Segunda Parte: El derecho fundamental a la protección de datos personales: Principios, Derechos y Órganos de Control

7

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

7. EL DERECHO A LA PROTECCIÓN DE DATOS

La protección de datos de carácter personal es un derecho fundamental que garantiza la Constitución Española de 1978, cuya regulación y desarrollo se especifica en la vigente Ley Orgánica 15/1999, de 13 de diciembre (en adelante LOPD), que lleva a cabo la transposición al ordenamiento jurídico español de la Directiva Comunitaria 95/46/CEE, 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 esos datos.

Desde una perspectiva de dimensión europea, la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en la Cumbre de Niza, el 7 de diciembre de 2000, recoge en su Artículo 8, dentro del capítulo relativo a las Libertades, el reconocimiento del derecho a la protección de datos de carácter personal, estableciendo que "*Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan*".

En cumplimiento del mandato impuesto por el Artículo 18.4 de la Constitución Española de 1978 (en adelante CE), en el que se establece que "*La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*", la LOPD se constituye así en la norma sobre la materia en nuestro país y la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000, ha definido y delimitado el contenido esencial del derecho a la protección de datos como un derecho independiente y autónomo en nuestro sistema constitucional, deslindado del derecho a la intimidad. En este sentido, la citada Sentencia recalca lo siguiente:

"*Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (artículo 81.1 CE), bien regulando su ejercicio (artículo 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta fundamentación, lo que apareja, por consiguiente, que también su objeto y contenido difieran*.

En esencia, 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 estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, permitiendo también al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Su carácter de derecho fundamental le otorga unas determinadas características, como la de ser irrenunciable y el hecho de prevalecer sobre otros derechos no fundamentales".

De acuerdo con el Artículo 1 de la LOPD, el objeto de esta Ley es: "*garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*".

La LOPD, para facilitar la aplicación efectiva de sus mandatos, establece que "*las funciones de la Agencia de Protección de Datos [...] en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control y a los que se garantizará la plena independencia y objetividad en el ejercicio de su cometido*".

Como consecuencia de esta habilitación, la Comunidad de Madrid ha aprobado una normativa específica sobre esta materia, mediante la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, que derogó la Ley 13/1995, de 21 de abril, de Regulación del Uso de la Informática en el Tratamiento de Datos Personales por la Comunidad de Madrid.

En consonancia con el reconocimiento de este derecho, desde el mismo momento del nacimiento del individuo, cuando se está produciendo la inscripción en el Registro Civil de los datos del recién nacido, ya se está produciendo un primer acto con trascendencia en materia de protección de datos, puesto que el nombre, los apellidos, la fecha de nacimiento y los nombres y apellidos de los padres, son datos de carácter personal.

En la actualidad, la protección de datos de carácter personal, debido al uso de las tecnologías de la información, y sobre todo a la utilización de Internet, ha cobrado una nueva dimensión, de manera que los datos personales de los ciudadanos deben quedar aún más garantizados, salvaguardando dichos datos ante cualquier fallo de seguridad de los sistemas informáticos, o incluso, ante cualquier ataque que sufran estos sistemas informáticos por los denominados 'hackers'.

Asimismo, cobra también especial importancia la denominada 'Administración Electrónica' que, si bien en un principio se configuró como una herramienta para que los ciudadanos pudiesen llevar a cabo sus trámites con las distintas Administraciones Públicas por Internet, tiene otras manifestaciones que se han plasmando recientemente en diversos ámbitos de la actividad administrativa, tales como los relativos a la expedición del DNI o del pasaporte electrónico, la tarjeta sanitaria electrónica o la receta electrónica.

7.1. Normativa

Además de la LOPD, podemos destacar la siguiente normativa en materia de protección de datos personales:

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

En la Comunidad de Madrid es de aplicación además la siguiente normativa:

a) Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid;

b) Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal así como su inscripción en el Registro de Ficheros de Datos Personales;

c) Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de las funciones de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal;

d) Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid.

Para adaptar los tratamientos de datos de diversos sectores a la normativa de protección de datos, la Agencia de Protección de Datos de la Comunidad ha aprobado una serie de Instrucciones y Recomendaciones:

a) Instrucción 1/2007, de 16 de mayo, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid;

b) Recomendación 1/2004, de 14 de abril, sobre la utilización y tratamiento de datos del padrón municipal por los Ayuntamientos de la Comunidad de Madrid;

c) Recomendación 2/2004, de 30 de julio, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas;

d) Recomendación 1/2005, de 5 de agosto, sobre archivo, uso y custodia de la documentación que compone la Historia Social no informatizada por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid;

e) Recomendación 1/2006, de 3 de abril, sobre cesiones de datos de empleados públicos de la Comunidad de Madrid a las secciones sindicales, comités de empresas y juntas de personal;

f) Resolución de 9 de enero de 2007, del Director de la Agencia de Protección de Datos de la Comunidad de Madrid, por la que se establecen los modelos de impresos y los medios por los que debe procederse a la notificación de inscripciones de creación, modificación o supresión de ficheros, en el Registro de Ficheros de Datos Personales;

g) Resolución de 12 de abril de 2006, del Director de la Agencia de Protección de Datos de la Comunidad de Madrid, por la que se incorpora al Anexo I del Decreto 175/2002, de 14 de noviembre, por el que se regula la utilización de las técnicas electrónicas, informáticas y telemáticas por la Administración de la Comunidad de Madrid, el procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales.

Por otra parte, existen una serie de normas sectoriales, tanto estatales como del ámbito propio de la Comunidad de Madrid, en las que se contienen diversos artículos relativos a la protección de datos. Entre ellas destacan la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos; la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información; la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; y la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid.

La normativa referida puede consultarse en la página Web de la Agencia de Protección de Datos de la Comunidad de Madrid, www.apdcm.es, dentro del Canal Legislación.

7.2. Ámbito

"*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*" (Art. 2 de la LOPD).

Del ámbito general de aplicación que establece la LOPD debe destacarse lo siguiente: por una parte, su aplicación a los datos registrados en cualquier soporte físico susceptible de tratamiento; por otra, su aplicación tanto al sector público como al privado.

Por lo que se refiere al primero, la Ley debe entenderse aplicable no sólo a datos almacenados en soportes electrónicos o informáticos, sino también a los recogidos en papel, siempre y cuando la información se encuentre estructurada de acuerdo con criterios relativos a personas identificadas o identificables.

Asimismo, también podemos encontrarnos el supuesto de que un fichero sea en parte informatizado y en parte manual. En este caso, estamos ante lo que se denomina fichero parcialmente automatizado ("mixto").

De esta manera, puede distinguirse entre ficheros informatizados, ficheros no informatizados (o ficheros manuales en formato papel) y ficheros parcialmente automatizados (parte informatizado, parte no informatizado).

Con ello, se da cumplimiento al Considerando 15 de la Directiva 95/46/CE según el cual "*los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata"; y al Considerando 27 de la misma Directiva, según el cual "la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva*".

Por todo ello, la Directiva 95/46/CE define el concepto de fichero de datos personales como "*todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica*".

En resumen: la LOPD es aplicable a todos los ficheros informatizados que contengan datos de carácter personal, a aquellos ficheros no informatizados (manuales) que contengan datos de carácter personal, y a los ficheros parcialmente automatizados (datos informatizados y datos en soporte papel) siempre que la información almacenada se organice según algún criterio relativo a las personas, de forma que permita acceder a los datos de una persona en concreto.

Por ejemplo:

Cuando las instancias (en formato papel) presentadas por los interesados en participar en un proceso selectivo, se almacenen por orden alfabético, por DNI o número de opositor, estaremos ante un tratamiento de datos personales sometido a la aplicación de la legislación sobre protección de datos, por tratarse de un conjunto de información estructurado por un criterio relativo a las personas que permite acceder fácilmente a los datos de un interesado concreto.

Si esas mismas instancias se almacenan por el orden cronológico de recepción no nos encontramos ante un fichero no informatizado (manual), por lo que no sería de aplicación la legislación de protección de datos.

Cuando se recaben datos personales y se almacenen utilizando alguna herramienta informática (base de datos, Excel, Access) estamos ante un fichero informatizado.

Puede ocurrir que se hayan recabado datos personales mediante documentación en papel y posteriormente se almacenen informáticamente. En este caso, nos encontramos ante un fichero parcialmente automatizado (mixto), ya que parte de los datos personales están en formato papel y otra parte se ha almacenado informáticamente.

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, contiene por primera vez las medidas de seguridad a aplicar a los ficheros manuales. Asimismo, en la Disposición Transitoria Segunda de dicho Reglamento, se establecen los plazos de adaptación de las medidas de seguridad de los ficheros manuales preexistentes a la futura entrada en vigor del citado Reglamento, que serán de un año para los ficheros manuales de nivel básico, de 18 meses para los ficheros manuales de nivel medio, y de dos años para los ficheros manuales de nivel alto.

Por otra parte, la LOPD y los principios de protección de datos en ella contenidos se aplican tanto al tratamiento de datos personales en el sector público como en el privado. Asimismo, los derechos que la LOPD reconoce a las personas físicas deben ser respetados por cualquier entidad pública o privada que trate datos de carácter personal, con independencia de la naturaleza de ésta.

Sin embargo, la LOPD establece diferencias entre los ficheros públicos y privados en materia de creación, modificación y supresión de ficheros, consentimiento, cesiones de datos personales y en materia sancionadora. Asimismo, la LOPD contiene artículos específicos para determinados ficheros privados como sucede con el caso de los ficheros de solvencia patrimonial y crédito, y los ficheros creados con fines de publicidad y prospección comercial. En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, contiene un Título específico, el IV, titulado Disposiciones aplicables a determinados ficheros de titularidad privada, donde se regulan este tipo de casos.

Un ejemplo de la especialidad de los tratamientos de datos realizados en el ámbito público es el siguiente:

Cuando una Administración/organismo/entidad pública pretenda crear un fichero que vaya a contener datos de carácter personal, deberá aprobar una disposición de carácter general que se publicará en el Boletín o Diario Oficial correspondiente.

Las empresas privadas podrán crear un fichero siempre y cuando lo notifiquen, con carácter previo a dicha creación, a la Agencia Española de Protección de Datos.

Cuando una Administración/organismo/entidad pública cometa una infracción relacionada con la LOPD, la resolución sancionadora determinará la infracción cometida, y en su caso, las medidas a adoptar, comunicando la resolución al infractor, a su superior jerárquico y al Defensor del Pueblo, no imponiendo sanción económica al respecto.

Si la infracción es cometida por una empresa privada, la resolución sancionadora puede imponer una multa que va desde los 600 a los 600.000 euros, dependiendo del tipo de infracción que se haya cometido y de los criterios de graduación de la cuantía de la sanción.

Por otra parte, respecto al ámbito territorial de aplicación de la LOPD, ésta regirá 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, siempre que éste se encuentre ubicado en territorio español.

Si el responsable del tratamiento no está ubicado en territorio español, pero exista un encargado de tratamiento ubicado en dicho territorio, este encargado de tratamiento deberá cumplir con las medidas de seguridad.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en asignación de normas de Derecho Internacional público.

d) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

   En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

El régimen de protección de datos de carácter personal que se establece en la LOPD *no* será de aplicación:

a) A los ficheros o tratamientos mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. En este caso, sólo se considerarán relacionados con actividades personales o domésticas los ficheros o tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los ficheros o tratamientos sometidos a la normativa sobre protección de materias clasificadas. Las materias clasificadas se encuentran reguladas por la Ley 9/1968, sobre secretos oficiales.

c) A los ficheros o tratamientos establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. Tendrán esta consideración aquellos tratamientos respecto de los que el responsable del fichero haya comunicado previamente a la Agencia Española de Protección de Datos sus características generales y su finalidad.

Para finalizar en lo referente al ámbito de aplicación, la LOPD establece una serie de materias que se regularán por su normativa específica y por lo especialmente previsto, en su caso, por la propia LOPD. Se trata de los siguientes supuestos:

Los ficheros reglados por la legislación de régimen electoral, cuya regulación viene dada por la Ley Orgánica 5/1985, de 19 de junio, sobre Régimen Electoral General. En este sentido, el Artículo 41.2 de la citada Ley establece que queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial.

a) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. En materia estadística son de aplicación la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en el ámbito de la Comunidad de Madrid la Ley 12/1995, de 21 de abril, de Estadística.

b) En este último caso, corresponde a la Agencia de Protección de Datos de la Comunidad de Madrid velar por el cumplimiento de las disposiciones que las leyes sobre estadística pública de la Comunidad de Madrid establezcan respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar instrucciones precisas y dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.

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.

   Según el Artículo 103 de la Ley 17/1999, de 18 de mayo, reguladora del Régimen del Personal de las Fuerzas Armadas, los militares profesionales serán evaluados para determinar su aptitud para el ascenso al empleo superior e idoneidad para desempeñar distintos cometidos y para comprobar la existencia de insuficiencia de facultades profesionales o de condiciones psicofísicas. Esta información se almacena en un registro (fichero informatizado) en el que consta el historial de cada militar.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

   Respecto al Registro Civil, la Ley de 8 de junio de 1957 y su Reglamento, Decreto de 14 de noviembre de 1958, regulan supuestos específicos del acceso a la documentación obrante en el citado Registro Civil. En cuanto al Registro Central de Penados y Rebeldes, está regulado por la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, y por la Real Orden de 1 de abril de 1896, que regula el acceso de los particulares al citado Registro.

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.

   A este respecto, se ha citado anteriormente la Instrucción 1/2007, de 16 de mayo, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid.

8

DEFINICIONES

8. DEFINICIONES

Una correcta interpretación de la normativa vigente en materia de protección de datos se obtiene de las definiciones que la LOPD especifica en su Artículo 3. Estas definiciones se encuentran también en el Real Decreto 1720/2007, de 21 de diciembre. En algunos casos, se ha producido un desarrollo de las mismas en relación con las definiciones previamente contenidas en la propia LOPD, mientras que en otras ocasiones se han introducido nuevas definiciones. Asimismo, y puesto que el citado Real Decreto 1720/2007, de 21 de diciembre, ha derogado el Real Decreto 994/1999, de 11 de junio (Reglamento de Medidas de Seguridad de los ficheros automatizados), se han incluido en el primero el conjunto de las definiciones relativas a las medidas de seguridad de los ficheros.

8.1. Datos de carácter personal

"*Cualquier información concerniente a personas físicas identificadas o identificables*". (Art. 3.a LOPD).

Esta información, que puede manifestarse de diferente manera (numérica, alfabética, gráfica, fotográfica y acústica), y que debe referirse siempre a una persona física identificada o identificable, puede ser muy diversa: nombre y apellidos, correo electrónico, estado civil, número de cuenta bancaria, etcétera.

El elemento fundamental para determinar que se trata de un dato de carácter personal es que la información, por sí misma o combinada, permita conocer datos de una persona concreta, bien por estar directamente identificada a través de algún dato, o bien porque pueda llegar a ser identificada por otro medio.

De acuerdo con la definición que contiene la Directiva 95/46/CE, "*se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*".

La citada Directiva 95/46/CE, indica en su considerando 26 que: "*[...] para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta […] pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado*".

Así, a modo de ejemplo:

El nombre, apellidos, DNI o la dirección de correo electrónico son datos de carácter personal.

Por otra parte, el Tribunal Constitucional se ha manifestado sobre qué se entiende por dato de carácter personal. Así, la Sentencia 292/2000 dice que "*el derecho 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 el Art. 18. 1 CE, 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 constituye una amenaza para el individuo*".

En conclusión:
Se considerará dato de carácter personal, objeto de la protección de datos, cualquier información referente a una persona física de la cual se pueda conocer quién es su titular, por intrascendente que pueda parecernos el dato almacenado.

Una persona estará identificada cuando conste en el fichero algún dato que tenga por finalidad diferenciarla del resto del colectivo cuyos datos se hayan recabado. Da igual que se le identifique por el nombre, el DNI, el número de empleado u opositor, siempre que su finalidad sea identificar al interesado.

A modo de ejemplo, en relación con las subvenciones, nos podemos encontrar con supuestos en los cuales se recaben de los interesados o afectados (ciudadanos) diferentes tipos de datos (nombre, apellidos, nivel de renta, situación laboral, minusvalía), y con otros con los que sólo se recabe el nombre y apellidos de los interesados (ciudadanos). En ambos casos, los datos recabados son datos de carácter personal ya que identifican al interesado o afectado (ciudadano) solicitante de la subvención.

Por otra parte, la LOPD, además del concepto de dato personal anteriormente referido, contiene una regulación específica para los datos especialmente protegidos a los que dota de una particular protección. Dentro de este tipo de datos se pueden distinguir los datos de salud. Tanto los datos especialmente protegidos como los datos de salud son analizados en la parte de Principios de esta Guía.

8.2. Fichero

"*Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*." (Art. 3.b LOPD).

Atendiendo a esta definición, y tal y como se ha adelantado, se pueden distinguir tres tipos de ficheros: los informatizados, los no informatizados –denominados también 'ficheros manuales'–, y los ficheros parcialmente automatizados –parte informatizado, parte manual–.

Respecto a los ficheros no informatizados, para considerar un fichero como tal, la documentación en papel tiene que estar organizada de forma estructurada basada en criterios relativos a personas físicas identificadas o identificables, es decir, que se pueda acceder a la misma de tal manera que se puedan conocer los datos personales obrantes en papel. Los ficheros parcialmente automatizados, como ya se ha indicado anteriormente, cuentan con parte de los datos personales en soporte informático y parte en soporte papel.

Ejemplos:

Los supuestos más comunes de ficheros manuales los constituyen expedientes académicos de los alumnos de Colegios, Institutos y Universidades, ya que suelen organizarse y ordenarse por nombres y apellidos.

También constituiría un fichero manual, la documentación en papel de los clientes de un banco, siempre y cuando estuviese ordenada por nombre y apellidos de los respectivos clientes.

El archivador existente en todos los departamentos de personal en el que se recogen los datos relevantes que se han generado a lo largo de la relación laboral entre el empleado y el empleador, y que afectan a su desarrollo.

Por el contrario, no es un fichero manual los expedientes en papel relativos a un procedimiento sancionador que tramita una Administración Pública si los expedientes se organizan por números sucesivos.

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, define tanto 'fichero' como 'fichero no automatizado' (manual).

Respecto al primero, considera 'fichero' a todo conjunto organizado de datos de carácter personal que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Respecto al segundo, considera 'fichero no automatizado' a todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a las personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

En esta última definición, el Real Decreto 1720/2007, de 21 de diciembre, sigue la definición de fichero contenida en la Directiva 95/46/CE. Esta Directiva define el fichero de datos personales como: "*todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica*".

También los Tribunales españoles se han manifestado en este sentido. Así, según la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 17 de marzo de 2006: "*todo fichero de datos exige para tener esta consideración una estructura u organización con arreglo a criterios determinados. El mero cúmulo de datos sin criterio alguno no podrá tener la consideración de fichero a los efectos de la ley*".

Por último, cabe la posibilidad de que un fichero tenga varios responsables. En este supuesto, existirá un único fichero, si bien cada uno de los responsables tendrá que comunicar al Registro de Ficheros –ya sea estatal o autonómico– competente la creación de dicho fichero, a fin de proceder a su inscripción.

8.3. Tratamiento de datos

"*Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*" (Art. 3.c LOPD).

No basta, sin embargo, la realización de una de estas actuaciones en relación con datos personales para que la LOPD despliegue sus efectos protectores y sus garantías, ni tampoco para que pueda hablarse de derechos del afectado. Es preciso algo más, que las actuaciones de recogida, grabación, conservación, etcétera, se realicen de forma automatizada, o bien, si se realizan de forma manual, que los datos personales se almacenen en un fichero.

Ejemplos:

La recogida de los impresos de solicitud de matrícula en un centro de enseñanza.

La grabación en una aplicación informática (fichero) de la cita concertada por un padre de alumno para entrevistarse con su tutor.

La obtención de nuevos datos a partir de la información recabada (la calificación académica de un alumno).

La actualización de la información existente en un fichero a partir de los nuevos datos recabados o de los obtenidos en un proceso de elaboración, como puede ocurrir con la actualización del Padrón Municipal de Habitantes.

La eliminación de los datos existentes en un fichero.

La mera consulta de los datos de un fichero.

Facilitar el acceso a los datos de una persona por parte de un tercero, mediante cualquier tipo de comunicación, consulta, interconexión o transferencia (envío a una agencia de viajes de los datos de un grupo de alumnos para la organización de una excursión o actividad extraescolar).

Es importante diferenciar los conceptos 'fichero' y 'tratamiento'. El fichero es cualquier soporte, ya sea informático o manual (en este caso siempre y cuando esté estructurado), que permita el almacenamiento de datos personales de personas físicas y su posterior tratamiento.

Por su parte, el tratamiento comporta posibilidades de reelaboración, de modificación de los datos y de intercambio. Asimismo, mientras que el fichero únicamente permite ordenar y facilitar el acceso y localización de información, el tratamiento, a la posibilidad de interconexión de datos, añade la obtención de resultados y la reelaboración de los mismos.

8.4. Afectado o interesado

"*Persona física titular de los datos que sean objeto del tratamiento*." (Art. 3.e LOPD).

De una parte, se debe tener en cuenta que no es necesario que la persona física esté plena y actualmente identificada, basta con que sea identificable; y, de otra parte, que sólo pueden ser afectados las personas físicas, ya que la protección de datos 'personales' no afecta a los datos de las personas jurídicas.

En relación con la condición de afectado o interesado nos podemos encontrar ante varias situaciones:

— Menores de edad: el Real Decreto 1720/2007, de 21 de diciembre, regula en su Artículo 13 el consentimiento para el tratamiento de datos de los menores de edad. Dicho Artículo establece que "*podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores. En ningún caso podrán recabarse del menor, datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización correspondiente*".

— Discapacitados mentales, intelectuales o psíquicos: sin perjuicio de ley especial o sectorial aplicable, al igual que en el anterior caso, será necesario el consentimiento de sus padres o representantes.

— Nasciturus: la Recomendación del Consejo de Europa de 13 de febrero de 1997 sobre los derechos del paciente ante el tratamiento informático considera que la protección de datos se debe extender a la figura del nasciturus.

— Fallecidos: a este respecto, el Real Decreto 1720/2007, de 21 de diciembre, establece que éste no será de aplicación a los datos referidos a personas fallecidas, si bien las personas vinculadas al fallecido por razones familiares o de hecho, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

— Extranjeros: el Artículo 1 del Convenio nº 108 de 28 de enero de 1981, del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, resolvió esta cuestión al establecer que dicho Convenio es aplicable "*a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona*".

Por otra parte, en el ámbito de actuación de las Administraciones Públicas, el concepto de afectado o interesado en la mayoría de los supuestos va a corresponder con el ciudadano. Ello resulta conforme con la consideración más moderna '*proactiva*' de dicho ciudadano que, en el moderno derecho administrativo, ha pasado de ser considerado en su vertiente meramente pasiva (como 'administrado'), a verse impulsado en su vertiente más activa y de participación en la vida pública como 'ciudadano'.

Ejemplo:

Desde el punto de vista de la normativa de protección de datos, un solicitante de una subvención para una guardería del que se recaben datos de carácter personal para gestionar dicha subvención, es un afectado o interesado. Pero también, desde el punto de vista del Derecho Administrativo, es un ciudadano.

8.5. Consentimiento

"*Toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*." (Art. 3.h LOPD).

Dependiendo de cada caso concreto, el consentimiento podrá solicitarse de manera expresa o tácita, si bien, en ambos casos, se deberá cumplir con lo establecido en el Artículo 5 de la LOPD (derecho de información en la recogida de datos). No obstante, en el caso de los datos especialmente protegidos el consentimiento deberá ser siempre expreso.

Ejemplos:

Para almacenar en un fichero datos relativos a la salud, origen racial o vida sexual de una persona, será necesario su consentimiento expreso, puesto que son datos especialmente protegidos.

Si los datos personales son relativos a la ideología, afiliación sindical, religión y creencias, el consentimiento expreso deberá presentarse por escrito.

Cuando un opositor rellena con sus datos personales la solicitud para participar en un proceso selectivo de acceso a una Administración Pública, nos encontramos ante un consentimiento tácito para recabar y tratar dichos datos personales.

8.6. Cesión de datos

"*Toda revelación de datos realizada a una persona distinta del interesado*." (Art. 3.i LOPD).

Como regla general, los datos personales sólo pueden ser comunicados a una persona o entidad distinta del interesado con el consentimiento inequívoco de éste.

La LOPD ha regulado en diversos artículos, como veremos en la parte de esta Guía relativa al Principio de comunicación de datos, las cesiones de datos. Así, el Artículo 11 de la LOPD denominado 'Régimen general de las cesiones', establece la regla general de consentimiento del afectado o interesado (ciudadano) para que se produzca una cesión de datos personales. Sin embargo, el apartado 2 de dicho precepto regula una serie de excepciones en las que no es necesario el consentimiento para que la cesión tenga lugar. Asimismo, el Artículo 21 de la citada LOPD, regula la comunicación de datos entre Administraciones Públicas, que podrán ser cedidos siempre y cuando se trate del ejercicio de las mismas competencias o de competencias que versen sobre la misma materia.

En relación con las cesiones de datos, el Real Decreto 1720/2007, de 21 de diciembre, define de la siguiente forma los conceptos de destinatario o cesionario y de tercero:

- Destinatario o cesionario: la persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

-Tercero: la persona física o jurídica, pública o privada, u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Asimismo, pueden tener también la condición de terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Ejemplos de cesiones de datos:

Los funcionarios públicos que ejercen la función inspectora, cuando realizan una inspección a un Centro de Servicios Sociales Privado acceden a datos de terceras personas.

Los responsables de ficheros, cualquiera que sea su titularidad, deben ceder los datos de salud a la Administración sanitaria de la Comunidad de Madrid, cuando resulten necesarios para prevenir enfermedades y para realizar estudios epidemiológicos.

En los procedimientos de responsabilidad patrimonial que tramitan las Administraciones Públicas, en ocasiones, el órgano que está tramitando dicho procedimiento necesita acceder a datos personales que obran en ficheros informatizados o manuales de otros órganos de la Administración.

La comunicación de los datos del Padrón Municipal de Habitantes a las Fuerzas y Cuerpos de Seguridad del Estado, siempre y cuando la comunicación obedezca a dos finalidades, que son, la prevención de un peligro real para la seguridad pública o la represión de infracciones penales.

La cesión de los datos de menores nacidos entre 1990 y 1991 para que un organismo pueda realizar una campaña de emisión de cartas sobre una campaña de alcoholismo.

8.7. Responsable del fichero

"*Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decide sobre la finalidad, contenido y uso del tratamiento*." (Art. 3.d LOPD).

Puesto que la LOPD no contiene una definición concreta de lo que debe entenderse por ficheros de titularidad pública y por ficheros de titularidad privada, en el Real Decreto 1720/2007, de 21 de diciembre, se aborda dicha definición.

Así, se entiende que los ficheros de titularidad pública son los ficheros de los que son responsables los Órganos constitucionales o con relevancia constitucional del Estado o las Instituciones Autonómicas con funciones análogas a las mismas, las Administraciones Públicas Territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

Por otra parte, los ficheros de titularidad privada tienen como responsables a las personas, empresas o entidades sometidas al derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que son responsables las corporaciones de derecho público, mientras dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

En relación con los ficheros de titularidad pública, el responsable del fichero siempre será una Administración Pública, un órgano administrativo, o cualquier otro ente de derecho público. Así, en el ámbito de la Administración Pública de la Comunidad de Madrid, podemos encontrarnos, entre otros, los siguientes responsables de ficheros: Direcciones Generales de las Consejerías, Ayuntamientos, Universidades y Corporaciones de derecho público (Colegios Profesionales y Cámaras). En este último caso, el fichero será público siempre y cuando sea creado o gestionado para el ejercicio de potestades de derecho público.

Asimismo, en la disposición general de creación, modificación o supresión del fichero correspondiente se debe indicar quién es el órgano administrativo responsable.

Por otra parte, podemos distinguir las siguientes obligaciones del responsable del fichero:

El responsable del fichero decide la creación del fichero, la finalidad, contenido y uso de los datos almacenados en ese fichero. Además deberá dar respuesta a los ciudadanos cuando éstos ejerciten ante el mismo sus derechos de acceso, rectificación, cancelación y oposición. También deberá adoptar las medidas de seguridad del fichero, ya sean de nivel básico, medio o alto.

En caso de que el responsable del fichero vulnere la legislación sobre protección de datos, se le podrá imputar la comisión de alguna de las infracciones tipificadas en la LOPD.

Si el responsable del fichero pertenece a una Administración Pública del ámbito territorial de una Comunidad Autónoma que cuente con Agencia de Protección de Datos, será ésta la que tramitará el correspondiente procedimiento sancionador, por ser competente para hacerlo.

Si el responsable es una empresa privada o una Administración Pública cuyo ámbito territorial de actuación exceda del de una Comunidad Autónoma, o bien, sin exceder de dicho ámbito territorial no exista en el mismo una Agencia de Protección de Datos de ámbito autonómico, el procedimiento sancionador será tramitado por la Agencia Española de Protección de Datos.

8.8. Encargado del tratamiento

"*Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*." (Art. 3.g LOPD).

El Real Decreto 1720/2007, de 21 de diciembre, ha completado esta definición añadiendo la existencia de una relación jurídica que vincula al encargado del tratamiento con el responsable del fichero. Dicha relación jurídica delimita el ámbito de actuación para la prestación de un servicio. También podrán tener la consideración de encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

En el ámbito de actuación de las Administraciones Públicas, éstas suelen contratar con frecuencia la realización de servicios por cuenta de terceros, tal y como ocurre en el mantenimiento de equipos informáticos, el envío de documentación a particulares o la grabación de datos en ficheros informatizados. La empresa que efectúa estos servicios será la 'encargada del tratamiento'.

Cuando el encargado del tratamiento accede a datos personales no se considera que exista una cesión de datos personales, por lo que no es necesario el consentimiento previo de los afectados. No obstante, la relación entre el responsable del fichero y el encargado del tratamiento deberá quedar formalizada en un contrato por escrito o por cualquier otra forma que permita acreditar su celebración (por *ejemplo*, un convenio), y contenido, en el cual se especifique que el encargado del tratamiento tratará los datos conforme a las instrucciones del responsable del fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Algunos ejemplos serían los siguientes:

La contratación de un hospital con un tercero del almacenamiento, custodia y gestión de las historias clínicas.

La contratación por parte de un Órgano administrativo de una empresa de mailing para enviar cartas a unos opositores a los cuales se les quiere comunicar un acto administrativo del proceso selectivo en el que están participando.

Un convenio realizado entre una Consejería con una Universidad Pública para que ésta realice un trabajo de investigación que afecte a un determinado sector social.

8.9. Procedimiento de disociación

"*Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable*." (Art. 3.f LOPD).

Dicho de otro modo, el dato disociado es aquel que no permite la identificación de un afectado o interesado.

Cuando los datos personales no permiten la identificación de una persona concreta pierden el carácter de personales, quedando al margen de la normativa sobre protección de datos.

Un ejemplo típico de disociación es el realizado para el desarrollo de funciones de estadística.

La utilización de este procedimiento, con carácter previo al acceso y tratamiento de los datos, permite eximir al mismo del cumplimiento de las obligaciones que establece la LOPD. Así, por ejemplo, será innecesario requerir el consentimiento del interesado para poder utilizar esos datos en el tratamiento previsto.

En algunos supuestos, debe actuarse con especial cautela, ya que en ocasiones un dato aparentemente disociado puede asociarse a una determinada persona física. El

ejemplo más claro son los exámenes de oposiciones, ya que, si bien en el examen de un opositor aparece un código numérico que garantiza su anonimato, se puede asociar posteriormente a la persona que corresponda abriendo la plica a la cual se encuentra asociado dicho examen.

8.10. Fuentes accesibles al público

"*Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación*." (Art. 3.j LOPD).

Las fuentes de acceso público se encuentran enumeradas y tasadas por la LOPD. Solamente son consideradas fuentes de acceso público: el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, los Diarios y Boletines Oficiales y los medios de comunicación social.

Respecto a esta enumeración, debemos destacar que Internet no tiene la consideración de fuente accesible al público, de manera que no se podrán tratar los datos personales que aparezcan en una página web para una finalidad distinta de la que motivó su recogida sin consentimiento del titular de dichos datos personales.

Asimismo, para que los supuestos enumerados puedan ser considerados fuentes accesibles al público es necesario que la consulta de dichas fuentes pueda ser realizada por cualquier persona, sin que exista una norma que limite su consulta. Sin embargo, al realizar dicha consulta se podrá exigir una contraprestación.

El Real Decreto 1720/2007, de 21 de diciembre, especifica en relación con las listas pertenecientes a grupos profesionales, qué datos pueden incluirse en estos listados respecto a la dirección profesional. Dichos datos son los siguientes: domicilio postal completo, número telefónico, número de fax y dirección electrónica.

El citado Real Decreto establece específicamente que, en el supuesto de los Colegios Profesionales, podrán indicarse en estos listados como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

8.11. Usuarios

Son usuarios el personal al servicio del responsable del fichero o encargado del tratamiento, que tenga acceso a los datos de carácter personal como consecuencia de tener encomendadas tareas de utilización material de los datos almacenados o que se almacenarán en los ficheros.

Los usuarios deben cumplir con las medidas de seguridad establecidas para el uso de los datos personales y están sujetos al deber de secreto, teniendo en cuenta, además, que los usuarios son los que mantienen un contacto directo con los datos personales, y en muchas ocasiones, directamente con las personas titulares de los datos. En este sentido, la relación de usuarios que puedan acceder al correspondiente fichero debe estar en todo momento actualizada en el documento de seguridad.

Aunque los usuarios no tienen capacidad de decisión en la gestión del tratamiento de datos, es de vital importancia que éstos conozcan y se atengan fielmente a las disposiciones establecidas en la LOPD. En consecuencia, todo órgano administrativo debe responsabilizarse de la formación de sus empleados en materia de protección de datos.

Así, por ejemplo:

Un empleado público que accede al fichero de personal de su respectivo órgano administrativo para tramitar una excedencia voluntaria de un compañero/a tiene la consideración de usuario.

8.12. Transferencias internacionales

"*El transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o cualquier otro medio convencional, siempre y cuando dicho transporte tenga lugar fuera del territorio nacional.*" (Art. 1.6 y 3 Real Decreto1332/1994, de 20 de junio).

La LOPD regula en su Título V el Movimiento Internacional de Datos, estableciendo que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento, o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

El carácter adecuado del nivel de protección que ofrece el país de destino será evaluado por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

No obstante lo anterior, existen una serie de excepciones:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que forme parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, establece que el Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable a la LOPD. Esta lista se publicará y mantendrá actualizada a través de medios informáticos y telemáticos.

En relación a estas transferencias internacionales en el ámbito de la Comunidad de Madrid, de conformidad con la Disposición Adicional Segunda del Decreto 99/2002, de 13 de junio, si el proyecto de disposición de creación o modificación de un fichero contemplara la posibilidad de transferencias internacionales de datos, será necesario que, con carácter previo al informe preceptivo de la Agencia de Protección de Datos de la Comunidad de Madrid, se pronuncie la Agencia Española de Protección de Datos en los términos previstos en el Artículo 37.l) de la LOPD.

Por otra parte, el Real Decreto 1720/2007, de 21 de diciembre, precisa la definición de transferencia internacional al considerar la transferencia internacional de datos como el "*tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español*".

Asimismo, dicho Real Decreto también define los conceptos de exportador de datos personales e importador de datos personales de la siguiente forma:

"*Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una transferencia de datos de carácter personal a un país tercero*.

I*mportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero*".

9

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

9. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los Principios de la Protección de Datos se encuentran regulados en el Título II de la LOPD. Estos principios constituyen la base mediante la cual se articula el derecho fundamental a la Protección de Datos de Carácter Personal, siendo de obligado cumplimiento desde el momento en que se produce la recogida de datos de un afectado o interesado (ciudadano), siempre y cuando dichos datos sean almacenados en un fichero, ya sea informatizado, manual o parcialmente automatizado.

Debido a su carácter obligatorio, el responsable del fichero y, en su caso, el encargado del tratamiento, deben adoptar las medidas necesarias para que no se produzca una vulneración de los mismos. También deben ser conocidos y respetados por los usuarios de los ficheros con datos personales, ya que éstos son los que, en la mayoría de los casos, van a proceder a la recogida y tratamiento de los datos de los afectados o interesados. En este sentido, una buena política de protección de datos en un órgano administrativo conlleva que todo el personal adscrito a ese órgano conozca y respete estos Principios.

El incumplimiento de los Principios de Protección de Datos puede suponer una lesión del derecho fundamental de la protección de datos de los afectados o interesados, y la comisión de una infracción susceptible de ser sancionada, aplicándose, en estos casos, el régimen sancionador correspondiente, dependiendo de la naturaleza pública o privada del responsable del fichero o encargado del tratamiento infractor.

Por otra parte, el Real Decreto 1720/2007, de 21 de diciembre, también se refiere en su articulado a los Principios de Protección de Datos, llevándose a cabo un desarrollo de los mismos.

9.1. Principio de calidad de los datos

Este Principio, regulado en el Artículo 4 de la LOPD, introduce un criterio de racionalidad y proporcionalidad en el tratamiento de los datos personales. Aparece en el Considerando 28 de la Directiva 95/46/CE que dice:

"*Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal respecto al interesado; que debe referirse en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originariamente especificados*."

En este sentido, y como manifestación de este Principio, podemos distinguir lo siguiente:

a) Recogida de datos adecuados, pertinentes y no excesivos.

Sólo se podrán solicitar aquellos datos que sean estrictamente necesarios para la finalidad para la cual se procede a la recogida de los mismos.

Ejemplo:

En una subvención que se va a otorgar sin valorar si la persona está afectada o no por una minusvalía, no debe solicitarse este dato, puesto que no va a ser baremado.

b) Finalidad.

Los datos personales recabados sólo podrán utilizarse para el fin que motivó su recogida, no pudiendo utilizarse para una finalidad incompatible. Esta finalidad debe estar descrita en la disposición de carácter general que haya creado el fichero en el cual se almacenan esos datos.

Respecto a la finalidad podemos citar la Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional de 8 de febrero de 2006:

'*[...] aunque el artículo 4.2 de la Ley 15/99, en contraposición con el artículo 4.2 de la Ley 5/92, ya no se refiere a "finalidades distintas": sino a "finalidades incompatibles": revelando una ampliación de la posibilidad de utilización de los datos, sin embargo la interpretación sistemática del precepto y la ambigüedad del término "finalidades incompatibles" avalan la interpretación realizada en el acto administrativo impugnado. En efecto, según el diccionario de la Real Academia "incompatibilidad" significa "repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre sí", por tanto, una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida e ilimitada de finalidades, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que "semejante interpretación conduce al absurdo y como tal ha de rechazarse", como hemos declarado en Sentencia de 8 de febrero de 2002. Teniendo en cuenta, además, que dicho término se introduce en el Ley de 1999, como ha declarado la doctrina, por una traducción poco precisa del artículo 6 de la Directiva 46/1995, de 24 de octubre*.'

También podemos citar la Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que dice: "*Las normas de la LOPD deben bastar, y no se trata de hacer ninguna innovación al respecto, pero sí de establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración*."

Ejemplo:

Los datos del Padrón Municipal de Habitantes pueden usarse para enviar información a los vecinos sobre la apertura de un nuevo Centro de Servicios Sociales (finalidad compatible). Sin embargo, no pueden utilizarse para enviar una felicitación de navidad o para pedir el voto (finalidad incompatible).

La LOPD no considera incompatible el uso posterior de los datos para fines históricos, estadísticos o científicos. Para determinar estos fines se recurrirá a la legislación que, en cada caso, resulte aplicable, y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública, la Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español y la Ley 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación Científica y Técnica. En la Comunidad de Madrid, se recurrirá, además, a lo dispuesto en la Ley 12/1995, de 21 de abril, de Estadística de la Comunidad de Madrid, la Ley 10/1998, de 9 de julio, de Patrimonio Histórico de la Comunidad de Madrid, y la Ley 5/1998, de 7 de mayo, de Fomento de la Investigación Científica y la Innovación Tecnológica.

Ejemplo:

Como regla general, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, permite el uso de las historias clínicas para fines de investigación y docencia, siempre y cuando los datos de identificación personal del paciente estén separados de los de carácter clínico-asistencial de manera que se garantice su anonimato. Por lo tanto, deben separarse dichos datos, salvo que el paciente haya dado su consentimiento para no separarlos.

c) Exactitud, veracidad y rectificación de oficio.

La LOPD exige que los datos de carácter personal sean exactos y estén puestos al día de forma que respondan con veracidad a la situación del afectado o interesado. Si los datos fueron recogidos directamente del afectado o interesado se considerarán exactos los facilitados por éste.

El Real Decreto 1720/2007, de 21 de diciembre, en relación con la exactitud, veracidad y rectificación de oficio, establece en su Artículo 8.5 lo siguiente:

"*Cuando los datos de carácter personal sometidos a tratamiento sean inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello*.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio de los derechos por parte de los interesados reconocidos en la LOPD."

La Sentencia de 15 de diciembre de 2000 del Tribunal Superior de Justicia ha interpretado la exactitud, veracidad y rectificación de oficio de los datos de la siguiente forma:

"*De tal modo que […] tiene que realizar de oficio frecuentes barridas a fin de sacar del[…]aquellos datos que no sean ciertos y así, habiendo sido abonada la letra el 29 de marzo de 1995, continuó manteniendo a D.[…] dos años después de haber pagado su deuda*."

Ejemplo:

No envíe una comunicación a un afectado o interesado (ciudadano) cuya dirección postal no sea correcta.

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, establece la verificación de los datos facilitados por las Administraciones Públicas, de manera que cuando se formulen solicitudes por medios electrónicos en las que el interesado (ciudadano) declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos.

d) Derecho de acceso.

La LOPD establece que los datos de carácter personal deben almacenarse de forma que permitan el ejercicio del derecho de acceso de los afectados o interesados. No es posible alegar como causa para denegar el derecho de acceso la imposibilidad de realización del mismo como consecuencia del modo en que los datos están almacenados.

e) Cancelación de datos innecesarios

Otra manifestación del Principio de Calidad de Datos regulado en el Artículo 4 de la LOPD es la cancelación de los datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La cancelación es el procedimiento en virtud del cual el responsable del fichero cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

En el supuesto de que los datos resulten inadecuados o excesivos, la cancelación conlleva la supresión de los mismos.

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, especifica que podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado. Cumplido este período, los datos sólo podrán ser conservados previa disociación de los mimos, sin perjuicio de la obligación de bloqueo prevista en la LOPD. Asimismo, dicho Real Decreto establece también, como ya se ha dicho anteriormente, que la cancelación dará lugar a que se supriman los datos que resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme al citado Real Decreto.

También pueden mantenerse los datos personales, no dando lugar a la cancelación cuando atendiendo a los valores históricos, estadísticos y científicos, de acuerdo con la legislación específica anteriormente mencionada, se decida su mantenimiento.

El Real Decreto 1720/2007, de 21 de diciembre, regula el procedimiento mediante el cual se autoriza la conservación de datos para fines históricos, estadísticos o científicos. Este procedimiento se inicia mediante una solicitud del responsable del fichero dirigida a la Autoridad de Control competente (Agencia Española de Protección de Datos o Agencias de Protección de Datos autonómicas) en la cual justifique la existencia de los valores anteriormente citados. El plazo para resolver la solicitud es de tres meses, considerándose el silencio administrativo positivo.

f) Prohibición de recogida fraudulenta de datos.

El último requisito que establece el Artículo 4 de la LOPD respecto al Principio de calidad de los datos es la prohibición de la recogida de datos personales por medios fraudulentos, desleales e ilícitos, tipificando como infracción muy grave la recogida en dichos términos.

9.2. Principio de información en la recogida de datos

Cuando se lleva a cabo la recogida de datos personales de un afectado o interesado (ciudadano), el responsable del fichero debe informarle de lo siguiente:

a) Que sus datos van a ser almacenados en un fichero, la finalidad para la que se recogen y los destinatarios de la información.

b) Si es obligatoria o no su respuesta a las distintas preguntas que se le planteen.

c) Las consecuencias de la obtención de los datos o de su negativa a suministrarlos.

d) La posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

e) La identidad y dirección del responsable del fichero.

Esta comunicación se podrá facilitar al afectado o interesado (ciudadano) por cualquier medio que permita asegurar que ha recibido la información que contempla este principio: de palabra, por escrito en el propio formulario, impreso o encuesta en la que se recojan sus datos, o en documento aparte, mediante carteles o anuncios situados en el lugar donde vayan a recabarse los datos que completen aquella información que no se facilite de palabra o en el impreso en que se recaben los datos, etc. No es admisible una información genérica que no permita saber quién es el responsable del fichero y para qué se están recabando los datos.

Se debe cumplir con este Principio de información cualquiera que sea el procedimiento de recogida de datos. Estos procedimientos pueden ser de diversos tipos: formularios, encuestas, entrevistas, transmisión electrónica de datos, registros públicos, directorios electrónicos, currículos, páginas Web o teléfono.

Cuando los órganos administrativos del ámbito territorial de la Comunidad de Madrid utilizan estos procedimientos para la recogida de datos personales, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda usar una cláusula-tipo con la que se dé cumplimiento a este principio.

Conviene recordar de nuevo el contenido de dicha cláusula-tipo, que puede descargase del Canal Servicios de la página Web de la Agencia, www.apdcm.es, cuyo contenido es:

"*Los datos personales recogidos serán incorporados y tratados en el fichero (indicar nombre), cuya finalidad es (describirla) y podrán ser cedidos a (indicar), además de otras cesiones previstas en la Ley. El órgano responsable del fichero es (indicarlo), y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es (indicarla). Todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*."

En todo caso, el deber de información deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse prueba del mismo mientras persista el tratamiento de datos del afectado. Así, el responsable del fichero deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero podrá utilizar medios informáticos o telemáticos. En particular, podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

En el caso de menores de edad, cuando el tratamiento se refiera a datos de éstos, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible.

Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por padres, tutores o representantes.

No será necesaria la información referente a si es obligatoria o no su respuesta a las preguntas que se le planteen, las consecuencias de la obtención de los datos o de su negativa a suministrarlos, y la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, si su contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Muchas veces resulta fácilmente discernible si es necesario o no facilitar el dato que se está demandando, atendiendo a la naturaleza de la relación entre el responsable del fichero y el interesado, así como a las consecuencias de no facilitar determinada información, sobre todo en los supuestos de relaciones con las Administraciones Públicas.

Ejemplo:

Cuando se solicitan datos para la tramitación de una subvención, resulta obvio que es obligatorio ofrecer esos datos para dicha tramitación, dado que en caso de no suministrarlos no se podrá tramitar la solicitud de dicha subvención. No obstante, sólo se deberá solicitar aquellos datos que sean estrictamente necesarios para la tramitación de la citada subvención.

Por otra parte, 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). El supuesto más claro en que se debe cumplir

con este deber de información es cuando se produce una cesión de datos personales. La obligación de informar de la cesión, y en consecuencia obtención de los datos, recae sobre el cesionario.

No es preciso cumplir con el requisito de informar a posteriori al interesado o afectado (ciudadano) cuando los datos no se hayan recabado directamente de él, en los siguientes supuestos:

- Cuando una ley lo prevea.
- Cuando el tratamiento tenga fines históricos, estadísticos o científicos.
- Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos, o en su caso, Agencias de Protección de Datos autonómicas, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Respecto a esta última posibilidad de exención del deber de información, el Real Decreto 1720/2007, de 21 de diciembre, regula el procedimiento para determinar si debe aplicarse dicha exención. Este procedimiento se inicia mediante solicitud del responsable del fichero en la cual deberá justificar que es imposible o que exige esfuerzos desproporcionados cumplir con el deber de información al interesado, debiendo acompañar una cláusula informativa mediante la cual se compense la exención de dicho deber. El procedimiento tiene una duración máxima de seis meses, considerándose el silencio administrativo positivo.

No sólo cláusula informativa, como se dice, sino también 'medidas compensatorias', que en la práctica se resuelven obligando al responsable del fichero, por ejemplo, a informar a los interesados a través de un anuncio en los medios de comunicación social –prensa escrita–.

9.3. Principio de consentimiento

La LOPD exige la prestación del consentimiento previo e inequívoco del afectado para el tratamiento de sus datos, recayendo sobre el responsable del fichero la obligación de obtener el consentimiento del interesado. La solicitud de dicho consentimiento debe ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para la que se recaba, así como de las restantes condiciones que concurran en el tratamiento.

En el caso del consentimiento de los menores de edad, nos remitimos al apartado referente a los menores que ha sido analizado anteriormente.

El afectado o interesado (ciudadano) debe prestar su consentimiento de manera libre, inequívoca, específica e informada, pudiendo manifestar el consentimiento de forma

expresa o tácita. En ningún caso podrá entenderse prestado de forma presunta. Además, corresponderá al responsable del fichero la prueba de la existencia del consentimiento del afectado.

No obstante lo anterior, la LOPD recoge una serie de supuestos en los que no es necesario prestar el consentimiento:

a) Cuando una ley así lo dispone. Obsérvese que se hace referencia a una norma con rango de Ley, no bastando cualquier otro tipo de norma. Estamos ante un claro supuesto de reserva legal.

Esta excepción se encuentra ligada a numerosos supuestos de cesión y a otras formas de tratamiento de datos personales, algunos de los cuales veremos a continuación. Por ejemplo, cuando la Agencia Tributaria solicita datos personales para el ejercicio de sus funciones.

b) Cuando los datos son recogidos para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.

El uso de cámaras de video vigilancia en la entrada a las dependencias de las Consejerías de la Comunidad de Madrid, ya que una de las funciones de la Administración de la Comunidad de Madrid es garantizar la seguridad de edificios públicos.

c) Cuando se refieren a las partes de un contrato o precontrato de una relación *negocial*, laboral o administrativa y los datos personales son necesarios para el mantenimiento y cumplimiento de ésta.

Cuando los datos personales son usados para elaborar una tarjeta para el control de fichaje no es necesario que se preste el consentimiento, puesto que uno de los deberes que tienen los empleados públicos es el cumplimiento de la jornada laboral.

Algunas Administraciones Públicas utilizan como sistema de control horario la huella dactilar de los empleados públicos. La huella dactilar forma parte de lo que se conoce con el nombre de "datos biométricos", entre los que también se incluye el iris o la voz.

En este sentido, la Sentencia de 2 de julio de 2007 de la Sala de lo Contencioso-Administrativo del Tribunal Supremo ha legitimado el uso de la huella para el control horario de los trabajadores. Considera el Tribunal Supremo que "*cumplir con el control horario es una obligación inherente a la relación que une a los funcionarios con la Administración, no siendo necesario obtener previamente su consentimiento ya que el artículo 6.2 de la LOPD lo excluye en estos casos. Asimismo, no hay norma que prohíba el recurso a la tecnología escogida para realizar el control del cumplimiento del horario de trabajo. Su novedad o complejidad no la convierten en lesiva de los derechos fundamentales invocados*".

d) Cuando el tratamiento resulte necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

Esta excepción también se aplicará cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento..

e) Cuando los datos figuren en fuentes accesibles al público. En este punto, conviene recordar que dichas fuentes están enumeradas de forma limitativa en la LOPD, tal y como se indicó al exponer su definición.

En relación con este Principio de consentimiento podemos citar también el Artículo 6.2 b) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos que establece que "*los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa el derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la LOPD, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos*".

En todo caso, la excepción del consentimiento no exime de la obligación de informar en los términos expuestos en el punto anterior, relativo al Principio de información, ni permite el tratamiento de cualquier dato, sino únicamente de aquellos que cumplan con el Principio de calidad (datos adecuados, pertinentes y no excesivos).

En todo caso, el interesado o afectado (ciudadano) puede revocar su consentimiento cuando exista causa justificada para ello. En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, exige que la revocación pueda producirse a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. Por ejemplo, puede utilizarse para ello un número gratuito de teléfono o, en el ámbito de las Administraciones Públicas, acudiendo a las Oficinas de Atención al Ciudadano.

En ningún caso el responsable del fichero podrá exigir que esta revocación tenga lugar mediante cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o, como ya se ha citado anteriormente, mediante cualquier medio que implique un coste adicional al interesado.

Cuando el responsable del fichero reciba la solicitud de revocación del consentimiento deberá cesar en el tratamiento de datos del interesado en el plazo máximo de diez días a contar desde la recepción de la solicitud, sin perjuicio de la obligación de bloqueo de datos, conforme a lo dispuesto en el Artículo 16.3 de la LOPD.

En caso de que los datos hayan sido cedidos previamente, el responsable del fichero, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios para que en el plazo de diez días cesen en el tratamiento de dichos datos en caso de que aún lo mantuvieran.

9.4. Datos especialmente protegidos

Los datos especialmente protegidos son aquellos que revelan la ideología, afiliación sindical, religión y creencias de una persona física, y que sólo con el consentimiento expreso y por escrito del afectado pueden ser objeto de tratamiento.

Son también datos especialmente protegidos los que hacen referencia al origen racial, a la salud y a la vida sexual, que sólo podrán ser recabados cuando, por razones de interés general, así lo disponga una Ley o el afectado lo consienta expresamente.

Esta especial protección se fundamenta en los Artículos 10 y 16.2 de la Constitución y en el Convenio Europeo para la Protección de los Derechos de las Personas con respecto al tratamiento automatizado de datos de carácter personal, firmado en Estrasburgo el 28 de enero de 1981 (ratificado por España en fecha 27 de enero de 1982), y se justifica en el hecho de que, debido a la información a la que se refiere este tipo de datos, el tratamiento indebido de los mismos, además de lesionar el derecho fundamental a la protección de datos, podría dañar otros derechos fundamentales.

Por ejemplo, el derecho a la libertad de pensamiento o a la libertad religiosa, puede ser lesionado por el tratamiento de datos relativos a la ideología o las creencias sin las debidas garantías.

Precisamente para evitar estos riesgos, la LOPD establece en su Artículo 7 una serie de refuerzos, con el fin de que se preste especial cuidado en el tratamiento de estos datos, de manera que:

— Reitera el mandato constitucional de que nadie puede ser obligado a declarar sobre su ideología, religión o creencias; lo que afecta al modo específico de cumplimiento del Principio de información que se ha analizado anteriormente (obligación de informar de qué datos son obligatorios o no, y de las consecuencias de que no se suministren los datos que se soliciten).

— Exige el consentimiento expreso y por escrito del afectado si los datos son de ideología, afiliación sindical, religión o creencias; y consentimiento expreso cuando los datos se refieran al origen racial, la salud o la vida sexual.

— En el caso de la comisión de una infracción que afecte a este tipo de datos será tipificada como muy grave.

— En materia de medidas de seguridad, los ficheros que contengan este tipo de datos, deberá adoptar seguridad de nivel alto.

Sin embargo, existe una excepción en virtud de la cual no será necesario el consentimiento expreso y por escrito para el tratamiento de los datos especialmente protegidos: cuando se trate de ficheros mantenidos por partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros. No obstante, también en estos casos será necesario el consentimiento previo del afectado en caso de que se vayan a ceder este tipo de datos.

Mención aparte merecen los datos de salud que, como ya se ha indicado anteriormente se encuentran dentro de la categoría de datos especialmente protegidos, y sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente.

Podemos definir este tipo de datos como las informaciones concernientes a la salud pasada, presente y futura, física y mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

No obstante lo anterior, la propia LOPD establece una excepción en la que no es necesario el consentimiento expreso y por escrito del afectado para el tratamiento de datos que hagan referencia al origen racial, a la salud o a la vida sexual. Esta excepción tiene lugar cuando el tratamiento de los datos especialmente protegidos resulte necesario para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto.

Esta misma excepción concurrirá cuando el tratamiento de los datos especialmente protegidos sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar tal consentimiento. Esta circunstancia deriva de la lógica prevalencia del derecho a la vida sobre el derecho a la protección de datos.

A este respecto, conviene citar la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, cuyo Artículo 8 regula el consentimiento informado de la siguiente manera:

"*1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4 de esta Ley, haya valorado las opciones propias del caso.*

2. El consentimiento será verbal por regla general. Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente.

3. El consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos.

4. Todo paciente o usuario tiene derecho a ser advertido sobre la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen en un proyecto docente o de investigación, que en ningún caso podrá comportar riesgo adicional para su salud."

En relación con el consentimiento, la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, establece en su Artículo 27.4 que "el ciudadano como paciente tiene derecho a conocer la identidad de su médico o facultativo, quien será responsable de proporcionarle toda la información necesaria que requiera, para poder elegir y, en su caso, otorgar su consentimiento a la realización de los procedimientos diagnósticos, terapéuticos, profilácticos y otros, que su estado de salud precise".

No obstante lo anterior, el Artículo 9 de la Ley 41/2002, de 14 de noviembre, regula los límites del consentimiento informado:

"*1. La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso. Cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención.*

2. Los facultativos podrán llevar a cabo las intervenciones clínicas indispensables a favor de la salud del paciente, sin necesidad de contar con su consentimiento, en los siguientes casos:

a) Cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas.

b) Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho a él."

9.5. Principio de seguridad de los datos

El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales integrados en los ficheros, evitando que éstos puedan perderse, alterarse, usarse o ser accesibles a personas no autorizadas.

Las medidas de seguridad se adoptarán tomando en consideración el 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.

Las medidas de seguridad de los ficheros informatizados y no informatizados (manuales) están reguladas en el Real Decreto 1720/2007, de 21 de diciembre, que distingue entre medidas de seguridad de nivel básico, medio y alto.

Nivel básico: todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad de nivel básico.

Nivel medio: los ficheros o tratamientos de datos de carácter personal que contengan datos relativos a la comisión de infracciones administrativas o penales; aquéllos cuyo funcionamiento se rija por el Artículo 29 de la LOPD (prestación de servicios de información sobre solvencia patrimonial y crédito); aquéllos de los que sean responsables Administraciones tributarias y se relación con el ejercicio de sus potestades tributarias; aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros; aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias; aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; y aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o comportamiento del individuo.

Nivel alto: los ficheros o tratamientos de datos de carácter personal que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual; los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas; y los que contengan datos derivados de actos de violencia de género.

En los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicará, además de las medidas de nivel básico y medio, la medida de seguridad alta relativa al registro de accesos.

No obstante lo anterior, el Real Decreto 1720/2007, de 21 de diciembre, regula dos excepciones respecto a las medidas de seguridad de nivel alto: los ficheros que contengan datos relativos a la ideología, afiliación sindical, religión o creencias, así como a la salud, cuya finalidad sea únicamente la transferencia dineraria a las entidades de las que los afectados sean asociados o miembros o se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria contengan datos sin guardar relación con su finalidad; y los ficheros que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos (por ejemplo, un fichero de nóminas). En estos casos se deberán adoptar las medidas de seguridad de nivel básico.

Las medidas de seguridad incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos descritos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, establece las medidas de seguridad de los ficheros informatizados en los siguientes artículos:

- Artículos 89 a 94, regulan las de nivel básico (Documento de Seguridad; funciones y obligaciones del personal; registro de incidencias; control de acceso; gestión de soportes y documentos; identificación y autentificación; copias de respaldo y recuperación).

- Artículos 95 a 100, las de nivel medio (Responsable de Seguridad; auditoría; gestión de soportes y documentos; identificación y autentificación; control de acceso físico; registro de incidencias).

- Artículos 101 a 104, las de nivel alto (gestión y distribución de soportes, copias de respaldo y recuperación; registro de accesos; telecomunicaciones).

Por otra parte, una de las principales novedades del Real Decreto 1720/2007, de 21 de diciembre, es que por primera vez se regulan las medidas de seguridad para los

ficheros no automatizados (manuales). En este sentido, se han seguido algunas de las medidas de seguridad contenidas en la Recomendación 2/2004, de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas, y en la Recomendación 1/2005, de 5 de agosto, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre Archivo, Uso y Custodia de la Documentación que compone la Historia Social no informatizada por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid.

La primera novedad introducida por el Real Decreto 1790/2007, de 21 de diciembre, es la previsión de que las medidas de seguridad 'genéricas' de los ficheros automatizados resultan de aplicación a los ficheros no automatizados. Estas medidas son, entre otras, la elaboración del documento de seguridad –que suele ser un documento en formato papel, o en su caso, un documento en Word o PDF; las obligaciones respecto al encargado del tratamiento, cuyo acceso deberá estar delimitado en el documento de seguridad; y el régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento –debiendo ser autorizado este supuesto por el responsable o encargado– constando dicha autorización en el documento de seguridad.

Partiendo de los tres niveles de seguridad descritos anteriormente, se enumeran las medidas de seguridad que deben ser adoptadas por el responsable del tratamiento en los ficheros no automatizados en función de dicho nivel de seguridad.

Sin perjuicio de la adopción de estas medidas de seguridad, el Real Decreto 1720/2007, de 21 de diciembre, contiene, además, tres criterios específicos para los ficheros no automatizados, que son los siguientes: los criterios referentes al archivo, con una referencia a la legislación aplicable en esta materia que será la relativa a la normativa que regula los Archivos; los referentes a los dispositivos de almacenamiento, que deberán disponer de mecanismos que obstaculicen su apertura; y los referentes a la custodia de soportes, en virtud de los cuales la persona encargada de la custodia, mientras la documentación en formato papel esté en proceso de revisión o tramitación, deberá vigilarla e impedir que cualquier persona no autorizada pueda acceder a ella.

Por último en el supuesto de los ficheros parcialmente automatizados ("mixtos"), la parte del fichero que sea automatizada deberá adoptar las medidas de seguridad de acuerdo con lo establecido para dichos ficheros automatizados, mientras que la parte de ese mismo fichero que no sea automatizada, adoptará las referentes a los ficheros no informatizados, si bien, a efectos de la creación del fichero, en la disposición general de creación y en su inscripción en el Registro se realizarán las más altas de las que puedan corresponderles.

En conclusión:

El Real Decreto 1720/2007, de 21 de diciembre, regula las medidas de seguridad para los ficheros informatizados y no informatizados.

Una de las obligaciones del responsable del fichero es adoptar las medidas de seguridad, ya sean de nivel básico, medio o alto.

9.6. Deber de secreto

El deber de secreto, respecto a los datos personales tratados, es una obligación que corresponde al responsable del fichero, al encargado de tratamiento, si lo hubiera, y a todos aquellos que intervengan en cualquier fase del tratamiento de datos de carácter personal. Esta obligación se mantiene incluso finalizada la relación que permitió el acceso al fichero.

No debe confundirse este Deber de secreto con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen. Este Deber de secreto es un deber genérico que alcanza a cualquier persona que intervenga en el tratamiento de los datos.

La Agencia de Protección de Datos de la Comunidad de Madrid recomienda la inclusión de cláusulas específicas en esta materia en los contratos laborales que suscriban las Administraciones Públicas de su ámbito de actuación con empleados públicos, según un texto que podría ser el siguiente:

"El trabajador se compromete a guardar secreto sobre las informaciones confidenciales y los datos de carácter personal de los que tenga conocimiento en el ejercicio de las funciones que le sean encomendadas, de conformidad con lo establecido en el Artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el Artículo 11 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, incluso tras haber finalizado su relación profesional con la Administración Pública contratante.

El trabajador deberá cumplir con el resto de principios y obligaciones establecidos por la normativa de protección de datos.

Igualmente, el trabajador estará obligado a atender las instrucciones relativas a la seguridad de los datos de carácter personal contenidas en las políticas de seguridad y en el documento de seguridad y difundidas, en su caso, por el responsable del fichero o el responsable de seguridad, de conformidad con lo establecido en el Real Decreto

1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."

Esta cláusula se encuentra disponible en la página Web de la Agencia, www.apdcm.es, Canal Servicios.

9.7. Principio de comunicación de datos

La comunicación o cesión de datos personales tiene lugar cuando los datos del afectado o interesado (ciudadano) se comunican a un tercero. Dos son los requisitos necesarios para que se produzca la cesión de datos personales: primero, que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario; segundo, el consentimiento previo del interesado.

Sin embargo, existen una serie de supuestos regulados en la LOPD en relación con los cuales no es necesario el segundo de los requisitos. En estos casos, la cesión de datos personales tiene lugar sin el consentimiento previo del afectado o interesado. Dichos supuestos, regulados en el Artículo 11.2 de la LOPD, son los siguientes:

a) Cuando la cesión esté autorizada por una ley.

Debe tratarse de una norma con rango de ley formal (Ley Orgánica, Ley Ordinaria, Real Decreto-Ley, Real Decreto Legislativo, Ley Autonómica, etcétera), no siendo posible que la cesión de datos personales se ampare en una norma de carácter reglamentario. Un ejemplo claro de cesión amparada en una ley es la del Artículo 94 de la Ley 58/2003, de 17 de diciembre, General Tributaria, que dice lo siguiente:

"1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones. Asimismo, participarán en la gestión o exacción de los tributos mediante las advertencias, repercusiones y retenciones, documentales o pecuniarias, de acuerdo con lo previsto en las Leyes o disposiciones reglamentarias vigentes.

2. A las mismas obligaciones quedarán sujetos los partidos políticos, sindicatos y asociaciones empresariales.

3. Los juzgados y tribunales deberán facilitar a la Administración tributaria, de oficio o a requerimiento de la misma, cuantos datos con trascendencia tributaria se desprendan de las actuaciones judiciales de las que conozcan, respetando, en su caso, el secreto de las diligencias sumariales.

4. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, así como la Secretaría de ambas comisiones, facilitarán a la Administración tributaria cuantos datos con trascendencia tributaria obtengan en el ejercicio de sus funciones, de oficio, con carácter general o mediante requerimiento individualizado en los términos que reglamentariamente se establezcan.

Los órganos de la Administración tributaria podrán utilizar la información suministrada para la regularización de la situación tributaria de los obligados en el curso del procedimiento de comprobación o de inspección, sin que sea necesario efectuar el requerimiento al que se refiere el apartado 3 del artículo anterior.

5. La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."

b) Cuando se traten datos recogidos de fuentes accesibles al público.

Como ya veíamos en el apartado referente a conceptos, sólo tienen la consideración de fuentes accesibles al público, a efectos de protección de datos: el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos profesionales, los Diarios y Boletines Oficiales y los medios de comunicación.

En relación con los Boletines y Diarios Oficiales, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece en su Artículo 11 que "*la publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano o Entidad competente tendrá, en las condiciones y garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa.*

La publicación del Boletín Oficial del Estado en la sede electrónica del organismo competente tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables".

No obstante lo anterior, y de conformidad con la Disposición Final Segunda de la Ley 11/2007, de 22 de junio, la publicación electrónica del Boletín Oficial del Estado tendrá carácter y los efectos previstos en el Artículo 11.2 de la presente Ley desde el 1 de enero de 2009.

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, siempre que se limite a la finalidad que la justifique.

Al igual que no era necesario el consentimiento para recabar los datos de una persona si los datos se referían a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa, tampoco lo será para comunicar (ceder) los datos a un tercero, siempre que sea preciso y necesario para el cumplimiento y control de la relación jurídica establecida. Esta relación jurídica puede ser de carácter laboral, administrativa, asociativa, corporativa, negocial, contractual.

Por ejemplo, la cesión de datos personales de unos médicos de un hospital de la Comunidad de Madrid, en el cual trabajaban, a otro hospital de la Comunidad de Madrid al cual han sido trasladados.

d) Cuando la comunicación tenga por destinatarios 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. Igualmente a Instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

Por ejemplo, cuando en el marco de un procedimiento judicial, un Juez o Tribunal solicita documentación con datos personales a un órgano de la Administración.

e) Cuando la cesión de datos 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.

Nuevamente se reitera el criterio de que en caso de colisión de los derechos a la vida o integridad física y el derecho a la protección de datos, debe prevalecer el primero.

En el supuesto de que la finalidad sea la realización de estudios epidemiológicos, con el objeto de velar por la salud desde un punto de vista preventivo, la cesión de datos para estos fines podrá efectuarse sin consentimiento del interesado, siempre que el estudio epidemiológico se realice en los términos que establezca la legislación específica sobre sanidad. En este sentido, la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid dispone que los datos relativos a la

salud serán cedidos a la Administración Sanitaria de la Comunidad de Madrid por parte de los responsables de los ficheros, cualquiera que sea su titularidad, cuando resulten necesarios para prevención de la enfermedad, o la realización de estudios epidemiológicos. Asimismo, como ya hemos analizado, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, exige que los datos de identificación personal del paciente se separen de los de carácter clínico-asistencial, de forma que, como regla general, quede asegurado el anonimato del paciente, salvo que haya dado su consentimiento para no separarlos.

f) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Por ejemplo, la cesión de datos al Instituto de Estadística de la Comunidad de Madrid para realizar un estudio estadístico sobre una determinada materia.

La regulación de las cesiones de datos personales entre Administraciones Públicas se completa con el régimen jurídico previsto en el Artículo 21 de la LOPD. En virtud de dicho artículo, podemos distinguir otras dos cesiones de datos personales entre Administraciones Públicas en las que no es necesario el consentimiento del afectado o interesado:

— Cuando la cesión de datos personales entre las Administraciones Públicas tenga lugar para el ejercicio de las mismas competencias.

Ejemplo:

La cesión de datos de carácter personal de la Consejería de Familia y Asuntos Sociales a la Concejalía de Servicios Sociales de un Municipio, relativos a las personas con discapacidad residentes en el mismo, al objeto de constituir un Censo Municipal que facilite una acción eficaz y óptima de los recursos existentes y en orden al desarrollo de las competencias que legalmente corresponden al citado municipio, está amparada en la Ley 11/2003, de 27 de marzo, de Servicios Sociales de la Comunidad de Madrid.

— En el supuesto en que se trate de datos personales que una Administración obtenga o elabore con destino a otra.

Ejemplo:

Los escritos, solicitudes y comunicaciones que en virtud del Artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, pueden presentarse en cualquiera de los Registros de la Administración General del Estado, Comunidades Autónomas y Municipios.

Por otra parte, el Real Decreto 1720/2007, de 21 de diciembre, contiene un artículo referente a los supuestos que legitiman el tratamiento o cesión de los datos. Este artículo dice lo siguiente:

"*1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.*

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de Ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

— El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

— El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de Ley.

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de Ley o una norma de derecho comunitario de aplicación directa.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

4. *Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:*

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) 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 o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la Ley les atribuya expresamente.

c) La cesión entre Administraciones Públicas cuando concurra uno de los siguientes supuestos:

— Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

— Los datos de carácter personal hayan sido recogidos o elaborados por una Administración Pública con destino a otra.

— La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. *Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.*

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud."

9.8. Acceso a los datos por cuenta de terceros

Avanzamos algo sobre este principio cuando nos referimos a la definición del encargado de tratamiento. El acceso a los datos por cuenta de terceros es el acceso

permitido a terceros que no tienen la condición de responsable del fichero, usuario o interesado, sin que por ello se produzca una cesión o comunicación de datos.

Se trata de la posibilidad de que los datos personales puedan ser tratados por personas distintas de los usuarios de la propia organización del responsable del fichero, por encargo de éste. Esta tercera persona se convierte en este caso en encargado de tratamiento, y presta servicios al responsable del fichero, siempre que dichos servicios tengan como objeto una finalidad lícita y legítima. El servicio prestado por el encargado podrá tener o no carácter remunerado y ser temporal o indefinido.

Ejemplos:

La contratación por parte de un hospital del depósito, custodia y gestión integral del archivo de la documentación clínica.

El soporte y mantenimiento de un servidor que realiza una empresa para un organismo público.

La LOPD regula la relación entre el responsable del fichero y el encargado del tratamiento, estableciendo una serie de obligaciones encaminadas a garantizar la seguridad del tratamiento de los datos personales.

Esta relación debe regularse en un contrato escrito o en alguna otra forma que permita acreditar su celebración (por ejemplo, un convenio) en el que conste:

— Que el encargado únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

— Las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

— Que el encargado del tratamiento no utilizará los datos con fines distintos a los que figuren en el contrato.

— Que el encargado del tratamiento no cederá los datos a otras personas, ni siquiera para su conservación.

— Que una vez cumplida la prestación, los datos serán destruidos o devueltos al responsable, al igual que cualquier soporte o documentos en que consten datos objeto del tratamiento.

Para cumplir con estas obligaciones, como ya se apuntó en el apartado de Obligaciones de esta Guía, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda el uso de diferentes tipos de cláusulas. Éstas se encuentran en el Canal Servicios de la página Web de la Agencia, www.apdcm.es.

Por otra parte, el encargado del tratamiento responderá de las infracciones en las que hubiera incurrido personalmente, equiparándose en tal caso su figura, en materia de responsabilidad, a la del responsable del tratamiento, con independencia de las posibles y concretas obligaciones propias del responsable del tratamiento.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio.

Respecto a la figura del encargado del tratamiento, el Real Decreto 1720/2007, de 21 de diciembre, regula la posibilidad de que dicho encargado del tratamiento subcontrate a su vez el servicio que ha contratado con el responsable del fichero.

Para que esta subcontratación tenga lugar será necesario que el encargado del tratamiento haya obtenido la autorización del responsable del fichero. Esta subcontratación se efectuará siempre en nombre y por cuenta del responsable del fichero.

Sin embargo, será posible la subcontratación sin necesidad de autorización del responsable del fichero siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y la empresa con la que se vaya a subcontratar.
b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos para el contrato entre el responsable del fichero y el encargado del tratamiento.

En este caso, el subcontratista será considerado encargado del tratamiento.

En el supuesto que durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del fichero los extremos señalados anteriormente.

Por último, el Real Decreto 1720/2007, de 21 de diciembre, contempla la posibilidad de que los derechos de acceso, cancelación, oposición y rectificación, se ejerciten ante un encargado del tratamiento. En este caso, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

10

DERECHOS DE LAS PERSONAS

10. DERECHOS DE LAS PERSONAS

La LOPD no sólo establece las obligaciones que debe cumplir el responsable del fichero, y en su caso, el encargado del tratamiento, sino que también reconoce una serie de derechos de carácter personal que pueden ser ejercitados por el interesado o afectado (ciudadano).

Estos derechos son los siguientes:

- Derecho de acceso.
- Derecho de cancelación.
- Derecho de oposición.
- Derecho de rectificación.

Estos derechos pueden ser ejercitados por:

a) El afectado, acreditando su identidad.

b) Su representante legal, cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos. En este caso será necesario que acredite tal condición.

c) Un representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones Públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

En el caso de que la solicitud de ejercicio de estos derechos sea formulada por persona distinta del afectado o interesado (ciudadano) podrá ser denegada cuando no se acredite la representación.

Por otra parte, a la hora de ejercitar estos derechos es importante tener en cuenta lo siguiente:

— Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

— El interesado contará con un medio sencillo para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

— El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

— No se considerará conforme a lo dispuesto en la LOPD que el responsable del fichero establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

— Cuando el responsable del fichero disponga de servicios de cualquier índole para la atención al público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la contratación de sus servicios o productos.

— El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos a continuación.

Forma de ejercitar estos derechos.

El ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su Documento Nacional de Identidad, pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

Todo ello se entiende sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición donde se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que se formula, en su caso.

Obligaciones del responsable del fichero cuando recibe la solicitud de ejercicio de estos derechos

— Deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

— En el caso de que la solicitud no reúna los requisitos citados anteriormente, el responsable del fichero deberá solicitar la subsanación de los mismos.

— Corresponderá al responsable del tratamiento cumplir con el deber de respuesta además de conservar la acreditación del cumplimiento del mencionado deber.

— El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

Por último, y como ya se ha indicado anteriormente, el Real Decreto 1720/2007, de 21 de diciembre, regula la posibilidad de que estos derechos se ejerciten ante un encargado del tratamiento.

10.1. Derecho de acceso

Es el derecho de todo afectado o interesado (ciudadano) 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.

El derecho de acceso es independiente del que otorgan a los interesados otras leyes y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (derecho de acceso a los expedientes administrativos).

Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.

b) Escrito, copia o fotocopia remitida por correo, certificado o no.

c) Telecopia.

d) Correo electrónico u otros sistemas de comunicaciones electrónicas.

e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

Si el responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.

Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un mayor coste, serán de su cuenta los gastos derivados de su elección.

El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada, pudiendo presentar el afectado o interesado una reclamación ante la Autoridad de Control de Protección de Datos competente.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

Si la solicitud fuera estimada y el responsable no acompañase en su comunicación la información que debe facilitar al interesado o afectado, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se ofrecerá en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los usos concretos y finalidades para los que se almacenaron los datos.

El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

Podrá denegarse el ejercicio de este derecho en los siguientes casos:

— En ficheros de Fuerzas y Cuerpos de Seguridad 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.

— En ficheros de la Hacienda Pública cuando obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando estén siendo objeto de actuaciones inspectoras.

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, contempla un supuesto más de denegación del derecho de acceso: cuando así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el uso de los datos a los que se refiera el acceso.

En todo caso, el responsable del fichero deberá justificar su denegación e informar al afectado de su derecho a recabar la tutela de las Autoridades de Control.

Por último, en cuanto al ejercicio de este derecho en algunos supuestos específicos, habrá que estimar lo que establezca la legislación específica existente, como sería el caso de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que regula alguna característica especial para el acceso a los archivos de documentación clínica por parte de los pacientes, o la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que regula el acceso a los expedientes administrativos.

10.2. Derecho de oposición

Es el derecho del afectado o interesado (ciudadano) a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo, siempre y cuando medie causa justificada. Según la LOPD, podrá ser ejercitado cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

El Real Decreto 1720/2007, de 21 de enero, establece también los siguientes supuestos en los que se debe fundamentar el derecho de oposición del afectado o interesado:

a) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.

b) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

Un ejemplo de derecho de oposición es la posibilidad que tiene todo ciudadano de que su número de teléfono no aparezca en la guía telefónica.

Asimismo, cabe la posibilidad de ejercitar el derecho de oposición 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 automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el párrafo anterior:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán este tipo de decisiones, y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

El Derecho de oposición se ejercitará mediante solicitud dirigida al responsable del fichero, con los mismos requisitos que en el caso del Derecho de acceso.

Cuando la oposición se realice con base en el supuesto contemplado en la LOPD, anteriormente citado, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, ésta podrá entenderse desestimada pudiendo presentar el afectado o interesado una reclamación ante la Autoridad de Control de Protección de Datos competente.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo máximo de 10 días.

10.3. Derecho de rectificación y Derecho de cancelación

El Derecho de rectificación es el derecho del afectado a que se modifiquen sus datos que resulten ser inexactos o incompletos. Podemos entender también que este derecho lleva implícita la obligación de que las Administraciones Públicas tengan en todo momento sus ficheros actualizados. Esta obligación la hemos analizado anteriormente en relación con el Principio de calidad de los datos. Piénsese en el caso del Padrón Municipal de Habitantes, en el que los datos obrantes en el mismo deben estar actualizados.

En cuanto al Derecho de cancelación, es el derecho del afectado o interesado a que se supriman sus datos que resulten ser inadecuados o excesivos. 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 su supresión.

Para ejercitar estos derechos, la solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, ésta podrá entenderse desestimada pudiendo presentar el afectado o interesado una reclamación ante la Autoridad de Control de Protección de Datos competente.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la LOPD.

Sólo podrá denegarse el ejercicio de estos derechos en los siguientes casos:

— En ficheros de Fuerzas y Cuerpos de Seguridad 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.

— En ficheros de la Hacienda Pública cuando obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando esté siendo objeto de actuaciones inspectoras.

— La cancelación, además, no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables. Del mismo modo, tampoco procederá la cancelación durante la vigencia de las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

El Real Decreto 1720/2007, de 21 de diciembre, contempla también la posibilidad de denegar los derechos de rectificación o cancelación en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

En todo caso, el responsable del fichero deberá justificar su denegación e informar al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las Agencias de Protección de Datos de las Comunidades Autónomas.

Además de los derechos de acceso, cancelación, oposición y rectificación, la LOPD reconoce a los afectados (ciudadanos) otros derechos que son los siguientes:

10.4. Derecho de impugnación de valoraciones

Este derecho permite al interesado impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

El interesado podrá impugnar actos jurídicos o decisiones privadas que impliquen una valoración de su comportamiento basado únicamente en un tratamiento de datos personales que ofrezca una definición de su personalidad.

Para el ejercicio de este derecho el afectado podrá solicitar información del responsable del fichero sobre:

— los criterios de valoración utilizados
— el programa utilizado en el tratamiento

La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

El Real Decreto 1720/2007, de 21 de diciembre, ha regulado el derecho de impugnación de valoraciones en su Artículo 36 como derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos, ya referido anteriormente en el apartado sobre el Derecho de oposición de esta Guía.

10.5. Derecho a indemnización

El afectado o interesado tendrá derecho a solicitar una indemnización económica cuando, a consecuencia del incumplimiento por el responsable del fichero de lo dispuesto en la Ley Orgánica 15/1999, sufra daño o lesión en sus bienes o derechos.

La indemnización se exigirá de acuerdo a la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas cuando la lesión provenga de organismos públicos, es decir, se podrá exigir responsabilidad patrimonial a la Administración Pública causante del perjuicio.

Cuando la lesión provenga de entidades privadas se solicitará ante la jurisdicción ordinaria.

10.6. Derecho de consulta al Registro General de Protección de Datos

Cualquier persona podrá conocer de forma gratuita la existencia de tratamientos de datos de carácter personal (ficheros), sus finalidades y la identidad del responsable del fichero mediante consulta al Registro de Ficheros de Datos Personales. En este sentido, existe el Registro de Ficheros de Datos Personales de la Agencia Española de Protección de Datos y los respectivos Registros de Ficheros de las Agencias de Protección de Datos autonómicas allá donde éstas se hayan creado.

La información existente y objeto de consulta se refiere a determinadas características de los ficheros, tales como, identificación, quién es el responsable del mismo, dónde se ubican, el tipo de datos que tratan, órgano ante el cual ejercitar los derechos de acceso, rectificación, cancelación y oposición, y los colectivos de los que se recabaron los datos, entre otras. En definitiva, estos Registros no recogen el contenido de los ficheros, sino las características de los mismos.

La solicitud del afectado no puede expresarse de forma genérica, es decir, no se puede solicitar la identificación de todos los ficheros donde se esté tratando nuestro nombre, apellidos, fecha de nacimiento, etcétera.

En consecuencia, la Agencia de Protección de Datos de la Comunidad de Madrid tiene su propio Registro de Ficheros de Datos de Carácter Personal, en el cual se inscriben:

a) Los ficheros de datos de carácter personal de titularidad de los órganos y organismos públicos (excepto las Sociedades Anónimas) de la Administración de la Comunidad de Madrid, Ayuntamientos y Universidades Públicas.

b) Los ficheros de datos de carácter personal de titularidad de los Colegios Profesionales y Cámaras cuyo ámbito territorial no exceda la Comunidad de Madrid, siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público.

c) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los Derechos de información, acceso, rectificación, cancelación y oposición.

d) Los códigos tipo.

El Registro de Ficheros de la Agencia de Protección de Datos de la Comunidad de Madrid puede consultarse a través de su página Web, www.apdcm.es, Canal Registro. El procedimiento para la inscripción, modificación o supresión de un fichero en el citado Registro se encuentra regulado por el Decreto 99/2002, de 13 de junio.

11

AUTORIDADES DE CONTROL: LA AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID

11. AUTORIDADES DE CONTROL: LA AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID

Con el objetivo de asegurar el cumplimiento de la legislación de protección de datos y, por ende, el respeto a la protección de datos de los ciudadanos, la LOPD creó las Autoridades de Control de Protección de Datos, tanto a nivel estatal como autonómico, de manera que "*las funciones de la Agencia Española de Protección de Datos [...] en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control y a los que se garantizará la plena independencia y objetividad en el ejercicio de su cometido*".

En la actualidad, además de la Agencia de Protección de Datos de la Comunidad de Madrid, existe la Agencia de Protección de Datos de Cataluña, creada por la Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos, y la Agencia de Protección de Datos del País Vasco, creada por la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

En las últimas reformas llevadas a cabo en sus respectivos Estatutos de Autonomía, algunas Comunidades Autónomas han asumido competencias en materia de desarrollo legislativo y ejecución de la legislación básica del Estado en protección de datos de carácter personal. Es el caso de las reformas de los Estatutos de Autonomía de Baleares, Aragón y Castilla y León. Además, tanto Aragón como Castilla y León han previsto en dichas reformas estatuarias la posibilidad de crear una Agencia de Protección de Datos Personales.

Entre las funciones de las Agencias de Protección de Datos destaca la atención de peticiones y reclamaciones de los ciudadanos, la información sobre sus derechos y el ejercicio de la potestad inspectora y sancionadora.

En este sentido, la Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por las Instituciones de la Comunidad de Madrid y por los Órganos, Organismos, Entidades de Derecho Público y demás Entes Públicos integrantes de su Administración Pública, exceptuándose las sociedades mercantiles a que se refiere el Artículo 2.2.c)1 de la Ley 1/1984, de 19 de enero, reguladora de la Administración Institucional de la Comunidad de Madrid.

Dichas funciones también se ejercen sobre los ficheros de datos de carácter personal creados o gestionados por los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, de conformidad con lo previsto en el Artículo

41 de la LOPD, así como sobre los ficheros creados o gestionados por las Universidades Públicas y por las Corporaciones de Derecho Público representativas de intereses socioeconómicos y profesionales de la Comunidad de Madrid (Colegios Profesionales y Cámaras), en este último caso siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público.

Los ficheros regulados por la Ley Estatal 12/1989, de 9 de mayo, de la Función Estadística Pública, creados o gestionados por las entidades y empresas de la Comunidad de Madrid y Entidades Locales referidos en el apartado anterior, para fines no estatales, se regirán por dicha disposición en defecto de la legislación estadística de que pueda dotarse por la Comunidad de Madrid, pero estarán sometidos al control de la Agencia de Protección de Datos de la Comunidad de Madrid.

Una de las manifestaciones de esta función de control que tiene atribuida la Agencia de Protección de Datos de la Comunidad de Madrid es la potestad de inspección de los ficheros de datos de carácter personal.

El objeto de esta inspección es comprobar que los responsables de ficheros cumplen con la normativa de protección de datos, garantizando el derecho a la protección de datos de los ciudadanos.

En caso de detectar una posible comisión de infracción a la normativa de protección de datos, se podrá abrir el correspondiente procedimiento para determinar la existencia o no de la infracción y el responsable o responsables de la misma. Los procedimientos abiertos contra responsables de ficheros de titularidad pública podrán finalizar con la declaración de la existencia o no de la infracción, pudiendo proponer en el primer supuesto que se inicie expediente disciplinario a la persona que ha resultado responsable de la infracción cometida.

También cabe mencionar el procedimiento de tutela de derechos tiene lugar cuando el afectado o interesado (ciudadano) no ha visto satisfecho su derecho de acceso, cancelación, oposición o rectificación. Es un procedimiento contradictorio, en el cual pueden presentar alegaciones tanto el responsable del fichero como el ciudadano, y que finaliza mediante resolución de la Agencia de Protección de Datos de la Comunidad de Madrid otorgando o no la tutela de su derecho al afectado o interesado (ciudadano).

Además de las funciones de control, la Agencia de Protección de Datos de la Comunidad de Madrid desarrolla también una labor de consultoría, fundamental para procurar el efectivo cumplimiento de la normativa sobre protección de datos. En este sentido, la labor de información y asesoramiento se lleva a cabo aconsejando sobre el procedimiento de creación, modificación y supresión de ficheros, adopción de las medidas de seguridad, cumplimiento del deber de información, así como evacuando informes que resuelven las consultas planteadas por los propios responsables de ficheros.

La Agencia de Protección de Datos de la Comunidad de Madrid también presta formación a los distintos colectivos de empleados públicos con el objetivo de que conozcan el derecho fundamental a la protección de datos y que de esta manera se pueda garantizar que las Administraciones Públicas respetan el derecho de los ciudadanos a la protección de datos.

Cabe destacar también la labor internacional que realiza la Agencia de Protección de Datos de la Comunidad de Madrid, participando en diversos foros como son la Conferencia Mundial de Autoridades de Protección de Datos, la Conferencia Europea de Autoridad de Protección de Datos, el Grupo Europeo de Trabajo de Gestión de Reclamaciones de Protección de Datos y el Grupo Europeo de Trabajo de Telecomunicaciones.

Siguiendo con esta proyección internacional, la Agencia de Protección de Datos de la Comunidad de Madrid ha liderado el proyecto europeo "E-Prodat: Mejores Prácticas en Protección de Datos y Administración Electrónica" (www.eprodat.org), proyecto realizado en el marco del programa comunitario Interreg3C; participa como socio en el proyecto europeo "EuroPriSe" (www.european-privacy-seal.eu) que tiene como objetivo la creación de un sello de privacidad europeo; y ha presentado su candidatura a liderar el proyecto europeo "E-participation and privacy: Identificación de las Mejores Prácticas en participación electrónica y privacidad" en el marco del programa comunitario Interreg4C.

La Agencia de Protección de Datos de la Comunidad de Madrid dispone de una Colección "Protección de Datos" con la editorial Civitas-Thomson-Aranzadi, en la que se han editado distintos Manuales y Guías de Protección de Datos, así como un Repertorio de Legislación y Jurisprudencia sobre Protección de Datos. Podemos destacar también la publicación de la revista digital www.datospersonales.org, nacida en marzo de 2003 y que cuenta con más de 7.000 suscriptores, la revista digital www.dataprotectionreview.eu, publicación en inglés dirigida a un público internacional interesado en protección de datos, y la Revista Española de Protección de Datos, revista de contenido científico, todas ellas publicadas por la Agencia.

Por otra parte, la Agencia de Protección de Datos de la Comunidad de Madrid ha sido pionera al organizar el primer y segundo encuentros entre Agencias Autonómicas de Protección de Datos. Estos dos primeros encuentros se celebraron en los años 2004 y 2005. En el año 2008 la APDCM volverá a organizar este encuentro que cumplirá su quinta edición.

Por último, la Agencia de Protección de Datos de la Comunidad de Madrid organiza anualmente el "Premio Europeo sobre mejores prácticas públicas en protección de datos", del cual ya se han celebrado cuatro ediciones, y cuyo objetivo es dar a conocer las mejores prácticas en materia de protección de datos, propuestas o implantadas, para el tratamiento de datos por cualquier órgano o institución de la Administración

Pública de cualquiera de los países adheridos al Convenio del 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales.

En la Cuarta Edición celebrada el 11 de diciembre de 2007, el proyecto premiado ha sido "*My Privacy. Don´t look, don´t poke about* " de la Oficina de Protección de Datos Personales de la República Checa y la ONG Iuridicum Remedium, consistente en una campaña de introducción de la materia de Protección de Datos en el sistema educativo checo, a través de la formación de los profesores y el estudio de la materia en las diferentes asignaturas de su plan de estudios.