador en la Europa occidental*, Ariel, Barcelona, 1998; M. L. VOLCANSEK, *Judicial Politics and Policy-Making in Western Europe*, Frank Cass, London, 1992; D. AMIRANTE, *Giudici costituzionale e funzione legislativa. L'esperienza francese*, Cedam, Padova, 1991.

[99] Cfr. F. RUBIO LLORENTE, voz «Igualdad», en *Enciclopedia Jurídica Civitas*, Madrid, 1995, II, pág. 3367.

cuando desarrolla su actividad política[100]— marcos de legitimidad dentro de los cuales se puede mover libremente[101]. El hecho de que los derechos fundamentales sean proclamados constitucionalmente a través de cláusulas generales, es decir, el hecho de que el constituyente haya elegido preferentemente valores como la clase de norma apropiada para reconocer derechos fundamentales, es un claro indicio de la delegación de estas materias al legislador; en el caso de los derechos de la Sección I del Capítulo II del Título I, al legislador orgánico. Así, los órganos jurisdiccionales —y la doctrina académica—, a la hora de analizar la legitimidad constitucional de la actividad legislativa que desarrolla el artículo 18.4 CE —tanto de la LOPD como de la LORTAD—, tienen la obligación de respetar la legítima libertad del legislador y del gobierno. Este artículo 18.4 CE delega en el legislador una gran capacidad de configuración del derecho a la protección de datos personales. Sólo pueden declararse o considerarse inconstitucionales aquellos preceptos legales que salgan fuera del marco del artículo 18.4 CE, marco que está delimitado por el contenido esencial de este derecho. Este contenido esencial es un contenido mínimo, que deja un amplio margen de libertad para el legislador[102]. Por ello, el método jurídico que se tiene que aplicar tiene como contenido principal el respeto al principio democrático. Se trata de aplicar un principio de restricción judicial, que significa que sólo se podrán declarar inconstitucionales —o considerar inconstitucionales por la doctrina académica— los preceptos de la LOPD o de la LORTAD que representen supuestos claros de incompatibilidad con la Constitución, recibiendo el poder político el beneficio del *in dubio* en los casos oscuros[103].

De esta forma, en la resolución de recursos de inconstitucionalidad sobre preceptos de la legislación de protección de datos, y en general en el análisis de constitucionalidad de estas normas, hay que distinguir entre la valoración política que nos pueden merecer estas leyes y el análisis jurídico, que debe tener en cuenta que la Constitución es una norma con voluntad propia, fre-

---

[100] Cuando hablamos de la actividad política del gobierno en materia de protección de datos, nos estamos refiriendo, por ejemplo, al margen de maniobra que deja el principio de seguridad del artículo 9 LOPD para desarrollar un Reglamento de Seguridad que establezca distintos tipos de medidas de seguridad de nivel básico, medio y alto, para distintos tipos de ficheros.

[101] La afirmación del principio de deferencia al legislador se puede ver, por ejemplo, en la STC 107/1996, de 12 de junio; en la STC 78/1989, de 2 de noviembre —sobre la libertad del legislador para conformar el régimen de incompatibilidades de los empleados públicos—; en la STC 227/1988, de 29 de noviembre —sobre límites al derecho de propiedad en beneficio del interés general—; en la STC 37/1994, de 10 de febrero —sobre fórmulas de gestión privada en la Seguridad Social—; y en la STC 134/1987, de 21 de julio —sobre límites a las pensiones de jubilación—.

[102] Esta posición no está necesariamente en contradicción con la concepción espacial de los derechos fundamentales que propone M. MEDINA —*La vinculación negativa del legislador a los derechos fundamentales*, McGraw-Hill, Madrid, 1996—, siempre que se interprete restrictivamente el contenido esencial del derecho fundamental absolutamente intangible para el legislador y que no se desarrolle un juicio de proporcionalidad rígido cuando la ley afecta al contenido normal del derecho fundamental. No sería admisible para nosotros que la libertad amplia del legislador aparezca únicamente extramuros del contenido total de los derechos fundamentales, sólo en su contenido suplementario o adicional.

[103] Cfr., más ampliamente, A. TRONCOSO REIGADA, *Interpretazione della Costituzione e Judicial Restraint*, Bologna, 1993.

cuentemente distinta y más amplia que la voluntad de su intérprete. Así, el análisis constitucional de la LORTAD o de la LOPD que llevan a cabo la doctrina académica o el Tribunal Constitucional no tiene nada que ver con la valoración de su mayor o menor oportunidad. Es necesario separar la reflexión política sobre la protección de los datos personales del enjuiciamiento constitucional de una actividad política como es la actividad legislativa, evitando así que la interpretación de la Constitución se transforme en una búsqueda de la propia ideología. Lo contrario conllevaría que los órganos jurisdiccionales independientes practiquen un control político que no les corresponde.

De esta forma, el artículo 18.4 CE representa para el legislador y para el gobierno —cuando desarrolla una actividad política— un vínculo negativo, un marco de legitimidad política que les permite adoptar decisiones distintas, con el único límite de no salirse del marco constitucional y de no lesionar el contenido esencial de este derecho fundamental.

El planteamiento hecho hasta ahora cambia cuando lo que se enjuicia no es la actividad legislativa y la actividad política del gobierno, sino la actividad administrativa, que está sometida materialmente a la ley y al Derecho. Las cláusulas generales —especialmente aquellas que reconocen derechos fundamentales— son, para la Administración y para el resto de poderes públicos, cuando desarrollan una actividad jurídica sometida plenamente a la ley y al Derecho —art. 9.1 CE—, obligaciones positivas de buscar la máxima eficacia del derecho fundamental. En este caso, al no existir riesgos contramayoritarios, el criterio fundamental de interpretación debe ser la protección de los derechos fundamentales —el principio *pro libertate*[104]—, aunque éstos se recojan en cláusulas generales. Este principio insiste en la fuerza expansiva de los derechos fundamentales, exigiendo una interpretación más favorable a la efectividad de los mismos y más restrictiva con los límites a su ejercicio. Es decir, mientras que las cláusulas generales que recogen derechos fundamentales son —para el legislador y para el gobierno, cuando ejerce la dirección política— límites negativos, marcos que admiten muchas opciones legítimas, en cambio, las mismas cláusulas generales que albergan derechos fundamentales son vínculos positivos, que obligan a la Administración —cuando desarrolla una actividad jurídica— y a los Tribunales a aplicar siempre los principios constitucionales y los derechos fundamentales, dando la razón a quien tenga mejor derecho o, en expresión de DWORKIN, a aquel que tenga *derecho a vencer*[105].

Por ello, cuando la actividad de un poder público está sometida *plenamente* a la ley y al Derecho, ésta tiene que respetar los derechos en presencia, y entre ellos el derecho fundamental a la protección de datos personales. El parámetro último de la actividad *materialmente* jurídica de los poderes pú-

[104] Cfr. SSTC 21/1981, de 15 de junio, y 159/1986. Sobre la relevancia de este principio, cfr. A. PEREZ LUÑO, *op. cit.*, págs. 315-316.

[105] Cfr. R. DWORKIN, *Los derechos en serio*, cit., págs. 146-208.

blicos es siempre la propia Constitución[106]. Por ello, el derecho fundamental a la protección de datos personales reconocido en el artículo 18.4 CE tiene que ser aplicado plenamente por la Administración, no sólo en su contenido mínimo. La Administración tiene que buscar la eficacia máxima de los derechos fundamentales, y también de este derecho fundamental. Por ello, el enjuiciamiento por parte de los órganos jurisdiccionales de la actividad administrativa y de cómo ésta respeta el derecho fundamental a la protección de datos personales debe desarrollarse a partir del principio *pro libertate*, que demanda el máximo respeto al derecho fundamental y prohíbe cualquier arbitrariedad de los poderes públicos.

Por eso, el artículo 18.4 CE, en la actividad materialmente jurídica de la Administración y en su enjuiciamiento por los jueces ordinarios, no es un marco, sino un derecho que exige su máxima eficacia. La Administración y los Tribunales no son libres, sino que están obligados de manera positiva por los derechos fundamentales, de forma que el enjuiciamiento de sus decisiones se desarrollará aplicando el principio *pro libertate*. Por tanto, el mismo artículo 18.4 CE es una norma abierta para el legislador y para el gobierno —en su actividad de dirección política— y una norma cerrada para la Administración y los Tribunales ordinarios. La Constitución es, al mismo tiempo, un vínculo negativo —*negative Bindung*—, que respeta el pluralismo político del legislador y de la dirección política del gobierno, y un vínculo positivo —*positive Bindung*—, una exigencia *magis ut valeat* que alberga un imperativo unívoco para la actividad jurídica de los poderes públicos[107].

Como se ha podido ver, la interpretación de los preceptos constitucionales tiene que adaptarse al tipo de cláusula —abierta o cerrada— o a la naturaleza de la actividad enjuiciada —política o jurídica—. Como el enjuiciamiento de la legitimidad constitucional de la actividad legislativa se analiza principalmente a través de los recursos de inconstitucionalidad, y el enjuiciamiento de la legitimidad constitucional —del respeto a los derechos— de la actividad administrativa a través de los recursos de amparo, se puede afirmar igualmente que la interpretación constitucional tiene que adaptarse a cada uno de los procedimientos constitucionales. Por ello, a la hora de analizar la jurisprudencia constitucional sobre protección de datos personales, vamos a diferenciar aquellas sentencias que resuelven recursos de amparo de aquellas otras que resuelven recursos de inconstitucionalidad[108].

---

[106] Cfr. J. ESSER, *Principio y norma en la elaboración del Derecho privado*, Bosch, Barcelona, 1961; E. GARCÍA DE ENTERRÍA, *Reflexiones sobre la Ley y los principios generales del Derecho*, Civitas, Madrid, 1984.

[107] Cfr. P. HÄBERLE, «Die offene Gesellschaft der Verfassungsinterpreten», *JZ*, 1975, págs. 297 y ss., y *Die Verfassung des Pluralismus*, Athenäum, 1980. Cfr las referencias a este autor en A. TRONCOSO REIGADA, «Método jurídico, interpretación constitucional y principio democrático», cit.

[108] Hemos analizado la posición del legislador, de la Administración y de los Tribunales —tanto de los jueces ordinarios como del Tribunal Constitucional— ante el derecho fundamental a la protección de datos personales. Faltaría por delimitar la posición de los particulares, cuando no existía desarrollo legislativo —antes de la aprobación de la LORTAD y de la LOPD—. Esta cuestión está vinculada a la problemática de la eficacia horizontal de los derechos fundamentales y será abordada en el trabajo más amplio que se encuentra en preparación.

b) *La definición del contenido del derecho fundamental a la protección de datos personales a través de la resolución de recursos de amparo*

La Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, constituye el primer pronunciamiento de nuestro Alto Tribunal del que puede extraerse el reconocimiento de un verdadero derecho fundamental a la protección de datos personales. Esta Sentencia fue durante muchos años la resolución de referencia del Tribunal Constitucional sobre protección de datos personales, el auténtico *leading case*[109]. La Sentencia 254/1993, de 20 de julio, tiene su origen en la petición de información en 1986 por parte de un ciudadano vasco al Gobernador Civil de Guipúzcoa sobre los ficheros automatizados de la Administración General del Estado que pudiesen contener datos relativos a su persona: «si la Administración del Estado o cualquier organismo de ella dependiente dispone de ficheros automatizados donde figuren mis datos de carácter personal; que en caso afirmativo se me indique la finalidad principal de dichos ficheros, la autoridad que los controla y su residencia habitual; que se me comuniquen los datos existentes en dichos ficheros referidos a mi persona, de forma inteligible y sin demora». Esto lo fundamentaba el solicitante en virtud de la aplicación inmediata del artículo 8 del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que atribuía a toda persona un conjunto de facultades para controlar sus datos personales[110]. La solicitud fue denegada por silencio por la Administración —Gobierno Civil y Ministerio del Interior—, denegación que fue recurrida y desestimada por la jurisdicción contencioso-administrativa —Audiencia Territorial y Tribunal Supremo—[111]. El Tribunal Constitu-

---

[109] Sobre la Sentencia 254/1993, de 20 de julio, cfr. I. VILLAVERDE MENÉNDEZ, «Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993», *REDC,* n.º 41, 1994, págs. 187 y ss.; A. R. GONZÁLEZ MURUA, «Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales», *RVAP*, n.º 37, 1993; L. M. ARROYO YANES, «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*, n.º 16, 1993, págs. 119 y ss.

[110] El artículo 8, titulado «Garantías complementarias para la persona concernida», dispone que: «Cualquier persona deberá poder: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad o residencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo».

[111] La Audiencia desestimó el recurso por entender que los preceptos del Convenio 108 del Consejo de Europa no podían ser aplicados directamente hasta la adopción de las medidas necesarias de Derecho interno, lo que se encuentra también contemplado en el artículo 94.1.e) CE, donde se prevé que la ejecución de los tratados o convenios puede exigir medidas legislativas. El Tribunal Supremo confirmó que el Convenio 108, aunque incorporado al ordenamiento jurídico español, precisa para su aplicación práctica el complemento de una actividad interna legislativa y reglamentaria que el Estado no había desarrollado todavía.

cional conoció el asunto a través del procedimiento de amparo, en cuya demanda se sostenía que la negativa administrativa a comunicar la información solicitada representaba una vulneración por parte de los poderes públicos de los derechos fundamentales del recurrente recogidos en los artículos 18.1 y 18.4 CE, los cuales surten efectos directamente.

En esta Sentencia, el Tribunal Constitucional afirmó por primera vez la existencia de un derecho fundamental directamente derivado del artículo 18.4 CE, diferenciado del derecho a la intimidad, acogiendo de este modo las formulaciones de un sector doctrinal: «Dispone el art. 18.4 CE que "la 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". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática" —FJ 6.º—. De esta forma, el Tribunal Constitucional afirma que aunque el derecho a la protección de los datos personales en muchos supuestos es un derecho instrumental del derecho a la intimidad o de otros derechos fundamentales, es también un derecho o libertad fundamental en sí mismo, y no sólo por su carácter instrumental. Por otra parte, el Alto Tribunal identificó el uso de la informática con la protección de datos, de lo que se deduce, en principio, que el artículo 18.4 CE sólo opera en el marco de esta tecnología y no protege frente a tratamientos personales no automatizados.

De esta forma, el Tribunal Constitucional define la naturaleza jurídica y la eficacia normativa del artículo 18.4 CE. Este precepto constitucional contiene un derecho fundamental a la protección de datos personales. Como es sabido, la Constitución es norma jurídica y los derechos fundamentales vinculan a los poderes públicos —arts. 9.1 y 53.1 CE— aunque no exista ley que los desarrolle[112]. Esto es muy importante en este caso, ya que cuando su-

[112] Como señala LUCAS MURILLO DE LA CUEVA, «[a]l igual que ocurre en otros supuestos (por ejemplo en el artículo 17.4, cuando prevé que la ley regulará un procedimiento de habeas corpus o determinará el plazo máximo de duración de la prisión provisional), la remisión al legislador no debe distraernos de lo principal: la prohibición constitucional de la privación ilegal de libertad, de la prolongación indefinida de la prisión provisional, o de la destrucción de la autodeterminación informativa a causa de un uso abusivo de la informática. El retraso en el desarrollo legislativo no elimina lo anterior, ni la ausencia de los procedimientos oportunos ha de impedir al juzgador hacer efectivo un expreso requerimiento constitucional cuando a él se acojan personas perjudicadas por su inobservancia. La eficacia normativa directa y la supremacía de la Constitución imponen esta solución. Por lo demás, tampoco parece que deba impedir la afirmación del derecho a la autodeterminación informativa la crítica que se centre en su carácter derivado

cedieron los actos administrativos y las resoluciones judiciales impugnados ante el Tribunal Constitucional no existía aún desarrollo legislativo del artículo 18.4.

Como sabemos, que exista una norma legal o no es indiferente a la hora de tutelar los derechos fundamentales. Los derechos fundamentales no son principios programáticos que deben ser desarrollados por el legislador, sino que son origen de derechos y obligaciones que tienen una aplicación inmediata; es decir, a partir de la aprobación de la Constitución, los derechos fundamentales en ella reconocidos tienen un contenido que ha de ser respetado por los poderes públicos y tutelado en sede de amparo constitucional. Una cosa es que los derechos constitucionales adquieran mediante la *interpositio legislatoris* un mayor contenido y eficacia, y otra cosa distinta es convertir los derechos constitucionales en mandatos al legislador, sin virtualidad para ser exigidos si éste no los ha desarrollado. La falta de desarrollo legislativo del artículo 18.4 CE no puede implicar que el derecho fundamental a la protección de datos se convierta en un reconocimiento meramente teórico, sin ninguna relevancia práctica. Es necesario, por tanto, precisar el «mínimo contenido» del derecho fundamental a la protección de datos que opera sin desarrollo legislativo. Lo determinante es, por tanto, fijar el contenido constitucional —las facultades— del artículo 18.4 CE, que debe tener aplicación directa e inmediata a partir de su positivación constitucional, sin estar supeditado al desarrollo legislativo.

La consideración de la protección de datos personales como un derecho fundamental conlleva afirmar que tiene no sólo una vertiente subjetiva que exige la abstención de los poderes públicos, sino también una vertiente objetiva o prestacional que demanda una actividad positiva de los poderes públicos, y que atribuye facultades a los ciudadanos[113]. Así, como señala el Ministerio Fiscal —que informó favorablemente el otorgamiento del amparo—, la intimidad poseía en un primer momento un contenido negativo, de exclusión de intromisiones ilegítimas. Pero en la actualidad es concebida como una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona, que han salido ya de la esfera de la intimidad para convertirse en elementos de un archivo electrónico. La «libertad informática» reconocida por el artículo 18.4 CE «ya no es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de *habeas data*». La afirmación de estas facultades positivas del derecho fundamental a la protección de datos personales se obtiene a partir de la doctrina del contenido esencial de los derechos fundamentales, que se delimita a través de la vía de la naturaleza jurídica o

---

o instrumental respecto de otros derechos». Cfr. P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, cit., pág. 157.

[113] Cfr. también A. TRONCOSO REIGADA, «Dogmática administrativa y derecho constitucional; el caso del servicio público», *REDC*, n.º 57, 1999, págs. 147-164; íd., «El Estado Social», en *Manual de Derecho Constitucional* (dirigido por el Prof. Manuel ARAGÓN), Portalderecho. www.Iustelcom.

del tipo abstracto —a partir de las ideas generalmente admitidas entre los juristas y en el Derecho comparado de lo que este derecho a la protección de datos significa— y, especialmente, a partir de la vía de los intereses jurídicos en presencia[114]. Es claro que la facultad de acceder a la propia información personal que se encuentra en ficheros informatizados es un interés jurídico protegido que da vida a la libertad informática, y si esta facultad no se reconoce —tanto en la legislación como, en el caso que nos ocupa, en la aplicación por parte de la Administración Pública de este derecho fundamental a partir de su reconocimiento constitucional— los intereses jurídicos que dan vida al derecho fundamental a la protección de datos —que justifican que exista este derecho— quedarían desprotegidos y el derecho fundamental a la protección de datos personales no sería reconocible en la legislación como perteneciente a su tipo previo[115]. Otras facultades que estarían dentro del derecho fundamental a la protección de datos personales serían, por ejemplo, el principio de consentimiento —la negativa a suministrar los propios datos personales—, la oposición para que los datos sean conservados una vez finalizado el fin que justificó su obtención o para utilización para fines distintos[116].

Lógicamente, el Tribunal Constitucional también se sirve para la determinación del contenido esencial del derecho fundamental a la protección de datos personales del Convenio 108 del Consejo de Europa, de 28 de enero de 1981. Como es sabido, aunque el Convenio no puede invocarse directamente, el artículo 10.2 CE señala que «[l]as normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España». La interpretación del artículo 18.4 CE a partir de este Convenio lleva a afirmar que el derecho fundamental a la protección de datos personales integra también un conjunto de facultades positivas, como el derecho de los ciudadanos a conocer qué datos constan sobre ellos en los archivos automatizados[117].

---

[114] Cfr. STC 11/1981, de 8 de abril.

[115] «Esta constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el artículo 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente» —FJ 7.º—.

[116] La inclusión de facultades positivas dentro del derecho fundamental a la protección de datos personales también se deduce de la propia interpretación constitucional del legislador, que es otro intérprete de la Constitución, y que ha previsto un conjunto de garantías positivas tanto en la LORTAD como en la LOPD, lo que no suprime, obviamente, el fundamento constitucional de estas garantías.

[117] Sin embargo, como hemos señalado anteriormente, Rodríguez-Piñero manifiesta en su voto particular que el Convenio del Consejo de Europa no puede convertirse en parámetro constitucional ni en la legislación de desarrollo a la que se remite el artículo 18.4, ya que esto crearía una especie de procedi-

El hecho de que la Administración Pública —o las empresas privadas— no tenga medios materiales precisos para facilitar el derecho de acceso a la información personal recogida en un fichero informatizado no es un argumento que pueda justificar la vulneración de un derecho fundamental. Si bien es verdad que la inexistencia a estos efectos de una organización administrativa capaz de garantizar el derecho de acceso es consecuencia de la ausencia de desarrollo legislativo de este derecho, esto no suprime la vinculación a los derechos fundamentales de todos los poderes públicos —art. 53.1 CE—. Lo fundamental en el análisis constitucional en este caso es definir si hay o no derecho —si la libertad informática contiene el control sobre los propios datos, el *habeas data*—, no si hay o no capacidad administrativa[118].

Esta es la parte interesante —por su relevancia práctica— de esta Sentencia del Tribunal Constitucional. No obstante, la doctrina académica ha tratado de analizar también desde una perspectiva más teórica o filosófica si esta Sentencia reconoce un derecho fundamental a la protección de datos personales diferenciado del derecho a la intimidad. Así, en el fundamento jurídico sexto ya citado el Tribunal Constitucional afirma la existencia de un derecho fundamental autónomo en el artículo 18.4 CE, atribuyéndole a éste una doble naturaleza: por una parte, de instituto de garantía de la intimidad y de otros derechos fundamentales; por otra, de derecho fundamental propio «frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos»[119]. No obstante, en otros apartados de la Sentencia se observa también una voluntad de relacionar el artículo 18.4 CE hacia la tutela exclusiva de la *intimidad*[120]. Así, al principio parece que la argumentación se va a mover en el campo del derecho a la intimidad: «La cuestión suscitada en el presente recurso de amparo consiste en determinar si la negativa a suministrar la información solicitada, acerca de los datos personales del actor que la Administración del Estado posee en ficheros automatizados, vulnera o no los derechos fundamentales a la intimidad y a la propia imagen que le reconoce el artículo 18 de la Constitución, tanto en su apartado 1 como en el 4»[121]. El Tribu-

---

miento extralegislativo que generaría obligaciones para la Administración sin base legislativa. Este Magistrado señala que la existencia del Convenio no puede implicar un efecto directo e inmediato que obligue a los poderes públicos a su ejecución prescindiendo de la necesaria intermediación legislativa, como exige el artículo 94 CE. Cfr. *supra,* nota 20.

[118] Además, en este caso concreto, la Administración desestimó la solicitud de derecho de acceso por silencio negativo y no parece razonable que la Administración se beneficie del incumplimiento de su obligación de resolver. La respuesta podrá ser mejor o peor pero, en todo caso, los poderes públicos tienen la obligación de responder.

[119] Para ASPAS, el Tribunal Constitucional opta por una doble caracterización del artículo 18.4 como derecho fundamental y como garantía institucional, ya que así puede limitar la mayor libertad de configuración que tiene el legislador con las garantías institucionales. Cfr. J. M. ASPAS ASPAS, «La libertad informática, un nuevo derecho fundamental desvelado por el Tribunal Constitucional (STC 254/1993, de 20 de julio)», *Revista Aragonesa de Administración Pública*, n.º 4, 1994, pág. 424.

[120] Así, uno de los reproches que se han efectuado a la Sentencia es que no reconoce abiertamente un derecho autónomo a la autodeterminación informativa, sino que, con un discurso confuso, intercala referencias a la intimidad y a la libertad informática. Cfr. P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de los datos*, Comares, Granada, 1999, págs. 14 y 15, nota 8.

[121] FJ 1.º.

nal Constitucional reconoció el derecho a la autodeterminación informativa, pero fundamentó su planteamiento en el derecho a la intimidad. Así, el Tribunal Constitucional basó en el derecho a la intimidad y en los intereses jurídicos que le dan vida la afirmación de la existencia en el derecho a la protección de datos personales no sólo de facultades negativas o de exclusión, sino de facultades positivas, que atribuyen al titular de los datos la capacidad de exigir un *facere* —un deber de prestación— a la autoridad pública responsable del fichero[122]. Aunque se hacen referencias a la libertad informática y al *habeas data*, la resolución del Tribunal, estimando el amparo, se fundamenta en el derecho a la intimidad. Así, las facultades necesarias para obtener una tutela adecuada respecto del uso de los datos personales «*forman parte del contenido del derecho a la intimidad*», y es precisamente a causa de ello, y en tanto que los derechos fundamentales vinculan a todos los poderes públicos con independencia de su desarrollo legislativo, por lo que se otorga el amparo. Realmente, en esta Sentencia, el Tribunal Constitucional se refiere a los conceptos de derecho a la intimidad y de libertad informática a veces como equivalentes, a veces como términos distintos y complementarios. En los distintos fundamentos jurídicos, el Tribunal Constitucional fija su argumentación en uno o en otro, sin clarificar cuál es el derecho fundamental cuya tutela se pretende. Como señala Ricard MARTÍNEZ, a lo largo del azaroso discurrir de esta Sentencia se ha pasado del presunto nacimiento de un nuevo derecho fundamental a la aparente reconducción del problema hacia el derecho a la intimidad[123]. El Fundamento Jurídico 6.º proclama el nuevo derecho y, a continuación, el Fundamento Jurídico 7.º remite el bien jurídico protegido al ámbito de la intimidad[124]. El tenor de la Sentencia 254/1993, de 20 de julio, así como de otras que reproducen la doctrina de ésta, ha sido criticado por su ambigüedad en las afirmaciones relativas a la

---

[122] Así, decía la Sentencia que «las facultades precisas […] son absolutamente necesarias para que los intereses protegidos por el artículo 18 CE, y que dan vida al *derecho fundamental a la intimidad*, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad […]» —FJ 7.º—. La definición por parte del Tribunal Constitucional del artículo 18.4 como «garantía constitucional» alude así al carácter instrumental de este precepto en relación a otros derechos fundamentales, especialmente la intimidad.

[123] «No es ocioso advertir que la reciente aprobación de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (LO 5/1992, de 29 de octubre) no hace más que reforzar las conclusiones alcanzadas con anterioridad. La creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los de titularidad privada. Pero ello no desvirtúa el fundamento constitucional de tales derechos, en cuanto imprescindibles para proteger *el derecho fundamental a la intimidad* en relación con los ficheros automatizados que dependen de los poderes públicos. Ni tampoco exonera a las autoridades administrativas del deber de respetar ese derecho de los ciudadanos, al formar y utilizar los ficheros que albergan datos personales de éstos, ni del deber de satisfacer las peticiones de información deducidas por las personas físicas en el círculo de las competencias propias de tales autoridades» —FJ 9.º—. Cfr. R. MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, cit., págs. 254-300.

[124] Cfr. J. M. PRIETO GUTIÉRREZ, «La jurisprudencia constitucional ante la protección de datos personales», *Boletín del Ministerio de Justicia*, n.º 1880, noviembre de 2000, pág. 3638. Este autor señala que, a pesar de la contradicción entre el FJ 6.º y el 7.º, «ha de prevalecer la declaración de intenciones contenida en el FJ 6.º y, por lo tanto, ampliar las miras hacia el reconocimiento de un nuevo derecho fundamental independiente con base en el artículo 18.4 de la Constitución».

generación de un nuevo derecho fundamental[125]. En todo caso, parece adecuado afirmar que en esta Sentencia se configura la existencia de un derecho fundamental autónomo a la protección de datos personales, sin perjuicio de su carácter instrumental en relación con el derecho a la intimidad y con otros derechos fundamentales[126].

La segunda Sentencia del Tribunal Constitucional es la 143/1994, de 9 de mayo. Esta Sentencia fue dictada en el marco de un recurso de amparo interpuesto por el Consejo General de Colegios de Economistas de España contra la Sentencia de la Sala Tercera del Tribunal Supremo de 7 de octubre de 1992, a la que se reprochaba el haber declarado la inadmisibilidad, por falta de legitimación activa del Consejo, del recurso contencioso-administrativo interpuesto por dicha corporación contra el Real Decreto 338/1990, de 9 de marzo, y la Orden de 14 de marzo de 1990, por los que se regulaban la composición y forma del Número de Identificación Fiscal y la tarjeta acreditativa del mismo, por considerar que vulneraban el derecho fundamental a la intimidad consagrado en el artículo 18 CE[127].

En esta Sentencia se lleva a cabo una reconducción de la protección de datos personales dentro de la esfera del derecho a la intimidad, al que se le ha ampliado su ámbito material. El derecho a la intimidad contiene no sólo unas facultades de exclusión que limitan las intromisiones en la vida privada, sino también unas facultades positivas que permiten el control de la información personal. Es la existencia de estas facultades positivas, que se concretan en garantías, la que permite afirmar la constitucionalidad de una medida. La Sentencia reconoce que el incremento de medios técnicos para el tratamiento de la información puede ocasionar un uso desviado de la información personal y una invasión de la esfera privada de los ciudadanos. Por

---

[125] ROIG sostiene que el carácter dual que la Sentencia 254/1993 atribuye al derecho a la autodeterminación informativa (libertad informática, en sus propios términos), como derecho autónomo y a la vez instrumental de otros, produce la confusión de aquél con la intimidad. Cfr. A. ROIG, «La protección jurídica de las bases de datos personales. Análisis de la jurisprudencia del Tribunal Constitucional», *Revista Jurídica de Cataluña*, n.º 2, 2002, pág. 151.

[126] Para VILLAVERDE MENÉNDEZ, la argumentación inicial del TC conducía a la consideración del artículo 18.4 como sede de un nuevo derecho fundamental de configuración legal. Cfr. I. VILLAVERDE MENÉNDEZ, «Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993», cit., págs. 202 y ss.

[127] El Tribunal Supremo declaró la inadmisibilidad por entender que el Consejo General de Colegios de Economistas de España no tenía ni un interés directo ni un interés legítimo para impugnar el Real Decreto y la Orden reguladora del NIF. Sin embargo, el Tribunal Constitucional aplicó un criterio amplio de legitimación activa en el acceso a la jurisdicción, en virtud del derecho a la tutela judicial efectiva del art. 24.1 CE, que abarca también los intereses legítimos y la potencial ventaja o utilidad de la estimación de la pretensión. Así, entendió que el Consejo General de Colegios de Economistas tenía un interés suficiente para impugnar las disposiciones reguladoras del NIF a la vista de que los economistas estarían obligados en su ejercicio profesional a suministrar datos a la Administración a través de un instrumento que consideraban lesivo de derechos fundamentales. El Ministerio Fiscal interesó que se otorgara el amparo, por cuanto se había vulnerado el derecho a la tutela judicial efectiva del art. 24.1 CE, recordando la doctrina antiformalista en materia de admisibilidad. No obstante, en lo que se refiere a la posible quiebra del artículo 18.1 y 4 CE por parte del Real Decreto y de la Orden Ministerial, el Fiscal era favorable a que lo resolviera el Tribunal Supremo ya que se refería a la vulneración de derechos fundamentales por una normativa reglamentaria y corresponde a ese órgano jurisdiccional su resolución, dado el carácter subsidiario del recurso de amparo.

ello, «correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho —STC 254/1993—. En este sentido ya que "los datos personales que almacena la Administración son utilizados por sus autoridades y servicios", no es posible "aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión". En consecuencia, habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta»[128]. El artículo 18.4 CE se convierte, en el fondo, en una garantía más del derecho a la intimidad[129]. El ejercicio de facultades de control sobre los datos de carácter personal y el establecimiento de medios administrativos que lo hagan posible resultan indispensables para la tutela del derecho a la intimidad. El Tribunal Constitucional opta por un concepto amplio de intimidad que acoja, bajo su regulación, facultades de control por parte del individuo respecto de sus datos personales.

Llama la atención que el ponente de la Sentencia 143/1994, de 9 de mayo, es el Magistrado Rodríguez-Piñero, que emitió un voto particular en la STC 254/1993, de 20 de julio, antes analizada. Este Magistrado aprovecha la ponencia para evitar la afirmación del derecho fundamental a la protección de datos personales como derecho autónomo del derecho a la intimidad. Lo que hace es interpretar el derecho a la intimidad a partir de las necesidades que se derivan de la informática, apoyándose en el Convenio 108, que se interpreta a la luz del derecho fundamental a la intimidad. La Sentencia no realiza esfuerzo alguno por completar e integrar el contenido del artículo 18.4 CE con el Convenio 108 por la vía del artículo 10.2 CE.

El Tribunal no afirma la existencia del derecho a la autodeterminación informativa como derecho fundamental autónomo a partir de artículo 18.4 CE. El Alto Tribunal concibe este artículo como una garantía de protección de la intimidad en sentido amplio. Es decir, el artículo 18.4 CE está protegiendo a la persona frente a la utilización ilegítima de sus datos personales. La informática atenta contra la vida privada del ciudadano, al tratarse de otra modalidad de in-

[128] FJ 7.º.

[129] Para LUCAS MURILLO DE LA CUEVA, todo el razonamiento «se funda en una concepción tradicional del derecho a la intimidad y a que, si bien se resiste a admitir que el NIF pueda constituir una amenaza potencial para los aspectos económicos de la intimidad, acaba concluyendo que, efectivamente el riesgo no existe, no porque sea imposible, sino porque las cautelas establecidas por el ordenamiento jurídico para su utilización lo conjuran». Cfr. P. LUCAS MURILLO DE LA CUEVA, «La primera jurisprudencia sobre el derecho a la autodeterminación informativa», cit.

tromisión, es decir, de injerencia física en ámbitos reservados para la persona. El artículo 18.4 CE y la legislación de desarrollo tratan de establecer mecanismos para que el ciudadano controle el uso de sus informaciones personales.

Lógicamente, el planteamiento de la protección de datos en virtud del derecho a la intimidad presenta muchos aspectos vulnerables. Así, si se considera que el derecho a la intimidad y, en última instancia, el respeto a la dignidad de la persona implican la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, que es además necesario para mantener una calidad mínima de la vida humana, es cuestionable que en abstracto se afirme un ámbito reservado para sí mismo y una eventual vulneración de la intimidad en actividades desenvueltas en el tráfico económico y negocial: «Unas actividades que tienden a desarrollarse en el ámbito de relación con terceros, y a estar sometidas a fórmulas específicas de publicidad, en aras de la seguridad jurídica y de la transparencia en el tráfico económico, de ahí que sólo con extremada dificultad puedan calificarse como reservadas, en el sentido antes descrito típico del juego del derecho a la intimidad. […]. Podría sin embargo aceptarse, como hipótesis, que hubiera casos en que alguno de los extremos sobre los que ha de versar la información puede incidir sobre el ámbito del derecho a la intimidad, pero tampoco sería por ello mismo rechazable a priori la imposición de estas cargas informativas, dado que el derecho a la intimidad, como el resto de los derechos fundamentales no es un derecho absoluto sino que está sometido a límites, especialmente en lo que afecta a la efectividad de otros derechos o deberes constitucionales, en este caso, del deber tributario —art. 31.1 CE—»[130]. El problema reside en que la protección de datos personales, como veremos después, no ofrece su tutela únicamente a los datos íntimos, sino a cualquier dato o información personal, afecte o no al ámbito de la intimidad.

Lo que verdaderamente es importante de esta Sentencia, aparte del debate nominalista sobre el derecho a la protección de datos como derecho autónomo o como garantía del derecho a la intimidad, es el contenido que el Alto Tribunal atribuye al artículo 18.4 CE. Para el Tribunal Constitucional, este precepto exige la necesidad de incluir facultades positivas que permitan el control de la información personal. Esto tiene que darse tanto en la legislación general que desarrolle el artículo 18.4 CE como en la propia legislación sectorial, en este caso de ámbito tributario[131].

---

[130] Así, «no hay un derecho absoluto e incondicionado a la reserva de los datos económicos del contribuyente, con relevancia fiscal», esgrimible ante la Administración u otros poderes públicos, puesto que, si lo hubiera, se haría imposible toda actividad de recaudación tributaria prevista en el artículo 31.1 CE —STC 76/1990—. Sobre la cuestión, cfr., posteriormente, A. GONZÁLEZ MÉNDEZ, *La protección de datos tributarios y su marco constitucional*, Tirant lo Blanch, Valencia, 2003, págs. 145-150; J. ORTIZ LIÑÁN, *Derechos y garantías del contribuyente ante la utilización por la Hacienda Pública de sus datos personales*, Comares, Granada, 2003, págs. 29-67.

[131] La presencia de estas garantías ha sido un dato fundamental para afirmar la legitimidad constitucional de la normativa reglamentaria. «Ahora bien, pudiendo ser estos principios de aplicación también al ámbito de la información económica con fines de control tributario, no puede afirmarse que las disposiciones reglamentarias desconozcan por sí mismas estas garantías. El Real Decreto 338/1990, lo mismo

La posterior jurisprudencia del Tribunal Constitucional parece alinearse con los postulados doctrinales más favorables al reconocimiento interpretativo en nuestro ordenamiento de un derecho fundamental a la autodeterminación informativa, aunque sigue utilizando como cobertura el derecho a la intimidad como un recurso retórico. En efecto, en el bloque de sentencias dictadas con motivo del caso RENFE, la principal y primera de las cuales es la STC 11/1998, de 13 de enero[132], se afirma de nuevo la presencia de un nuevo derecho fundamental en el artículo 18.4 CE. El supuesto de hecho que da lugar a la STC 11/1998, de 13 de enero, y a este grupo de sentencias es el siguiente: la empresa RENFE restó a un grupo de trabajadores de su sueldo los haberes correspondientes a los días en los cuales hubo una huelga convocada por los sindicatos Comisiones Obreras y la Confederación General del Trabajo, que no fue apoyada por UGT y SEMAF. El criterio utilizado para gravar esa inasistencia al trabajo no fue la comprobación material del hecho, sino la afiliación sindical de los trabajadores, dato que RENFE conocía porque facilitaba el pago de la cuota sindical mediante el descuento practicado sobre la nómina de los empleados, teniendo habilitado para ello un proceso informático en el que se asignaba un código numérico a cada sindicato a fin de facilitar y automatizar la operación. Todo esto a pesar de que el recurrente no participó en la huelga —aunque sí lo habían hecho mayoritariamente los trabajadores afiliados a ese sindicato— y así se lo comunicó a la empresa el responsable de la dependencia donde realizaba su labor, siendo atendida su reclamación de reintegro el mes siguiente. El trabajador había proporcionado a la empresa sus datos de afiliación sindical con la finalidad de que aquélla descontara de sus haberes la cuota sindical y la transfiriera al sindicato al que estaba afiliado. En este caso, RENFE utilizó el dato personal del pago de la cuota sindical contenido en un fichero automatizado para una finalidad dis-

---

que su orden de desarrollo, forman parte de un conjunto normativo que introduce garantías suficientes frente al eventual uso desviado de la información que aquellas normas permiten recabar. En este marco destaca, en desarrollo del artículo 18.4 CE, la Ley Orgánica de 29 de octubre de 1992, de regulación del tratamiento automatizado de los datos de carácter personal, que aparte, de las reglas generales sobre tratamiento de datos que no vienen ahora al caso, establece normas específicas para restringir el defecto que la parte imputa a la norma reglamentaria impugnada. En concreto, garantizándose la seguridad de los archivos (art. 9), imponiéndose un deber específico de secreto profesional, incluso después de finalizadas sus tareas al respecto, al "responsable del fichero automatizado y (a) quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal" (art. 10) e impidiendo la transmisión de datos de carácter personal almacenados, con la excepción de que concurra el consentimiento del interesado, la autorización legal específica o la conexión y reconocida necesidad de la transmisión de datos para el logro de finalidades constitucionalmente relevantes (art. 11) en las condiciones dispuestas en la norma. Todas ellas como garantías para determinar el carácter proporcionado y razonable de la obligación de transmitir información fiscal puesto de manifiesto en la doctrina de este Tribunal (STC 110/1984, fundamento jurídico 4.º)» —FJ 7.º—.

[132] Un breve resumen del supuesto de hecho puede verse en J. J. MARCO MARCO, «Comentario a la Sentencia del Tribunal Constitucional 11/1998, de 13 de enero: la vulneración de los derechos fundamentales mediante el uso de datos informáticos automatizados», *Revista General de Derecho*, n.º 645, 1998, págs. 7159 y ss. Este caso, en la medida en que afecta a un colectivo de trabajadores, ha generado un conjunto de sentencias coincidentes tanto en los antecedentes como en los fundamentos jurídicos y en el fallo: SSTC 33/1998 y 35/1998, 45/1998, 60/1998, 77/1998, 94/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 126/1998, 158/1998, 198/1998, 223/1998, 30/1999, 44/1999 y 45/1999.

tinta como es la retirada automática de la parte proporcional de salario correspondiente a una jornada de huelga. Por ello, el trabajador recurrió ante los Tribunales por el procedimiento de tutela de derechos fundamentales y el Juzgado de lo Social de Madrid, en Sentencia de 7 de noviembre de 1994, condenó a la empresa a abonar al recurrente una indemnización por lesión de su derecho de libertad sindical —art. 28.1 CE— en conexión con los artículos 16.1 y 18.1 y 4 CE, porque el dato de la afiliación sindical facilitado a la empresa y que tiene el carácter de especialmente protegido ha sido utilizado para una finalidad distinta. La Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid de 30 de junio de 1995, dictada en procedimiento de tutela de derechos fundamentales, estimó el recurso de suplicación y revocó la Sentencia de instancia, absolviendo a la empresa, rechazando la vulneración de derechos fundamentales al no apreciar en la conducta empresarial un *animus laedendi,* ya que la empresa se limitó, ante la falta de información sobre el seguimiento de los paros, a aceptar la afirmación de la central sindical de que sus afiliados habían secundado mayoritariamente la huelga. Esta Sentencia afirmó, en relación con el artículo 18 CE, que «la intimidad y la privacidad de los datos personales ideológicos, en tanto voluntariamente ofrecidos a la contraparte, trascienden de ese mundo reservado para incardinarse en la relación laboral». El recurso de casación fue inadmitido por la Sala de lo Social del Tribunal Supremo[133].

Así, el Tribunal Constitucional estimó el amparo, que también solicitó el Ministerio Fiscal, retomando con rotundidad en el Fundamento Jurídico 4.º una parte de la doctrina de la STC 254/1993, de 20 de julio: «Por su parte, la STC 254/1993 declaró con relación al artículo 18.4 CE, que dicho precepto incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho o la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos (Fundamento Jurídico 6.º). La garantía de la intimidad, *latu sensu*, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así un 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 (Fundamento Jurídico 7.º)».

Esta Sentencia es importante porque de ella se pueden extraer conclu-

[133] Por estos hechos, el Director de la Agencia de Protección de Datos, en Resolución de 18 de diciembre de 1995, impuso a la empresa una multa por la comisión de una infracción muy grave tipificada en el artículo 43.4.c) de la Ley Orgánica 5/1992, ya que de la práctica de la prueba en el expediente sancionador quedó acreditado que el 99% de los errores afectaron a trabajadores afiliados a los sindicatos convocantes de la huelga.

siones acerca del contenido del artículo 18.4 CE. Así, en primer lugar, se evidencia que el derecho fundamental a la protección de datos personales es un derecho autónomo, que implica el control de la propia información personal frente a las nuevas amenazas de los tratamientos automatizados de datos —*habeas data*— y que faculta para exigir que no se utilicen los datos personales para una finalidad distinta para la cual han sido recabados. En este caso se utilizó un dato sensible, como es el de afiliación sindical, proporcionado para una determinada finalidad —facilitar el ejercicio de la libertad sindical y el pago de las cuotas sindicales—, para un fin radicalmente distinto —retener la parte proporcional de un salario por un período de huelga— que, además, menoscababa el legítimo ejercicio de la libertad sindical. Es importante incidir en el método empleado, es decir, dar instrucciones al sistema informático para que se descuenten todos los días de paro a los que tienen una determinada clave que corresponde a los afiliados a CC.OO. El Tribunal Constitucional entiende que la utilización desviada de un dato para otro fin puede invadir directamente la libertad del individuo. La libertad informática significa el control de los datos personales insertos en un programa informático —*habeas data*—, lo que implica la oposición de los ciudadanos para que los datos sean utilizados con fines distintos a los que justificaron su obtención.

En segundo lugar, queda claro que este derecho fundamental es a controlar el flujo de informaciones que conciernen a cada persona —«a la privacidad según la expresión utilizada en la Exposición de Motivos de la LORTAD», afirma la Sentencia—, aunque no pertenezcan al ámbito estricto de la intimidad, ya que la afiliación sindical es un dato que no siempre es íntimo y que puede ser conocido por actividades externas. No se pueden utilizar los sistemas de información y pulsar en el ordenador una clave informática para utilizar indebidamente cualquier dato personal, sea o no íntimo.

Además, en tercer lugar, esta Sentencia manifiesta que la protección de datos personales no garantiza únicamente el derecho a la intimidad, sino también otros derechos fundamentales, en este caso la libertad sindical y el derecho de huelga, reconocidos en el artículo 28.1 CE. Como señala la Sentencia, «el artículo 18.4 en su último inciso establece las limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, lo que significa que, en supuestos como el presente, el artículo citado es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical»[134]. Se perjudica la pertenencia a una organización sindical, ya que la retención con carácter generalizado del salario correspondiente al seguimiento de la huelga a personas pertenecientes al sindicato convocante provoca efectos disuasorios en los perjudicados en cuanto a su permanencia en la afiliación o, cuando menos, en cuanto al pago de su cuota a través de la nómina, lo que perjudica la financiación y el funcionamiento de la actividad sindi-

[134] FJ 5.º.

cal[135]. Por tanto, estamos ante una decisión unilateral del empresario que supone un trato peyorativo para el trabajador por razón de su pertenencia a un sindicato. Además, la protección de datos personales también garantiza en este caso el principio de igualdad —art. 14 CE—, tratando de evitar, por ejemplo, que la informatización de los datos personales propicie comportamientos discriminatorios. El Tribunal Constitucional afirmó en el fallo «reconocer al recurrente su derecho a la libertad sindical, artículo 28.1 CE en conexión con el artículo 18.4 de la misma», de la cual la protección de datos personales es, en este caso, un instituto de garantía. Con esta Sentencia queda fortalecida la visión del artículo 18.4 CE como un derecho autónomo en relación con el derecho a la intimidad. Este precepto configura tanto un derecho autónomo a la protección de datos frente al uso indebido de la tecnología informática como un instituto de garantía que permite preservar el pleno ejercicio de otros derechos fundamentales, entre ellos principalmente el derecho a la intimidad, pero no exclusivamente éste.

No obstante, esta exposición aparentemente clara de la Sentencia se vuelve confusa cuando la leemos detenidamente, ya que también parece que el Tribunal Constitucional entiende que este derecho al control sobre los datos relativos a la propia persona provendría del derecho a la intimidad entendido en un sentido amplio y con una vertiente positiva. Lógicamente, este último aspecto incorpora elementos de confusión en la relación entre el derecho fundamental a la protección de datos personales y el derecho a la intimidad. Una cosa es que el derecho fundamental a la protección de datos personales tenga su origen y mantenga una estrecha vinculación con el derecho a la intimidad, y otra cosa distinta es que éste sea la dimensión informática de un derecho a la intimidad en un sentido omnicomprensivo interpretado a la luz del Convenio 108. Nosotros entendemos, por las razones expuestas, que debe existir un derecho a la autodeterminación informativa como derecho específico de protección de datos personales. En el supuesto de hecho que resuelve la STC 11/1998, de 13 de enero, el derecho a la intimidad no se ve comprometido, ni siquiera el recurrente en amparo lo alega, sino que simplemente requiere la tutela de su derecho a la libertad sindical —art. 28.1 CE—, que se ve vulnerado a consecuencia de la utilización ilegítima de un tratamiento informatizado de datos, con lo que se alude asimismo a la vulneración del derecho contenido en el artículo 18.4 CE. El Tribunal Constitucional reconoce de alguna manera que los derechos tutelados a través de la protección de datos pueden ser muy diversos y en modo alguno reconducibles sólo a la intimidad.

Sin embargo, en la Sentencia del Tribunal Constitucional 144/1999, de 22 de julio, el Alto Tribunal vuelve a fundamentar la protección de datos

[135] Además, la devolución de las cantidades descontadas estuvo sujeta a una reclamación individualizada, lo que supuso una inversión de la carga de la prueba. La negativa de los trabajadores a manifestarse previamente sobre el seguimiento de la huelga es, para el Tribunal Constitucional, una justificación insuficiente.

personales como una dimensión del derecho a la intimidad. En esta Sentencia se analiza la solicitud sobre datos de antecedentes penales del recurrente que realiza el Presidente de la Junta Electoral de Zona de Santander, el 26 de mayo de 1995, al Registro Central de Penados y Rebeldes, que fueron remitidos a esa Junta por el citado Registro el mismo día 26, todo ello en el marco de un procedimiento en el que se discute la presencia de causas de inelegibilidad. Previamente fue desestimado su recurso por la Sala Tercera del Tribunal Supremo en Sentencia de 25 de mayo de 1996. El recurrente alega en amparo constitucional que la obtención por parte de la Junta Electoral de Zona de su hoja histórico-penal, al margen de los procedimientos legalmente previstos, invadía su intimidad y vulneraba el artículo 18.1 CE.

El Tribunal analiza la tutela del derecho a la intimidad entendido como el derecho a tener vida privada y que supone la existencia de límites al acceso a la información personal, en este caso de la historia penal. El Tribunal circunscribe al artículo 18.1 CE y a la tutela del derecho a la intimidad toda su argumentación, sin hacer referencia al derecho fundamental a la protección de datos personales. Debe subrayarse que en ese momento estaba vigente el artículo 2.3 de la LORTAD, que remitía a sus disposiciones específicas los ficheros derivados del Registro Central de Penados y Rebeldes[136]. El Tribunal Constitucional tuvo que definir qué principios cabe aplicar a un Registro regulado por normas preconstitucionales[137] y que se rige sólo supletoriamente por la LORTAD. El Tribunal optó por aplicar los principios de protección de datos personales que son incluidos en el derecho a la intimidad al amparo del artículo 10.2 CE, a la luz del Convenio 108 del Consejo de Europa, que prohíbe el tratamiento de datos penales sin las garantías adecuadas. El respeto a la vida privada de la persona, de la que la historia penal forma parte, obliga a limitar el tratamiento y el acceso a esa información, que está sometida a fuertes condiciones, incluso para la cesión entre Administraciones Públicas. También aplica el artículo 105.b) CE, que reconoce el derecho de acceso a los archivos y registros administrativos. Este Registro Central de Penados y Rebeldes no es un registro público, por lo que sólo se emiten certificaciones —se hacen cesiones— con las garantías establecidas en la ley, que sólo admite la cesión a órganos judiciales u otros órganos previstos legalmente. Fuera de estos supuestos hay que respetar el derecho a la intimidad personal[138].

---

[136] Sobre los principios que rigen el funcionamiento de este tipo de ficheros, cfr. J. F. ETXEBERRÍA GURIDI, *La protección de los datos de carácter personal en el ámbito de la investigación penal,* Agencia de Protección de Datos, Madrid, 1998, págs. 47-119.

[137] El Registro Central de Penados y Rebeldes estaba regulado por una prolija legislación de rango reglamentario preconstitucional —Reales Decretos de 18 de febrero de 1901; Reales Órdenes de 30 de noviembre de 1910, de 9 de enero de 1914 y de 13 de junio de 1929—, siendo la última el Real Decreto 340/1997, de 7 de marzo. A este Registro se refieren aquellas leyes que disponen la necesidad de presentar un certificado negativo de antecedentes penales para obtener determinadas licencias, autorizaciones o prestaciones de la Administración Pública.

[138] «Este Registro, que se rige por su propia y dispersa normativa, conforme a lo establecido por el artículo 37.5.e) de la Ley 30/1992, y también por el artículo 2.3.c) de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, no deja por ello de

De esta forma, parece que el Tribunal Constitucional aplica el derecho a la autodeterminación informativa a los ficheros incluidos en la legislación general de protección de datos —LORTAD y, ahora, LOPD—. En cambio, los ficheros que esta legislación remite a su normativa específica[139], además de otras vulneraciones de derechos a través de las nuevas tecnologías —que no impliquen tratamiento de datos—, se reconducen al derecho a la intimidad entendido en un sentido amplio, al que se le aplicarían muchos principios de la protección de datos personales, en la medida en que existe una intromisión en la vida privada, esto es, «en un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean éstos poderes públicos o simples particulares, que está ligado al respeto de su dignidad». No obstante, el Tribunal afirma al mismo tiempo que «[e]s 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 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

---

estar sometido al límite de la debida garantía de la intimidad de las personas en lo que al acceso a sus asientos se refiere. Así lo dispone genéricamente el artículo 105.b) CE para todos los archivos administrativos, sin eludir, pues así lo exige el artículo 10.2 CE a efectos interpretativos, lo previsto en el artículo 8 CEDH y en el artículo 6 del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, de 28 de enero de 1981, del Consejo de Europa, que prohíbe, aunque con excepciones (art. 9) el tratamiento automatizado de los datos de carácter personal referentes a condenas penales, a menos que el Derecho interno prevea garantías adecuadas, y, por último, en términos similares al anterior, el artículo 8 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, 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. De estas normas cabe desprender, no sólo que la vida privada de la persona o su familia, en la que a todas luces parece integrarse su historial penal, constituye un límite al acceso de la información relativa a esas circunstancias, sino que el propio almacenamiento y tratamiento automatizado de aquélla está sometido a fuertes constricciones, que obligan a una interpretación restrictiva y rigurosa de los términos en los que esa información puede divulgarse o transmitirse, incluso (y, quizá, sobre todo) entre distintos órganos del Estado. Y esta interpretación restrictiva se reafirmaba en lo que ahora interesa con mayor rotundidad, si cabe, en el artículo 118, tercer párrafo, 3.º CP de 1973, al establecer que las inscripciones de antecedentes penales en dicho Registro no son públicas, y sólo se emitirán certificaciones con las limitaciones y garantías previstas en sus normas específicas y en los casos establecidos en la Ley, y, en todo caso, se librarán las que soliciten los Jueces y Tribunales. Conforme a esa legalidad, resulta que las certificaciones de antecedentes penales sólo pueden solicitarse por el interesado o por los órganos judiciales u otros poderes públicos cuando así lo disponga una norma con rango legal. Fuera de estos casos, y dada la naturaleza de los datos contenidos en el referido Registro, el acceso a ellos vulnera el derecho a la intimidad de aquel a quien se refieran» —FJ 8.º—.

[139] El artículo 2 LOPD afirma: «2. 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 normativa sobre protección de materias clasificadas. c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. 3. 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».

que esos aspectos de la vida individual sean públicos y conocidos, o puedan serlo». De esta forma, constituye una vulneración del derecho a la intimidad personal reconocido en el artículo 18.1 CE el conocimiento indebido de informaciones personales y familiares, «con independencia de que esa información sea objetivamente considerada de las íntimas o de que su conocimiento o divulgación pueda ser perniciosa 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 artículo 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 lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio»[140].

Los hechos descritos, que son analizados por el Tribunal Constitucional al amparo del artículo 18 CE, dan ocasión para que reitere su doctrina sobre la intimidad en sentido amplio, que implicaría muchos principios de protección de datos personales. Así, el Tribunal Constitucional invoca, entre otros precedentes, su primera Sentencia en materia de protección de datos personales, la STC 254/1993, de 20 de julio: «El derecho a la intimidad salvaguardado en el artículo 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 éstos 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».

La Sentencia amplía así el contenido clásico del derecho a la intimidad, extendiéndolo hacia el control sobre la información personal. Para el Tribunal, el artículo 18 CE garantiza al individuo un poder jurídico de control sobre la información relativa a su persona o a su familia, pudiendo imponer tanto a particulares como a poderes públicos su voluntad de no dar a conocer dicha información. Este derecho es especialmente importante cuando estamos hablando de una información sensible de la persona. Así, dice la Sentencia: «el artículo 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[141]. 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».

Por tanto, el derecho a la intimidad reconocido en el artículo 18.1 CE exige el cumplimiento por parte de los poderes públicos de un conjunto de

[140] FJ 8.º.
[141] En el mismo sentido, véase la STC 115/2000.

obligaciones positivas para garantizar a cada persona el poder de disposición sobre la propia información personal y la capacidad de preservar un ámbito reservado de la vida personal y familiar, no accesible a los demás[142]. Esto es especialmente aplicable en un supuesto como el Registro Central de Penados y Rebeldes, donde se archivan informaciones personales tan sensibles como los antecedentes penales, que indudablemente afectan a la integridad moral y deben, por ello, «estar a recaudo de una publicidad indebida y no consentida por el afectado», ya que por sí mismos constituyen un grave riesgo para la intimidad individual. Esto hay que tenerlo en cuenta cuando se analizan los posibles accesos a este Registro y las peticiones de cesiones de datos entre Administraciones Públicas. Como regla general, cualquier acceso a esta información personal debe estar justificado en la ley que crea el archivo, que debe especificar su finalidad y las condiciones de utilización: «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 artículo 18.1 CE la infracción de las normas sobre acceso a la información relativa a una persona o su familia». Le corresponde, por tanto, al legislador el establecimiento de límites al derecho a la intimidad, autorizando no sólo los sujetos que pueden acceder a este Registro Central de Penados y Rebeldes, los límites y el procedimiento, sino también las finalidades que justifican este Registro y que deben coincidir con «limitaciones constitucionalmente impuestas a la esfera íntima del individuo y su familia». Si no se respetan los supuestos legítimos de acceso, este archivo se convertiría en una fuente de información sobre la vida de una persona o su familia, lo que vulneraría el derecho a la intimidad[143].

El Registro Central de Penados y Rebeldes no es un registro público. El artículo 118 del Código Penal y las leyes a las que éste se remite establecen los supuestos legítimos de acceso a los antecedentes penales de las personas, entre los que se encuentran el interesado, los jueces y Tribunales y aquellos órganos habilitados legalmente, entre los que no está la Administración electoral. Sin embargo, la Junta Electoral en el supuesto analizado por la Sentencia obtuvo del citado Registro la hoja histórica penal sin habilitación legal y al margen del procedimiento. Como señala el Tribunal Constitucional, la Administración electoral, a pesar de su importante función de garantía del proceso electoral, no tiene «poderes exorbitantes» que le permitan «sobreponerse a las formalidades legales propias del Estado de Derecho» con la excusa de una más efectiva realización del principio democrático[144].

---

[142] El Tribunal Constitucional cita algunas 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*, de 25 de febrero de 1997.

[143] FJ 8.º.

[144] FJ 5.º.

El Estado democrático tiene que desarrollarse dentro del Estado de Derecho.

Corresponde al Registro de Penados y Rebeldes proteger el derecho a la intimidad de las personas y velar por la confidencialidad de la información contenida en él. Sin embargo, esto se vulneró produciéndose un acceso a una información personal sin consentimiento del interesado y sin habilitación legal, por lo que tanto este Registro como la Junta Electoral de Zona vulneraron en este supuesto el derecho a la intimidad del recurrente[145].

Por tanto, se puede afirmar que las sentencias en las que se resuelven recursos de amparo han servido al Tribunal Constitucional para interpretar el derecho fundamental a la protección de datos personales. Así, a pesar de la escueta mención que se encuentra en el artículo 18.4 CE, el Tribunal Constitucional ha afirmado que dentro del contenido esencial de este derecho fundamental se encontrarían el derecho de acceso a la propia información personal, un conjunto de facultades positivas que permiten el control de la propia información personal, el principio de calidad y la prohibición de que los datos se empleen para una finalidad distinta, la prohibición de cesiones de datos sin consentimiento del interesado y sin habilitación legal, sin perjuicio de las necesarias excepciones en el ámbito público. La Administración, cuando desarrolla una actividad administrativa, no es libre ni tiene derecho a la arbitrariedad, sino que tiene que actuar siempre vinculándose de manera fuerte al derecho fundamental a la protección de datos personales. Como hemos señalado antes, la aplicación extensiva de cláusulas generales para analizar la actividad jurídica de los poderes públicos no es contramayoritaria ni atenta contra el principio democrático. No obstante, la interpretación del contenido de este derecho por parte del Tribunal Constitucional no puede menoscabar la legitimidad del legislador para desarrollar activamente este derecho fundamental, como seguidamente veremos. Así, como hemos señalado antes, una cosa es la aplicación fuerte del derecho fundamental a la protección de datos cuando se analiza la actividad jurídica de la Administración y de los particulares, en que tiene plena vigencia el principio *pro libertate*, y otra cosa distinta es el principio de deferencia al legislador cuando se analiza el desarrollo legislativo de este derecho fundamental positivizado a través de una cláusula general.

[145] Hay otras sentencias importantes del Tribunal Constitucional que resuelven recursos de amparo en materia de protección de datos, que no pueden recibir un estudio detenido por los límites de espacio de este trabajo. Nos estamos refiriendo, por ejemplo, a la STC 202/1999, de 8 de noviembre, en relación a la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de bajas por incapacidad temporal, y su continuación en la STC 153/2004, de 20 de septiembre.

c) *La definición del contenido del derecho fundamental a la protección de datos personales a través de la resolución de recursos de inconstitucionalidad*

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, es la última que se ha ocupado de la protección de datos personales. Esta Sentencia resolvió el recurso de inconstitucionalidad presentado por el Defensor del Pueblo contra algunos preceptos de la LOPD que reproducían la LORTAD y que habían sido antes impugnados ante el Alto Tribunal, aunque no recayó sentencia al haber sido derogada esta Ley con anterioridad. Los artículos impugnados son el 21.1 LOPD —«Comunicación de datos entre Administraciones Públicas»—, que permitía la comunicación de datos para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas «cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso», y el 24 LOPD —«Otras excepciones a los derechos de los afectados»—, que, en su apartado 1.º, excepciona el principio de información en la recogida de los datos cuando ésta impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte «a la persecución de infracciones administrativas» y, en su apartado 2.º, establece que los derechos de acceso, rectificación y cancelación «no será[n] de aplicación si, 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».

La STC 292/2000, de 30 de noviembre, representa el pronunciamiento del Tribunal Constitucional más claro en relación a la existencia de un derecho fundamental a la protección de datos personales, a partir del artículo 18.4 CE, con autonomía respecto del derecho a la intimidad[146]. Así, como señala el Fundamento Jurídico 5.º de esta Sentencia, «el Tribunal ya ha declarado que el artículo 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (F. 6, reiterado luego en las SSTC 143/1994, F. 7, 11/1998, F. 4, 94/1998, F. 6, 202/1999, F. 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positi-

[146] Tal vez la razón de la proclamación tan clara de este derecho fundamental a la protección de datos personales se debe a que el ponente de la Sentencia —el Magistrado D. Julio Diego González Campos—, o más bien el Letrado encargado, había ya leído los borradores de la Carta de Derechos Fundamentales de la Unión Europea, donde se afirma este derecho de manera autónoma. De hecho, el propio texto de la Sentencia se encuentra muy influido por la Carta.

va que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. 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 (SSTC 11/1998, F. 5, 94/1998, F. 4)».

De esta forma, el Tribunal Constitucional ha definido específicamente el derecho a la protección de datos personales, sin utilizar la expresión derecho a la autodeterminación informativa, de la siguiente manera: «el contenido del derecho fundamental a la protección de los datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» —FJ 7.º—.

El Tribunal Constitucional ha dedicado parte de la fundamentación de esta Sentencia 292/2000, de 30 de noviembre, a diferenciar este derecho fundamental a la protección de datos personales del derecho más general a la intimidad, y lo hace con distintos argumentos.

El primer argumento para diferenciar ambos derechos fundamentales es el objeto de los mismos. El derecho a la intimidad protege tradicionalmente los datos íntimos de la persona que, por el hecho de serlo, deben estar excluidos del conocimiento de los demás; en cambio, el derecho fundamental a la protección de datos personales tutela cualquier dato, sea o no íntimo, y, por tanto, también los datos que son de conocimiento público pero que no dejan, por ello, de pertenecer al poder de disposición de la persona. Este derecho fundamental no protege únicamente la información privada del individuo, sino cualquier información referida a una persona; incluso la información conocida por toda la sociedad. La definición de datos de carácter personal hace referencia a datos atribuibles a una persona, que la identifiquen, que puedan facilitar la configuración de un perfil, aunque no pertenezcan al reducto de la intimidad de la persona. Este criterio facilita la eficacia jurídica y otorga seguridad al ordenamiento de protección de datos personales. Por tanto, este derecho fundamental da una protección más amplia que el derecho a la intimidad[147]: «De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga,

[147] Esto ya había sido defendido entre nosotros por P. LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales*, CEC, Madrid, 1993, págs. 32-34.

sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo» —FJ 6.º—. De esta manera, el Tribunal Constitucional ha afirmado la autonomía del derecho fundamental a la protección de datos personales respecto del derecho a la intimidad. Toda persona tiene derecho a controlar sus datos para evitar que se elabore un perfil suyo, un retrato de su personalidad[148]. El contenido nuclear de este nuevo derecho fundamental es el control, no el secreto[149]; la facultad de decidir sobre el uso y destino de los propios datos, impidiendo de esta manera su tráfico ilícito y lesivo para la dignidad y derecho del afectado[150].

Así, en la intimidad, la lesión del derecho proviene de una injerencia o intromisión ilegítima en sentido estricto[151]. En cambio, la idea de injerencia o intromisión no encaja bien con la protección de datos personales, ya que es el propio interesado quien revela sus datos personales, en muchas ocasiones de forma voluntaria o por obligación legal. No existe, por tanto, una intromisión ilegítima, ya que la persona ha consentido en la entrega de los datos, salvo en los supuestos de recogida de datos fraudulenta, desleal o ilícita —art.

---

[148] Cfr. G. Orozco Pardo, «Los derechos de las personas en la LORTAD», *Informática y Derecho*, n.os 6 y 7, UNED, Mérida, 1994, pág. 171.

[149] Cfr. M. L. Fernández Esteban, *Nuevas tecnologías, Internet y derechos fundamentales,* McGraw-Hill, Madrid, 1998, pág. 130.

[150] Por ello, entiende el Tribunal Constitucional que «la peculiaridad de este derecho fundamental a la protección de datos *respecto de aquel derecho fundamental tan afín como es el de la intimidad* radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran». La función del derecho fundamental a la intimidad del artículo 18.1 CE «es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. [...] De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal como el derecho al honor, citado expresamente en el artículo 18.4 CE, e igualmente, en expresión bien amplia del propio artículo 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado» —FF.JJ. 5.º y 6.º—.

[151] Cfr. el concepto de intromisión ilegítima en los artículos 1 y 7 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.

4.7 LOPD—. El problema estriba en que los datos pueden ser sometidos a un uso distinto de la finalidad para la cual han sido recabados, pueden haberse recogido sin garantizar la información o pueden ser cedidos a terceros, de forma irregular. En estos supuestos el derecho a la intimidad no ha sido vulnerado. Se puede decir así que el derecho a la intimidad no ofrece para estos y otros supuestos una protección suficiente, pues se centra en la prohibición de terceras personas de entrometerse en la esfera íntima de las personas. Por ello, es necesario facilitar a la persona una capacidad de control sobre sus datos personales, aunque hayan sido recogidos con su consentimiento.

La segunda diferencia entre el derecho fundamental a la protección de los datos personales y el derecho a la intimidad estriba en que el primero no es sólo un derecho de libertad, que exige la abstención de poderes públicos y particulares en la esfera íntima, sino un derecho que atribuye al ciudadano un conjunto de facultades positivas para controlar la información personal, entre las que se encuentran la exigencia del consentimiento para el tratamiento de los datos, la obligación de ser informado y los derechos de acceso, oposición, rectificación y cancelación[152]. Este derecho fundamental a la protección de datos, «a diferencia del derecho a la intimidad del artículo 18.1 CE, *con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar*, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE)» —FJ 6.º—[153]. Así, el contenido del derecho a la protección de datos no se agota en la posibilidad de conocer el destino de los mismos. La disposición y el control sobre los datos personales se proyectan en un conjunto de principios y derechos que terminan por configurar el contenido esencial de este derecho fundamental. No obstante, la dimensión

[152] Así dice el Tribunal Constitucional: «Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del artículo 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales» —FJ 8.º—.

[153] Estas facultades permiten que tenga la persona efectivamente el control y el poder de disposición sobre sus datos personales: «dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico» —F J. 4.º—.

más activa del derecho fundamental a la protección de datos personales no debe hacer olvidar que el derecho a la intimidad también tiene, aunque en mucha menor medida, algunas facultades positivas[154].

Entre estas facultades positivas que conforman el derecho fundamental a la protección de datos personales hay que destacar el consentimiento del afectado para el tratamiento de sus datos personales. Llama la atención que la Sentencia 292/2000, a diferencia de la STC 290/2000, ha denominado éste como derecho fundamental a la protección de datos personales, olvidando así el término de derecho a la autodeterminación informativa. La expresión de derecho a la autodeterminación informativa tenía la ventaja de reflejar mejor el aspecto central de este derecho, cual es el principio de consentimiento y la importancia de la voluntad del interesado[155]. En efecto, el derecho del interesado a prestar un consentimiento para el tratamiento de sus datos personales es la garantía y el instrumento principal para la protección de este derecho fundamental, el núcleo fuerte de su contenido, aunque en ocasiones tenga que ceder, como veremos más adelante, en el ámbito de las Administraciones Públicas. Así lo ha reconocido la propia Carta de Derechos Fundamentales de la Unión Europea, al afirmar en su artículo 8.1 que el tratamiento de los datos personales sólo es posible previo consentimiento del afectado. El consentimiento, si bien es clave en el momento de la recogida de los datos, también lo es en todas las etapas del tratamiento y se extiende al derecho de oposición y cancelación de los datos personales[156]. Lógicamente, para que este consentimiento sea realmente libre y consciente ha de ser un consentimiento «informado», información que debe alcanzar a los posibles destinatarios de sus datos personales. Así, muchas vulneraciones de este derecho fundamental se producen por una falta o por una deficiente información en el momento de la recogida de los datos. La información es

---

[154] Como ha señalado el Tribunal Constitucional, «el constituyente quiso garantizar mediante el actual artículo 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto». Sin embargo, algunos autores han señalado para rechazar la autonomía del derecho fundamental a la protección de datos personales respecto del derecho a la intimidad que este último no es un derecho que requiera sólo la abstención del Estado o de los particulares y que atribuya sólo facultades de defensa frente a las intromisiones exteriores en la vida íntima, sino que tiene también un aspecto positivo, de control de la información. Para RUIZ MIGUEL, la intimidad contiene un aspecto dinámico, por lo que el artículo 18.4 sólo incluye una limitación del uso de la informática en defensa de la intimidad. Se habla así de intimidad informática. Cfr. C. RUIZ MIGUEL, «En torno a la protección de los datos», pág. 240.

[155] LUCAS MURILLO DE LA CUEVA señala que el consentimiento del afectado es la expresión quintaesenciada de la autodeterminación o autodisposición sobre la información que le atañe. Cfr. P. LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales*, cit., pág. 56. Cfr. P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento de datos personales,* págs. 7 y ss.; A. I. HERRÁN ORTIZ, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, cit., pág. 220.

[156] «En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele» —FJ 7.º—.

también núcleo de este derecho fundamental, a la vez que una exigencia del propio consentimiento[157].

De esta forma, el control del titular de los datos personales no es abstracto, sino concreto, con una capacidad real de informarse, exigir el consentimiento, acceder, rectificar, cancelar y oponerse al tratamiento de sus datos de carácter personal. Este derecho fundamental equivale a conocimiento y control. Este control se desarrolla en dos momentos: el primero, en la decisión de entregar los datos personales; el segundo, durante todo el tratamiento de los mismos, a través de los derechos de acceso, oposición, rectificación y cancelación, que permiten seguir la vida del dato personal. Por lo tanto, el contenido esencial del derecho a la protección de datos contiene un conjunto de principios y de derechos que garantizan la protección de la persona frente al manejo de sus datos personales. Hay que resaltar la contundencia del Tribunal para incluir todos estos elementos mencionados dentro de la definición del contenido esencial de este derecho fundamental. Las leyes que desarrollen el mandato constitucional del artículo 18.4 deben respetar el contenido esencial descrito.

En tercer lugar, también como diferencia entre el derecho fundamental a la protección de datos personales y el derecho a la intimidad, el Tribunal Constitucional no entiende que la expresión del artículo 18.4 de la Constitución deba remitirse sólo a la tutela del derecho al honor y a la intimidad, ni siquiera sólo a los derechos fundamentales y libertades públicas. El Tribunal Constitucional va incluso más allá de la referencia constitucional, afirmando la necesidad de protección no sólo de los derechos constitucionales, sino también de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado. De esta forma, el Tribunal Constitucional sostiene una concepción de este derecho bastante amplia y abierta, que supera el planteamiento más estricto propio de la intimidad[158].

En esta dirección, el Tribunal Constitucional también aporta un argumento de interpretación constitucional originalista —*original under-*

[157] «[...] es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia» —FJ 13—.

[158] Para PÉREZ LUÑO, «si se deseaba extender la garantía frente a los abusos informáticos no sólo al honor y a la intimidad, sino a todos los derechos fundamentales hubiera sido preferible dedicar por entero un artículo de la Constitución, siguiendo el modelo portugués, al tratamiento global de la informática y sus repercusiones». Cfr. A. E. PÉREZ LUÑO, *Derechos Humanos,* cit., pág. 363.

standing— en relación con la diferencia entre el derecho fundamental a la protección de datos personales y el derecho a la intimidad[159]. Para el Alto Tribunal, con la previsión del artículo 18.4 CE, el constituyente establece un derecho fundamental en sí mismo frente a los riesgos que podría entrañar el uso de la informática, para garantizar no sólo el derecho a la intimidad y al honor, sino también el pleno ejercicio de los derechos de la persona: «Preocupación y finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del Texto Constitucional ya se incluía un apartado similar al vigente artículo 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada».

No obstante, aunque el Tribunal Constitucional diferencie el derecho fundamental a la protección de datos personales del derecho a la intimidad, esto no le hace olvidar la fuerte conexión entre ambos derechos, considerándoles derechos «afines», que comparten el «objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar»[160].

Es importante señalar que, dentro del contenido de este derecho fundamental, el Tribunal Constitucional ha incluido también los tratamientos no automatizados. El Tribunal Constitucional, en esta Sentencia 292/2000, de 30 de noviembre, no diferencia entre tratamiento informático o no[161]. No obstante, la extensión del derecho fundamental a la protección de datos personales a los ficheros manuales tiene difícil encaje a partir del artículo 18.4 CE, que se refiere únicamente a la informática y, por tanto, a los tratamientos automatizados. Esta ampliación es una consecuencia de la propia Directiva 95/46/CE, de la que la LOPD es transposición. Sin embargo, una cosa es que el legislador se haya visto obligado a ampliar la protección a los ficheros en soporte papel, a consecuencia de la Directiva comunitaria, y otra cosa distinta es que esto sea una exigencia constitucional.

La existencia de un derecho fundamental a la protección de datos personales no quiere decir que este derecho sea ilimitado. Como ha señalado el Tribunal Constitucional, no existen derechos absolutos ya que todos ellos están sometidos a límites[162]. Esto significa que el derecho fundamental a la protección de datos personales tiene que ceder ante otros derechos o bienes constitucionales, siempre respetando su contenido esencial. Como ha señalado el Tribunal Constitucional en la Sentencia 292/2000: «el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le impon-

[159] Cfr., más ampliamente, E. ALONSO, *La interpretación de la Constitución*, CEC, Madrid, 1984.
[160] Cfr. *supra,* referencias en cursiva.
[161] Cfr. FJ 7.º.
[162] STC 11/1981, de 8 de abril.

ga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución. Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el artículo 53.1 CE» —FJ 11—.

Por tanto, a pesar de que el artículo 18.4 CE sólo establezca expresamente como objeto de limitación a la informática, este derecho fundamental a la protección de datos personales se encuentra sometido a límites, al igual que lo está expresamente el derecho de acceso a los archivos y registros administrativos —art. 105.b) CE— «en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas»[163].

En similares términos se expresa la normativa europea de protección de datos personales. Así, el propio Convenio 108 del Consejo de Europa permite en su artículo 9 las excepciones a los principios de este Tratado cuando tal excepción, prevista por la Ley de la Parte, constituya una medida necesaria en una sociedad democrática para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales, y para la protección de la persona concernida y de los derechos y libertades de otras personas[164]. La Directiva 95/46/CE en su artículo 13.1 permite a los Estados la adopción de medidas legales para limitar este derecho a la protección de datos personales, especialmente en lo relativo al principio de calidad, al principio de información, al derecho de acceso cuando tal limitación constituya una medida necesaria para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales, un interés económico y financiero importante —incluidos los asuntos monetarios, presupuestarios y fiscales—, una función de control, inspección o reglamentaria relacionada —aunque sólo sea ocasionalmente— con el ejercicio de autoridad pública, y, en general, la limitación de este derecho para la protección del interesado o de los derechos y libertades de otras personas.

---

[163] Artículo 37 LRJAPyPAC. Cfr. *supra,* nota 93.

[164] La expresión que utiliza frecuentemente el Tribunal de Estrasburgo para justificar las excepciones al artículo 8 del Convenio es *pressing social need*, que podría ser traducido como «acuciante presión social». Así, la jurisprudencia del Tribunal Europeo de Derechos Humanos reconoce límites como la seguridad del Estado —caso *Leander,* de 26 de marzo de 1987—, la persecución de infracciones penales —casos *Z*, de 25 de febrero de 1997, y *Funke*, de 25 de febrero de 1993—. Cfr. C. RUIZ MIGUEL, *El derecho a la protección de la vida privada*, cit.

Los límites a este derecho fundamental a la protección de datos personales, como señala la Sentencia, tienen que cumplir tres condiciones para que sean constitucionales. En primer lugar, estos límites tienen que ser establecidos por ley, ya que sólo por ley se pueden desarrollar y limitar los derechos constitucionales —arts. 53.1 y 81 CE—. En segundo lugar, estos límites sólo están justificados «si responde[n] a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos», siempre que este límite «sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo». En tercer lugar, estos límites tienen que respetar el contenido esencial del derecho fundamental a la protección de datos personales, que se extiende a un conjunto de garantías y facultades que conforman el poder de disposición sobre la propia información personal[165]. La ley no puede limitar tanto el contenido del derecho fundamental que impida el reconocimiento de este derecho como perteneciente a su tipo previo, ni puede despojarle de las necesarias facultades para que los intereses jurídicos que le dan vida sean efectivamente protegidos. Si los límites al derecho fundamental a la protección de datos personales no son establecidos por ley, no se justifican en otros derechos o bienes constitucionales o lesionan el contenido esencial de aquél, se puede afirmar que son inconstitucionales.

Pues bien, la STC 292/2000, de 30 de noviembre, ha declarado inconstitucionales distintos preceptos de la LOPD, previstos antes por la LORTAD, referidos a los ficheros públicos, en lo relativo a las cesiones de datos entre Administraciones Públicas sin consentimiento del interesado para el ejercicio de competencias diferentes que versen sobre materias distintas —art. 21.1 LOPD—, a los límites al principio de información al interesado cuando impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la persecución de infracciones administrativas —art. 24.1 LOPD—, y a los límites a los derechos de acceso, rectificación y cancelación por razones de interés público o intereses de terceros más dignos de protección —art. 24.2 LOPD—[166]. Vamos a analizar seguidamente estos preceptos y la argumentación del Tribunal Constitucional para determinar, vistas las premisas planteadas, si eran realmente inconstitucionales o si, por el contrario, cabían dentro del marco constitucional.

El artículo 21.1 LOPD en su redacción original establecía que «[l]os 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

[165] FJ 11.

[166] Cfr. D. LÓPEZ GARRIDO, «Aspectos de inconstitucionalidad de la Ley Orgánica 5/92, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal», *Revista de Derecho Político*, n.º 38, 1993. Cfr., especialmente, R. MARTÍNEZ MARTÍNEZ, *Tecnologías de la información, Policía y Constitución,* Tirant lo Blanch, Valencia, 2001, págs. 144-193.

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».

El argumento principal para considerar inconstitucional este inciso es la vulneración del principio de reserva de ley para limitar derechos fundamentales —art. 53.1 CE—, al considerar que una cesión de datos sin consentimiento es una limitación al derecho fundamental a la protección de datos y este artículo autoriza que se lleve a cabo a través de una norma con rango inferior a la ley. Para el Defensor del Pueblo, el legislador no regula los criterios que justifican la cesión de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o que versen sobre materias distintas ni establece los límites, sino que simplemente «apodera a la Administración para que restrinja tales derechos a su discreción, al permitir que una norma de rango inferior a la Ley autorice la cesión de datos entre Administraciones Públicas sin el consentimiento ni el conocimiento del afectado, e incluso para fines diversos para los que fueron recogidos y automatizados»[167]. Para el Tribunal Constitucional, «cuando la Constitución no contempla esta posibilidad de que un Poder Público distinto al Legislador fije y aplique los límites de un derecho fundamental o que esos límites sean distintos a los implícitamente derivados de su coexistencia con los restantes derechos y bienes constitucionalmente protegidos, es irrelevante que la Ley habilitante sujete a los Poderes Públicos en ese cometido a procedimientos y criterios todo lo precisos que se quiera, incluso si la Ley habilitante enumera con detalle los bienes o intereses invocables por los Poderes Públicos en cuestión, o que sus decisiones sean revisables jurisdiccionalmente (que lo son en cualquier caso, con arreglo al art. 106 CE). Esa Ley habrá infringido el derecho fundamental porque no ha cumplido con el mandato contenido en la reserva de ley (arts. 53.1 y 81.1 CE), al haber renunciado a regular la materia que se le ha reservado, remitiendo ese cometido a otro Poder Público, frustrando así una de las garantías capitales de los derechos fundamentales en el Estado democrático y social de Derecho (art. 1.1 CE)» —FJ 11—.

Así, las normas que pueden habilitar la cesión de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas serían las disposiciones de creación de ficheros de titularidad pública, que se encuentran reguladas en el artículo 20 LOPD —que habla de «disposiciones generales»— o disposición de superior rango que regule su uso. En todo caso, no hay duda que este artículo 21.1 CE se está refiriendo a normas de rango infralegal. De hecho, muchos de los ficheros públicos de la Administración General del Estado y de las Comunidades Autónomas fueron inicialmente creados por Real Decreto de Consejo de Ministros o Decreto de Consejos de Gobierno, aunque posteriormente lo han sido por Órdenes Ministeriales u Órdenes de las Consejerías, principalmente para evitar el trámite más lento y exigente de los pri-

[167] Argumentación del Defensor del Pueblo.

meros y las dificultades que presentaban en términos de congelación de rango para facilitar posteriormente posibles modificaciones o supresiones de ficheros. Mucho más claro se ve el carácter inferior a la ley de estas disposiciones en otros ámbitos públicos como las Universidades públicas, que crean sus ficheros por resolución del Rector o acuerdo de la Comisión de Gobierno; los Ayuntamientos, que crean —o deben crear— sus ficheros por ordenanza o reglamento orgánico del Pleno o bando del Alcalde, o los Colegios Profesionales, que crean sus ficheros públicos por acuerdo de su Consejo de Gobierno[168].

Vamos a analizar ahora la constitucionalidad de este artículo 21.1 LOPD. Así, en lo que hace referencia a la vulneración de la reserva de ley para limitar derechos fundamentales, tenemos que afirmar que es la propia Ley Orgánica la que establece y da cobertura legal a la comunicación de datos entre Administraciones Públicas para competencias diferentes o que versen sobre materias distintas. No otra cosa es el propio artículo 21.1 LOPD. Así, los supuestos en que es posible la cesión de datos sin consentimiento del interesado están previstos en la propia LOPD. Además, la habilitación legal del artículo 21.1 LOPD es igual que otras muchas que aparecen ya mencionadas en el artículo 11.2 LOPD, como la relativa a las fuentes accesibles al público o la existencia de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. Da la impresión, como comentaremos después, que el Tribunal Constitucional pretenda ser más exigente con los ficheros públicos que con los ficheros privados.

Lo que el artículo 21.1 LOPD hace, en el fondo, es establecer una excepción más —lógicamente, con la defectuosa sistemática que le caracteriza— al principio general de consentimiento para la comunicación de datos previsto en el artículo 11 LOPD. Este precepto establece que «[l]os datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado». Sin embargo, este artículo establece un conjunto de excepciones al consentimiento cuando la cesión esté autorizada en una ley; cuando se trate de datos recogidos de fuentes accesibles al público; cuando el tratamiento responda a una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros; cuando la comunicación tenga como destinatarios a los órganos judiciales, Ministerio Fiscal, Defensor del Pueblo y Tribunal de Cuentas; cuando la cesión se produzca entre Administraciones Públicas para fines históricos, estadísticos o científicos; o cuando la cesión de datos relativos a la salud

[168] Lógicamente, el tipo de norma de creación de ficheros de titularidad pública entraña una mayor complejidad que no puede ser abordada en estas páginas. Cfr., más ampliamente, A. TRONCOSO REIGADA, «Introducción», en *Guía de Protección de Datos para Ayuntamientos, para Colegios Profesionales y para Universidades Públicas*, Civitas-APDCM, 2004, págs. 14-17, 14 y 24-27, respectivamente.

sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos. Por tanto, este artículo 21.1 LOPD configuraría una excepción adicional al consentimiento del interesado que permite la comunicación de datos entre ficheros públicos habilitada por la propia norma de creación del fichero o por una norma de superior rango que regule su uso.

No se entiende por qué hay que exigir más precisión a la limitación del consentimiento para las cesiones entre Administraciones Públicas del artículo 21.1 LOPD que otras limitaciones al consentimiento previstas en el artículo 11.2 LOPD. Así, no parece clara la excepción del consentimiento cuando el tratamiento responda a una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros —art. 11.2.c)—, ni tampoco están convenientemente reguladas muchas de las fuentes accesibles al público establecidas en el artículo 3.j) LOPD.

Es verdad que el artículo 21.1 LOPD no limita materialmente la comunicación de datos entre Administraciones Públicas, pero tampoco lo hace con los otros supuestos mencionados en el artículo 11.2 LOPD. Así, tampoco limita —porque no lo puede hacer— la comunicación de datos al Defensor del Pueblo, al Tribunal de Cuentas o a los órganos judiciales, o cuando se trata de datos recogidos de fuentes accesibles al público; lo único que se hace es situar a las Administraciones Públicas en el marco del resto de los poderes públicos y, en muchos supuestos, con el estatus que tienen algunos particulares.

Además, no se entiende por qué el Tribunal Constitucional prohíbe que la norma de creación de ficheros públicos prevea otros posibles cesionarios o destinatarios de la información, ya que ésta es una posibilidad de cualquier responsable de ficheros, tanto público como privado, que procede a recabar datos de personas. Así, el artículo 20.2.e) LOPD establece que el responsable del fichero público debe indicar en la disposición de creación de fichero las posibles cesiones de datos de carácter personal[169]. Además, al regular el derecho de información en la recogida de los datos, se establece la obligación de informar a las personas a las que se les soliciten sus datos «de los destinatarios de la información» —art. 5.1.a) LOPD—. Cumplidos estos dos requisitos, nada obsta para que pueda producirse una cesión de datos a otras Administraciones Públicas.

El artículo 21.1 LOPD ha establecido una previsión legal para la comunicación de datos entre Administraciones Públicas, que es considerada por el legislador como necesaria para el funcionamiento de los poderes públicos en una sociedad democrática, dadas las competencias constitucionales de la Administración, dentro de la llamada reserva de Administración —*verwaltungsvorbehalt*—[170]. Existe una habilitación legal en virtud de los bienes constitu-

[169] Esta misma posibilidad se establece para el responsable de ficheros privados que en el documento de notificación de ficheros debe indicar las cesiones de datos previstas —art. 6.g) del Real Decreto 1332/1994, de 20 junio—.

[170] Sobre la reserva de Administración, cfr. A. TRONCOSO REIGADA, *Privatización, empresa pública y*

cionales a los que va encaminada la actividad administrativa. Esta habilitación legal es accesible para los ciudadanos, resultando suficientemente previsibles las consecuencias que para ellos puede tener su aplicación[171]. Además, el artículo 21.1 LOPD establece un importante condicionante a la comunicación de datos entre Administraciones Públicas, si bien de carácter formal, y es que la cesión esté prevista en la norma de creación del fichero o en norma de superior rango que regule su uso, lo que permite una publicidad formal que facilita su conocimiento y eventual impugnación por los ciudadanos. Así, la habilitación de la cesión de datos personales entre Administraciones Públicas realizada a través de un Real Decreto establece un conjunto de garantías, tanto en lo que afecta al trámite de información pública como al informe del Consejo de Estado, además de ser elaborada por un órgano superior al que ha creado el fichero. Por último, la comunicación de datos personales establecida por la norma de creación del fichero o por disposición de superior rango siempre puede ser fiscalizada por las Autoridades de control y por la jurisdicción contencioso-administrativa teniendo en cuenta el principio de proporcionalidad.

Esto no quiere decir que dentro de una valoración de oportunidad y no de un juicio de constitucionalidad se pueda criticar el artículo 21.1 LOPD, ya que el legislador podía haber establecido no sólo una habilitación para la cesión a través de normas reglamentarias, sino también la delimitación más precisa de las circunstancias o las causas que lo justifican, en especial de la necesidad de facilitar la actividad administrativa en beneficio de otros bienes y derechos constitucionales, pero esto no significa que el artículo 21.1 LOPD sea inconstitucional.

Hay que analizar también si esta excepción al consentimiento del interesado para la cesión de datos entre Administraciones Públicas vulnera el contenido esencial del derecho fundamental a la protección de datos personales. Pues bien, no parece razonable exigir el consentimiento del ciudadano para la cesión de datos entre Administraciones Públicas cuando este consentimiento tampoco fue necesario para la recogida y el tratamiento de los datos de carácter personal para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias —art. 6.2 LOPD—. Al permitir la cesión de datos entre Administraciones Públicas sin consentimiento, lo único que se evita es que la Administración Pública, también sin consentimiento del interesado, proceda a la recogida y la obtención de los datos personales partiendo de cero, con el consiguiente esfuerzo administrativo.

No se puede considerar que es inconstitucional la cesión de datos entre Administraciones Públicas sin consentimiento del interesado y considerar

---

Constitución, Marcial Pons, Madrid, 1997, págs. 130-135; L. LÓPEZ GUERRA, «Funciones del Gobierno y dirección política», *Documentación Administrativa,* n.º 215, 1988, págs. 15-40, y H. DREIER, «Zur Eigeständigkeit der Verwaltung», *Die Verwaltung,* n.º 25-2, 1992, págs. 137-156.

[171] Cfr. Sentencias del Tribunal Europeo de Derechos Humanos, 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.

constitucional que las Administraciones Públicas procedan a la recogida y al tratamiento de datos personales sin consentimiento del interesado. No se puede exigir una ley expresa para cada cesión de datos entre Administraciones Públicas sin consentimiento y no exigir la misma habilitación legal para el tratamiento de los datos personales por los poderes públicos sin consentimiento. El tratamiento de datos personales sin consentimiento del interesado es el principal elemento que diferencia a los ficheros públicos de los ficheros privados —aunque éstos también tengan esta prerrogativa en algunos tratamientos específicos como los relativos a los ficheros de solvencia patrimonial y de crédito—.

Por tanto, el derecho fundamental a la protección de datos personales no exige el consentimiento para la cesión de datos personales entre Administraciones Públicas, como tampoco lo exige para el tratamiento en el desarrollo de funciones administrativas. Así, no podemos compartir la afirmación del Tribunal Constitucional de que la LOPD «no ha fijado por sí misma, como le impone la Constitución (art. 53.1 CE), los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado». Esto no es correcto ya que los datos personales son tratados por las Administraciones Públicas sin consentimiento del interesado.

Además, si no se ha demandado al legislador una mayor precisión sobre lo que significa la expresión «funciones administrativas» del artículo 6.2 LOPD, tampoco se le puede exigir una mayor concreción cuando se habilita la cesión de datos entre Administraciones Públicas para competencias diferentes que versen sobre materias distintas, porque también se trata de funciones administrativas. Si es constitucional la expresión «funciones administrativas» para el tratamiento sin consentimiento, no puede afirmarse al mismo tiempo que esta expresión utilizada para las cesiones supone una renuncia del legislador a la facultad para establecer los límites a los derechos fundamentales. Lo fundamental aquí es que tanto la recogida de los datos sin consentimiento por una Administración Pública como la cesión a otras Administraciones Públicas se hagan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Es decir, es el ejercicio de funciones administrativas lo que legitima la actividad de tratamiento de datos personales por las Administraciones Públicas. El desarrollo de estas funciones que tratan de garantizar bienes constitucionales en beneficio del interés general —art. 103.1 CE—, y en especial en la actividad de prestación de derechos fundamentales, es lo que justifica determinadas facultades y prerrogativas de las Administraciones Públicas.

Además, la comunicación de datos entre Administraciones Públicas está justificada en los principios de lealtad y cooperación interadministrativa, mencionados en los artículos 3 y 4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento

Administrativo Común[172]. Como señaló con acierto el abogado del Estado, la comunicación de datos entre Administraciones Públicas evita que la Administración receptora «deba pechar con los costes de una nueva recogida y tratamiento de esos datos», a la vez que se ahorra al ciudadano la molestia de someterse a ella. Lógicamente, sólo se pueden ceder los datos a otra Administración Pública para el cumplimiento de funciones administrativas. Exigir una habilitación legal para la comunicación de datos entre Administraciones Públicas limita mucho la eficacia administrativa. Téngase en cuenta que el legislador —y el gobierno en los distintos anteproyectos— valora muchos aspectos a la hora de definir el contenido de una ley, pero frecuentemente olvida todo lo relativo a la habilitación para los tratamientos de datos personales. Además, algunas leyes se han aprobado con anterioridad a la LORTAD y a la LOPD y no preveían la necesidad de una autorización legal para la cesión de datos sin consentimiento del interesado entre Administraciones Públicas.

La posibilidad de comunicación de datos entre Administraciones Públicas para funciones administrativas es especialmente importante para la puesta en marcha de proyectos de Administración electrónica, que se basan en la comunicación de datos administrativos. No estamos hablando únicamente de la ventanilla única y de la interconexión de registros administrativos, pues esta cesión de datos entre Administraciones Públicas estaría amparada por el artículo 21.2 LOPD, que permite la comunicación de los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra. Nos referimos ahora a la necesidad de comunicar datos entre Administraciones Públicas en algunos procedimientos administrativos, lo que lleva a la interconexión de las bases de datos públicas[173]. Éste sería el caso, por ejemplo, de la posibilidad de que una Administración no exija al ciudadano para la concesión de una subvención estar al día de sus obligaciones tributarias o con la Tesorería de la Seguridad Social si la Administración puede obtener esta información directamente de otras Administraciones Públicas sin pedírsela al interesado. Se trata así de eliminar los certificados físicos aportados por el ciudadano y sustituirlos por el intercambio de certificados telemáticos y transmisiones de datos entre los diferentes registros y ficheros administrativos. Esta posibilidad, además de ser una exigencia de la eficacia y de la propia simplificación administrativa, de una Administración Pública que busca la calidad de los servicios y la satisfacción de los ciudadanos, es una consecuencia del derecho reconocido en la Ley 30/1992, de 26 de noviembre, a todos los ciudadanos de que no les sea exigida ninguna documenta-

---

[172] Cfr. J. González Pérez y F. González Navarro, *Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común*, I, cit., págs. 486 y ss. Este principio también es mencionado en el artículo 55 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

[173] Recientemente, el Ministerio de Administraciones Públicas ha aprobado el «Plan Conecta para el desarrollo de la Administración Electrónica en España 2004-2007». Este Plan tiene entre sus objetivos eliminar el 80% de los certificados que actualmente la Administración exige al ciudadano.

ción que ya está en poder de la propia Administración Pública. Las finalidades de las distintas bases de datos públicas que se pretenden interconectar son casi siempre distintas, lo que exigiría una habilitación legal que dé cobertura al intercambio de datos personales entre las Administraciones Públicas. Una posible solución en este caso es pedirle al ciudadano el consentimiento para recabar sus datos de otras Administraciones Públicas. Es necesario en este ámbito explorar las posibilidades de establecer un sistema de autorizaciones que facilite el control de las autoridades de protección de datos en el intercambio de datos entre Administraciones Públicas. En todo caso, lo principal en este momento es señalar que la Administración electrónica está encaminada a ofrecer servicios administrativos transversales a través de la red.

Por lo tanto, si no hay que exigir el consentimiento para el tratamiento de datos entre Administraciones Públicas, al no formar parte este consentimiento del contenido esencial en el ámbito de las Administraciones Públicas para el cumplimiento de funciones administrativas, tampoco hay que exigir este consentimiento para la cesión de datos entre Administraciones Públicas para competencias diferentes o que versen sobre materias distintas. Si no hay consentimiento, no hay tampoco derecho de oposición y se encuentra muy limitado el derecho de cancelación, salvo que existan motivos fundados y una ley no disponga lo contrario.

Lo afirmado hasta ahora se muestra aún más claro cuando se analiza la normativa europea en este ámbito. Tanto la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, como el Convenio 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, exceptúan la exigencia de consentimiento para el tratamiento de datos para las Administraciones Públicas, por lo que este consentimiento no forma parte de su contenido esencial. La exigencia del consentimiento del interesado para la comunicación de datos entre Administraciones Públicas no se prevé en el artículo 8 del Convenio 108 del Consejo de Europa, que además establece excepciones, que han sido interpretadas por el Tribunal de Estrasburgo tratando de tener en cuenta intereses sociales importantes[174].

En la misma dirección, el artículo 7.e) y f) de la Directiva 95/46/CE establece que los Estados miembros dispondrán que el tratamiento de datos personales pueda efectuarse sin consentimiento del interesado cuando sea «necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comunique los datos», o «sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por

[174] Una de las Sentencias del Tribunal de Estrasburgo que hablaba de la necesidad social apremiante en relación con la aplicación del artículo 8 del Convenio es *Klass v. Germany,* de 1978.

el tercero o terceros a los que se comunique los datos, siempre que no prevalezca el interés o los derechos o libertades fundamentales del interesado que requieran protección». El artículo 7 de la Directiva no habla de cesiones, habla de tratamientos, aunque la cesión es un tipo de tratamiento de datos personales. Este artículo establece que la ley no es la única forma de habilitación para la cesión de datos entre Administraciones Públicas a partir del Derecho comunitario. Existe un conjunto de excepciones al consentimiento de entre las cuales la ley sólo es un supuesto más. En virtud del Derecho comunitario, se puede afirmar que la cesión de datos entre Administraciones Públicas es legítima si existe un interés legítimo importante. Habrá que valorar los intereses en presencia, pero no se exige una habilitación legal. Es decir, se pueden tratar datos personales, incluso se pueden ceder datos personales, si no se vulnera un interés importante del afectado. A esta previsión habría que añadir lo ya afirmado sobre las excepciones a los principios de protección de datos y a los derechos ya mencionados anteriormente —art. 13 de la Directiva—.

Esta reflexión nos lleva a analizar cómo se hizo la transposición de la Directiva comunitaria en el Derecho interno español, especialmente en lo que hace referencia al artículo 7. Da la impresión de que el artículo 6 LOPD es correcto, mientras que el artículo 11 LOPD y el artículo 21 LOPD son demasiado restrictivos, sobre todo a partir de esta Sentencia del Tribunal Constitucional que declaró inconstitucional las cesiones de datos entre Administraciones Pública para el ejercicio de competencias diferentes o que versen sobre materias distintas. De hecho, da la impresión de que el artículo 21.1, declarado inconstitucional, es, en cierta medida, reflejo del artículo 7.e) de la Directiva 95/46/CE, al conceder relevancia a la misión de interés público no sólo del cedente, sino también del cesionario[175]. Además, a mayor abundamiento, recientemente se ha aprobado una Directiva que permite la cesión de datos desde las Administraciones Públicas a los particulares, siempre que se tengan en cuenta los intereses en presencia. Nos estamos refiriendo a la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público. En esta dirección llama la atención que el *Dictamen del Grupo del artículo 29 sobre protección de datos 7/2003, sobre reutilización de la información del sector público y la protección de datos personales,* haya sido subtitulado «En busca del equilibrio»[176]. Lógicamente, si se pueden ceder datos a los particulares, con mayor motivo se podrán ceder entre Administraciones Públicas.

En todo caso, queremos que se nos entienda bien. Nosotros no afirmamos que exigir mayores requisitos para la comunicación de datos entre Administraciones Públicas sea irrazonable. Lo que decimos es que le correspon-

---

[175] Una velada crítica a la transposición española de la Directiva 95/46/CE puede verse en el Informe de la Comisión sobre la aplicación de la Directiva, Bruselas, 15-5-2003.

[176] Cfr. en esta misma dirección el *Dictamen del Grupo del artículo 29 sobre protección de datos 7/2003, sobre reutilización de la información del sector público y la protección de datos personales* —«En busca del equilibrio»—, adoptado el 12 de diciembre de 2003.

de al legislador establecer los criterios que justifican estas cesiones. La reserva es una reserva de ley, de Poder Legislativo, no una decisión que pueda ser adoptada por el Tribunal Constitucional. Y mucho menos alegando como fundamento para la declaración de inconstitucionalidad la doctrina del contenido esencial de los derechos fundamentales y la referencia a la noción generalmente admitida por los juristas y en el Derecho comparado de lo que este derecho significa. La normativa europea, tanto el Convenio 108 como la Directiva 95/46/CE, no exige una habilitación legal para la cesión de datos entre Administraciones Públicas, por lo que no se entiende la integración que hizo el Tribunal Constitucional del artículo 18.4 para poder llegar a afirmar la inconstitucionalidad del artículo 21.1 LOPD[177]. Lo mismo se puede decir de la normativa de los distintos países de la Unión Europea que facilitan la cesión de datos entre Administraciones Públicas sin la exigencia de una habilitación legal[178].

Hay dos posibles vulneraciones del artículo 21.1 LOPD que no se afirman claramente en la demanda y que van a ser analizadas seguidamente: la del principio de calidad o del principio de finalidad y la del principio de información, como contenidos del derecho fundamental a la protección de datos personales. Así, el principio de calidad exige que el responsable de un fichero público sólo pueda recoger los datos adecuados y pertinentes para una finalidad explícita y legítima y no pueda recoger datos excesivos, y si durante la vida del fichero no puede destinar los datos a una finalidad distinta, si se produce una comunicación de datos entre Administraciones Públicas sin consentimiento del interesado para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, lo que se está produciendo es un tratamiento de datos para una finalidad distinta para la cual estos datos han sido recogidos. Además, se está animando a la Administración Pública a coger datos personales excesivos «por si acaso» pueden ser utilizados después por otra Administración para una finalidad distinta, lo que vulneraría *de facto* el principio de calidad. Además, este principio de calidad —a diferencia del consentimiento para la cesión, como hemos visto— sí se encuentra en la noción generalmente admitida de lo que el derecho fundamental a la protección de datos personales significa, sí es un contenido sin el cual este derecho no es reconocible como perteneciente a su tipo previo, si tene-

[177] Cosa distinta es que el artículo 11 del Convenio 108 afirme que ninguna de sus disposiciones «se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el Convenio». Así, una cosa es que el legislador pueda ampliar el contenido del derecho fundamental a la protección de datos personales más allá de lo establecido en el Convenio, y otra cosa distinta es que se utilice el Convenio para declarar inconstitucionales preceptos de las leyes de protección de datos que no entran en contradicción con éste.

[178] Por tanto, no se entiende cómo tanto la demanda del Defensor del Pueblo como la Sentencia del Tribunal Constitucional tienen el atrevimiento de citar el Convenio 108 y la Directiva 95/46/CE, para afirmarlos como valiosos criterios hermenéuticos del sentido y alcance de los derechos y libertades que la Constitución reconoce, para luego exigir lo contrario a lo que estos textos internacionales dicen. O incluso llegar a citar el ordenamiento jurídico alemán, país en el que es posible la cesión de datos entre Administraciones Públicas sin consentimiento del interesado.

mos en cuenta las referencias a este principio de calidad y de finalidad en el Convenio 108 del Consejo de Europa, en la Directiva 95/46/CE y en las legislaciones de los países europeos[179]. También es trascendente y fue omitida por la Sentencia del Tribunal Constitucional la exigencia del principio de información para la cesión de datos. El principio de información es otro elemento clave del contenido esencial del derecho fundamental a la protección de datos personales, también en virtud de la noción generalmente admitida de lo que este derecho significa[180].

Pues bien, el ciudadano podrá no tener que consentir para la comunicación de datos entre Administraciones Públicas para competencias diferentes o que versen sobre materias distintas en virtud de la legitimidad de la actividad administrativa. Tampoco es imprescindible que preste su consentimiento para el tratamiento de datos personales para finalidades distintas por parte del mismo responsable del fichero. No tendría sentido que prestara su consentimiento para tratamientos de un mismo responsable para finalidades distintas si tampoco lo prestó para la primera finalidad. Pero lo que no se le puede suprimir es su facultad de estar informado de la cesión, de la entidad cesionaria, de la nueva finalidad del tratamiento, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del tratamiento. Tampoco se le puede suprimir la facultad de estar informado de la existencia de un tratamiento para una finalidad distinta por parte del mismo responsable del fichero. Así, el principio de información es una facultad esencial del derecho fundamental a la protección de datos personales, que puede y debe ser respetada en todo caso por las Administraciones Públicas. En esta misma dirección, si la información es un principio básico en la recogida de datos por las Administraciones Públicas, este principio refuerza la importancia del derecho de acceso. El interesado tiene derecho a solicitar y a obtener información sobre sus datos sometidos a tratamiento, tanto del mismo responsable del fichero que va a tratar los datos para una finalidad distinta como de la Administración Pública cesionaria de la información.

De lo que también se deduce que a partir de este planteamiento cobra una gran importancia la declaración de los ficheros[181]. El responsable que ya

---

[179] Cfr. artículo 5 del Convenjo 108 y artículo 6 de la Directiva 95/46/CE, y la totalidad de las leyes de protección de datos de los países europeos.

[180] Cfr. artículo 8.a) del Convenio 108 y artículos 10 y 11 de la Directiva 95/46/CE.

[181] Nosotros consideramos que la declaración de ficheros en el ámbito público a través de una disposición de carácter general y su inscripción en el registro de ficheros es un trámite esencial y, en absoluto, una formalidad burocrática. El responsable público que declara un fichero se conciencia de que los datos no son suyos, sino de los ciudadanos, y se sitúa en mejor disposición para respetar los principios de protección de datos —especialmente el de calidad y el de información en la elaboración del impreso de recogida— y los derechos de acceso, rectificación y cancelación. La experiencia demuestra que un responsable público que no declara los ficheros, no respeta ni los principios ni los derechos de protección de datos personales. En todo caso, hay que reconocer que la declaración e inscripción de ficheros no está extendida en la Unión Europea. Sólo es obligatoria en España y Austria. En Gran Bretaña se inscriben casi todos los ficheros, a excepción de algunas categorías de tratamientos. En cambio, en Italia la regla general es la no inscripción, salvo supuestos específicos como los ficheros genéticos o de seguros.

tenía el fichero público pero que vaya a tratar los datos personales de los ciudadanos para una finalidad distinta tiene obligación de declarar de nuevo el fichero, a través de una disposición de carácter general, y proceder a una modificación en el registro de ficheros. Igualmente, la Administración Pública cesionaria de la información tiene la obligación, con anterioridad al tratamiento de los datos, de proceder a la declaración del nuevo fichero a través de una disposición de carácter general y a su inscripción en el registro correspondiente.

De esta forma, se puede afirmar que los requisitos tanto para la cesión de datos entre Administraciones Públicas sin consentimiento del interesado como para el tratamiento de los datos por el mismo responsable del fichero para una finalidad distinta serían: en primer lugar, que se produzca para el ejercicio de funciones propias de las Administraciones Públicas en el ámbito de sus competencias; en segundo lugar, que se respete siempre el principio de información al titular de los datos, tanto por parte del responsable del fichero que procede a un tratamiento distinto como del cesionario de los datos, de las nuevas finalidades y de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación; y, en tercer lugar, que se produzca una nueva declaración del fichero y su inscripción en el registro general, de manera que se garantice el principio de publicidad de los tratamientos.

Además, los planteamientos restrictivos con la comunicación de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o competencias que versen sobre materias distintas plantean el problema de qué se entiende por distintas Administraciones Públicas. No parece que tenga sentido afirmar que los distintos Ministerios de la Administración General del Estado, las distintas Consejerías de una misma Comunidad Autónoma y las Concejalías de un mismo Ayuntamiento son distintas Administraciones Públicas cuando todas tienen la misma personalidad jurídica[182]. Así, hemos manifestado que los distintos accesos al fichero del padrón municipal en el ámbito de un mismo Ayuntamiento no pueden ser calificados como cesión de datos, ya que un departamento municipal de un mismo Ayuntamiento no puede ser considerado un tercero[183]. Así, el acceso a un fichero municipal por las diferentes áreas del Ayuntamiento no sería un supuesto de comunicación de los datos de manera que tuviera que justificarse en virtud de las excepciones al consentimiento para la cesión previstas en el artículo 11.2 LOPD, especialmente la existencia de una habilitación legal expresa que justificara la cesión. Tampoco haría falta alegar que se trata de una comunicación de datos entre Administraciones Públicas para el ejercicio de competencias semejantes o que versan sobre las mismas materias —art. 21.1 LOPD *sensu contrario*—.

---

[182] Sobre la personalidad jurídica del Estado, cfr. L. LÓPEZ GUERRA, «Sobre la personalidad jurídica del Estado», *Revista de Derecho Político*, 1980; A. GALLEGO ANABITARTE, *Derecho Administrativo,* I, Materiales, Madrid, 1989.

[183] Cfr., más ampliamente, A. TRONCOSO REIGADA, «Introducción y Presentación», en *Guía de Protección de Datos para Ayuntamientos*, APDCM-Civitas, Madrid, 2004, págs. 34-38.

La razón de ser de la distribución de competencias entre distintas Áreas y Concejalías de un mismo Ayuntamiento, o entre distintas Consejerías o Direcciones Generales de una misma Comunidad Autónoma, reside en que las competencias versan sobre materias distintas, lo que no facilitaría inicialmente la comunicación de datos. De esta forma, la habilitación prevista en el artículo 21.1 LOPD para la comunicación de datos sin consentimiento del interesado para el ejercicio de competencias semejantes o que versen sobre materias distintas sólo es posible entre las distintas Administraciones territoriales —Concejalía de Sanidad de un Ayuntamiento, Consejería de Sanidad de una Comunidad Autónoma y Ministerio de Sanidad—, pero no desde una misma Administración territorial, que distribuye sus competencias entre los distintos departamentos. Esto dificultaría la comunicación de datos entre la misma Administración territorial, es decir, entre la misma Comunidad Autónoma o el mismo Ayuntamiento.

Además, un planteamiento que considere cesión de datos los distintos accesos a un fichero de algún departamento de la misma Administración Pública estaría desincentivando el proceso de descentralización y desconcentración de competencias. Considerar cesión el acceso a un fichero de personal gestionado por la Dirección General de Recursos Humanos por otra Dirección General de la misma Comunidad Autónoma competente en materia de calidad en los servicios públicos o de medición del desempeño, lo que está es animando la creación de pocas Direcciones Generales o favoreciendo el establecimiento de ficheros muy centralizados para así evitar la consideración de cesión. Lo mismo cabe decir del acceso a determinados ficheros de naturaleza horizontal por las distintas Consejerías de un mismo gobierno autonómico.

Así, en el caso de que entendiéramos que el acceso a los datos del fichero por parte de departamentos de la misma Administración territorial es un supuesto de comunicación de datos, no sería posible su tratamiento ya que éste se producirá habitualmente para finalidades distintas. La única solución es que existiera una habilitación legal, cosa que no siempre existe. Por tanto, debe entenderse que es legítimo el acceso de los distintos departamentos de una misma Administración territorial a los ficheros que obran en poder de ésta. Inicialmente, este acceso a los datos debería estar limitado por el propio principio de calidad, esto es, por la finalidad del fichero. El problema, como acabamos de señalar, está en qué ocurre cuando la misma Administración Pública quiere utilizar el fichero para una función radicalmente distinta a aquella que justificó su obtención. Si interpretáramos el principio de calidad en sentido estricto, se dificultaría el tratamiento de una información que dispone una misma Comunidad Autónoma para finalidades distintas. Este planteamiento restrictivo tendría sentido si la persona hubiera dado su consentimiento para el primer tratamiento, lo que no ocurre dada la excepción a este consentimiento para el tratamiento de datos para funciones administrativas. Parece razonable que la Administración pueda tratar los datos personales para una finalidad distinta, siempre que garantice el principio de información. No se puede afirmar que habrá que exigir el consentimiento para el nuevo trata-

miento al ser la finalidad distinta, cuando tampoco se exigió este consentimiento en el momento de la recogida de los datos —art. 6 LOPD—. Lo que habrá que hacer es, sencillamente, informar al ciudadano, no tratar más que los datos indispensables para esta finalidad, implantar las medidas de seguridad, garantizar el deber de secreto y, sobre todo, facilitar el ejercicio de los derecho de acceso, rectificación y cancelación. Por ello, el tratamiento de datos dentro de la misma Administración Pública tiene que tener presente el principio de calidad, respetando la finalidad del tratamiento y sólo modificándola después de garantizar el principio de información.

Lo afirmado hasta ahora no significa dejar abandonado el derecho fundamental a la protección de datos personales en manos de la Administración, que tendría las manos libres para llevar a cabo todo tipo de tratamientos de datos personales. La Administración tiene que respetar los principios de protección de datos, especialmente por el principio de información, y los derechos de los afectados —especialmente por el derecho de acceso y rectificación—, y que se materializan también a través de los criterios que hemos manifestado anteriormente[184]. No obstante, como ya hemos señalado en otras ocasiones, el derecho a la protección de datos de los ciudadanos tiene contenidos distintos frente a tratamientos realizados por las Administraciones Públicas y por los particulares. Así, existe un mayor derecho fundamental a la protección de datos de carácter personal frente a ficheros privados; en cambio, existe un menor derecho a la protección de los 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[185].

Además, sin negar la vocación transformadora de la propia Constitución y la necesidad de modificar algunas prácticas administrativas y privadas que no se ajustan a los preceptos constitucionales, no parece que tenga sentido considerar como manifiestamente inconstitucional la cesión de datos entre Administraciones Públicas sin consentimiento del interesado, que ha sido no sólo una práctica habitual en el ámbito público, refrendada, no lo olvide-

---

[184] La verdad de estas afirmaciones se puede corroborar en el incremento exponencial de la actividad inspectora y de tutela de derechos de la APDCM en el ámbito público, en comparación con el resto de las Autoridades de Control. Cfr. *Memoria de la Agencia Española de Protección de Datos 2003, Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid 2003* y *Memoria de la Agencia Catalana de Protección de Datos 2003*.

[185] Cfr. A. TRONCOSO REIGADA, «Prólogo» a M. FERNÁNDEZ SALMERÓN, cit., págs. 23-45, esp. págs. 44-45. Ésta es una excepción frente a la teoría general de los derechos fundamentales que afirma que tenemos más derechos fundamentales frente a los poderes públicos y menos frente a los particulares. Cfr. J. M. BILBAO UBILLOS, *La eficacia de los derechos fundamentales frente a particulares*, CEPC, Madrid, 1997; J. F. LÓPEZ AGUILAR, *Derechos fundamentales y libertad negocial*, Ministerio de Justicia, Madrid, 1990; P. CRUZ VILLALÓN, *Derechos fundamentales y Derecho privado*, Academia Sevillana del Notariado, 1988, págs. 97-114; J. ALFARO ÁGUILA-REAL, «Autonomía Privada y derechos fundamentales», *Anuario de Derecho Civil*, XLVI, 1993, págs. 57-122.

mos, tanto por la LORTAD como por la LOPD, que la autorizaban expresamente, sino también una conducta desarrollada con posterioridad a la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. En otras ocasiones, se ha pretendido encontrar una habilitación legal muy indirecta para justificar la cesión, a través de una expresión legal vaga que pueda justificar la comunicación de datos entre Administraciones Públicas y otras muchas cosas contradictorias, a base de forzar el tenor literal[186]. No se trata de hacer normal en las leyes lo que es normal en la calle, parafraseando una expresión de nuestra transición a la democracia, porque en la calle a veces se lesionan gravemente los derechos. Se trata de no generar esquizofrenias entre lo que se exige a las Administraciones Públicas y sobre lo que éstas hacen en realidad. En este ámbito demostró más sentido común el legislador —no el legislador de una mayoría política, sino el de dos mayorías políticas distintas— que el Tribunal Constitucional[187].

En todo caso, queremos manifestar abiertamente que no podemos compartir las reflexiones que se hacen habitualmente sobre protección de datos personales y que siempre son contrarias a los tratamientos de datos personales por las Administraciones Públicas. Estos planteamientos dejan entrever un cierto prejuicio anti-Estado, sin tener en cuenta la superación del Estado liberal por el Estado social[188], a la vez que se mantiene una mirada complaciente hacia los tratamientos de datos personales llevados a cabo por sujetos privados. Esta diferencia de criterio y, en especial, el recelo hacia los tratamientos de datos personales desarrollados por los poderes públicos no coinciden con la opinión de los ciudadanos, que, de manera muy clara y mayoritaria, consideran mucho más agresivos hacia sus derechos los tratamientos de datos personales desarrollados por empresas privadas[189]. Así, llama la atención que el legislador haya previsto algunas pre-

---

[186] Si no existe un alto nivel de cumplimiento de la obligación de declaración de ficheros en todas las Administraciones Públicas, a excepción de aquellas del territorio de la Comunidad de Madrid, tampoco existe un seguimiento de la prohibición del Tribunal Constitucional de las cesiones de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o que versen sobre materias distintas. No vamos a afirmar que existe una prevaricación tácita, pero sí que la legislación no se cumple. Cfr. la *Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid 2003* y la *Memoria de la Agencia Española de Protección de Datos 2003*.

[187] Llama la atención la diferente posición que mantuvo el Grupo Parlamentario Popular, que pasó de presentar un recurso de inconstitucionalidad contra la LORTAD a votar a favor de una LOPD que mantenía los preceptos impugnados. En estos casos, la diferencia fundamental está en conocer la realidad y tener experiencia de gobierno. Lo mismo se puede decir de las críticas a la legislación de protección de datos desde la Asociación Jueces para la Democracia, que no son seguidas por el actual Ministro del Interior, que defiende la ampliación de las comunicaciones de datos en el ámbito europeo en beneficio de la seguridad ciudadana.

[188] Cfr. A. Troncoso Reigada, «El Estado social», cit.

[189] Así, los resultados del Eurobarómetro de la Comisión Europea sobre protección de datos personales, realizado por iniciativa de la Dirección General del Mercado Interior y publicado el 2 de marzo de 2004, que analiza la visión que los ciudadanos europeos tienen en relación con el tratamiento de sus datos personales por organizaciones públicas y privadas, da como resultado que las organizaciones consideradas más fiables en relación con el tratamiento de datos personales son las sanitarias, policiales, agencias de recaudación de impuestos y entidades financieras. En el lado opuesto se situarían las empresas de comercio por correspondencia, emisores de tarjetas de crédito y compañías de seguros. http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_highlights.pdf

rrogativas a determinados ficheros privados, tal vez necesarias para el funcionamiento de una economía de mercado y para la estabilidad de los sistemas financieros, como es el tratamiento de datos sin consentimiento del interesado en los ficheros de solvencia patrimonial y de crédito o en los ficheros de seguros, o la propia habilitación de un censo promocional, también sin consentimiento del interesado, sin que esto haya sido analizado por el Tribunal Constitucional con el mismo nivel de exigencia que han sido analizados los ficheros públicos por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre[190]. Es posible que esto haya sido debido a que el recurso de inconstitucionalidad es presentado por el Defensor del Pueblo, que tiene como función constitucional la defensa de los derechos fundamentales en la actividad administrativa y que tiene una legitimación específica para impugnar los preceptos relativos a los ficheros públicos —art. 54 CE—. No queremos decir con ello que todos estos tratamientos privados sean ilegítimos, especialmente a partir de la habilitación que les da la propia Directiva 95/46/CE. Lo único que queremos señalar es que ha habido un menor control jurisdiccional sobre éstos y una gran diferencia de rasero entre lo que se exige a los ficheros públicos y a los ficheros privados.

Esta reflexión se ve corroborada igualmente si se analizan las legislaciones de protección de datos personales de los países de la Unión Europea. Si España tiene una legislación en general más estricta —una buena demostración de que hemos llegado los últimos a legislar sobre esta materia y queremos ser ahora los más rigurosos—, esto se manifiesta especialmente en las cesiones de datos entre Administraciones Públicas, conducta habilitada en otros países de la Unión Europea. Puede llamar la atención esta afirmación si se tienen en consideración únicamente las Memorias de las Autoridades de Control europeas. Es fundamental no llevarse a engaño. La mayoría de las Autoridades de Control de los países de la Unión Europea —a excepción de España y de Portugal— suelen tener un nivel de teorización bastante elevado sobre el derecho fundamental a la protección de datos personales —especialmente la Autoridad francesa[191] y la italiana—, que no se ve refrendado ni por el contenido de las legislaciones de estos países, ni por las potestades que éstas atribuyen a las Autoridades de Control, ni por la actividad de inspección y sanción, que no llevan a cabo en realidad[192]. En pocos ámbitos se ve

---

[190] Así, si se quiere desarrollar un control estricto y severo, se puede afirmar que más sospechas de inconstitucionalidad presentan el censo promocional o la propia existencia de ficheros de solvencia patrimonial y de crédito, donde se producen tantas vulneraciones del principio de calidad y del principio de información, vistas las resoluciones sancionadoras y las inspecciones sectoriales de la Agencia Española de Protección de Datos en esos ámbitos. Estos ficheros podrían ser sustituidos por ficheros positivos de solvencia, donde no habría tratamientos de datos personales sin consentimiento del interesado.

[191] Un estudio comparativo entre las Agencias de Protección de Datos a nivel europeo se puede ver en T. GARCÍA-BERRIO HERNÁNDEZ, *Informática y libertades. La protección de datos personales y su regulación en Francia y España,* cit., págs. 353-415.

[192] Y aunque tengan estos poderes, no los ejercen por sus tradiciones jurídicas. La Autoridad alemana, además de estar encuadrada en el Ministerio del Interior, no desarrolla una labor real de inspección.

tanta incongruencia entre lo que se predica en los foros internacionales y lo que efectivamente se lleva a cabo en los respectivos países. No existe realmente una tutela del derecho fundamental a la protección de datos personales en el ámbito europeo, tal vez porque este derecho no está todavía en sus respectivos textos constitucionales.

El segundo inciso declarado inconstitucional por la STC 292/2000, de 30 de noviembre, ha sido el artículo 24.1 LOPD, que afirmaba: «Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado *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*»[193]. El Tribunal Constitucional entendió que era legítima la excepción del principio de información cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales pero no era constitucional excepcionar del cumplimiento de la obligación de información con la mera justificación de que tal cosa puede impedir o dificultar gravemente las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la persecución de infracciones administrativas.

La expresión elegida por el legislador en el artículo 21.1 LOPD es, a juicio del Tribunal Constitucional, tan genérica que en ella tiene cabida prácticamente toda la actividad administrativa. Así, se entiende que este precepto permite a la Administración Pública decidir libremente cuándo denegar al interesado la información sobre la existencia de un fichero, sobre la finalidad de la recogida de los datos y de los destinatarios de la información, sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y sobre la identidad y dirección del responsable del tratamiento. Así, teniendo en cuenta la importancia del principio de información en el Convenio 108 —art. 8—, se entiende que el legislador ha hecho un uso excesivo de la habilitación establecida en el mismo para justificar la omisión del principio de información, que sí cubriría la protección de la seguridad del Estado, de la seguridad pública o la represión de infracciones penales —art. 9.2.a)—, pero no las dificultades graves que la obligación de información pueda acarrear a las funciones de control y verificación de las Administraciones Públicas o la persecución de infracciones administrativas, que no tienen fácil encaje en el Convenio, ni siquiera como medida necesaria en una sociedad democrática para la protección de la persona concernida y de los derechos y libertades de otras personas —art. 9.2.b)—.

La Autoridad italiana elige los temas que investiga y sólo lleva a cabo inspecciones puntuales. La Autoridad francesa hace básicamente deliberaciones, pero tampoco lleva a cabo inspecciones realmente. No obstante, la Comisión francesa tiene un importante poder político al ser sus miembros diputados. La Agencia de Gran Bretaña tiene que pedir permiso para hacer una inspección al responsable del fichero —orden de *enforcement*—. Si el responsable se niega, sólo le queda ir a los Tribunales. La Agencia irlandesa ha hecho una sola inspección en los últimos cinco años. Sólo Portugal y Grecia atribuyen poderes reales de inspección en materia de protección de datos, lo que no es decir mucho.

[193] Se señalan en cursiva los incisos declarados inconstitucionales.

Lo mismo cabe deducir del análisis de la Directiva 95/46/CE. Como hemos señalado anteriormente, la Directiva reconoce la importancia del principio de información al afectado —arts. 10 y 11—, pero establece excepciones para salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la persecución de infracciones penales o de infracciones de la deontología en las profesiones reglamentadas; e) la existencia de un interés económico importante, incluidos los asuntos monetarios, presupuestarios o fiscales; f) para la «función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d), y e); g) la protección del interesado o de los derechos y libertades de otras personas». Por tanto, tampoco la Directiva da cobertura a los incisos sometidos a discusión, de forma que se puede afirmar que la LOPD ha ampliado las excepciones más allá de lo que admitían las normas internacionales. Como es lógico, éstas deben ser utilizadas para interpretar el contenido esencial del derecho fundamental a la protección de datos personales del artículo 18.4 CE[194].

Así, para el Alto Tribunal, el artículo 24.1 LOPD adolece, además, de falta de certeza y previsibilidad, lo que genera una indeterminación sobre los casos a los que se aplica tal restricción. Así, «cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública»[195]. El empleo por la LOPD en su artículo 24.1 de la expresión «funciones de control y verificación», «abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia; […] permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración»[196]. De esta forma, el artículo 24.1 LOPD deja a la Administración Pública competente la facultad de conceder o denegar discrecionalmente el principio de información para los tratamientos[197].

---

[194] No parece razonable la afirmación del abogado del Estado de que una parte significativa de las infracciones administrativas se encuadran en la protección de la seguridad pública y los intereses financieros del Estado. En cambio, sí parece tener razón cuando critica la equiparación que hace la Directiva, a efectos de la excepción del principio de información, de la persecución de las infracciones penales y de las infracciones de la deontología en las profesiones reglamentadas. Así, no parece acertado que la persecución de las infracciones deontológicas disponga de una posición privilegiada respecto de las infracciones administrativas, cuando las primeras son perseguidas y sancionadas por las Administraciones corporativas en el ordenamiento jurídico español. Además, no parece tener sentido la protección reforzada de estas profesiones en detrimento de otras actividades administrativas como la persecución del incumplimiento de deberes tributarios, la estabilidad del sistema financiero, la conservación del medio ambiente o los derechos de los consumidores y usuarios.

[195] FJ 16.

[196] FJ 17.

[197] Sin embargo, para el abogado del Estado, por «funciones de control y verificación» debemos entender la comprobación administrativa de que el acto o la actuación de quien está sujeto a tal comproba-

El interés público, que sin duda existe, de sancionar infracciones administrativas no resulta suficiente para justificar la omisión del principio de información. Además, ésta es una práctica que puede conllevar una grave indefensión en el interesado para ejercitar su derecho de defensa en un procedimiento sancionador, al negarle la propia Administración acceso a los datos que sobre su persona pueda poseer y que puedan ser empleados en su contra. De hecho, la propia Directiva 95/46/CE —art. 15— y la LOPD —art. 13— reconocen el derecho de toda persona a no verse sometida a decisiones con efectos jurídicos sobre ella, o que le lleguen a afectar de manera significativa, que se basen únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad[198].

A nuestro parecer, la limitación del principio de información cuando impida o dificulte gravemente las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la persecución de infracciones administrativas representa una vulneración del derecho fundamental a la protección de datos personales. Como hemos razonado anteriormente, el principio de información es una garantía esencial del derecho fundamental en el ámbito público, que permite conocer la existencia de tratamientos con nuestros datos personales y facilita el ejercicio del derecho de acceso. Cuando se suprime de manera general el principio de información, también se dificulta sobremanera el derecho de acceso, que sólo puede apoyarse en la publicidad de los tratamientos a través del Registro General de Protección de Datos —art. 39 LOPD—. No hay ninguna actividad administrativa de control o verificación o de persecución de infracciones administrativas que impida a la Administración la obligación de informar al ciudadano de la existencia de un fichero con sus datos, de la finalidad del tratamiento, de los destinatarios de la información, de la identidad y dirección del responsable, y de las posibilidades de ejercitar los derechos de acceso, rectificación y cancelación. Este inciso del artículo 24.1 LOPD destruye una de las garantías de este derecho fundamental que pertenece a su naturaleza jurídica, elimina una de sus facultades esenciales que hacen que los intereses jurídicos queden desprotegidos, afectando gravemente a su contenido esencial. No parece razonable a primera vista que haya algún bien constitucional que se proteja si la Administración omite su obligación de informar de los tratamientos. Así, el artículo 105.b) CE, cuando reconoce el derecho de acceso de los ciudadanos a los archivos y registros administrativos, sólo establece como excepciones lo que afecte a la seguridad del Estado, la averiguación de los delitos y la intimidad de las personas, sin mención alguna a la persecución de infracciones administrativas.

El tercer inciso declarado inconstitucional es el apartado segundo del artículo 24, que decía: «Lo dispuesto en el artículo 15 y en el apartado 1 del

---

ción se ajusta a las normas que la rigen y al interés general, de manera que grandes esferas de la actividad administrativa (como la prestacional o la sancionadora o ablativa de derechos e intereses privados) quedan fuera de esas funciones de comprobación y verificación.

[198] FJ 18.

artículo 16 no será de aplicación si, 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. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas». Así, este precepto suprime para estos supuestos el derecho de acceso y limita el derecho de rectificación y cancelación de los datos personales[199].

Para el Defensor del Pueblo, la afirmación de que los derechos de acceso, rectificación y cancelación tuvieran que ceder, ponderados los intereses en presencia, ante razones de interés público representa una «cláusula en blanco bajo la cual podría encontrar cobijo toda la actividad administrativa», ya que toda la actividad administrativa, *ex* artículo103.1 CE, está encaminada a la consecución del interés general. Además, la limitación del derecho de acceso, rectificación y cancelación ante «intereses de terceros más dignos de protección» es excesiva, ya que supone una limitación al derecho fundamental a la protección de datos no necesariamente en virtud de los derechos y libertades de terceros, sino de cualquier interés que se entienda merecedor de protección[200]. Para el Tribunal Constitucional, este inciso vuelve a incurrir en una falta de certeza y previsibilidad en el establecimiento de límites al derecho fundamental a la protección de datos personales, que genera una gran indeterminación acerca de los casos en los que puede limitarse el derecho de acceso, rectificación y cancelación, dejando al libre albedrío de la Administración Pública la determinación de los intereses que pueden justificar la limitación de este derecho fundamental. Además, en ningún caso estas limitaciones parecen estar justificadas en la protección de otros derechos o bienes constitucionales[201].

Un estudio de la normativa internacional resulta esclarecedor a la hora de determinar los límites que pueden ser planteados a los derechos de acceso, rectificación y cancelación y, de esta forma, ayudar a configurar el contenido esencial de este derecho fundamental a la protección de datos personales[202]. El Convenio 108 del Consejo de Europa atribuye a cualquier persona la facultad de: «a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la resi-

[199] El abogado del Estado mantenía que el artículo 24.2 LOPD imponía límites al derecho de acceso y sólo parcialmente a los derechos de rectificación y cancelación, pues afectaba sólo al plazo obligatorio para que el responsable del fichero haga efectivos esos derechos, no limitando la rectificación y cancelación de los datos inexactos o incompletos o la obligación del responsable del fichero de notificar al cesionario de los datos su rectificación o cancelación. Es decir, para éste, la función del precepto impugnado era conceder al responsable del fichero administrativo únicamente el poder de imponer provisionalmente su punto de vista, fundamentando así una denegación cautelar de estos derechos, hasta que se resuelva la controversia definitivamente por la Autoridad de Protección de Datos, estatal o autonómica.

[200] Antecedentes II y FJ 18.

[201] FJ 12.

[202] Lógicamente, no para convertir a la normativa europea en parámetro de constitucionalidad.

dencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio» —art. 8—. No obstante, como hemos señalado anteriormente, el artículo 9 establece como excepciones de este artículo 8 «la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales» o «para la protección de la persona concernida y de los derechos y libertades de otras personas». Lo mismo ocurre en la Directiva 95/46/CE, que, después de afirmar el derecho de acceso —art. 12—, establece un conjunto de excepciones y limitaciones ya mencionadas —art. 13—, como las relativas a la seguridad del Estado, la defensa, la seguridad pública, la persecución de infracciones penales o de la deontología profesional, la protección de intereses económicos o financieros importantes —incluidos los asuntos monetarios, presupuestarios o fiscales—, la función de control y de inspección de las autoridades públicas en los casos mencionados anteriormente, y la protección del interesado o de los derechos y libertades de otras personas.

Estas excepciones a los derechos de acceso, rectificación y cancelación han sido ya transpuestas en nuestra legislación —art. 23 LOPD—, que establece un conjunto de excepciones a estos derechos, en los ficheros para fines policiales de las Fuerzas y Cuerpos de Seguridad del Estado, «en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando». Igualmente, los responsables de los ficheros de la Hacienda Pública pueden denegar estos derechos cuando obstaculicen «las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras». Sin embargo, la normativa europea no habilita la posibilidad de suprimir los derechos de acceso, rectificación y cancelación por razones de interés público o ante intereses de terceros más dignos de protección. Esta posibilidad no quedaría cubierta con las referencias en los textos europeos a «la protección del propio interesado» —por ejemplo, para supuestos de limitación del derecho de acceso del propio paciente a la historia clínica por necesidades terapéuticas[203]— o a «los derechos y libertades de otras personas», lo que no equivale a las cláusulas genéricas incluidas en el artículo 24.2 LOPD.

[203] Esta posibilidad la contempla la propia Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica —art. 18.3—.

Como hemos señalado antes, el derecho de acceso, rectificación y cancelación es una facultad imprescindible del derecho fundamental a la protección de datos personales. La interpretación de este derecho a la luz de la opinión generalmente admitida de lo que este derecho significa incluye los derechos de acceso, rectificación y cancelación como parte del contenido esencial del derecho fundamental a la protección de datos personales, sin el cual este derecho no es reconocible como perteneciente a su tipo previo y sin cuyo ejercicio los intereses jurídicos que dan vida a este derecho resultan desprotegidos. Por tanto, se puede afirmar en este caso también, con el Tribunal Constitucional, que el artículo 24.2 LOPD vulneraba el contenido esencial del derecho fundamental a la protección de datos. Suprimir las facultades de acceso, rectificación y cancelación equivale a vaciar de contenido efectivo este derecho fundamental, imponerle restricciones injustificadas y desproporcionadas que lo hacen impracticable y lo despojan de su necesaria protección[204].

3. REFLEXIÓN FINAL[205]

La Constitución española de 1978, junto con la Constitución portuguesa de 1976, han sido los primeros textos constitucionales en hacer una referencia específica a la protección de datos personales. Con posterioridad, las reformas constitucionales de los países europeos han incluido distintos preceptos que garantizan la protección de los datos personales. Recientemente, tanto la Carta de los Derechos Fundamentales de la Unión Europea, aprobada por el Tratado de Niza de 10 de diciembre de 2000, como la Constitución europea, aprobada por el Tratado de Roma de 29 de octubre de 2004 y pendiente de ratificación por los Estados, reconocen el derecho fundamental a la protección de datos personales como derecho autónomo.

La Constitución española de 1978 establece que «[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» —art. 18.4 CE—. El texto constitucional español no ha aprovechado la experiencia de la Constitución portuguesa. No ha proclamado de manera clara un derecho fundamental a la protección de datos personales, sino que ha establecido únicamente un mandato al legislador para que limite la informática en garantía del derecho al honor y a la intimidad personal y familiar y del pleno ejercicio de los derechos. Es, por tanto, un precepto que presenta insuficiencias, al centrarse únicamente en el aspecto defensivo y restrictivo. En todo caso, la

[204] Sin perjuicio de las posibilidades de incrementar las facultades tuitivas de las Autoridades de Control, no parece suficiente garantía de los derechos de acceso, rectificación y cancelación la intervención de éstas prevista en el segundo párrafo del artículo 24.2 LOPD o el recurso ante la jurisdicción contencioso-administrativa.

[205] En este apartado se recogen, de manera más resumida, a modo de *abstract*, los principales argumentos de este trabajo.

propia existencia de este precepto constitucional supuso, sin duda, un elemento positivo. Difícilmente se puede criticar la parquedad del constituyente, vista la falta de sensibilidad del legislador, que esperó al año 1992 para aprobar la LORTAD y cumplir, de esta forma, este mandato constitucional.

El Tribunal Constitucional ha tenido que desarrollar una intensa exégesis para afirmar un derecho fundamental a la protección de datos personales, a partir del tenor literal del artículo 18.4 CE, y para establecer, aunque sea de manera mínima, su núcleo a partir de la doctrina del contenido esencial de los derechos fundamentales. Entre esta jurisprudencia constitucional destaca la Sentencia 292/2000, de 30 de noviembre, muy influida por los borradores de la Carta de Derechos Fundamentales de la Unión Europea. La antigua proclamación del derecho a la intimidad no era una protección bastante frente a la nueva realidad del progreso tecnológico. El derecho fundamental a la protección de datos es, por una parte, un *derecho autónomo nuevo*, con un contenido específico que atribuye a la persona un control de sus datos personales, sean o no íntimos —los datos de conocimiento público pertenecen también al poder de disposición de la persona—; que protege a la persona —en especial, la propia información personal— frente a las tecnologías de la información y configura un derecho general frente a estas tecnologías; que dispone de una dimensión más activa que el derecho a la intimidad, al implicar conocimiento y control; que no encaja bien con la idea de injerencia o intromisión ilegítima ya que es el propio interesado quien revela sus datos personales, en muchas ocasiones, de forma voluntaria o por obligación legal. Por otra parte, es un *instrumento de garantía* de otros derechos fundamentales, en especial del derecho a la intimidad, pero no sólo de este derecho. La informática puede ser utilizada para limitar el «*pleno ejercicio de* [otros] *derechos*», distintos del derecho a la intimidad. Así, un tratamiento indebido del dato relativo a la cuota sindical de un trabajador supone una vulneración de la libertad sindical —art. 28 CE—. La protección especial de los datos de ideología, afiliación sindical, religión o creencias —art. 7 LOPD— es una exigencia de otros derechos fundamentales como la libertad ideológica y religiosa. Así, el hecho de que las vulneraciones de la libertad sindical, de la libertad ideológica y religiosa por tratamientos informáticos ilegítimos tengan también tutela en sus propios derechos específicos no suprime la garantía que presta en este caso el propio derecho fundamental a la protección de datos personales.

No obstante, hay que señalar que de la ubicación en el artículo 18 y de la propia mención expresa en el apartado 4 al derecho a la intimidad personal y familiar se desprende que el derecho a la protección de datos personales no debe ser visto como un derecho absolutamente independiente, sino dentro de la esfera amplia del derecho a la intimidad, como una especie de manifestación más de la protección de la vida privada, aunque tutele también el ejercicio de otros derechos fundamentales —como, por otra parte, también le ocurre al propio derecho a la intimidad—. El derecho a la protección de datos personales representa, de alguna manera, una concretización del derecho

a la intimidad en los tratamientos de datos personales, una actualización del derecho a la privacidad frente al desarrollo de las tecnologías de la información, un derecho más específico dentro del más general derecho de privacidad personal. De hecho, otros países como Italia y Alemania han buscado otros preceptos constitucionales como los derechos de libertad, el libre desarrollo de la personalidad o el reconocimiento de la dignidad de la persona para fundamentar el derecho a la protección de datos personales porque carecían de un precepto constitucional específico que reconociera el derecho a la intimidad. De la propia legislación española se deduce que el tratamiento de datos personales, especialmente a través de las tecnologías de la información, afecta principalmente a la intimidad —o la privacidad, por utilizar un término empleado por la Exposición de Motivos de la LORTAD— y, por ello, el legislador busca configurar ámbitos y registros personales ajenos al tratamiento por los demás. Esta relación del derecho fundamental a la protección de datos personales con el derecho a la intimidad no suprime ni atenúa su carácter de derecho autónomo. Sencillamente, resalta su carácter mixto o bifronte. No obstante, este debate, frecuentemente presente en nuestra jurisprudencia y doctrina constitucional, se caracteriza principalmente por su inutilidad. Ambas concepciones tienen la tutela constitucional reforzada de los derechos fundamentales de la Sección 1.ª del Capítulo II del Título I. Considerar el derecho a la protección de datos personales o derecho a la autodeterminación informativa como un derecho autónomo o instrumental del derecho a la intimidad no debe hacernos olvidar que ambos derechos poseen el mismo origen: la dignidad de la persona.

Al precisar el artículo 18.4 CE que la ley limitará el uso de la *informática*, parece que este derecho fundamental a la protección de datos sólo existe frente a los tratamientos automatizados y no frente a los no automatizados, ya que la informática se refiere a tratamientos mecanizados. Sin pretender restar importancia a los riesgos de los modernos sistemas de información y a la necesidad de tutelar los derechos fundamentales frente al incremento de las bases de datos, en la elaboración de nuestra Constitución se perdió la oportunidad de reconocer expresamente un derecho fundamental a la protección de datos personales, no limitando la tutela a los tratamientos automatizados, sino abarcando también los no automatizados, como ha hecho no sólo la Directiva comunitaria 95/46 y la LOPD, sino la propia Constitución europea. No obstante, a pesar del difícil encaje constitucional, el Alto Tribunal ha incluido también en la Sentencia 292/2000, de 30 de noviembre, los tratamientos no automatizados dentro del contenido de este derecho fundamental. Nuestra Constitución también perdió la oportunidad de establecer una protección más clara de los derechos frente al desarrollo de las nuevas tecnologías —no sólo de la informática—, que en ese momento no se podía precisar pero tal vez sí se podía intuir.

El artículo 18.4 CE obligaba al legislador a aprobar una ley general de protección de datos personales. La opción por aprobar legislaciones sectoriales sin ley general era, a nuestro parecer, difícilmente compatible con el man-

dato del artículo 18.4 CE. En cambio, no se extrae de este precepto constitucional el rechazo a la presencia de leyes sectoriales, que, por otra parte, ya existían con anterioridad. Con la aprobación de la LORTAD y de la LOPD, nuestro legislador ha optado por disponer de una norma general sobre protección de datos, sin perjuicio de que existan diversas regulaciones sectoriales a las que éstas se remiten. Una Ley general de protección de datos tiene la ventaja de facilitar la configuración de un ordenamiento jurídico de protección de datos, que permite una interpretación uniforme y una mayor seguridad jurídica, reduciendo el riesgo de incoherencias. No obstante, la normativa sectorial se adapta mejor a las especificidades y a las necesidades concretas. La complejidad técnica de muchas materias y la propia tendencia a la superproducción normativa en el Estado contemporáneo hacen difícil que una sola norma regule la informática y las tecnologías de la información. Además, la normativa sectorial no siempre ha sido utilizada para excepcionar y limitar las garantías de la legislación general, sino también para intensificar la tutela, como ha hecho la Ley 41/2002, de 14 de noviembre, en relación a los datos de salud. El modelo mixto de norma general y remisión a normas sectoriales ayuda, además, a abreviar las normas generales, que así no tienen la necesidad de reproducir ni derogar la normativa sectorial precedente y que pueden diferir en la regulación sectorial futura aspectos nuevos sobre informática y protección de datos. De hecho, la propia ley general llama a la aprobación de otras leyes cuando justifica como excepción del consentimiento del afectado para el tratamiento de sus datos la existencia de una habilitación legal. Esto lleva a un modelo de coexistencia de ley general y leyes sectoriales, que presenta como principal inconveniente que el sistema jurídico de protección de datos se pueble de reenvíos y de excepciones, que dificultan no sólo la seguridad jurídica, sino su propia lectura, y matizan en parte su unidad jurídica. La adecuación de la normativa de protección de datos a los distintos sectores a través de la interpretación de la normativa general por las Autoridades de Control es una vía aún sin explorar que puede facilitar la adaptación de la normativa a determinados ámbitos sin necesidad de aprobar normas específicas. En todo caso, sí se echa en falta alguna remisión de la LOPD a otras Leyes con las que está conectada materialmente. Así, hubiera sido positiva una mayor coordinación entre la LOPD y la Ley 30/1992, de 26 de noviembre, para evitar incongruencias, por ejemplo, entre el derecho de acceso a los datos personales —art. 15 LOPD—, facultad contenida en el derecho fundamental a la protección de datos personales, y el derecho de acceso de los ciudadanos a los archivos y registros administrativos, previsto en el artículo 105.b) CE y en el artículo 37 LRJAPyPAC; o entre la tutela de la Agencia por denegación de los derechos de acceso, rectificación y cancelación —art. 18 LOPD— y los recursos administrativos ordinarios.

Tanto la LORTAD como la LOPD han establecido un régimen, definido por la doctrina como *represivo* aunque tenga realmente un carácter *permisivo,* que afirma el principio de libertad de tratamientos de datos, estableciendo garantías de los ciudadanos para la protección de sus datos

personales. Frente a las primeras leyes que centraban su atención en el control de la informática como técnica que hay que dominar para evitar abusos, pasando la persona y sus derechos a un segundo plano, las leyes de última generación relegan los aspectos técnicos a unas pautas generales y se orientan hacia el establecimiento de unos principios de protección de datos y unos derechos y garantías del individuo frente a la acumulación de datos personales.

La LORTAD fue la primera norma de desarrollo del artículo 18.4 CE y, por ello, representó un hito en la legislación española sobre tecnologías de la información. El motivo definitivo para su aprobación fue la necesidad de ratificar el Acuerdo de *Schengen*, que establecía la transmisión de información policial entre los países europeos, suprimiendo los controles interiores pero reforzando al mismo tiempo los mecanismos de información sobre sospechosos. Fue una norma intensamente criticada durante su proceso de tramitación, que fue objeto de gran número de enmiendas. La LOPD ha reproducido la mayoría de preceptos de la LORTAD y de la Directiva, incluidos algunos artículos sobre los que habían versado diversos recursos de inconstitucionalidad. Sin embargo, son muchos los defectos de la LOPD. Por una parte, hay que reconocer que ha sido redactada con una técnica legislativa deficiente. Así, no tiene Exposición de Motivos —algo completamente inusual en los textos normativos—, por lo que no conocemos la *voluntas legislatoris*. Además, carece de una sistemática razonable, especialmente en lo relativo a la regulación de los tratamientos realizados por las Administraciones Públicas. No tiene sentido, por ejemplo, la autorización de la cesión de datos sin consentimiento a los comisionados del Parlamento y no a éste. Estas dificultades traen causa de su azarosa tramitación parlamentaria. Lo que inicialmente era un Proyecto de Ley de reforma de algunos preceptos de la LORTAD para adecuarla a la Directiva 95/46/CE, sobre la base de un Anteproyecto elaborado por el Gobierno, en el que había intervenido decisivamente la Agencia Española de Protección de Datos, se transformó en un nuevo texto completo de Proyecto de Ley Orgánica de Protección de Datos Personales, elaborado por la Comisión Constitucional del Congreso de los Diputados, que se sintió con la voluntad y la capacidad de hacer una reforma global de la LORTAD a todas luces innecesaria. Además, la LOPD no ha sido objeto hasta ahora de desarrollo reglamentario, estando todavía vigente la normativa de rango infralegal de desarrollo de la LORTAD. Uno de los retos principales de la Agencia Española de Protección de Datos para el futuro es acometer el desarrollo reglamentario de la LOPD que dé coherencia al sistema, por ejemplo, en lo relativo a las medidas de seguridad de los ficheros manual-estructurados.

El artículo 18.4 CE, tal como se encuentra redactado, representa una cláusula general o una cláusula abierta que ha servido al Tribunal Constitucional para reconocer el derecho fundamental a la protección de datos personales. Las Sentencias que resuelven recursos de amparo han servido al Alto Tribunal para interpretar el derecho fundamental a la protección de datos

personales. A pesar de la escueta mención del artículo 18.4 CE, el Tribunal Constitucional ha afirmado que dentro del contenido esencial de este derecho fundamental se encontrarían el derecho de acceso a la propia información personal, un conjunto de facultades positivas que permiten el control de la propia información, el principio de calidad y la prohibición de que los datos se empleen para una finalidad distinta, la prohibición de cesiones de datos sin consentimiento del interesado y sin habilitación legal, sin perjuicio de las necesarias excepciones en el ámbito público. En el desarrollo de la actividad administrativa y jurisdiccional, las cláusulas generales que reconocen derechos fundamentales, y por tanto la cláusula general del artículo 18.4 CE, que recoge un derecho fundamental a la protección de datos personales, son vínculos positivos que habilitan al Tribunal Constitucional y obligan a la Administración y a los Tribunales ordinarios a aplicar siempre los principios constitucionales y los derechos fundamentales, dando la razón a quien tenga mejor derecho, o, en expresión de DWORKIN, a aquel que tenga derecho a vencer. La Administración, cuando desarrolla una actividad administrativa, está sometida plenamente a la ley y al Derecho; no es libre ni tiene derecho a la arbitrariedad, sino que ha de actuar siempre vinculándose de manera fuerte y buscando la eficacia del derecho fundamental a la protección de datos personales.

En cambio, las cláusulas abiertas —y, entre ellas, el art. 18.4 CE— son para el legislador —y para el gobierno cuando desarrolla su actividad política— marcos de legitimidad —vínculos negativos— dentro de los cuales se puede mover libremente. El hecho de que los derechos fundamentales sean proclamados constitucionalmente a través de cláusulas generales, es decir, el hecho de que el constituyente haya elegido preferentemente valores como la clase de norma apropiada para reconocer derechos fundamentales, es un claro indicio de la delegación de estas materias al legislador; en el caso de los derechos de la Sección I del Capítulo II del Título I, al legislador orgánico. Así, el Tribunal Constitucional y los órganos jurisdiccionales —también la doctrina académica—, a la hora de analizar la legitimidad constitucional de la actividad legislativa que desarrolla el artículo 18.4 CE —tanto la LOPD como la LORTAD—, tienen la obligación de respetar la legítima libertad del legislador y del gobierno, que mantienen una gran capacidad de configuración. Sólo pueden declararse o considerarse inconstitucionales aquellos preceptos legales que salgan fuera del marco del artículo 18.4 CE, marco que está delimitado por el contenido esencial de este derecho, que es un contenido mínimo. Por ello, el método jurídico que se tiene que aplicar para analizar la legitimidad constitucional de los preceptos legales tiene como contenido principal el respeto al principio democrático. Se trata de aplicar un principio de restricción judicial, que significa que sólo se podrán declarar inconstitucionales —o considerar inconstitucionales por la doctrina académica— los preceptos de la LOPD o de la LORTAD que representen supuestos claros de incompatibilidad con la Constitución, recibiendo el poder político el beneficio del *in dubio* en los casos oscuros. La aplicación extensiva de cláu-

sulas generales para afirmar la inconstitucionalidad de estas Leyes podría atentar contra el principio democrático y sería, por tanto, contramayoritaria. El análisis constitucional de la LORTAD o de la LOPD que llevan a cabo la doctrina académica o el Tribunal Constitucional no tiene nada que ver con la valoración de su mayor o menor oportunidad. Es necesario separar la reflexión política sobre la protección de los datos personales del enjuiciamiento constitucional de una actividad política como es la actividad legislativa, evitando así que la interpretación de la Constitución se transforme en una búsqueda de la propia ideología.

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, resolvió el recurso de inconstitucionalidad presentado por el Defensor del Pueblo contra algunos preceptos de la LOPD que reproducían la LORTAD. En ella se señala que los límites a este derecho fundamental a la protección de datos personales tienen que cumplir tres condiciones para que sean constitucionales: en primer lugar, tienen que ser establecidos por ley —arts. 53.1 y 81 CE—; en segundo lugar, estos límites sólo están justificados «si responde[n] a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos», siempre que este límite «sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo»; y, en tercer lugar, estos límites tienen que respetar el contenido esencial del derecho fundamental a la protección de datos personales, que se extiende a un conjunto de garantías.

El Tribunal Constitucional consideró inconstitucional el artículo 21.1 LOPD, que permitía la comunicación de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas «cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso». El argumento principal para considerar inconstitucional este inciso es la vulneración del principio de reserva de ley para limitar derechos fundamentales —art. 53.1 CE—, al considerar que una cesión de datos sin consentimiento es una limitación al derecho fundamental a la protección de datos y este artículo autoriza que se lleve a cabo a través de una norma con rango inferior a la ley.

No obstante, tenemos que afirmar que es la propia LOPD la que establece y da cobertura legal a la comunicación de datos entre Administraciones Públicas para competencias diferentes o que versen sobre materias distintas. No otra cosa es el propio artículo 21.1 LOPD. La habilitación legal del artículo 21.1 LOPD es la misma que otras muchas que para la cesión de datos personales sin consentimiento del interesado aparecen ya mencionadas en el artículo 11.2 LOPD. Da la impresión que el Tribunal Constitucional pretenda ser más exigente con los ficheros públicos que con los ficheros privados. Lo que el artículo 21.1 LOPD hace en el fondo es establecer una excepción más —lógicamente, con la defectuosa sistemática que le caracteriza— al principio general de consentimiento para la comunicación de datos previsto en el artículo 11 LOPD que permita la comunicación de datos entre ficheros

públicos habilitada por la propia norma de creación del fichero o por una norma de superior rango que regule su uso. No se entiende por qué hay que exigir más precisión a la limitación del consentimiento para las cesiones entre Administraciones Públicas del artículo 21.1 LOPD que a otras limitaciones al consentimiento previstas en el artículo 11.2 LOPD. Así, no parece clara la excepción del consentimiento cuando el tratamiento responda a una relación jurídica cuyo desarrollo, cumplimiento y control impliquen necesariamente la conexión de dicho tratamiento con ficheros de terceros —art. 11.2.c)—, ni tampoco están convenientemente reguladas muchas de las fuentes accesibles al público establecidas en el artículo 3.j) LOPD. Además, no se entiende por qué el Tribunal Constitucional prohíbe que la norma de creación de ficheros públicos prevea otros posibles cesionarios o destinatarios de la información, ya que ésta es una posibilidad de cualquier responsable de ficheros, tanto público como privado, que procede a recabar datos de personas.

El artículo 21.1 LOPD contenía una previsión legal para la comunicación de datos entre Administraciones Públicas, que el legislador consideraba necesaria para el funcionamiento de los poderes públicos en una sociedad democrática, dadas las competencias constitucionales de la Administración, dentro de la llamada reserva de Administración —*verwaltungsvorbehalt*—. Era, por tanto, una habilitación legal suficientemente previsible para los ciudadanos en virtud de los bienes constitucionales a los que va encaminada la actividad administrativa. Además, el artículo 21.1 LOPD establecía un importante condicionante a la comunicación de datos entre Administraciones Públicas, si bien de carácter formal, y es que la cesión esté prevista en la norma de creación del fichero o en norma de superior rango que regule su uso, lo que permite su conocimiento y eventual impugnación por los ciudadanos. Así, la habilitación de la cesión de datos personales entre Administraciones Públicas realizada a través de un Real Decreto permitía un conjunto de garantías, tanto en lo que afecta al trámite de información pública como al informe del Consejo de Estado, además de ser elaborada por un órgano superior al que ha creado el fichero. Por último, la comunicación de datos personales establecida por la norma de creación del fichero o por disposición de superior rango siempre podía ser impugnada por las Autoridades de Control y fiscalizada por la jurisdicción contencioso-administrativa teniendo en cuenta el principio de proporcionalidad. Esto no quiere decir que dentro de una valoración de oportunidad y no de un juicio de constitucionalidad se pueda criticar el artículo 21.1 LOPD, ya que el legislador podía haber establecido no sólo una habilitación para la cesión a través de normas reglamentarias, sino también una delimitación más precisa de las circunstancias o las causas que la justifican, en especial la necesidad de facilitar la actividad administrativa en beneficio de otros bienes y derechos constitucionales, pero esto no significa que el artículo 21.1 LOPD sea inconstitucional.

Hay que analizar también si esta excepción al consentimiento del interesado para la cesión de datos entre Administraciones Públicas vulnera el contenido esencial del derecho fundamental a la protección de datos personales.

Pues bien, no parece razonable exigir el consentimiento del ciudadano para la cesión de datos entre Administraciones Públicas cuando este consentimiento tampoco fue necesario para la recogida y el tratamiento de los datos de carácter personal para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias —art. 6.2 LOPD—. Al permitir la cesión de datos entre Administraciones Públicas sin consentimiento, lo único que se evita es que la Administración Pública, también sin consentimiento del interesado, proceda a la recogida y la obtención de los datos personales partiendo de cero, con el consiguiente esfuerzo administrativo. No se puede considerar que es inconstitucional la cesión de datos entre Administraciones Públicas sin consentimiento del interesado y considerar constitucional que las Administraciones Públicas procedan a la recogida y al tratamiento de datos personales sin consentimiento de éste. No se puede exigir una ley expresa para cada cesión de datos entre Administraciones Públicas sin consentimiento y no exigir la misma habilitación legal para el tratamiento de los datos personales por los poderes públicos sin consentimiento. El tratamiento de datos personales sin consentimiento del interesado es el principal elemento que diferencia a los ficheros públicos de los ficheros privados —aunque éstos también tengan esta prerrogativa en algunos tratamientos específicos como los relativos a los ficheros de solvencia patrimonial y de crédito—.

Además, si no se ha demandado al legislador una mayor precisión sobre lo que significa la expresión «funciones administrativas» del artículo 6.2 LOPD, tampoco se le puede exigir una mayor concreción cuando se habilita la cesión de datos entre Administraciones Públicas para competencias diferentes que versen sobre materias distintas porque también se trata de funciones administrativas. Si es constitucional la expresión «funciones administrativas» para el tratamiento sin consentimiento, no puede afirmarse al mismo tiempo que esta expresión utilizada para las cesiones supone una renuncia del legislador a la facultad para establecer los límites a los derechos fundamentales. Lo fundamental aquí es que tanto la recogida de los datos sin consentimiento por una Administración Pública como la cesión a otras Administraciones Públicas se hagan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Es decir, es el ejercicio de funciones administrativas lo que legitima la actividad de tratamiento de datos personales por las Administraciones Públicas. Lógicamente, sólo se puede ceder los datos a otra Administración Pública para el cumplimiento de funciones administrativas. El desarrollo de estas funciones que tratan de garantizar bienes constitucionales en beneficio del interés general —art. 103.1 CE—, y en especial en la actividad de prestación de derechos fundamentales, es lo que justifica determinadas facultades y prerrogativas de las Administraciones Públicas.

La comunicación de datos entre Administraciones Públicas se justifica también por los principios de lealtad y cooperación interadministrativa mencionados en los artículos 3 y 4 de la Ley 30/1992, de 26 de noviembre,

que evita que la Administración receptora «deba pechar con los costes de una nueva recogida y tratamiento de esos datos», a la vez que se ahorra al ciudadano la molestia de someterse a ella. Exigir una habilitación legal para la comunicación de datos entre Administraciones Públicas limita mucho la eficacia administrativa. Téngase en cuenta que el legislador —y el gobierno en los distintos anteproyectos— valora muchos aspectos a la hora de definir el contenido de una ley, pero frecuentemente olvida todo lo relativo a la habilitación para los tratamientos de datos personales. Además, algunas leyes se han aprobado con anterioridad a la LORTAD y a la LOPD y no preveían la necesidad de una autorización legal para la cesión de datos sin consentimiento del interesado entre Administraciones Públicas.

La posibilidad de comunicación de datos entre Administraciones Públicas para funciones administrativas es especialmente importante para la puesta en marcha de proyectos de Administración electrónica, que se basan en la comunicación de datos administrativos. Se trata así de eliminar los certificados físicos aportados por el ciudadano y sustituirlos por el intercambio de certificados telemáticos y transmisiones de datos entre los diferentes registros y ficheros administrativos. Esta posibilidad, además de ser una exigencia de la eficacia y de la propia simplificación administrativa, de una Administración Pública que busca la calidad de los servicios y la satisfacción de los ciudadanos, es una consecuencia del derecho reconocido en la Ley 30/1992, de 26 de noviembre, a todos los ciudadanos de que no les sea exigida ninguna documentación que ya está en poder de la propia Administración Pública. Las finalidades de las distintas bases de datos públicas que se pretenden interconectar son casi siempre distintas, lo que exigiría una habilitación legal que de cobertura al intercambio de datos personales entre las Administraciones Públicas. Una posible solución en este caso es pedirle al ciudadano el consentimiento para recabar sus datos de otras Administraciones Públicas. Es necesario en este ámbito explorar las posibilidades de establecer un sistema de autorizaciones que facilite el control de las autoridades de protección de datos en el intercambio de datos entre Administraciones Públicas. En todo caso, lo principal en este momento es señalar que la Administración electrónica está encaminada a ofrecer servicios administrativos transversales a través de la red.

El consentimiento no forma parte del contenido esencial del derecho fundamental a la protección de datos ni para el tratamiento de datos por las Administraciones Públicas ni para la cesión de datos entre Administraciones, siempre que en ambos supuestos se haga para el cumplimiento de funciones administrativas. La exigencia del consentimiento del interesado para la comunicación de datos entre Administraciones Públicas no se prevé en el artículo 8 del Convenio 108 del Consejo de Europa, que además establece excepciones que han sido interpretadas por el Tribunal de Estrasburgo tratando de tener en cuenta intereses sociales importantes. Igualmente, en virtud del Derecho comunitario es legítima la cesión de datos entre Administraciones Públicas si existe un interés legítimo. Habrá, pues, que valorar

los intereses en presencia, pero no se exige una habilitación legal. Esta reflexión nos lleva a analizar cómo se hizo la transposición de la Directiva 95/46/CE en el Derecho interno español, especialmente en lo que hace referencia al artículo 7. Da la impresión de que el artículo 6 LOPD es correcto, mientras que el artículo 11 LOPD y el artículo 21 LOPD son demasiado restrictivos, sobre todo a partir de esta Sentencia del Tribunal Constitucional que declaró inconstitucional las cesiones de datos entre Administraciones Pública para el ejercicio de competencias diferentes o que versen sobre materias distintas. Además, a mayor abundamiento, recientemente se ha aprobado una Directiva que permite la cesión de datos desde las Administraciones Públicas a los particulares, siempre que se tengan en cuenta los intereses en presencia. Nos estamos refiriendo a la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público. En esta dirección, llama la atención que el *Dictamen del Grupo del artículo 29 sobre protección de datos 7/2003, sobre reutilización de la información del sector público y la protección de datos personales,* haya sido subtitulado «En busca del equilibrio». Lógicamente, si se pueden ceder datos a los particulares, con mayor motivo se podrán ceder entre Administraciones Públicas.

En todo caso, queremos que se nos entienda bien. Nosotros no afirmamos que exigir mayores requisitos para la comunicación de datos entre Administraciones Públicas sea irrazonable. Lo que decimos es que le corresponde al legislador establecer los criterios que justifican estas cesiones. La reserva es una reserva de ley, de Poder Legislativo, no una decisión que pueda ser adoptada por el Tribunal Constitucional. Y mucho menos alegando como fundamento para la declaración de inconstitucionalidad la doctrina del contenido esencial de los derechos fundamentales y la referencia a la noción generalmente admitida por los juristas y en el Derecho comparado de lo que este derecho significa. La normativa europea, tanto el Convenio 108 como la Directiva 95/46/CE, no exigen una habilitación legal para la cesión de datos entre Administraciones Públicas, por lo que no se entiende la integración que hizo el Tribunal Constitucional del artículo 18.4 para poder llegar a afirmar la inconstitucionalidad del artículo 21.1 LOPD. Lo mismo se puede decir de la normativa de los distintos países de la Unión Europea que facilitan la cesión de datos entre Administraciones Públicas sin la exigencia de una habilitación legal.

Hay dos posibles vulneraciones del artículo 21.1 LOPD que no fueron analizadas por el Tribunal Constitucional: la del principio de calidad o del principio de finalidad y la del principio de información como contenidos del derecho fundamental a la protección de datos personales. El principio de calidad prohíbe destinar los datos a una finalidad distinta para la cual han sido recabados, por lo que si se produce una comunicación de datos entre Administraciones Públicas sin consentimiento del interesado para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, lo que se está produciendo es un tratamiento de datos para una finalidad

distinta para la cual estos datos han sido recogidos. Pues bien, el ciudadano podrá no tener que consentir para la comunicación de datos entre Administraciones Públicas para competencias diferentes o que versen sobre materias distintas en virtud de la legitimidad de la actividad administrativa. Tampoco es imprescindible que preste su consentimiento para el tratamiento de datos personales para finalidades distintas por parte del mismo responsable del fichero. No tendría sentido exigir el consentimiento del ciudadano para el tratamiento de sus datos por parte de un mismo responsable para finalidades distintas si tampoco lo prestó para la primera finalidad. Pero lo que no se le puede suprimir es su facultad de estar informado de la cesión, de la entidad cesionaria, de la nueva finalidad del tratamiento, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del tratamiento. Tampoco se le puede suprimir la facultad de estar informado de la existencia de un tratamiento para una finalidad distinta por parte del mismo responsable del fichero. El principio de información es un elemento clave del contenido esencial del derecho fundamental a la protección de datos personales, en virtud de la noción generalmente admitida de lo que este derecho significa, que puede y debe ser respetada en todo caso por las Administraciones Públicas. En esta misma dirección, si la información es un principio básico en la recogida de datos por las Administraciones Públicas, este principio refuerza la importancia del derecho de acceso.

A partir de este planteamiento cobra una gran importancia la declaración de los ficheros y su inscripción en el registro que garantiza la publicidad de los tratamientos. El responsable que ya tenía el fichero público pero que va a tratar los datos personales de los ciudadanos para una finalidad distinta tiene obligación de declarar de nuevo el fichero, a través de una disposición de carácter general y proceder a una modificación en el registro de ficheros. Igualmente debe declarar el nuevo fichero la Administración Pública cesionaria de los datos personales. Nosotros consideramos que la declaración de ficheros en el ámbito público a través de una disposición de carácter general y su inscripción en el registro de ficheros es un trámite esencial, y en absoluto una formalidad burocrática. El responsable público que declara un fichero se conciencia de que los datos no son suyos, sino de los ciudadanos, y se sitúa en mejor disposición para respetar los principios de protección de datos —especialmente el de calidad y el de información en la elaboración del impreso de recogida— y los derechos de acceso, rectificación y cancelación. La experiencia demuestra que un responsable público que no declara los ficheros no respeta ni los principios ni los derechos de protección de datos personales. En todo caso, hay que reconocer que la declaración e inscripción de ficheros no está extendida en la Unión Europea.

De esta forma, se puede afirmar que los requisitos tanto para la cesión de datos entre Administraciones Públicas sin consentimiento del interesado como para el tratamiento de los datos por el mismo responsable del fichero para una finalidad distinta serían: que se produzca para el ejercicio de fun-

ciones propias de las Administraciones Públicas en el ámbito de sus competencias; que se respete siempre el principio de información al titular de los datos tanto por parte del responsable del fichero que procede a un tratamiento distinto como del cesionario de los datos; y que se produzca una nueva declaración del fichero y su inscripción en el registro.

Además, los planteamientos —como el de la Sentencia— restrictivos con la comunicación de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas plantean el problema de qué se entiende por distintas Administraciones Públicas. No parece que tenga sentido afirmar que los distintos Ministerios de la Administración General del Estado, las distintas Consejerías de una misma Comunidad Autónoma y las Concejalías de un mismo Ayuntamiento son distintas Administraciones Públicas cuando todas tienen la misma personalidad jurídica. Un planteamiento que califique como cesión de datos los distintos accesos a un fichero de algún departamento de la misma Administración Pública estaría desincentivando el proceso de descentralización y desconcentración de competencias. Considerar cesión el acceso a un fichero de personal —gestionado por la Dirección General de Recursos Humanos— por otra Dirección General de la misma Comunidad Autónoma competente en materia de calidad de los servicios públicos o de medición del desempeño, lo que está es animando la creación de pocas Direcciones Generales o favoreciendo el establecimiento de ficheros muy centralizados para así evitar la consideración de cesión. Lo mismo cabe decir del acceso a determinados ficheros de naturaleza horizontal por las distintas Consejerías de un mismo gobierno autonómico.

Así, en el caso de que entendiéramos que el acceso a los datos del fichero por parte de departamentos de la misma Administración territorial es un supuesto de comunicación de datos, en virtud de la interpretación del Tribunal Constitucional no sería posible su tratamiento ya que éste se producirá habitualmente para finalidades distintas. La única solución es que existiera una habilitación legal, cosa que no siempre se da. Por tanto, debe entenderse que es legítimo el acceso de los distintos departamentos de una misma Administración territorial a los ficheros que obran en poder de ésta. Inicialmente, este acceso a los datos debería estar limitado por el propio principio de calidad, esto es, por la finalidad del fichero. Este planteamiento restrictivo tendría sentido si la persona hubiera dado su consentimiento para el primer tratamiento, lo que no ocurre dada la excepción a este consentimiento para el tratamiento de datos para funciones administrativas. De nuevo parece razonable que la Administración pueda tratar los datos personales para una finalidad distinta, siempre que garantice el principio de información. No se puede afirmar que habrá que exigir el consentimiento para el nuevo tratamiento al ser la finalidad distinta, cuando tampoco se exigió este consentimiento en el momento de la recogida de los datos —art. 6 LOPD—. Lo que habrá que hacer es, sencillamente, informar al ciudadano, no tratar más que los datos indispensables para esta finalidad, implantar las medidas de seguridad, ga-

rantizar el deber de secreto y, sobre todo, facilitar el ejercicio de los derechos de acceso, rectificación y cancelación. Por ello, el tratamiento de datos dentro de la misma Administración Pública tiene que tener presente el principio de calidad, respetando la finalidad del tratamiento y sólo modificándola después de garantizar el principio de información.

Además, sin negar la vocación transformadora de la propia Constitución, y la necesidad de modificar algunas prácticas administrativas y privadas que no se ajustan a los preceptos constitucionales, no parece que tenga sentido considerar como manifiestamente inconstitucional la cesión de datos entre Administraciones Públicas sin consentimiento del interesado, que ha sido no sólo una práctica habitual en el ámbito público, refrendada, no lo olvidemos, tanto por la LORTAD como por la LOPD, que la autorizaban expresamente, sino también una conducta desarrollada con posterioridad a la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Se trata de no generar esquizofrenias entre lo que se exige a las Administraciones Públicas y lo que éstas hacen en realidad. En este ámbito demostró más sentido común el legislador —no el legislador de una mayoría política, sino el de dos mayorías políticas distintas— que el Tribunal Constitucional.

En todo caso, queremos manifestar abiertamente que no podemos compartir las reflexiones que se hacen habitualmente sobre protección de datos personales y que siempre son contrarias a los tratamientos de datos personales por las Administraciones Públicas. Estos planteamientos dejan entrever un cierto prejuicio anti-Estado —sin tener en cuenta la superación del Estado liberal por el Estado social—, a la vez que se mantiene una mirada complaciente hacia los tratamientos de datos personales llevados a cabo por los sujetos privados. Así, llama la atención que el legislador haya previsto algunas prerrogativas a determinados ficheros privados, tal vez necesarias para el funcionamiento de una economía de mercado y para la estabilidad de los sistemas financieros, como es el tratamiento de datos sin consentimiento del interesado en los ficheros de solvencia patrimonial y de crédito o en los ficheros de seguros, o la propia habilitación de un censo promocional, también sin consentimiento del interesado, sin que esto haya sido estudiado por el Tribunal Constitucional con el mismo nivel de exigencia que han sido analizados los ficheros públicos por la Sentencia 292/2000, de 30 de noviembre.

Esta reflexión se ve corroborada igualmente si se analizan las legislaciones de protección de datos personales de los países de la Unión Europea. Si España tiene una legislación más estricta en general —una buena demostración de que hemos llegado los últimos a legislar sobre esta materia y queremos ser ahora los más rigurosos—, esto se manifiesta especialmente en las cesiones de datos entre Administraciones Públicas, conducta habilitada en otros países de la Unión Europea. La mayoría de las Autoridades de Control de los países de la Unión Europea —a excepción de España y de Portugal— suelen tener un nivel de teorización bastante elevado sobre el derecho fundamental a la protección de datos personales —especialmente la Autoridad

francesa y la italiana—, que no se ve refrendado ni por el contenido de las legislaciones de estos países, ni por las potestades que éstas atribuyen a las Autoridades de Control, ni por la actividad de inspección y sanción, que no llevan a cabo en realidad. En pocos ámbitos se ve tanta incongruencia entre lo que se predica en los foros internacionales y lo que efectivamente se lleva a cabo en los respectivos países. No existe realmente una tutela del derecho fundamental a la protección de datos personales en el ámbito europeo, tal vez porque este derecho no está todavía en sus respectivos textos constitucionales.

Sí compartimos otras consideraciones del Tribunal Constitucional presentes en la Sentencia 292/2000, de 30 de noviembre. A nuestro parecer, la limitación del principio de información cuando impida o dificulte gravemente las funciones de control y verificación de las Administraciones Públicas, o cuando afecte a la persecución de infracciones administrativas —art. 24.1 LOPD—, representa una vulneración del derecho fundamental a la protección de datos personales. Como hemos razonado anteriormente, el principio de información es una garantía esencial del derecho fundamental en el ámbito público, que permite conocer la existencia de tratamientos con nuestros datos personales y facilita el ejercicio del derecho de acceso. Igualmente, el derecho de acceso, rectificación y cancelación es una facultad imprescindible del derecho fundamental a la protección de datos personales, que forma parte de su contenido esencial, sin el cual este derecho no es reconocible como perteneciente a su tipo previo y sin cuyo ejercicio los intereses jurídicos que dan vida a este derecho resultan desprotegidos. Por tanto, suprimir las facultades de acceso, rectificación y cancelación por razones de interés público o ante intereses de terceros más dignos de protección —art. 24.2 LOPD— equivale a vaciar de contenido efectivo este derecho fundamental, imponerle restricciones injustificadas y desproporcionadas que lo hacen impracticable y lo despojan de su necesaria protección.