ESTUDIOS

Protección de datos personales y padrón municipal[1]

Ignacio Villaverde Menéndez
Profesor titular de Derecho Constitucional de la Universidad de Oviedo

1. Padrón y protección de datos.
2. Objeto, contenido y límites del derecho fundamental a la protección de datos y su proyección sobre el padrón municipal.
2.1. El objeto: los datos personales. 2.2. El contenido: el poder jurídico de disposición sobre los datos. 2.3. Los límites del derecho fundamental a la protección de datos. 2.3.1. El marco constitucional. 2.3.2. La concreción legal de los límites al derecho fundamental a la protección de datos personales en relación con el padrón. 2.3.3. La obligatoriedad de los datos del padrón y los límites a los derechos a saber y a consentir. 2.3.4. Los límites a los derechos de rectificación y cancelación.
3. Nota bibliográfica.

1. Este trabajo constituye la primera parte de un opúsculo de mayor extensión de pronta publicación en el que se estudia, además del objeto del presente artículo, la aplicación al padrón municipal de las reglas sobre creación y registro de ficheros informatizados y sus medidas de seguridad, y el régimen jurídico del acceso y la cesión de los datos contenidos en el padrón municipal.

1. Padrón y protección de datos

La disposición adicional segunda de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD), dispone lo que sigue:

"Ficheros y registro de población de las administraciones públicas.

"1. La Administración General del Estado y las administraciones de las comunidades autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

"2. Los ficheros o los registros de población tendrán co-mo finalidad la comunicación de los distintos órganos de cada administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las administraciones públicas."

Esta norma establece, pues, dos reglas: de un lado, autoriza la cesión genérica de los censos de población en posesión del Instituto Nacional de Estadística a las administraciones estatal y autonómica sin consentimiento del interesado; de otro lado, impone un fin, tanto a la cesión como al uso de los censos de población. En el primer caso, la cesión universal lo será de los datos de los habitantes de los territorios en los que la administración cesionaria, esto es, la que solicita la cesión, ejerce sus competencias. En el segundo de los casos, y repárese en que es una regla general, el uso de los datos de los censos de población, tanto por quien los posee y gestiona (ayuntamientos e INE), como por las administraciones cesionarias, sólo puede emplearse con el fin de facilitar la comunicación de los distintos órganos de las diferentes administraciones afectadas con los residentes en el territorio en el que ejercen sus competencias y respecto de las relaciones jurídicas que medien entre dichas administraciones y los administrados.

Son varias las conclusiones que ya se pueden extraer de esta disposición adicional. En primer lugar, cualquier administración pública no puede crear censos de población. Estos censos sólo pueden crearlos los ayuntamientos, mediante la confección de los padrones municipales (artículo 17 de la Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local (en adelante, LBRL) y artículo 60 del Reglamento de población y demarcación territorial de las entidades locales, aprobado por el Real decreto 1690/1986, de 11 de julio –en adelante, RPT–), y el INE (con arreglo a lo que establece la Ley 12/1989, de 9 de mayo de 1989, de la función estadística pública –en adelante, LFEP–, para el censo de población del Estado; dejando a un lado el censo electoral y los cometidos de la Oficina del Censo Electoral, integrada en el INE, según lo dispuesto en la Ley orgánica 5/1985, de 19 de junio, del régimen electoral general –en adelante, LOREG– en su sección III, capítulos III y IV).[2] En segundo lugar, las administraciones incompetentes para crear sus propios censos de población tienen la potestad de ser cesionarias del censo de población o del padrón correspondientes al territorio en el que, para el ejercicio de sus competencias, requieren el conocimiento de sus residentes, y a los solos efectos, pues así lo dispone el apartado 2 de esta disposición adicional, de la comunicación de dichas administraciones (parece que incluidas las cedentes también) con los administrados en las relaciones jurídicas que medien entre ambos. En tercer lugar, la cesión de datos universal prevista en el apartado primero es una excepción a la regla general sobre la cesión consentida de datos del artículo 11.1 de la LOPD, que debe sumarse a las previstas ya en el apartado segundo de este mismo precepto. En cuarto lugar, sólo se cederán los datos relativos al nombre, los apellidos, el domicilio, el sexo y la fecha de nacimiento. Y en quinto y último lugar, esa cesión sólo podrá realizarla el INE.

Así pues, los ayuntamientos sólo podrán hacer uso del padrón, con arreglo a lo dispuesto en la LOPD, para comunicarse con sus vecinos "respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas de las administraciones públicas"; y, en principio, la LOPD no lo prevé como autoridad cedente de los datos de los vecinos de su demarcación territorial a otras administraciones, ya que esa cesión está encomendada al INE.

Este es el punto de arranque de la relación entre padrón municipal y protección de datos personales. Lo cierto es que la LOPD nada dice sobre esta institución. Sin embargo, de ello no cabe deducir que el padrón no está sujeto al régimen jurídico de protección de datos. Y ello por dos razones. En primer lugar, después de la Sentencia del Tribunal Constitucional (en adelante, STC) 292/2000, en el ordenamiento jurídico español la protección de datos personales es un nuevo derecho fundamental ubicado en el artículo 18.4 de la Constitución española de 1978 (en adelante, CE). Por tanto, no se trata tan sólo de un derecho legal creado al tiempo que se cumplía con la reserva de ley establecida en ese precepto constitucional. Se trata, en cambio, de un verdadero derecho fundamental, con su propio objeto y contenido constitucional, y con el rango y la eficacia de

2. Recuérdese además la STC 154/1988, por la que se niega a las comunidades autónomas la competencia para crear sus propios censos electorales.

cualquier otro derecho fundamental de la Constitución española. Como tal se irradia a todo el ordenamiento jurídico, y lo hace, desde luego, sobre el padrón municipal. En segundo lugar, el padrón municipal también está sujeto a lo dispuesto en la LOPD. Cuando el artículo 2 de la LOPD define el ámbito de aplicación de esta ley orgánica, que lo es de desarrollo del derecho fundamental a la protección de datos personales (artículo 18.4 de la CE), en ninguno de sus apartados excluye el padrón municipal.[3]

En efecto, los apartados a) y b) del artículo 2.3 de la LOPD, en el cual se establece qué tratamientos de datos están sujetos a su propia normativa, contemplan los ficheros regulados por la legislación de régimen electoral y los que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. El primero es el censo electoral, regulado en el capítulo IV de la LOREG, y el segundo son los distintos y posibles *censos de población* sujetos a la LFEP o a las leyes autonómicas correspondientes.[4] Ninguno de ellos es el padrón municipal. El padrón es un censo de población peculiar y específico sujeto a lo dispuesto en la LBRL y en el RPT, confeccionado y gestionado exclusivamente por los ayuntamientos, sin perjuicio de que sus datos sean la fuente para la confección de los censos de población del Instituto Nacional de Estadística y para la elaboración del censo electoral. Pero se trata de un censo de población distinto de aquéllos, como se desprende en particular del artículo 44 de la LFEP, del artículo 17 de la LBRL o del propio artículo 60 del RPT.

Por otro lado, de la circunstancia de que el artículo 16 de la LBRL y el artículo 53.1 del RPT lo definan como el registro administrativo en que constan los vecinos del municipio, no es un obstáculo para la plena sujeción del padrón a la LOPD. Ciertamente, el padrón es un registro administrativo, sometido por tanto a lo dispuesto en el artículo 105.b) de la CE, que remite a la ley la regulación del acceso a los archivos y a los registros administrativos. Pero es un registro peculiar en el sentido de que está compuesto únicamente por los datos personales de quienes sean vecinos de ese municipio (artículo 16 de la LBRL y 57 del RPT), y su gestión debe ser informática (artículo 17 de la LBRL y 60 del RPT).[5] Así pues, el padrón no es sino un "conjunto organizado de datos de carácter personal" [artículo 3.b) de la LOPD], que en cuanto tal, con arreglo a lo dispuesto en el artículo 2.1 de la LOPD,[6] está sujeto a las normas sobre protección de datos personales establecidas en ella y demás legislación concordante, en particular el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981[7] (en adelante, el Convenio), la Direc-

3. Artículo 2.2 de la LOPD: "El régimen de protección de los datos de carácter personal que se establece en la presente ley orgánica no será de aplicación: *a*) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. *b*) A los ficheros sometidos a la normativa sobre protección de materias clasificadas. *c*) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos. 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."

4. En la actualidad, poseen legislación estadística: Andalucía, Ley 4/1989, de 12 de diciembre, de estadística de la Comunidad Autónoma de Andalucía; Aragón, Decreto 208/1993, de 7 de diciembre, de la Diputación General de Aragón, por el que se crea el Instituto Aragonés de Estadística y se regula su funcionamiento; Canarias, Decreto 208/1993, de 7 de diciembre; Cantabria, Ley 3/1990, de 21 de marzo, de estadística de Cantabria; Castilla y León, Ley 7/2000, de 11 de julio, de estadística de Castilla y León; Castilla-La Mancha, Ley 10/2002, de 21 de junio, de estadística de Castilla-La Mancha; Cataluña, Ley 23/1998, de 30 de diciembre, de estadística de Cataluña; Comunidad Valenciana, Ley 5/1990, de 7 de junio, de estadística de la Comunidad Valenciana; Galicia, Ley 9/1988, de 19 de julio, de estadística de Galicia; Baleares, Ley 3/2002 de 17 de mayo, de estadística de las Islas Baleares; Madrid, Ley 12/1995, de 21 de abril, de estadística de la Comunidad de Madrid; Murcia, Ley 6/ 2002, de 25 de junio, de estadística de la Región de Murcia; Navarra, Ley foral 11/1997, de 27 de junio, de estadística de Navarra; País Vasco, Ley 4/1986, de 23 de abril, de estadística de la Comunidad Autónoma de Euskadi.

5. Incluso la comunicación interadministrativa de datos del padrón o relevantes para el mismo debe hacerse, siempre que sea posible, por medios informáticos o telemáticos "respetando las instrucciones normalizadoras sobre tratamiento de la información que se dicten al efecto", como dispone el artículo 64.1 del RPT. No obstante, la cuestión relativa a si el padrón es o no un fichero informatizado es irrelevante, salvo a los efectos del plazo para su registro en la Agencia de Protección de Datos con arreglo a la disposición adicional primera LOPD, ya que esta misma LOPD se aplica indistintamente a cualquier tipo de fichero de datos personales sea cual sea su modalidad de tratamiento, informático o manual [artículo 2.1, en relación con el artículo 3.b) de la LOPD].

6. "La presente ley orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Se regirá por la presente ley orgánica todo tratamiento de datos de carácter personal: *a*) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento."

7. Dicho Convenio estuvo precedido de varias resoluciones del Comité de Ministros del Consejo de Europa (las número 73/22, 74/29 y 80/13) y dio lugar a una larga serie de recomendaciones (las número 81/1, 83/10, 85/20, 86/1, 87/15, etc.), de las que deben destacarse ahora la Resolución 74/29, sobre bancos de datos electrónicos en el sector público, y las recomendaciones 80/13, sobre intercambio de informaciones jurídicas, 83/10, sobre datos con fines de investigación científica y de estadísticas, 86/1, sobre datos con fines de seguridad social, 87/15, respecto de los empleados en el sector de la policía, 89/2, sobre los datos con fines de empleo –también en el sector público–. Téngase en cuenta también las directrices aprobadas por el Consejo de la OCDE el 23 de septiembre de 1980 sobre protección de la vida privada y los flujos transfronterizos de datos de carácter personal y el instrumento de ratificación (BOE de 5 de abril de 1994) del Acuerdo de adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de

tiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, la Directiva).[8] Textos a los que debe unirse la Recomendación 81/679/CEE, y más recientemente el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, que recoge expresamente en su elenco el derecho a la protección de datos personales. Por último, la LOPD ha dejado subsistente, en cuanto no se opongan a la presente ley (disposición transitoria tercera), los tres reglamentos que desarrollaron la derogada Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal: los reales decretos 428/1993, de 26 de marzo, por el que se regula el estatuto de la Agencia de Protección de Datos, el 1332/1994, de 20 de junio, que desarrolla en diversos aspectos la LORTAD, el 994/1999, de 11 de junio, que regula las medidas de seguridad de las bases de datos, y el 195/2000, de 11 de febrero, por el que se establece el plazo para implantar dichas medidas de seguridad.

Que esto sea así, como se verá, tiene gran importancia para determinar, por ejemplo, cuál es la ley, a la que remite el artículo 105.b) de la CE, que regula el acceso a este "registro" de vecinos del municipio y, en consecuencia, cuál haya de ser el régimen jurídico del acceso a la información contenida en ese registro y sus límites; o la adopción de las medidas de seguridad para los ficheros de datos personales impuestas por la LOPD (artículo 9) y precisadas en el Reglamento 994/1999, de 11 de junio; o en lo relativo a la identificación del responsable y del encargado de ese fichero [artículo 3.d) y g)].

En suma, el padrón es, al tiempo que un registro administrativo de vecinos, un fichero informatizado ("automatizado" en la terminología de la LOPD) de sus datos personales, cuyo régimen jurídico, además del establecido en la LBRL, que lo crea y lo regula, y el RPT, que desarrolla lo dispuesto en la LBRL, es el previsto en la LOPD en lo relativo a la protección de los datos personales de los vecinos en él contenidos.

Ahora bien, el régimen jurídico de la protección de datos no sólo se limita a lo dispuesto en la LOPD, la normativa convencional y los Reglamentos de desarrollo aludidos. Antes de nada es una cuestión constitucional.

Tras la STC 292/2000, el ordenamiento jurídico español posee un nuevo derecho fundamental a la protección de los datos personales, garantizado en el artículo 18.4 de la CE. Este derecho fundamental posee un objeto, contenido y límites definidos con toda claridad en la mencionada sentencia que no ha dejado lugar a dudas ni sobre el rango de este nuevo derecho ni sobre su contenido esencial ni sobre su eficacia directa. Por tanto, e incluso con independencia de que el régimen legal de la protección de datos se extienda o no al padrón municipal, es asunto indubitado que el padrón está sujeto, naturalmente, al contenido constitucionalmente declarado del derecho fundamental a la protección de datos. Por ello, su régimen jurídico-constitucional, al margen de lo que disponga la LBRL, el RPT o la propia LOPD, está definido ya en el artículo 18.4 de la CE, cuyo contenido pasamos a exponer a continuación y que debe ser escrupulosamente respetado tanto por las normas que regulan el padrón como por su gestión administrativa, so pena de vulnerar el artículo 18.4 de la CE.

2. Objeto, contenido y límites del derecho fundamental a la protección de datos y su proyección sobre el padrón municipal

Ha sido el Tribunal Constitucional quien ha considerado que en el apartado 4 del artículo 18 de la CE se garantizaba un nuevo derecho fundamental: el derecho fundamental a la protección de los datos personales.[9] El pro-

1985, capítulo III, "Protección de datos de carácter personal y seguridad de los datos en el marco del Sistema de Información de Schengen".

8. Deben tenerse presentes las directivas 96/9 de la CE, sobre protección jurídica de las bases de datos, que ha sido traspuesta por la Ley 5/1998, de 6 de marzo, de incorporación al derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos, y la 97/66/CE sobre procesamiento de datos personales y la protección de la vida privada en el sector de las telecomunicaciones. Téngase en cuenta también las resoluciones de 8 de mayo de 1979 (y la recomendación aneja) y de 9 de marzo de 1982 del Parlamento Europeo sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática.

9. Así lo ha hecho en la capital Sentencia 292/2000 (y en su antecedente más inmediato, la STC 290/2000), de inexcusable lectura y estudio, que estimó el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la LOPD (deben citarse también las STC 110/1984, 254/1993, 143/1994, 11/1998, 94/1998, 144/1999 y 202/1999). Dicha sentencia define con una claridad y firmeza inusuales en la jurisprudencia del Tribunal Constitucional su contenido, su objeto y sus límites. Dice esta STC 292/2000, fundamento jurídico 6: "Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, 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 (artículo 18.1 de la CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico. [...] Ahora bien, con la inclusión del vigente artículo 18.4 de la CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía 'como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona', pero que es también, 'en sí mismo, un derecho o libertad fundamental' (STC 254/1993, de 20 de julio, FJ 6). 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 de la 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

pósito de la protección de datos es la garantía del pleno dominio del individuo sobre su identidad personal. Ni se trata de proteger su intimidad, para lo cual ya existe el artículo 18.1 de la CE, que garantiza el derecho a tenerla (STC 134/1999), ni el honor, cuyo amparo debe buscarse también en el artículo 18.1 de la CE. La función del derecho a la protección de datos personales, parafraseando lo dicho por la STC 292/2000, es la de garantizar a la persona (nacional o extranjera, ya que se trata, sin duda, de un derecho ligado a la dignidad personal –STC 115/1987 y 99/1985–), un poder de control sobre sus datos personales, sobre su uso y su destino, con el propósito de impedir su tráfico ilícito y lesivo para su dignidad y sus derechos, así como para oponerse a cualquier reconstrucción, conocida o no, de su identidad, su comportamiento o su ideología y su opinión a partir de sus datos personales por quien los posea.

El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos, e 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 la divulgación indebidos de dicha información (STC 144/1999 y 292/2000). El derecho a la protección de datos consiste, pues, en un poder sobre el uso del dato revelado, poniendo a disposición del afectado la facultad de controlar ese uso y el destino del dato que revela a un tercero con el fin de atajar el uso fraudulento o el tráfico ilegal de sus datos personales, e incluso cualquier evaluación de su persona que se haga a partir de ellos si la obtención, el almacenamiento y el tratamiento de esos datos se ha hecho sin su conocimiento y su consentimiento (STC 292/2000, artículo 13 de la LOPD).[10]

2.1. El objeto: los datos personales

El objeto del derecho fundamental a la protección de los datos personales es la información relativa a una persona que permita su identificación. En palabras de la LOPD [artículo 3.a)], "cualquier información concerniente a personas físicas identificadas o identificables" (véase también el artículo 1.4 del Real decreto 1332/1994, de 20 de junio).[11] Estos datos no tienen por qué ser "íntimos", ni siquiera ser informaciones relativas a su vida privada personal o familiar. El objeto del derecho fundamental son las informaciones que permitan la identificación de la persona, no que esa información sea relativa a aspectos de su vida más o menos confidenciales. No debe confundirse el objeto del derecho con su función en el marco de un sistema democrático. No cabe duda de que lo pretendido con la protección de datos es una más eficaz garantía de la vida íntima y privada de la persona. Pero también se persigue con la protección del buen uso de la información relativa a su persona el aseguramiento del "pleno ejercicio de sus derechos" (palabras del artículo 18.4 de la CE), no sólo de los relativos a su intimidad y su honor (que también enumera el aludido apartado 4 del artículo 18 de la CE); ni tan siquiera es necesario que esos derechos, cuyo pleno ejercicio también se persigue con la protección de datos, sean de rango constitucional.

"De ahí la singularidad del derecho a la protección de datos –dice el TC en su Sentencia 292/2000–, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, pues 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 de la CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el artículo 18.4 de la CE, e igualmente, en expresión bien amplia del propio artículo 18.4 de la 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 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." (STC 292/2000, fundamento jurídico 6)

Conviene reparar también en que, a nuestro juicio, la diferencia decisiva entre el derecho a la intimidad (artí-

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. De manera que el constituyente quiso garantizar mediante el actual artículo 18.4 de la 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."

10. Artículo 13. Impugnación de valoraciones. 1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. 2. El afectado podrá impugnar los actos administrativos o las decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. 3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. 4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

11. "Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable."

culo 18.1 de la CE) y el derecho fundamental a la protección de datos personales (artículo 18.4 de la CE), radica en que el primero protege la *confidencialidad* de la información relativa a una persona, mientras que el segundo garantiza el buen uso de la información relativa a una persona una vez ésta se ha revelado a un tercero.

El derecho a la intimidad presupone la falta de publicidad (de accesibilidad general) de la información personal, y pone a disposición del individuo el poder jurídico de imponer a terceros el deber de no revelar información relativa a su persona sin su autorización o de no obligarlo a que revele él mismo esa información en contra de su voluntad. Sin embargo, el derecho fundamental a la protección de datos garantiza a la persona el control jurídico sobre el uso y la circulación de la información personal que haya revelado a un tercero, sea éste un particular o sea el Estado. La información ya no es *íntima* porque ya ha sido revelada. Pero ese dato ya divulgado a un tercero no es por ello público (de acceso general), ni puede, por ello, circular libremente. El derecho fundamental a la protección de datos proporciona precisamente al interesado el poder jurídico de controlar en todo momento el uso y la circulación de sus datos una vez los haya revelado.[12] Por esta razón, el derecho fundamental a la protección de datos personales no es, en rigor, un derecho al secreto o a la confidencialidad de los datos (aunque uno de los posibles efectos que tenga su ejercicio es restringir al máximo el alcance de la publicidad actual o potencial del dato personal revelado), sino al control sobre su publicidad.[13]

Dice, en este sentido, la STC 292/2000 a continuación del párrafo antes transcrito:

"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 de la CE otorga, 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."

No cabe la menor duda sobre el carácter de "datos personales" de aquellos datos que obligatoria, o también voluntariamente, deben constar en el padrón municipal. Con arreglo a los artículos 16 de la LBRL y 57 del RPT, dichos datos son: nombre y apellidos, sexo, domicilio, nacionalidad, fecha de nacimiento, documento nacional de identidad (o similar de tratarse de un extranjero), certificado o título escolar o académico, y otros datos necesarios para la elaboración del censo electoral (artículo 32.2 de la LOREG).

Este apartado no puede concluirse sin detenerse en la "calidad de los datos personales". Es una expresión con la que se ha querido hacer referencia a los principios generales del tratamiento (automatizado o no) de los datos personales. Con arreglo al artículo 4 de la LOPD:

"Calidad de los datos.

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

"2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

"3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

12. De ahí que el régimen sobre la recogida de datos personales, siempre que no se destinen a un tratamiento, automatizado o no, posterior (no ya sobre su almacenamiento, artículos 4.7 y 5 de la LOPD), y sobre la obligatoriedad de la revelación por el afectado de cierta información relativa a su persona (caso por ejemplo de los datos del padrón enumerados en los artículos 16 LBRL y 57 RPT) sean más bien cuestiones encuadrables en el derecho fundamental a la intimidad (artículo 18.1 de la CE) que en el derecho fundamental a la protección de datos (artículo 18.4). En la fase de recogida de datos personales lo que se limita es el poder jurídico de la persona sobre la privacidad de informaciones relativas a ella, ya que con la recogida de datos lo que se hace, de forma obligatoria o voluntaria, es revelar información privada de la persona. A partir de ese momento, a partir de la revelación a terceros de esos datos, el poder jurídico de la persona se proyecta sobre el almacenamiento, el uso y la circulación de los mismos (un poder de control sobre el alcance de su publicidad).

13. Piénsese en un fichero sobre personas infectadas del VIH. Claro que el dato sobre la infección es una información íntima amparada por el derecho a la intimidad, y por el hecho de que esa información quede almacenada en una base de datos no pierde su condición de íntima. Lo que sucede es que, una vez se accede a que ese dato ingrese en un fichero, el derecho que garantiza que esa información siga siendo una información reservada, de uso restringido y no susceptible de cesiones a terceros, es el derecho fundamental a la protección de datos y no el derecho a la intimidad. Otra cosa es que su condición de dato *sensible* (íntimo, en definitiva) además imponga (y justifique por proporcionado ese deber) que su almacenamiento y tratamiento se sujeten a estrictas medidas de seguridad y a procesos de disociación y encriptamiento dirigidos a salvaguardar la debida reserva (es decir, la publicidad restringida) de dicha información.

"4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

"5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines sobre la base de los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

"6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

"7. Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos."

Estos son los principios básicos de necesaria observancia también en el caso del padrón municipal. No sólo la LBRL y el RPT adolecen de norma contraria a estos principios (que de existir pesarían sobre ella serias dudas sobre su constitucionalidad, ya que dichos principios son expresión de los principios constitucionales de "adecuación y proporcionalidad" que rigen la protección de datos, y por ello es también posible tenerla por derogada tras la aprobación de la LOPD), sino que la "calidad de los datos" contenidos en el padrón son objeto de especial atención en el artículo 62 (deber de mantener actualizado el padrón),[14] artículo 66 (correcciones debidas a discrepancias puestas de manifiesto por el INE y la OCE a los ayuntamientos), artículo 69 (deber general de actualización del padrón), artículos 71 y 72 (baja de oficio en caso de duplicidad de empadronamientos o de inscripciones indebidas) y artículo 73 (altas de oficio en el padrón), todos del RPT. Todas ellas son reglas que persiguen que el padrón municipal cumpla con la exigencia contenida en el artículo 17.2 de la LBRL, cual es que el padrón debe contener sus datos actualizados "de modo [...] que los datos [...] concuerden con la realidad".

Un deber relativo a la "calidad de los datos" que pesa sobre los ayuntamientos (artículo 60.1 del RPT, en relación con el artículo 17.1 de la LBRL), y no sobre el vecino. Éste tiene la obligación, ciertamente, de comunicar a los ayuntamientos las variaciones que hayan podido producirse en sus datos relevantes para el padrón (artículo 68 del RPT). Sin embargo, existe una capital diferencia entre ambos deberes. Mientras que el que pesa sobre el ayuntamiento tiene su inmediato fundamento en los principios de calidad de datos exigidos en la LOPD y ligados al contenido esencial del derecho fundamental a la protección de datos personales por cuanto constituyen un instrumento indispensable para el efectivo disfrute de este derecho, el deber que pesa sobre los vecinos es de mera naturaleza reglamentaria (ni siquiera legal), y su fin es el de asegurar una información actual sobre los datos de los vecinos que permitan al consistorio llevar a cabo las actuaciones oportunas dentro de las relaciones jurídicas que mantengan con aquéllos.

2.2. El contenido: el poder jurídico de disposición sobre los datos

El contenido del derecho fundamental a la protección de datos es igualmente peculiar respecto del derecho a la intimidad, dada su naturaleza prestacional. Ese poder jurídico de control sobre los datos personales se concreta en las siguientes facultades: el derecho a estar informado y consentir la recogida, el almacenamiento, el tratamiento y el uso de los datos personales, incluida su cesión a terceros, pudiendo oponerse a la recogida, el tratamiento, el almacenamiento, el uso y la cesión de sus datos personales, y los derechos de acceso a dichos datos, a su rectificación y, en su caso, a su cancelación. Todo este haz de facultades constituye, con arreglo a lo declarado en la STC 292/2000, el contenido esencial del derecho fundamental a la protección de datos.

La STC 292/2000, fundamento jurídico 7, no pudo ser más clara:

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

14. So pena de que el INE proceda a la ejecución sustitutoria del artículo 60 LBRL de no proceder el ayuntamiento al cumplimiento puntual de sus obligaciones (artículo 62.2 del RPT).

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

"En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y el 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 ese 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."

La STC 292/2000 estimó que este haz de facultades constituía el contenido esencial de este derecho fundamental, y, por consiguiente, un contenido indisponible incluso al legislador orgánico. Así las cosas, el escrupuloso respeto por el Estado, y también, claro está por los entes locales, de ese contenido supone que el mismo debe ser respetado y observado en todo momento por la Administración estatal, autonómica o local al margen de lo que pueda disponer la normativa con rango legal que regule, en lo que ahora interesa, el padrón municipal. Ninguno de aquellos derechos a consentir, saber y estar informado, a acceder, rectificar y cancelar, requieren de ningún desarrollo o concreción legal, siendo de aplicación directa e invocables por la persona al margen de lo que sobre el particular puedan disponer la LBRL, el RPT o la LOPD. Y lo que es aún más importante, las normas sobre el padrón o las que puedan aplicarse al padrón contenidas en cualquiera de los textos legales y reglamentarios citados deben interpretarse y aplicarse siempre y en todo caso de modo constitucionalmente conforme al derecho fundamental a la protección de datos personales y a su haz de facultades individuales que constituyen su contenido esencial.

STC 292/2000, fundamento jurídico 10:

"Por tanto, las facultades legalmente atribuidas a los sujetos concernidos y las consiguientes posibilidades de actuación de éstos son necesarias para el reconocimiento y la identidad constitucionales del derecho fundamental a la protección de datos. Asimismo, esas facultades o posibilidades de actuación son absolutamente necesarias para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos. De manera que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ 8), 'se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección'."

Los artículos 69.3 (derecho de información de los vecinos), 71 (duplicidades en el padrón) y 72 (inscripciones indebidas), y el capítulo IV (artículo 81 y siguientes, revisión del padrón), deben completarse necesariamente con el haz de facultades antes enumerado. Todo vecino tiene el derecho constitucional, y sólo limitable en los términos que veremos a continuación, a ser informado sobre los datos que de su persona consten en el padrón, sobre su uso y su destino, y las cesiones que hayan podido llevarse a cabo; a consentir la recogida, el almacenamiento, el uso y las cesiones de sus datos; a acceder a los mismos e instar a su rectificación y, en su caso, su cancelación.

Estos derechos han sido desarrollados por la LOPD y por el Real decreto 1332/1994, de 20 de junio. Así, en el artículo 5 de la LOPD[15] se regula el derecho de información, y exige la puntual información al afectado de la

15. Artículo 5. Derecho de información en la recogida de datos. 1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: *a*) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. *b*) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. *c*) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. *d*) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. *e*) De la identidad y la dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. 3. No será necesaria la información a que se refieren las letras *b*), *c*) y *d*) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. 4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras *a*), *d*) y *e*) del apartado 1 del presente artículo. 5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes

existencia de un fichero o un tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad y la dirección del responsable del tratamiento o, en su caso, de su representante. El artículo 6 de la LOPD[16] establece el régimen del consentimiento a que los datos sean tratados, previendo la posibilidad de que el afectado pueda oponerse de manera fundada al tratamiento de sus datos sin perjuicio de que éstos hayan podido ser tratados sin su consentimiento (artículo 6.4 de la LOPD), y en el artículo 11 de la LOPD[17] regula el consentimiento a su cesión (véase también el artículo 21 de la LOPD). El título III de la LOPD norma los "derechos de las personas", desarrollando el derecho de acceso (artículo 15 de la LOPD)[18] y los derechos de rectificación y cancelación (artículo 16 de la LOPD).[19] Todos ellos son derechos que cualquier vecino puede ejercitar frente al responsable del padrón municipal.[20] Y así lo declara expresamente el artículo 53.3 del RPT en lo relativo a los derechos de acceso, rectificación y cancelación de los vecinos respecto de sus datos contenidos en el padrón municipal (con una remisión a la Ley 5/1992, de 29 de octubre, que en la actualidad debe entenderse hecha en los artículos 15 y 16 de la LOPD).

Téngase en cuenta que el artículo 69.2 del RPT regula la debida notificación al correspondiente vecino de

accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

16. Artículo 6. Consentimiento del afectado. 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

17. Artículo 11. Comunicación de datos. 1. Los 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. 2. El consentimiento exigido en el apartado anterior no será preciso: *a*) Cuando la cesión está autorizada en una ley. *b*) Cuando se trate de datos recogidos de fuentes accesibles al público. *c*) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. *d*) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el ministerio fiscal o los jueces o tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. *e*) Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. *f*) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. 4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable. 5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente ley. 6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

18. Artículo 15. Derecho de acceso. 1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. 2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

19. Artículo 16. Derecho de rectificación y cancelación. 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o la cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o la entidad responsable del tratamiento y el interesado.

20. Asimismo, el Convenio señala en el § 50 de su introducción respecto de su artículo 8 que son elementos esenciales de las garantías que el Convenio pretende otorgar a los individuos el conocimiento sobre la existencia de un fichero automatizado, la información que ese fichero contenga, la rectificación de esa información y el derecho al recurso de no ser respetado alguno de estos elementos. La directiva, por su parte, establece en su preámbulo que "(38) [...] el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención". Y añade "(41) [...] que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan,

aquellas variaciones que se produzcan respecto de los datos que de su persona consten en el padrón municipal con ocasión de la actualización del mismo. Pero no sólo el RPT impone al ayuntamiento ese deber de información al vecino "siempre que se produzcan actualizaciones", con el objeto de facilitar al vecino el ejercicio de los derechos de rectificación y cancelación (artículo 69.2 del RPT). El apartado 3 del artículo 69 del RPT establece también un deber genérico de información a cargo de los ayuntamientos. Según este precepto, al menos cada cinco años, el ayuntamiento deberá notificar a cada vecino el contenido de sus datos en el padrón "de manera que todo vecino tenga la oportunidad de conocer la información que le concierne" al menos una vez en ese período de tiempo.

Dicho esto, y una vez conocido el marco constitucional de la protección de datos personales, al que está sujeto, desde luego, el padrón municipal, conviene también reparar en la advertencia hecha por el Tribunal Constitucional en la tantas veces citada STC 292/2000 (fundamento jurídico 10):

"Tanto en la STC 254/1993 con carácter general como en la STC 143/1994, de 9 de mayo, FJ 7, este Tribunal ha declarado que un régimen normativo que autorizase la recogida de datos personales, incluso con fines legítimos, vulneraría el derecho a la intimidad si no incluyese garantías adecuadas frente al uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento informático, al igual que lo harían las intromisiones directas en el contenido nuclear de ésta."

Donde se dice "derecho a la intimidad" en el párrafo transcrito, debe leerse derecho a la protección de datos personales. No basta con que el régimen legal de la protección de datos observe estrictamente las condiciones constitucionales de la protección de datos. También puede lesionarse el derecho fundamental si el régimen legal de recogida, almacenamiento, uso y cesión de datos personales no establece las garantías indispensables que permitan al individuo hacer un efectivo ejercicio del haz de facultades que le atribuye la CE, que son contenido esencial de su derecho fundamental a la protección de datos y, por tanto, indisponibles a cualquier poder público, incluido el legislador mismo.

En este sentido, además de las medidas de seguridad que deben adoptar todos los ficheros de datos personales (artículo 9 de la LOPD)[21] y el deber de secreto (artículo 10 de la LOPD),[22] la propia LOPD establece mecanismos complementarios de garantía de la efectividad de aquellos derechos, y que también deben adoptarse con respecto al padrón municipal. A saber: el artículo 17[23] remite al reglamento la regulación de los procedimientos de oposición, acceso, rectificación o cancelación, lo que ha hecho el Real decreto 1332/1994, de 20 de junio, que establece la forma de proceder en esos casos en su capítulo IV (artículo 11 y siguientes); y los artículos 18 y 19 de la LOPD, que prevén la posibilidad de denunciar ante la Agencia de Protección de Datos las actuaciones contrarias al derecho a la protección de datos personales y las indebidas denegaciones totales o parciales del ejercicio de cualquiera de los derechos aludidos,[24] y la posibilidad de obtener

al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informático; que no obstante esto no debe suponer que se deniegue cualquier información al interesado". Su artículo 12 dispone: "Derecho de acceso. Los estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: *a*) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; *b*) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente directiva, en particular a causa del carácter incompleto o inexacto de los datos; *c*) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra *b*), si no resulta imposible o supone un esfuerzo desproporcionado."

21. Artículo 9. Seguridad de los datos. 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta ley (Real decreto 994/1999, de 11 de junio).

22. Artículo 10. Deber de secreto. El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

23. Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación. 1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente. 2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

24. Artículo 18. Tutela de los derechos. 1. Las actuaciones contrarias a lo dispuesto en la presente ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada comunidad autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

una indemnización por los daños sufridos,[25] respectivamente.

2.3. Los límites del derecho fundamental a la protección de datos

2.3.1. El marco constitucional

Lo dicho antes sobre el contenido esencial del derecho fundamental a la protección de datos personales es especialmente relevante para la fijación de los límites posibles a aquellas facultades que constituyen el contenido esencial del derecho fundamental. Límites que también deben tenerse en cuenta en el caso del padrón municipal. La falta de una regulación precisa en la LBRL y el RPT sobre los límites a los derechos de las personas derivados de su derecho fundamental a la protección de sus datos personales hace aún más pertinente el estudio de los fijados en la propia LOPD, en correspondencia con lo dispuesto en el Convenio y la Directiva, y la doctrina sentada por el Tribunal Constitucional en su Sentencia 292/2000 sobre el particular.

Los derechos a saber, a consentir, a acceder, a rectificar y a cancelar antes enumerados, que componen el haz de facultades del contenido constitucionalmente declarado del derecho fundamental a la protección de datos personales, sólo pueden ser limitados en los estrictos términos que la Constitución autoriza. Así pues, son límites constitucionalmente idóneos del derecho fundamental a la protección de datos, y sólo éstos, la garantía de los restantes derechos fundamentales y constitucionales, en particular los derechos a la intimidad y el honor (artículo 18.1 de la CE) y a la libertad religiosa e ideológica (artículo 16 de la CE), y los bienes dignos de protección constitucional, muy en especial los enumerados en el artículo 105.b) de la CE, seguridad y defensa del Estado y la averiguación y la persecución del delito (STC 166/1999, fundamento jurídico 2, y 127/2000, fundamento jurídico 3.a); ATC 155/1999), y también el deber constitucional de todos a contribuir al sostenimiento de los gastos públicos, y los bienes y las finalidades constitucionales legítimos ligados a este deber, como la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria (artículo 31.1 de la CE, STC 110/1984 y 143/1994).

Fuera de estos casos, ninguna otra norma, incluso las de rango legal que tengan por cometido el desarrollo del derecho fundamental a la protección de datos personales, puede establecer límite alguno a este derecho fundamental, ya que la reserva de ley contenida en el artículo 18.4 de la CE no autoriza al legislador a la imposición de nuevos límites al derecho fundamental a la protección de datos, sino, al contrario, le exige la obligación de imponer límites a la recogida y el uso de esos datos con el objeto de garantizar justamente ese derecho fundamental. A esos derechos y bienes de rango constitucional deben reconducirse los límites previstos en la LOPD y en la normativa concordante.

Así, la STC 292/2000, fundamento jurídico 11:

"Justamente, si la ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un poder público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro poder público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese poder público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, el almacenamiento, el tratamiento, el uso y la cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional.

"De ser ese el caso, la ley habrá vulnerado el derecho fundamental en cuestión, ya que no sólo habrá frustra-

El título VI LOPD regula la Agencia de Protección de Datos (desarrollado por el Real decreto 428/1993, de 26 de junio –modificado por el 156/1996, de 2 de febrero–) y el título VII, las infracciones y las sanciones (desarrollado por el Real decreto 1332/1994, de 20 de junio, capítulo V).

25. Artículo 19. Derecho a indemnización. 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

do la función de garantía propia de toda reserva de ley relativa a derechos fundamentales al renunciar a fijar por sí misma esos límites, dado que la reserva de ley impone al legislador, además de promulgar esa ley, regular efectivamente en ella la materia objeto de la reserva, sino también al permitir que el derecho fundamental ceda ante intereses o bienes jurídicos de rango infraconstitucional en contra de lo dispuesto en la propia Constitución, que no lo prevé así."

Las exigencias no se paran sólo en los bienes o los derechos que puedan ser el fundamento de los límites al derecho fundamental a la protección de datos. El Tribunal Constitucional, en su Sentencia 292/2000 (fundamento jurídico 10), también ha exigido ciertas condiciones formales a la ley que regule esos límites, en aplicación de la doctrina del Tribunal Europeo de Derechos Humanos sobre el particular:

"El Convenio europeo de 1981 también ha tenido en cuenta estas exigencias en su artículo 9. Al igual que el Tribunal Europeo de Derechos Humanos, quien refiriéndose a la garantía de la intimidad individual y familiar del artículo 8 del CEDH, aplicable también al tráfico de datos de carácter personal, reconociendo que pudiera tener límites como la seguridad del Estado (STEDH caso Leander, de 26 de marzo de 1987, 47 y siguientes), o la persecución de infracciones penales (*mutatis mutandis*, STEDH, casos Z contra el Reino Unido, de 25 de febrero de 1997, y Funke contra Francia, de 25 de febrero de 1993), ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito (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; *mutatis mutandis*, caso Funke, de 25 de febrero de 1993; caso Z, de 25 de febrero de 1997)."

En suma, la ley que fije los límites al derecho fundamental a la protección de datos, debe ser una norma precisa, cierta y previsible en sus términos y consecuencias, y los límites que fije deben fundarse, además, en alguno de los derechos y/o bienes constitucionales antes enumerados, y que sean proporcionados al fin perseguido.

2.3.2. La concreción legal de los límites al derecho fundamental a la protección de datos personales en relación con el padrón municipal

La LOPD, a la hora de regular los límites que cabe imponer al ejercicio del derecho fundamental a la protección de datos personales, no ha hecho sino adoptar las cláusulas generales que a tal efecto ya establecían tanto el Convenio como la directiva. El Convenio, en su artículo 9, fija las excepciones a las garantías que el propio Convenio establece, señalando que no serán admisibles otras limitaciones salvo las que se definen en ese mismo precepto. Dichas excepciones deben estar previstas en la ley y deben constituir "una medida necesaria en una sociedad democrática". Esas excepciones son: la protección y la seguridad del Estado, y de sus intereses monetarios, la represión de las infracciones penales, la protección misma de la persona concernida, y la salvaguardia de los derechos y las libertades de terceras personas.[26]

La Directiva, por su parte, en su artículo 13, autoriza a los estados para adoptar medidas legales que limiten los derechos que constituyen el contenido del derecho a la protección de datos enumerando los siguientes bienes jurídicos "cuando tal limitación constituya una medida necesaria para la salvaguardia" de la seguridad y la defensa del Estado, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas, un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales, la protección del interesado o de los derechos y las libertades de otras personas.

Límites que, a grandes rasgos, vienen a coincidir con los que el artículo 105.b) de la CE fija para el acceso a los archivos y los registros administrativos, a saber: seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas. Es un precepto que en modo alguno debe desdeñarse, en la medida en que el padrón municipal es un registro administrativo de los vecinos de un municipio. Así pues, la ley, incluida la que regula el padrón municipal, sólo podrá limitar el haz de facultades del derecho fundamental a la protección de los datos personales si, y sólo si, concurre en el caso alguna de las causas enumeradas en el artículo 9 del Convenio, artículo 13 de la Directiva (so pena de que la ley contraríe los mencionados tratados y por ello el artículo 96 de la CE) y en el apartado b) del artículo 105 de la CE.

Cabría preguntarse si también son aplicables al padrón municipal las reglas relativas al acceso a los re-

26. El apartado 3 del artículo 9 establece un régimen propio de limitaciones para el caso de ficheros de uso estadístico o científico, pues la ley puede fijar otros límites a los derechos de acceso, rectificación y cancelación de la persona concernida distintos a los mencionados, siempre que "no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas". Es una nota común a la regulación de la protección de datos, y así lo contempla la LOPD, que sea distinto, y más flexible, el régimen legal de acceso a los datos personales con fines estadísticos (en los que cabría incluir, siquiera parcialmente, el acceso al padrón por el INE) y científicos.

gistros administrativos previstas en la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común. Sin perjuicio de que la cuestión se estudie con mayor detalle en la sección dedicada al acceso al padrón municipal,[27] dadas las dificultades constitucionales que plantean los artículos 37 y siguientes de la mencionada ley y su posible contradicción con la propia LOPD, baste decir por ahora que, a nuestro juicio, el padrón municipal es un registro público sujeto a su propia normativa.

En efecto, el artículo 37.6.e) de la Ley 30/1992, de 26 de noviembre, establece que se regirán por "sus disposiciones específicas [...] e) El Registro Civil y el Registro Central de Penados y Rebeldes y los registros de carácter público cuyo uso esté regulado por una ley". Este es el caso, así lo creemos, del padrón municipal, que es un registro administrativo de los vecinos del municipio "cuyo uso" posee normas específicas y peculiares contenidas en la LBRL (desarrollada por el RPT) y en la LOPD (en su condición, también, de fichero informatizado de datos personales).[28]

2.3.3. La obligatoriedad de los datos del padrón y los límites a los derechos a saber y a consentir

Con arreglo a los artículos 15 y 16.2 de la LBRL (artículos 54 y 57 del RPT) la inscripción en el padrón es obligatoria, e igualmente el padrón debe contener necesariamente ciertos datos de la persona (nombre y apellidos, sexo, domicilio habitual, nacionalidad, lugar y fecha de nacimiento, número de documento nacional de identidad o documento de identificación similar, certificado o título escolar o académico que se posea y otros datos necesarios a los efectos de la confección del censo electoral, siempre que se respeten, dice la norma, los derechos fundamentales reconocidos en la CE).

Ninguna de estas normas constituye un límite desproporcionado o inadecuado a los derechos individuales a saber y consentir la recogida, el uso y el tratamiento de los datos personales. El propio artículo 5.1.b) de la LOPD prevé la posibilidad de la obligatoriedad de la recogida de ciertos datos al establecer que el afectado debe ser informado de manera expresa, cierta e inequívoca de esa circunstancia.[29] Y el artículo 6.2 de la LOPD dispone que la ley podrá dispensar del previo consentimiento de la persona para el tratamiento (que no para su recogida) de sus datos; consentimiento que ni siquiera es necesario recabar en el caso de que "los datos de carácter personal se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias". Sin perjuicio de que el párrafo 4 de ese mismo artículo 6 señala que: "4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

En consecuencia, la obligatoriedad de la inscripción en el padrón y la obligatoriedad de ciertos datos del vecino, que no dejan de ser manifestaciones de la recogida y el tratamiento obligatorio de datos personales a cargo de una administración pública, son un límite constitucionalmente adecuado y proporcionado, con la debida cobertura legal, al derecho fundamental a la protección de datos personales. Ya se ha visto que este derecho garantiza a la persona la facultad de consentir la recogida y el tratamiento de sus datos personales. Una facultad que puede estar limitada por la ley si ésta impone la obligatoriedad de esa recogida y ese tratamiento siempre que la misma se funda en derechos o bienes constitucionalmente protegidos. No cabe duda de que el padrón municipal ancla sus cimientos en diversos preceptos constitucionales en cuanto que la inscripción en el mismo es el título constitutivo de la condición de vecino (artículo 15 de la LBRL y artículo 53.1 del RPT), lo que resulta ser condición para el disfrute de los derechos y el cumplimiento de los deberes aparejados a esa condición administrativa personal (artículo 18 de la LBRL y artículo 56 del RPT), que encuentran su estribo en los derechos fundamentales a participar en los asuntos públicos (artículo 23 de la CE) y en deberes constitucionales como la contribución personal al sostenimiento del gasto público (artículo 31 de la CE). Pero no sólo son ese derecho y este deber constitucionales la razón que justifica la existencia del padrón y la obligatoriedad de la inscripción en el mismo. También el principio de eficacia y objetividad de la acción administrativa al servicio del interés general justifica (artículo 103 de la CE) la existencia de ese instituto y la obligatoriedad de la inscripción en el padrón.

27. Sección que constituye la cuarta y última parte de este trabajo, en su versión completa, de pronta publicación.

28. Del mismo modo que ese mismo precepto en sus letras *c*) y *d*) excluye de la regulación general sobre archivos y registros administrativos contenida en la Ley 30/1992, de 26 de noviembre, a los archivos que persigan fines estadísticos únicamente (censos de población) y a los sujetos a la legislación electoral (censo electoral).

29. Muchos de los problemas que se suscitan sobre este y otros particulares relativos a la aplicación de la LOPD tienen su origen en el desconocimiento de lo dispuesto en ese mismo artículo 5.2 LOPD: "Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior." En la mayoría de los casos, y sobre todo a los efectos de considerar prestado el consentimiento de la persona para la recogida y el tratamiento de sus datos personales, basta con que el impreso correspondiente contenga de forma clara e inequívoca y en un lugar destacado del mismo las advertencias legales pertinentes que adviertan al interesado de sus derechos y las informaciones a las que alude el artículo 5 de la LOPD.

Sólo en la medida en que la Administración local conoce con exactitud quiénes sean los vecinos del ayuntamiento podrá actuar con la constitucionalmente exigida eficacia y objetividad y facilitar el ejercicio del derecho fundamental de participación de aquéllos y hacer efectivo su deber de contribuir equitativamente al sostenimiento del gasto de los entes locales. Éste debe ser el sentido que debe dársele al artículo 6.2 de la LOPD antes mencionado. En consecuencia, no hay reparo constitucional alguno a que la LOPD (u otra norma con rango de ley orgánica)[30] dé cobertura a sendos límites tanto al derecho a oponerse a la recogida de datos, como a consentir su tratamiento, en el caso del padrón; sin perjuicio de que se advierta de forma clara, inequívoca y cierta al afectado de la obligatoriedad de la inscripción y de ciertos datos personales, así como de los derechos que le asisten en los términos del artículo 5 de la LOPD.

La LOPD contempla otros posibles límites a los derechos a saber y a consentir que han sido objeto de examen por el Tribunal Constitucional en la citada STC 292/2000. El artículo 24, titulado "Otras excepciones a los derechos de los afectados", disponía antes de la STC 292/2000:

"1. Lo dispuesto en los apartados 1 y 2 del artículo 5 (derecho a saber)[31] 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."

A este respecto, debe indicarse que la STC 292/2000 declaró contrarios a la Constitución, por lesión del derecho fundamental a la protección de datos, el inciso "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las administraciones públicas" y el inciso final "o administrativas", al considerar que la ley había hecho dejación de sus funciones en observancia de la reserva dispuesta en el artículo 18.4 de la CE, permitiendo que la Administración pública pudiese restringir arbitrariamente el derecho a saber del interesado (afectando incluso a sus derechos de defensa en el marco de un procedimiento administrativo sancionador).

En consecuencia, tan sólo la defensa del Estado, la seguridad pública o la persecución de infracciones penales (todos ellos bienes constitucionalmente protegidos) constituyen los únicos límites posibles y, por consiguiente, las únicas causas lícitas de restricción del derecho a saber del artículo 5.1 y 2 de la LOPD. Denegación que por lo demás habrá de ser motivada y es susceptible de impugnación ante la Agencia de Protección de Datos y ante la jurisdicción contencioso-administrativa (artículo 5.4 de la LOPD).

Pues bien, no parece que en el supuesto del padrón municipal concurra ninguna de las posibles circunstancias previstas en el artículo 24.1 de la LOPD que permitirían restringir el derecho a saber del interesado respecto de la recogida de sus datos personales. Es difícil imaginar en qué casos la información al afectado sobre la obligatoriedad de su inscripción en el padrón, sobre los datos obligatorios, sobre el destino y el uso de esos datos o sobre el responsable del padrón, afectarían a la defensa y la seguridad del Estado o a la persecución de las infracciones penales.

De otro lado, el artículo 11 de la LOPD (en relación con el artículo 21 de la LOPD) prevé límites a los derechos a saber y consentir, en este caso, sobre la cesión de datos entre administraciones públicas. Asunto que será objeto de estudio en el último apartado de este trabajo.[32]

2.3.4. Los límites a los derechos de rectificación y cancelación

En la actualidad, sólo el artículo 23 de la LOPD establece las "excepciones a los derechos de acceso, rectificación y cancelación". Nos ocuparemos ahora de estos dos últimos.

"1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior[33] podrán denegar el acceso, la rectificación

30. Se trataría en este caso de un supuesto de colaboración entre ley orgánica y ley ordinaria. Desde luego, y máxime tras la STC 292/2000, los límites directos a un derecho fundamental, aunque lo sean a su ejercicio y no a su contenido constitucional, deben revestir la forma de ley orgánica, sin perjuicio de que la pertinente ley orgánica llame a la ordinaria para concretar esos límites (lo que, sin embargo, está vedado al reglamento, lo que incluye, claro está, a las ordenanzas y demás fuentes del ordenamiento jurídico local).

31. Artículo 5 de la LOPD: 1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: *a*) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. *b*) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. *c*) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. *d*) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. *e*) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

32. Sección cuarta, que constituye la última parte de este opúsculo en su versión completa.

33. Artículo 22. Ficheros de las fuerzas y los cuerpos de seguridad:

1. Los ficheros creados por las fuerzas y los cuerpos de seguridad que contengan *datos* de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente ley.

o la cancelación 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.

"2. Los responsables de los ficheros de la hacienda pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice 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.

"3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del director de la Agencia de Protección de Datos o del organismo competente de cada comunidad autónoma en el caso de ficheros mantenidos por cuerpos de policía propios de éstas, o por las administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación."

Bien se ve que ninguna de estas excepciones a los derechos de rectificación y de cancelación podrían afectar al padrón municipal.

Con anterioridad a la STC 292/2000, el párrafo 2 del artículo 24 de la LOPD fijaba nuevas excepciones a los derechos de acceso, rectificación y cancelación en los siguientes términos:

"2. Lo dispuesto en el artículo 15 (derecho de acceso) y en el apartado 1 del artículo 16 (derecho de rectificación y cancelación) 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."

Pues bien, dicho apartado fue declarado contrario al artículo 18.4 de la CE por el Tribunal Constitucional en su Sentencia 292/2000, al entender que en él el legislador había renunciado a fijar por sí mismo los límites a esos derechos, abandonándolos a la mera discrecionalidad administrativa. Por consiguiente, el ejercicio de los derechos de rectificación y cancelación de los datos contenidos en el padrón municipal no está sujetos a límite alguno (salvo los que deriven de la garantía de otros derechos fundamentales, que no requieren de concreción legal alguna).[34]

3. Nota bibliográfica

Sobre la teoría general del derecho fundamental a la protección de datos véanse los trabajos de DENNINGER, Erhard, "El derecho a la autodeterminación informativa", en *Problemas actuales de la documentación y la informática jurídica*, (Pérez Luño, dir.), Madrid: Tecnos, 1987, págs. 269 y ss.; LUCAS MURILLO, Pablo, *El derecho a la autodeterminación informativa*, Madrid: Tecnos, 1990; CASTELLS ARTECHE, José Manuel, "La limitación informática", en *Estudios sobre la Constitución española. Homenaje al profesor García de Enterría*, tomo II, Madrid: Civitas, 1991, págs. 907 y ss.; SANCHEZ CASABON y UBIETO ARTUR (coord.), *Jornadas sobre documentación administrativa y sociedad de la información*, Zaragoza: Gobierno de Aragón, Ayuntamiento de Zaragoza y Universidad de Zaragoza, 2001; VARIOS AUTORES, *La protección del derecho a la intimidad de las personas (ficheros de datos)*, Cuadernos del Poder Judicial, vol. XIII, 1997; VÁZQUEZ BAUTISTA, Rafael, *Protección jurídica de datos personales automatizados*, Madrid: Colex, 1993; VARIOS AUTORES, *XX Conferencia Internacional de Autoridades de Protección de Datos 1998*, Madrid: Agencia de Protección de Datos, 1999.

Sobre este régimen jurídico de la protección de datos en el derecho comparado y, en particular, en el ámbito europeo, véanse DE URIOSTE, Mercedes, "Protección de datos personales (I) (II) y (III)", en *Investigaciones* (Secretaría de Investigación de Derecho Comparado. Corte Suprema de Justicia de la Nación. República de Argentina), 1, 2 y 3, 1998, págs. 121 y ss., 371 y ss., 635 y ss.; SUÑÉ LLINÁS Emilio, "Marco jurídico del tratamiento de datos personales en la Unión Europea y en España",

2. La recogida y el tratamiento para fines policiales de *datos* de carácter personal por las fuerzas y los cuerpos de seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de *datos* que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y el tratamiento por las fuerzas y los cuerpos de seguridad de los *datos*, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los *datos* personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los *datos* almacenados, la necesidad de mantener los *datos* hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

34. No se debe concluir este apartado sin mencionar la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos relativa al ejercicio de los derechos de acceso y rectificación.

en *La armonización legislativa de la Unión Europea*, Madrid: Dykinson, 1999, págs. 245 y ss.; PRIETO GUTIÉRREZ, Jesús María, "La Directiva 95/46/CE como criterio unificador", *Revista del Poder Judicial*, 48, 1997, págs. 165 y ss.; HEREDERO HIGUERAS, Manuel, *La Directiva Comunitaria de protección de los Datos de Carácter Personal*, Pamplona: Aranzadi, 1997, y SÁNCHEZ BRAVO, Álvaro, *La protección del derecho a la libertad informática en la Unión Europea*, Sevilla: Publicaciones de la Universidad de Sevilla, 1998.

Sobre la legislación española, LUCAS MURILLO, Pablo, "La protección de los datos personales ante el uso de la informática en el derecho español (I y II)", *Estudios de Jurisprudencia*, núms. 3 y 4, 1992, págs. 7 y ss. en ambos casos, y también *Informática y protección de datos personales (Estudios sobre la LO 5/1992),* Centro de Estudios Constitucionales, colección "Cuadernos y Debates, núm. 43, Madrid, 1993; TÉLLEZ AGUILERA, Abel, *Nuevas tecnologías. Intimidad y protección de datos. Estudios sistemáticos de la Ley orgánica 15/1999*, Madrid: Edisofer, 2001; DAVARA RODRÍGUEZ, Miguel Ángel, *Los principios de la protección de datos y los derechos de las personas en la nueva Ley orgánica de protección de los datos de carácter personal*, Actualidad Informática Aranzadi, núm. 34, 2000, págs. 1 y ss.; FERNÁNDEZ LÓPEZ, Juan Manuel, *La nueva Ley de protección de datos de carácter personal de 13 de diciembre de 1999*, Actualidad Informática Aranzadi, núm. 34, 2000, pág. 1 y ss.; GARCÍA ONTOSA, Rosa María, *Comentarios a la nueva Ley de protección de datos de carácter personal*, Actualidad Informática Aranzadi, núm. 34, 2000, pág. 1 y ss.; consúltese también la *Memoria 2001*, Madrid: Agencia de protección de Datos, 2002; ALGUACIL GONZÁLEZ-AURIOLES, Jorge, "La libertad informática: aspectos sustantivos y competenciales (STC 290 y 292/2000)", *Teoría y realidad constitucional*, núm. 7, 2001, págs. 365 y ss.

Respecto del padrón municipal, MARTÍNEZ-ALONSO CAMPS, José Luis, "La encomienda de la gestión informatizada de los padrones municipales de habitantes: un ejemplo de colaboración entre administraciones públicas", *Revista de Estudios de la Administración Local y Autonómica*, núm. 1 (enero-abril), 1998, págs. 151 y ss.

Sobre el acceso a los archivos y a los registros administrativos, MARTÍNEZ PÉREZ, Pedro A., "Participación ciudadana: Modalidades. Información municipal: Acceso al registro", *Revista de Estudios Locales*, mayo de 2001, págs. 11 y ss.; MESTRE DELGADO, Juan Francisco, *El derecho de acceso a archivos y registros administrativos (análisis del artículo 105.b) de la Constitución)*, Madrid: Civitas, 1998 (2.ª edición); POMED SANCHEZ, Luis, *El derecho de acceso de los ciudadanos a los archivos y registros administrativos*, Madrid: INAP, 1989. ■