APDCM

Agencia de Protección de Datos
de la Comunidad de Madrid

Cuaderno de **protección** de **datos personales** para **empleados públicos**

EDITA:
La Agencia de Protección de Datos de la Comunidad de Madrid

Impreso en España
Producción Gráfica: PRINTERALIA, S.L.
Maquetación: Antonio González Retuerto

I.S.B.N.:
Depósito Legal:

faltan datos
ISBN - Depósito

ÍNDICE

PRESENTACIÓN

Las Administraciones Públicas recurren cada vez más a las nuevas tecnologías para el desarrollo de su actividad. La utilización de los nuevos sistemas de información y de comunicación para relacionarse con los ciudadanos y para mejorar el funcionamiento interno de la Administración es algo positivo porque contribuye a mejorar la propia legitimidad social de la Administración Pública. Al mismo tiempo, el desarrollo de una Administración electrónica y la consiguiente acumulación por parte de los poderes públicos de datos personales de los ciudadanos puede suponer una amenaza al derecho a la intimidad y a otros derechos constitucionales.

Nuestra Constitución, especialmente a partir de la interpretación establecida por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, ha establecido un derecho fundamental a la protección de datos personales, que puede ser definido como el derecho que tiene toda persona a controlar su información personal, lo que le faculta para decidir quién tiene sus datos y para qué los va a usar. Este derecho ha sido desarrollado por la legislación, y en especial por la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. El Legislador ha establecido reglas objetivas sobre el tratamiento de datos personales para que el ciudadano recupere el poder de disposición sobre sus datos y ha establecido instituciones específicas, como las Agencias de Protección de Datos, que refuerzan este derecho a la autodeterminación informativa. No obstante, ninguna norma jurídica puede sustituir al empleado público, que debe respetar los derechos de los ciudadanos en el desarrollo de la actividad administrativa.

La Agencia de Protección de Datos de la Comunidad de Madrid, que es la autoridad de control sobre los tratamientos de datos personales desarrollados por la Administración autonómica, Entidades Locales, Corporaciones de Derecho Público y Universidades Públicas del territorio de la Comunidad de Madrid, se ha caracterizado desde su inicio por impulsar una importante actividad formativa, celebrando jornadas que han alcanzado a cerca de 20.000 personas, manteniendo una política activa de publicaciones y desarrollando iniciativas como la revista digital www.datospersonales.org que cuenta con más de 2.600 suscriptores.

Es un motivo de satisfacción presentar el *Cuaderno de Protección de Datos Personales para Empleados Públicos*, que se inscribe en esta *batalla formativa* en la que está inmersa la Agencia de Protección de Datos de la Comunidad de Madrid.

Este *Cuaderno de Protección de Datos Personales para Empleados Públicos* contiene una breve exposición de los conceptos fundamentales de la protección de datos, los principios que rigen todo tratamiento de datos personales, los derechos de las personas en este ámbito y los órganos de control.

Las Leyes atribuyen a los ciudadanos un conjunto de garantías para que tengan un control efectivo sobre su información personal, estableciendo al mismo tiempo un conjunto de obligaciones que todos los empleados públicos debemos conocer y cumplir. No se trata de limitar la utilización de la informática en el ámbito público sino de hacerla compatible con los derechos de los ciudadanos, sin que esto signifique renunciar al progreso que el uso de los sistemas de información y la comunicación traen consigo.

Sólo me queda esperar que la publicación de este *Cuaderno de Protección de Datos Personales para Empleados Públicos* sirva para que éstos vean la tutela del derecho a la autodeterminación informativa no como una carga a soportar sino como un valioso instrumento y una oportunidad para ofrecer cada día a los ciudadanos unos servicios públicos de mayor calidad, en los que se hace compatible la eficacia administrativa y el respeto a los derechos.

Antonio Troncoso Reigada
Director de la APDCM

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

1

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

El derecho a la protección de datos personales es un derecho fundamental de todas las personas que se traduce en la potestad de control sobre el uso que se hace de sus datos personales. Este control permite evitar que, a través del tratamiento de nuestros datos, se pueda llegar a disponer de información sobre nosotros que afecte a nuestra intimidad y demás derechos fundamentales y libertades públicas.

La protección de datos nace en nuestra legislación en cumplimiento del mandato impuesto por el artículo 18 de la Constitución Española de 1978: "*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*". Será la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), la que inicie su regulación en nuestro país, ajustándose tanto a las previsiones del Convenio Europeo para la protección de los Derechos Fundamentales de la Persona (Convenio de 4 de noviembre de 1950, ratificado por Instrumento de 26 de noviembre de 1979), como al Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108 del Consejo de Europa, de 28 de enero de 1981, ratificado por Instrumento de 27 de enero de 1984).

La evolución en la regulación de este derecho llevará al Parlamento Europeo y al Consejo de la Unión Europea en el año 1995, a adoptar la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuya transposición a la legislación española se realizará mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), actualmente en vigor y que deroga a la Ley Orgánica 5/1992.

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*", si bien es en la Sentencia 292/2000, de 30 de noviembre, del Pleno del Tribunal Constitucional, donde se define el derecho fundamental a la Protección de Datos, separándolo del derecho a la intimidad:

> "*Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 C.E. 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, ... La peculiaridad de este derecho fundamental respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran".

"*De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, ...*".

"*... 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, y que también permite 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.

La Ley Orgánica 15/1999, 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, son varias las Comunidades Autónomas que han aprobado su normativa específica en la materia, desarrollando la norma básica estatal:

- La Comunidad de Madrid, mediante 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, modificada por la Ley de la Comunidad de Madrid 13/1997, de 16 de junio, y hoy derogada por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

- La Comunidad Catalana, mediante Ley del Parlamento de Cataluña 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos.

- La Comunidad Vasca, mediante 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.

2.1 Ámbito de aplicación

"*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 Ley Orgánica 15/1999, deben destacarse dos conceptos fundamentales: por una parte, su aplicación a los datos registrados en cualquier soporte físico susceptible de tratamiento y, 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 albergados en soportes electrónicos o informáticos, sino también a los recogidos en papel, microfichas, o cualquier otro que pueda ser objeto de utilización.

En lo que respecta al segundo concepto fundamental, la aplicación de la ley tanto al sector público como al privado, decir que los principios de la protección de datos en cuanto al tratamiento de los datos personales, así como los derechos específicos que concede la ley a los ciudadanos, son de obligado cumplimiento para cualquier persona que trate datos de carácter personal, con independencia de su naturaleza pública o privada. Las diferencias que se establecen en la Ley Orgánica 15/1999, son básicamente procedimentales, en cuanto a cómo debe realizarse determinada actuación o gestión, dependiendo de que el responsable del tratamiento sea uno u otro tipo de entidad.

Por ejemplo:

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 que sea necesario para la consecución de sus objetivos legítimos, si bien deberán notificarlo previamente a la Agencia Española de Protección de Datos.

Uno de los rasgos más destacados en la evolución de la legislación en materia de protección de datos es la ampliación del ámbito de aplicación. Inicialmente el objeto de la Ley era: "*limitar el uso de la informática en el tratamiento de datos personales*", por el peligro que implica el uso de esta herramienta como posible vía para facilitar la vulneración del derecho a la intimidad. Sin embargo, desde la Directiva 95/46/CE y la Ley Orgánica 15/1999, el derecho a la protección de datos no se limita a los tratamientos automatizados, es decir, a aquellos que se realizan utilizando técnicas y herramientas informáticas, sino que se aplica a cualquier tratamiento, con independencia de su soporte.

En lo que respecta al primer concepto, la Directiva 95/46/CE, en su considerando número 15 indica que "*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*". En su considerando número 27 reitera el mismo criterio: "*...la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; ... el alcance de dicha protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión*; ..."

Por lo tanto, la Ley Orgánica 15/1999 es aplicable a todos los ficheros informatizados que contengan datos de carácter personal y a aquellos ficheros manuales que contengan datos de carácter personal, siempre que la información almacenada se organice según algún criterio relativo a las personas, de forma que permita acceder fácilmente 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, también estamos ante un tratamiento de datos personales, pero quedaría excluido de la aplicación de la legislación en materia de protección de datos al no almacenarse los datos según un criterio relativo a las personas.

No obstante, la Ley Orgánica 15/1999, establece en su disposición adicional primera unos plazos de adaptación a la misma que están en función de si los ficheros están automatizados o no, y si estaban inscritos o no con anterioridad en el Registro General de Protección de Datos. En el caso de los ficheros automatizados, el plazo de adaptación es de 3 años desde su entrada en vigor. Para los ficheros y tratamientos no automatizados, su adaptación a la Ley Orgánica deberá realizarse en el plazo de 12 años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

En conclusión:

Todos los ficheros informatizados existentes en el momento de entrada en vigor la Ley Orgánica, o creados posteriormente, deben haber adaptado el tratamiento de los datos a esta norma, dado que el plazo de adaptación ya ha concluido (diciembre 2002).

Los ficheros no automatizados y estructurados, con independencia de la fecha en que hayan iniciado su funcionamiento, no estaban dentro del ámbito de aplicación de la derogada LORTAD, por lo que su adaptación a la LOPD y la obligación de su registro vence el 24 de octubre del 2007, sin perjuicio de que deberán garantizar el ejercicio de los derechos que ésta crea, por lo que pueden requerir determinadas adecuaciones.

Por ejemplo:

- *El almacenamiento de los datos deberá realizarse de forma que permita el ejercicio del derecho de acceso.*

En cuanto al régimen objetivo de delimitación del ámbito de aplicación de la Ley Orgánica 15/1999, 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 mismo.*

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

c) *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.*

El régimen de protección de datos de carácter personal que se establece en la Ley Orgánica 15/1999 no será de aplicación:

a) *A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.*

b) *A los ficheros sometidos a la normativa sobre protección de materias clasificadas.*

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

Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la Ley Orgánica 15/1999 los siguientes tratamientos de datos personales:

a) *Los ficheros regulados por la legislación de régimen electoral.*

b) *Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.*

c) *Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.*

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

e) *Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.*

2

CONCEPTOS FUNDAMENTALES

CONCEPTOS FUNDAMENTALES

Son conceptos que debemos conocer para el cumplimiento de los deberes que establece la normativa vigente en materia de protección de datos y el disfrute de los derechos que garantizan el respeto a la protección de los datos personales.

2.1 Datos de carácter personal

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

Esta información, referida siempre a personas físicas, puede ser muy diversa, desde nombre y apellidos, hasta número de cuenta bancaria. El elemento fundamental para determinar que se trata de un "dato personal" es que la información, combinada o por sí misma, permita conocer datos de una persona concreta, bien por estar directamente identificada a través de algún dato, o porque pueda llegar a ser identificable por otro medio.

La Sentencia del Tribunal Constitucional 292/2000 establece 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*".

De acuerdo con la definición que establece 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*".

También la 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*".

En conclusión:

Se considerará dato de carácter personal, como objeto de la protección de datos, cualquier información referente a una persona física de quien conste o podamos llegar a saber 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 la identifique por el nombre, el DNI, el número de empleado u opositor, o el más complejo código alfanumérico generado por cualquier algoritmo, siempre que su finalidad sea identificar al interesado.

2.2 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).

Como ya hemos comentado al analizar el ámbito de aplicación de la Ley Orgánica 15/1999, no se trata solamente de ficheros integrados en sistemas informáticos o telemáticos, sino también de ficheros manuales que pueden estar archivados en armarios, cajones o estanterías, siempre que los datos se encuentren estructurados (organizados) por algún criterio que permita acceder fácilmente a los referidos a una determinada persona.

Una matización importante en cuanto a qué se considera un fichero es la establecida por la Directiva 95/46/CE al definir 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*".

Ejemplos típicos de tratamientos no automatizados de datos:

- *El fichero manual, organizado en carpetas, que recoge toda la información clínica de un proceso asistencial a un paciente en un centro sanitario.*

- *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.*

- *Atendiendo a los criterios de la Directiva 95/46/CE, podría considerarse un único fichero el conjunto de historias clínicas existentes en un centro, bajo una única responsabilidad, aunque físicamente el fichero esté constituido por varios ficheros independientes (un archivo de historias clínicas en cada servicio o por cada especialidad sanitaria). También podría considerarse un único fichero aunque sus diferentes partes estuvieran distribuidas en puntos separados geográficamente, siempre que los datos, la finalidad y el responsable sea el mismo.*

2.3 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).

Prácticamente cualquier actuación vinculada al trabajo habitual que conlleve el manejo de datos personales, supone la realización de un tratamiento de datos.

Ejemplos:

- *La recogida de instancias de participantes en un proceso selectivo, siempre que se almacenen por un criterio relativo a las personas.*

- *La grabación en una aplicación informática de la cita concertada por un ciudadano para acudir a la consulta de su médico.*

- *La clasificación y archivo de la documentación recabada en el procedimiento de recogida de los datos (las instancias utilizadas en un proceso selectivo, en tanto éste no haya concluido por completo).*

- *La obtención de nuevos datos a partir de la información recabada (el establecimiento de un diagnóstico o un determinado tratamiento en función de los datos obtenidos de un paciente en su exploración).*

- *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.*

- *El almacenamiento de los datos de forma diferenciada, excluyéndolos de otros tratamientos de datos que se realicen con el solo objeto de disponer de los mismos cuando sean demandados por las Administraciones públicas, Jueces o Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el período de prescripción de éstas (el almacenamiento de las instancias utilizadas en un proceso selectivo una vez concluido éste o el historial clínico de un paciente relativo a un episodio asistencial que se ha dado por concluido).*

- *La supresión física de los datos existentes en el 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 entidad financiera de los datos de nómina de los empleados para que se proceda al abono de las mismas).*

2.4 Afectado o interesado

"*Persona física titular de los datos que sean objeto del tratamiento a que se refiere la definición anterior*". (Art. 3.e LOPD).

Es preciso tener muy en cuenta que sólo pueden ser afectados las personas físicas, una persona jurídica no puede nunca identificarse con el afectado o interesado titular de datos personales.

> *La protección de datos tiene como objeto una serie de derechos que se configuran como personalísimos, por lo que sólo podrán ser ejercidos por el propio titular, salvo que nos encontremos en el supuesto de un menor o un incapacitado, en cuyo caso podrán ejercerse por medio o valiéndose de su representante legal.*

2.5 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).

Para que el consentimiento sea válido no es siempre necesario que se preste de forma expresa, la Ley admite también, en determinados casos, el consentimiento tácito o presunto.

> *Una de las formas más usuales de prestar el consentimiento para el tratamiento de datos en ficheros de titularidad pública, es a través de la cumplimentación de impresos, en los que el consentimiento viene prestado por la simple declaración de los datos personales que se reflejan en el cuestionario por el propio interesado.*
>
> *Cuando los datos se recaben directamente del interesado por medio de una entrevista personal, se puede entender que éste da su consentimiento de forma tácita, al ser él mismo el que nos facilita la información, siempre que se hayan cumplido los principios que establece la Ley Orgánica 15/1999 para el tratamiento de los datos (información previa y adecuación de los datos, por ejemplo).*

2.6 Cesión de datos

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

La cesión de datos es uno de los puntos fundamentales de la normativa sobre protección de datos. Como regla general, los datos personales sólo pueden ser revelados a persona o entidad distinta del interesado con el consentimiento inequívoco de éste.

Otros dos conceptos estrechamente relacionados con la cesión son los de tercero y destinatario, que son definidos en la Directiva 95/46/CE de la siguiente forma:

"*Tercero: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, 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.

Destinatario: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios".

Ejemplos de cesiones de datos:

Se produce una cesión cuando los datos que se han obtenido para una determinada finalidad se ceden a un tercero para el ejercicio de otra finalidad distinta de aquella para la que se recogieron.

La simple visualización por un tercero o la comunicación de cualquier dato al mismo, por ejemplo al realizar una consulta telefónica, constituye una cesión de datos.

2.7 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).

Dentro del ámbito de los ficheros de titularidad pública, el responsable del fichero siempre es un órgano administrativo.

El responsable del fichero es quien decide la creación del fichero, para qué se va a utilizar y qué uso se va a dar a éste.

El responsable del fichero es la entidad obligada a dar respuesta a los ciudadanos ante el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición.

El responsable del fichero, en el supuesto de ser un órgano de la Administración pública, es el sujeto pasivo contra quien se dirigirá el procedimiento por infracción de Administración pública, o, si se trata de una empresa privada, será aquél en quien recaerán las posibles sanciones de tipo pecuniario en caso de comisión de infracciones a la legislación sobre protección de datos personales, sin perjuicio de la responsabilidad directa del autor de la infracción, si lo hubiera.

La Directiva 95/46/CE define al responsable del fichero como: "*la persona física o jurídica, autoridad pública o servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario*".

2.8 Encargado de 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 encargado de tratamiento tiene una especial importancia cuando hablamos de tratamiento de datos por parte de organismos públicos. En múltiples ocasiones las Administraciones contratan servicios de mantenimiento de equipos informáticos, servicios de recogida de datos a través de encuestas, etc. El encargado de la realización de estos servicios se constituye normalmente en encargado de tratamiento.

El encargado de tratamiento está legitimado para acceder a los datos personales obrantes en el fichero sin el requisito del consentimiento previo del afectado, siempre que la relación entre el primero y el responsable del fichero esté formalizada en un contrato que obedezca a fines lícitos y legítimos y se especifiquen las condiciones en que se va a llevar a cabo el tratamiento y que la utilización de los datos será únicamente para los fines establecidos por el responsable del fichero.

> *Un ejemplo típico de encargado del tratamiento es la empresa con la que podemos establecer una relación contractual para que se encargue de la destrucción de los documentos que contienen datos de carácter personal y ya no tengo por qué mantener en mis archivos.*
>
> *Otro supuesto es cuando encargo a una empresa u otro organismo de la Administración que almacene, custodie y me facilite la gestión de un archivo documental para cuya explotación yo no cuento con recursos directos suficientes (el supuesto típico de "externalización" de la gestión del fichero de historias clínicas de un centro hospitalario).*

También constituirá un tratamiento de datos el encargo a un tercero para que realice una campaña de correo personalizado (mailing) a las personas que están contenidas en un fichero determinado y que previamente no se han opuesto al envío publicitario, salvo que los datos los hubiera obtenido el responsable del fichero de fuentes accesibles al público (por Ej. Guías telefónicas).

2.9 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).

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 Ley Orgánica 15/1999, por ejemplo de requerir el consentimiento del interesado para poder utilizar esos datos en el tratamiento previsto.

2.10 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 están enumeradas y tasadas por la Ley Orgánica 15/1999. Así, únicamente son consideradas como fuentes de acceso público: el censo promocional (todavía sin regular), los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales, los diarios y boletines oficiales y los medios de comunicación.

Siempre que una norma reguladora en materia de protección de datos haga referencia a que los datos se hayan obtenido de una fuente accesible al público, debe tenerse en cuenta la enumeración con carácter exhaustivo que hace la Ley, no pudiendo considerar fuente accesible al público (en materia de protección de datos) ninguna otra fuente, aun cuando al crear un fichero se indique en su propia disposición de creación que tendrá carácter de acceso público.

2.11 Usuarios

Son usuarios el personal al servicio del responsable del fichero o encargado del tratamiento que tengan 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 están obligados al cumplimiento de las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de secreto.

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 Ley Orgánica 15/1999. 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.

3

PRINCIPIOS QUE RIGEN TODO TRATAMIENTO DE DATOS PERSONALES

PRINCIPIOS QUE RIGEN TODO TRATAMIENTO DE DATOS PERSONALES

Estos principios de obligado cumplimiento, que la Ley Orgánica 15/1999 agrupa en el título II, son la base de todo tratamiento de datos personales. Por ello, es fundamental que sean conocidos por los usuarios que tratan directamente la información, y que, en muchos casos, atienden personalmente a los interesados o afectados, titulares de los datos.

El responsable del fichero o el encargado del tratamiento de los datos, entre otras muchas obligaciones, debe asegurarse que cualquier tratamiento de los datos se adapte al cumplimiento de estos principios. Su incumplimiento puede ser motivo de sanción, aplicándose el procedimiento correspondiente, en función de la naturaleza pública o privada del responsable del fichero, de acuerdo con el régimen sancionador que establece la Ley Orgánica 15/1999.

3.1 El principio de calidad de los datos

La aplicación de este principio supone que los datos de carácter personal sólo podrán recogerse para su tratamiento cuando sean **adecuados**, **pertinentes** y **no excesivos** para el cumplimiento de las finalidades del fichero.

La Ley Orgánica 15/1999, a través del establecimiento de este principio, trata de introducir un criterio de racionalidad y proporcionalidad en el tratamiento de los datos personales.

Antes de empezar a recoger los datos de carácter personal se deberá analizar la finalidad que se persigue con el fichero, ya que la Ley sólo legitima el uso de aquellos datos que sean efectivamente necesarios por ser adecuados, pertinentes y no excesivos.

La creación de grandes bancos de datos personales de finalidad múltiple se ve limitada, adicionalmente, por la naturaleza variable de tales datos (la edad cambia constantemente, el estado de salud evoluciona, las personas cambian de domicilio, etc…).

Este principio no debe interpretarse como limitativo de la cantidad de datos que deben utilizarse en un determinado tratamiento, sino como un principio de proporcionalidad.

> *Para prestar determinados servicios sociales es posible que sea necesario recabar gran cantidad de datos de una persona, y de muy variado tipo, no debiendo entenderse que la protección de datos limita el número de datos a tratar.*

Las **finalidades** del fichero deben estar **determinadas de forma explícita** y ser **legítimas**. No podrán además ser utilizados los datos para finalidades incompatibles con las que motivaron su recogida. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

> *Toda actividad de recogida de datos personales debe estar fundamentada en una finalidad explícita. No es posible recopilar datos para su uso de forma generalizada y determinada a posteriori.*

> *Las entidades privadas podrán recabar aquellos datos que sean necesarios para conseguir la finalidad legítima que constituye su objeto. Es la relación directa entre la finalidad perseguida y el dato recabado lo que legitima o no la creación de un fichero con determinados datos de carácter personal.*

> *Las Administraciones públicas deberán respetar también ese principio de relación entre los datos recabados y las finalidades que tengan encomendadas, pero además, el procedimiento para poder crear un fichero con el que posteriormente abordar el tratamiento de los datos, requiere que se haga mediante disposición de carácter general publicada en el boletín o diario oficial correspondiente.*

Un posible uso que contempla la Ley Orgánica 15/1999 como legítimo, aun cuando los datos se hayan recabado para otra finalidad concreta, es su uso con fines históricos, estadísticos o científicos, si bien habrá que analizar otras posibles normas que incidan sobre la forma de realizar esos tratamientos.

> *Por ejemplo, la legislación sanitaria establece que el tratamiento de los datos contenidos en la documentación o historia clínica de los pacientes*

con fines de investigación o docencia se realizará siempre con datos disociados o con consentimiento previo del afectado.

Los datos personales deben ser exactos y mantenerse al día para que respondan con veracidad a la situación actual del afectado. Por tanto, si resultan ser inexactos o incompletos, deberán ser cancelados o sustituidos de oficio por los correspondientes datos rectificados o completados.

El carácter de volatilidad de los datos personales que antes hemos comentado, nos obliga a plantearnos siempre que vayamos a crear un fichero para almacenar tales datos, la necesidad de prever y arbitrar el procedimiento de actualización y mantenimiento de los datos que garantice la corrección de los mismos.

Desde el punto de vista de la protección de datos, es preferible no disponer de un determinado dato de una persona, antes que tenerlo erróneo.

Es preferible que el responsable del fichero no pueda enviar por correo determinada información a una persona, por no disponer de su dirección, que enviarla a un lugar equivocado y perder el control de quien acaba recibiendo esos datos.

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes, y no se conservarán en forma que permitan la identificación del interesado durante un período superior al necesario para la finalidad en base a la que fueron recabados o registrados.

Una vez cumplida la finalidad para la que se recabaron los datos, o cuando cambien las circunstancias de las personas contenidas en los ficheros haciendo no pertinente el mantenimiento de los datos, éstos deberán ser cancelados.

La cancelación, como borrado físico de los datos, en muchas ocasiones no es posible, pudiendo existir una norma que obligue al mantenimiento de los datos durante un período determinado de tiempo, o las posibles responsabilidades que se generen en el tratamiento hacen que los datos deban conservarse hasta la prescripción de las mismas. En estos

supuestos, los datos deben bloquearse, quedando almacenados de forma diferenciada del resto de los datos sometidos al tratamiento y asegurando que quedan excluidos de éste, estando sólo a disposición de las Administración públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento.

Si la conservación de los datos más allá de la consecución de la finalidad para que se recabaron es por fines históricos, estadísticos o científicos, los datos deberán conservarse, siempre que sea posible, disociados, aunque esta previsión está pendiente de desarrollo reglamentario.

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

No es posible alegar como causa para denegar el ejercicio del derecho de acceso la imposibilidad de su realización como consecuencia del modo en que los datos están almacenados, dado que este mandato se establecía ya en la Ley Orgánica de 1992 (LORTAD) y todas las normas han establecido plazos para la adaptación de los tratamientos de datos a estos principios.

3.2 Principio de información en la recogida de datos

El responsable del fichero debe arbitrar la fórmula que permita informar a los afectados de determinados extremos en el momento de la recogida de los datos, de modo que esta información sea conocida por el afectado antes de prestar su consentimiento.

Sólo cuando el ciudadano ha sido informado de forma expresa, precisa e inequívoca de la finalidad de la recogida de sus datos, podrá decidir si quiere que éstos estén, o no, almacenados en un fichero y que se utilicen, o no, para una determinada finalidad.

Los usuarios del fichero tienen en esta fase de recogida de datos una labor muy importante, la de procurar que esta información sea conocida por el interesado en el momento de recabar sus datos.

La información que se debe facilitar a los ciudadanos será expresa, precisa e inequívoca. No es admisible una información genérica que no permita saber quién y para qué se están recabando los datos.

La información que debe llegar al ciudadano que va a prestar sus datos personales es la siguiente:

a) Conocimiento de 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 información se podrá facilitar al afectado o interesado 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.

Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias que se han indicado anteriormente.

Cuando se recaban datos directamente del interesado utilizando un cuestionario que él cumplimenta, parte de la información que se debe facilitar está ya recogida en el propio impreso, por lo que no es necesario en ese caso un esfuerzo adicional para cumplir con este principio de información.

Por ejemplo: normalmente el responsable del fichero figurará en el encabezado del impreso y la finalidad para la que se recaben los datos será el título del formulario.

No será necesaria la información a que se refieren las letras b), c) y d), 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 obvio 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 las consecuencias de no facilitar determinada información, sobre todo en los supuestos de relaciones con las Administraciones Públicas.*
>
> *Si solicito por ejemplo una pensión no contributiva cuya concesión puede depender, entre otros datos, de mi nivel de rentas, es obvio que deberé facilitar estos datos al responsable del fichero para que pueda valorar si tengo derecho a la misma o no. También es obvio que si no facilito esos datos, difícilmente se podrá realizar la valoración y reconocerme mi derecho.*

En el caso de que 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).

No es preciso cumplir con el requisito de informar a posteriori al interesado, 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 de Protección de Datos, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

3.3 Principio de consentimiento

Este principio va íntimamente unido al anterior principio de información, y podríamos decir que es el principio legitimador de todo tratamiento. El consentimiento permite al afectado ejercer el control del uso de sus datos personales, lo que se viene denominando como derecho de autodeterminación informativa.

La Ley Orgánica 15/1999 exige la prestación del consentimiento previo e inequívoco del afectado para el tratamiento de sus datos, pero establece una serie de excepciones, de manera que no es necesario prestar consentimiento:

— 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.

— Cuando los datos son recogidos para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.

La concesión de una licencia de obras por una Entidad local constituye un ejemplo claro de función propia de una Administración pública, pues sólo un Ayuntamiento está legitimado para conceder esa licencia.

— 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.

En este supuesto podría considerarse que no es necesario el consentimiento del afectado, sino que éste está incluido en el consentimiento en virtud del cual se establece y perfecciona la relación negocial, laboral o administrativa.

Cuando firmo un contrato de trabajo en un departamento de personal, está implícito mi consentimiento para el tratamiento de mis datos de carácter personal, pero, ¿qué datos podrá tratar el departamento de personal?, sólo los adecuados, pertinentes y no excesivos para la relación que se está estableciendo, para el ejercicio de la relación laboral.

— Cuando el tratamiento tenga como finalidad proteger un interés vital del interesado y éste se encuentre física o jurídicamente incapacitado para dar su consentimiento.

Esta excepción es específica para el tratamiento de los datos en la actividad de prestación sanitaria asistencial y el afectado está incapacitado para dar su consentimiento. Se permite el tratamiento de datos personales sin consentimiento del interesado en este caso pues existe una colisión entre el derecho a la vida o a la integridad física y el derecho a la intimidad y a la protección de datos.

Parece obvio que debe primar el derecho a la vida sobre el derecho a la protección de datos, pero esta excepción a la necesidad de consentimiento debe ser matizada. Se podrán tratar los datos del interesado, sin su consentimiento, en el ejercicio de la actividad asistencial, pero para cualquier otra finalidad a la que se pretendan destinar esos mismos datos (investigación, docencia, etc.) se requerirá consentimiento del mismo, siempre que no exista una ley específica que diga lo contrario.

— Cuando los datos figuren en fuentes accesibles al público. Recordando que las fuentes están enumeradas de forma limitativa en la Ley Orgánica 15/1999, tal como se indicó al exponer la definición de que es una fuente accesible al público.

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

3.4 Principio de datos especialmente protegidos

El tratamiento especial de determinados datos, aquellos relativos a la ideología, la afiliación sindical, la religión o creencias, el origen racial, la salud y la vida sexual, se constituye en un principio más del tratamiento de datos personales.

La Ley Orgánica 15/1999 prevé la necesidad de proteger especialmente unos datos que, por la información a la que se refieren, pueden generar con mayor facilidad lesiones en otros derechos fundamentales, además del propio derecho a la protección de datos.

Podemos pensar que un tratamiento inadecuado de datos relativos al origen racial o a la salud, puede vulnerar el derecho a la igualdad y a la no discriminación. 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, etc. Precisamente para evitar estos peligros, la Ley establece una serie de refuerzos, con el fin de que se preste un 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).

— Prohíbe expresamente la creación de ficheros con la finalidad exclusiva de almacenar datos especialmente protegidos.

— 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.

> *Debe recomendarse que siempre que se traten datos especialmente protegidos, con independencia de cuáles sean, se procure obtener constancia del consentimiento expreso en forma escrita, puesto que recae sobre el responsable del tratamiento la carga de la prueba de demostrar que se disponía del consentimiento, con ese especial atributo de expreso.*

— En el caso de comisión de infracciones en materia de protección de datos, la gravedad de las mismas aumenta en un grado cuando el fichero contiene datos especialmente protegidos.

— Exige el establecimiento de medidas de seguridad de nivel alto para los ficheros que contienen datos especialmente protegidos, también llamados sensibles.

— Establece que los datos personales relativos a la comisión de infracciones penales o administrativas sólo pueden ser incluidos en ficheros de titularidad de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

No obstante todo lo anterior, la propia Ley Orgánica 15/1999 establece una excepción al consentimiento expreso y por escrito del afectado para el tratamiento de datos especialmente protegidos: cuando dicho 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 se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

En este supuesto concreto (atención asistencial por un profesional sanitario), el tratamiento de los datos especialmente protegidos puede realizarse amparado en un consentimiento tácito e implícito en la propia relación asistencial.

La misma situación analizada en el párrafo anterior se produce 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 lo ya indicado anteriormente sobre la primacía del derecho a la vida sobre la protección de datos, aunque éstos en este caso sean especialmente protegidos.

Debe tomarse en consideración la ambigüedad con que se enumeran los que la Ley considera datos especialmente protegidos. En el caso concreto de los datos referentes a la salud, deben considerarse incluidos los datos que hagan referencia a un diagnóstico médico concreto, pero también aquellos otros que, aun de forma indirecta, hagan referencia a la salud de una persona.

El dato que indica que una determinada persona se encuentra en la situación de Incapacidad Laboral Transitoria es un dato de salud, incluso si se desconoce la causa última (que como regla general no deberá ser conocida) de tal situación.

Incluso el hecho de que no conste que una persona se encuentra en la situación de ILT, también puede considerarse un dato de salud (de buena salud).

Si los datos (aun cuando sólo sea el nombre) de una persona figuran en un fichero de damnificados por determinada enfermedad, para gestionar la concesión de ayudas, debe considerarse como que contiene datos de salud.

3.5 Principio de seguridad de los datos

El responsable del fichero deberá 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 por 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.*

No será necesario adoptar las mismas medidas de seguridad para proteger un archivo de personas que se han inscrito para participar en una carrera popular que el que contenga su historia clínica o social.

En el supuesto de ficheros informatizados que contienen datos de carácter personal, se ha producido un desarrollo reglamentario de este principio mediante el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. De acuerdo con este reglamento:

- No se podrán registrar datos de carácter personal en los ficheros que no reúnan las condiciones que se determinan por vía reglamentaria.

- Las medidas de seguridad a adoptar se deben recoger en el ***documento de seguridad*** y se deberán dar a conocer a todos los usuarios del sistema de información, quedando obligados a su cumplimiento.

- Se prevé el establecimiento de distintos niveles de medidas de seguridad dependiendo de los datos que contenga el fichero, de manera que:

  — Serán de nivel básico para todos los ficheros que contengan datos personales.

  — Serán de nivel medio cuando, además, contengan datos relativos a infracciones administrativas o penales, Hacienda Pública, servicios financieros, información sobre solvencia patrimonial y crédito, o cuando

el fichero contenga un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

— Serán de nivel alto cuando en el fichero se traten datos sobre ideología, afiliación sindical, religión o creencias, origen racial, salud y vida sexual.

- El documento de seguridad deberá reflejar el nivel de seguridad que debe cumplir el fichero, siendo así distintas las medidas de seguridad a adoptar en cada uno de ellos.

En relación a los ficheros no automatizados (manuales estructurados), no existe en este momento ningún desarrollo reglamentario relativo a las condiciones que deben cumplirse con respecto a su integridad y seguridad y a las de los centros de tratamientos, locales, etc., si bien ello no debe interpretarse como que no haya que tomar medidas de seguridad.

¿Qué medidas habrá que adoptar?: las técnicas y organizativas que garanticen la seguridad de los datos, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos.

Existen muchas medidas que pueden adoptarse para el tratamiento de datos de forma manual, como por ejemplo:

— *recoger el expediente personal de un interesado que esté utilizando en mi actividad laboral o profesional cuando vaya a ausentarme de mi puesto de trabajo. Simplemente guardarlo en un cajón ya es una medida que aumenta la seguridad del tratamiento.*

— *romper cualquier papel que contenga datos de una persona y que vaya a tirar a la papelera.*

— *Establecer un procedimiento para la retirada de los papeles desechados, garantizando la confidencialidad de los datos hasta su destrucción, etc.*

3.6 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 es necesario que exista una dependencia laboral, funcionarial o administrativa indefinida para que el usuario con acceso al fichero esté sometido a este deber de secreto, el desempeño de cualquier prestación o trabajo que permita el acceso a datos personales, genera automáticamente la obligación de cumplir con este principio.

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.

3.7 Principio de Comunicación de datos

Este principio hace referencia al cumplimiento de determinadas obligaciones en el caso de que se produzca una cesión de datos personales, es decir, una revelación de éstos a persona distinta del interesado.

En todo caso, para que pueda llevarse a cabo una cesión legal de datos, deberán coincidir varios elementos fundamentales:

— Una premisa, que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.

— Una condición general, que exista previo consentimiento del interesado.

— Una información necesaria, que el interesado o afectado tenga conocimiento de la identidad del cesionario y de la finalidad para la que se van a ceder los datos.

El consentimiento, elemento fundamental para todo tratamiento de datos, no será necesario para la cesión en algunos casos:

— Cuando la cesión esté autorizada por una ley.

Remarcamos nuevamente el rango de la norma que habilita para excepcionar la necesidad de consentimiento. Debe tratarse de una ley, no siendo suficiente cualquier otro tipo de norma o disposición.

— Cuando se traten datos recogidos de fuentes accesibles al público (de alguna de las fuentes que enumera la Ley Orgánica 15/1999).

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 de profesionales, los diarios y boletines oficiales y los medios de comunicación.

— 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 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.

— 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.

Sólo para el ejercicio de las funciones que tienen atribuidas estas instituciones será posible la cesión de datos sin consentimiento del interesado.

— 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 intimidad o 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 hacerse sin consentimiento del interesado, siempre que el estudio epidemiológico se realice en los términos que establezca la legislación específica sobre sanidad.

— Cuando la cesión se produzca entre Administraciones públicas para el ejercicio de las mismas competencias.

Atendiendo al principio de cooperación y asistencia activa entre las administraciones que promueve la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá realizarse la cesión de datos entre dos administraciones cuando ambas tengan encomendado el ejercicio de la misma competencia para la que se recabaron los datos del interesado.

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

La excepción que contempla este supuesto está delimitada, desde un punto de vista subjetivo: cuando la cesión se produzca entre Administraciones públicas y, desde un punto de vista objetivo: cuando el tratamiento de los datos cedidos sea exclusivamente con fines históricos, estadísticos o científicos.

— Cuando los datos sean obtenidos o elaborados por una Administración pública con destino a otra.

Atendiendo también al mismo principio de cooperación y asistencia, se podrán ceder los datos sin consentimiento del interesado cuando éstos sean recabados por un órgano de la Administración en el ejercicio de una labor de asistencia, con destino a otra Administración que es la efectivamente competente para el ejercicio de la función para la que se recaba la información.

En estos dos últimos supuestos de excepción a la regla general de consentimiento, debe considerarse la necesidad establecida por el principio de información, de que el interesado pueda saber en el momento previo a la recogida de los datos, cuál va a ser el destino de los mismos, debiendo ser informado de forma expresa, precisa e inequívoca.

3.8 Principio de acceso a datos por cuenta de terceros

Avanzamos algo sobre este principio cuando nos referimos a la definición de **encargado de tratamiento**. El acceso a 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

Por ejemplo, si un Ayuntamiento encarga la gestión informática del padrón a una empresa privada, dicho encargo sería contrario a la Ley de Bases de Régimen Local, que en su artículo 17 únicamente habilita a las Diputaciones provinciales, Cabildos y Consejos insulares a asumir la gestión informática del padrón en los supuestos que los Ayuntamientos no dispongan de capacidad económica para ello.

En estos casos, la Ley Orgánica 15/1999 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.

La relación que se establece para el tratamiento de los datos personales debe regularse en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, 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.

> *Este punto de las estipulaciones que debe contener el contrato es muy importante, ya que trata de evitar que se puedan producir una serie de encargos en cadena. Sólo el responsable del fichero podrá encargar a un tercero el tratamiento de los datos.*

— 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.

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 responsabilidades propias del responsable del tratamiento.

4

DERECHOS DE LAS PERSONAS

DERECHOS DE LAS PERSONAS

Unidos al cumplimiento de las obligaciones que la Ley impone a los que participan en el tratamiento de datos personales, están los derechos que asisten al ciudadano en este mismo proceso de tratamiento de sus datos. Son las dos caras de la moneda que conforma el derecho a la protección de datos.

Es importante que los derechos sean conocidos por el ciudadano, pero casi aún más importante es que sean conocidos por aquellos que participan en el tratamiento, y una parte muy estimable de esa participación la conforman los usuarios.

Antes de abordar la exposición individualizada de los derechos, es necesario hacer una distinción de ellos en dos grupos:

- Los derechos que forman parte esencial del contenido del derecho fundamental a la protección de datos, que son:
  - el derecho de acceso,
  - el derecho de oposición,
  - el derecho de rectificación, y
  - el derecho de cancelación.
- Los otros derechos reconocidos por la Ley Orgánica 15/1999:
  - el derecho de impugnación de valoraciones,
  - el derecho a la consulta al Registro General de Protección de Datos, y
  - el derecho a indemnización.

4.1 El derecho de acceso

Es el derecho personal de todo ciudadano, sólo ejercitable respecto de él mismo, a conocer los datos que sobre su persona figuran en un fichero determinado sometidos a tratamiento, cuál ha sido el origen de éstos, y qué cesiones se han realizado o se prevé realizar en el futuro.

Para el ejercicio de este derecho, el ciudadano se dirigirá directamente al responsable del fichero mediante solicitud, por cualquier medio que garantice la identificación del afectado, haciendo constar el fichero o ficheros que se quieren consultar. Al tratarse de un derecho personalísimo, sólo podrá ser ejercitado por el propio interesado, excepto en el caso de menores o incapacitados, en que la solicitud la presentará el correspondiente representante legal.

El responsable del fichero deberá responder en el plazo máximo de un mes, contestando a los extremos solicitados, y facilitando la información en la forma elegida por el afectado, ya sea por medio de visualización en pantalla, mediante escrito, copia, telecopia o fotocopia, certificada o no, o por cualquier otro procedimiento adecuado, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Este derecho sólo podrá ser ejercitado a intervalos no inferiores a 12 meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Sólo 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.

Por último, en cuanto al ejercicio de este derecho en algunos supuestos específicos, habrá que estar a lo que establezca la legislación especial 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 Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que regula el acceso a los expedientes administrativos.

4.2 El derecho de oposición

En aquellos casos en los que no resulte necesario el consentimiento del interesado para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, éste podrá oponerse al tratamiento de sus datos cuando existan motivos fundados y legítimos relativos a una concreta situación personal. El responsable del fichero tendrá que proceder a la exclusión de los datos relativos al afectado.

Es obvio que para que el ejercicio de este derecho sea efectivo es necesario haber cumplido previamente con el principio de información.

4.3 El derecho de rectificación

Cuando el titular de los datos tuviera constancia de que sus datos personales tratados en un fichero son inexactos o incompletos, podrá solicitar del responsable del fichero la rectificación de los mismos.

Este derecho se ejercita ante el responsable del fichero por el titular de los datos o afectado, es un derecho personalísimo que no puede ejercitarse por persona distinta de su titular, a excepción de menores e incapacitados.

El derecho de rectificación se ejerce mediante solicitud dirigida al responsable del fichero o tratamiento por cualquier medio que garantice la identificación del afectado. El responsable deberá atender a la petición, previa comprobación de los documentos justificativos de la misma presentados por el interesado, en el plazo de diez días.

También el responsable podrá modificar por propia iniciativa los datos que resulten inexactos o incompletos.

Sólo 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.

4.4 El derecho de cancelación

Cuando el titular de los datos tuviera conocimiento de que los datos personales tratados en un fichero no se ajustan a lo dispuesto en la Ley Orgánica 15/1999, podrá solicitar del responsable del fichero la cancelación de los mismos.

La cancelación dará lugar al bloqueo de los datos, que no tiene que consistir necesariamente en el borrado físico de de la información. Dichos datos deberán conservarse a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Cumplido el citado plazo, deberá procederse a la supresión.

Este derecho se ejercita ante el responsable del fichero por el titular de los datos o afectado. Igualmente es un derecho personalísimo sólo ejercitable por el titular de los datos, de manera que la solicitud deberá contener la identificación del afectado.

El responsable deberá atender la petición en el plazo de diez días.

La petición de cancelación por parte del afectado está limitada por el deber de conservación de los datos durante los plazos previstos en las disposiciones aplicables o durante las relaciones contractuales con la persona o entidad responsable del tratamiento.

Sólo 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 esté siendo objeto de actuaciones inspectoras.

4.5 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:

- criterios de valoración utilizados, y
- 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.

4.6 Derecho a indemnización

El afectado o interesado tendrá derecho a solicitar una indemnización económica cuando, a consecuencia del incumplimiento por el responsable de 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.

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

4.7 Derecho de consulta al Registro General de Protección de Datos

No debe confundirse este derecho de consulta con el derecho de acceso, aun cuando se establece para facilitar el ejercicio de éste. El derecho de consulta a los registros de ficheros que existen en la Agencia de Protección de Datos Española (o de las

Comunidades Autónomas en que existen) es el derecho de los interesados o afectados a recabar información sobre la existencia de ficheros de datos de carácter personal inscritos en los referidos Registros, la finalidad de éstos y la identidad del responsable del fichero.

Esta información se puede solicitar ante la Agencia de Protección de Datos correspondiente, si bien se señala que los Registros de las Agencias Autonómicas son complementarios del Registro General de Protección de Datos de la Agencia Española de Protección de Datos que es el que, de conformidad con la LOPD, da publicidad de los ficheros inscritos.

La información existente en el Registro 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, y los colectivos de los que se recabaron los datos, entre otras.

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, ...etc. Los Registros antes mencionados no recogen el contenido de los ficheros, sino las características de los mismos.

5

ÓRGANOS DE CONTROL

ÓRGANOS DE CONTROL

Vistos los principios que deben regir el tratamiento de datos personales y los derechos que amparan a las personas para hacer efectivo su derecho fundamental a la protección de datos, es necesario ver ahora las garantías que la legislación prevé para asegurar la aplicación de los principios y el ejercicio de los derechos.

Las Agencias de Protección de Datos se constituyen en este punto en el garante de la aplicación de lo dispuesto en la Ley Orgánica 15/1999, o Ley Autonómica correspondiente, respecto del ámbito de aplicación determinado por la misma.

Tanto la Agencia Española de Protección de Datos como las autonómicas, cada una en su ámbito competencial (en el caso de las segundas, se circunscribe a los ficheros de datos de carácter personal creados o gestionados por las Administraciones Públicas de su ámbito territorial, mientras que todos los tratamientos de datos realizados por entidades privadas son siempre responsabilidad de la primera), tienen como función el control de la aplicación de la Legislación sobre protección de datos y la defensa de los derechos de los ciudadanos para el efectivo cumplimiento del derecho fundamental a la protección de datos personales.

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

Las Agencias de Protección de Datos tienen competencias para inspeccionar de oficio, o a instancia de parte, los ficheros de datos personales de lo que genéricamente hemos denominado Administración pública.

El objeto de las inspecciones es comprobar el cumplimiento de los principios de protección de datos en el desarrollo del tratamiento de los datos personales, y el respeto a los derechos 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.

Aparte de las funciones de control que competen a las Agencias de Protección de Datos, éstas pueden ejercer también una labor consultora, 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 tanto de forma individual, asesorando sobre el procedimiento de inscripción de ficheros y resolviendo las consultas puntuales planteadas por los responsables de los respectivos ficheros, como de forma colectiva, a través de la celebración de jornadas informativas organizadas por sectores de actividad, a fin de tratar en profundidad las cuestiones particulares que pueden plantearse en los distintos ámbitos de la actuación de la Administración.