TEMA 7

LA PROTECCIÓN DE DATOS

1. Concepto; 2. Clases de datos; 3. Fundamento de la protección de datos: El derecho a la autodeterminación informativa; 4. Ámbito internacional y comunitario; 5. El régimen jurídico español de la protección de datos de carácter personal: 5.1. El tratamiento de los datos de carácter personal; 5.2. El contenido del tratamiento: derechos y obligaciones de las partes: 5.2.1 Derechos y obligaciones del responsable del tratamiento; 5.2.2 Derechos y obligaciones del interesado o afectado; ; 5.3. Tratamientos especiales; 5.4. Especial referencia al movimiento internacional de datos; 5.5. Extinción del tratamiento; 5.6. Régimen de infracciones y sanciones; 5.7. El procedimiento sancionador; **6. La Agencia de Protección de Datos**

1. Concepto

Utilizamos la expresión "protección de datos" para referirnos a la protección jurídica de las personas en lo concerniente al tratamiento de sus datos personales. La ley define un concepto legal de "datos de carácter personal", y los define como "cualquier información concerniente a personas físicas identificadas o identificables".

Se trata de proteger a las personas ante el manejo o manipulación, no autorizada, de sus datos personales, pero siempre que estos datos sean susceptibles de tratamiento.

Tres son las características básicas con las que delimitaremos la llamada protección de datos:

a) que los datos sean susceptibles de tratamiento o se encuentren en soporte susceptible de ese tratamiento.
b) posibilidad de identificar el resultado del tratamiento de los datos con el titular.
c) el manejo o acceso a los datos sin permiso, o sin conocimiento, según los casos, del titular, independientemente de que ese acceso o manejo sea malintencionado o no.

2. Clases de datos

Puesto que estudiaremos el tratamiento de esos datos, es preciso clasificarlos en categorías por cuanto unos van a requerir de mayor protección que otros. Esa clasificación la haremos atendiendo a su confidencialidad, esto es, el mayor o menor grado de secreto con el que se van a guardar y tratar los datos personales.

Clasificación:

En todos los casos se trata de datos personales que pertenecen a la esfera privada del

individuo, pero no todos pueden ser tratados con en el mismo grado y con la misma posibilidad de defensa y capacidad de decisión sobre su difusión por el titular. Por ejemplo, los datos identificativos (nombre, apellidos, domicilio, lugar de nacimiento) de una persona, en términos generales, son datos de más débil protección que otros porque así lo considera la conciencia social. Por ello distinguimos primero entre datos personales públicos y privados.

Públicos serán aquellos que son conocidos por un cuantioso número de personas sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del dato, ni, por la calidad del dato, pueda impedir que una vez conocido sea libremente difundido dentro de unos límites de respeto y de convivencia cívicos, teniendo en cuenta además que la conciencia social es favorable a su publicidad, siendo frecuente su difusión como si no se tratara de datos personales.

Privados serán los datos personales que tienen reguladas y tasadas las situaciones o circunstancias en que la persona se ve obligada a ponerlos en conocimiento de terceros, siendo la conciencia social favorable a impedir su difusión y respetar la voluntad de secreto sobre ellos de su titular.

Dentro de estos distinguiremos entre íntimos y secretos. Íntimos: son aquellos datos que el individuo pueda proteger de su difusión frente a cualquiera, pero que, de acuerdo con un fin determinado, esté obligado -por mandato legal- a dar periódica o regularmente, en cumplimiento de sus obligaciones cívicas. Secretos: son los que el ciudadano no estará obligado a dar a nadie. A estos últimos la doctrina los denomina "datos sensibles".

3. El derecho a la autodeterminación informativa

Los datos personales están suficientemente protegidos en los ordenamientos constitucionales por el derecho al honor y a la intimidad. Pero cuando surge la informática, y la posibilidad de tratamiento automatizado de la información y su transmisión telemática, es cuando aparece una nueva relación entre datos y personas que necesita ser protegida más allá de las normas referentes a la intimidad. De todos es sabido que la tecnología informática permite ahora, a partir de informaciones dispersas e incluso anónimas, conocer múltiples facetas de la vida de hombres y mujeres perfectamente ajenos al hecho de que sus características y hábitos vitales están en manos de terceros que pueden utilizarlos de forma que les depare perjuicios importantes.

El derecho que se trata de proteger no es solamente el de la intimidad o al honor, sino algo más complejo que en los ordenamiento anglosajones se llama *privacy* y que nosotros identificamos como "privacidad". Ello se plasma en el reconocimiento constitucional de lo que se ha venido a llamar un nuevo derecho fundamental: el derecho a la autodeterminación informativa, que viene recogido en el artículo 18.4 de la Constitución:

"*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*".

Este derecho consiste sencillamente en el control que a cada uno de nosotros nos corresponde

sobre la información que nos concierne personalmente sea íntima o no para preservar, de este modo y en último extremo, la propia identidad, nuestra dignidad y libertad.

Implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos que desea que se conozcan, así como facultades que le aseguren que los datos de su persona que manejan informáticamente terceros son exactos, completos y actuales y que se han obtenido de modo leal y lícito.

También supone el control sobre el uso de esa información ya que ésta en sí misma no tiene ninguna utilidad si no es para ser utilizada en múltiples relaciones.

Naturalmente, el nivel de autodeterminación, es decir, de disposición de uno mismo sobre sus propios datos dependerá de la naturaleza de éstos y de su mayor o menor proximidad al núcleo de la intimidad. No obstante, aunque, cuando nos encontremos fuera de él, no será posible impedir que circule información sobre nuestras personas, siempre hemos de estar en condiciones de asegurarnos de su calidad y de conocer y controlar su utilización.

4. Ámbito internacional y comunitario

a) El Convenio del Consejo de Europa

Aunque lo antes referido es ya una realidad en nuestro ordenamiento jurídico, lo cierto es que tanto en otros ordenamientos jurídicos como en el ámbito de organizaciones internacionales como el Consejo de Europa se dejó sentir prontamente la preocupación que el uso de la informática generaba para la salvaguarda de los derechos de la persona.

Ello se plasmó en el Convenio del Consejo de Europa *para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal*, de 28 de enero de 1981.

Este Convenio fue ratificado por España y entró por ello en nuestro ordenamiento jurídico publicándose en el BOE el 15 de noviembre de 1985. No obstante, hay que tener en cuenta que esta no es una norma de aplicación directa, ya que, en su artículo 4.1, remite a los propios Estados firmantes para que desarrollen leyes y adopten medidas para dar cumplimiento a los principios enunciados en su texto. Es decir, que en nuestro país, para que de verdad sean efectivos los principios básicos de protección de las personas contra los posibles abusos de la utilización de sus datos personales que se encuentran en soportes susceptibles de tratamiento automatizado, se tendrá que adoptar previamente una ley de las llamadas de protección de datos, lo que se realizó varios años después con la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) y ahora con la nueva ley de 13 de diciembre de 1999.

b) La Directiva 95/46 CE de 24 de octubre de 1995

La Comunidad Europea aprueba la Directiva 95/46 CE del Parlamento Europeo y el Consejo de

24 de octubre de 1995 que vino a ocuparse de que los Estados garantizasen la protección de los derechos y libertades fundamentales de las personas físicas y en particular el derecho a la intimidad en lo que respecta al tratamiento de los datos personales. Por ello era necesario adaptar la Ley de 1992 a la Directiva a través de la Ley de 13 de diciembre de 1999.

5. El régimen jurídico español del tratamiento de datos de carácter personal: Ley Orgánica 15/1999 de 13 de diciembre de protección de datos de carácter personal (LOPD)

Hay que subrayar es una Ley Orgánica la norma que procede a regular la protección de los datos personales. La LOPD tiene por objeto garantizar y proteger en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas fisicas, y especialmente el honor e intimidad personal y familiar. El objetivo de la ley es garantizar la intimidad limitando el uso de la informática.

El objeto de la ley es la privacidad, es decir, aquél ámbito de la vida privada que se ve afectado por la posibilidad real de que las actuaciones cotidianas y la información de ellas se acumule o conserve esbozando lo que se llama el perfil del afectado.

La aplicación de la LOPD se extiende a todos aquellos datos de carácter personal que figuren en ficheros públicos y privados. Así, lo que queda claro es que la LOPD contiene el régimen jurídico general de la protección de los datos personales ante el uso de la informática. El ámbito de la ley será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento.

Se excluyen del ámbito de aplicación de la ley:

a) los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) 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 regularán por su legislación específica los ficheros que tengan por objeto las siguientes materias: el régimen electoral, los datos que sirvan exclusivamente para fines estadísticos, 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, el Registro Central de Penados y Rebeldes y 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.

5.1. El tratamiento de los datos de carácter personal

El tratamiento de los datos determina una relación jurídica entre el responsable del tratamiento y el interesado que tiene por objeto el tratamiento de los datos de carácter personal. El nacimiento de la relación puede surgir bien por el consentimiento de las partes o bien por un autorización legal (por ejemplo, el tratamiento de los datos por el Padrón municipal o la obligación de comunicar a la Hacienda Pública los cambios respecto de la información sometida a tratamiento).

Dentro de esta relación del tratamiento de los datos distinguimos:

- un elemento subjetivo: las partes de esa relación jurídica son el responsable del fichero y el interesado o afectado. El interesado o afectado es la persona física titular de los datos que son objeto de tratamiento. Las personas jurídicas (entes o empresas) están expresamente excluidas del ámbito de la ley.

- un elemento objetivo: el objeto de la relación jurídica de tratamiento es el dato de carácter personal. Para que exista un dato de carácter personal es preciso que exista la información y la persona a la que concierne esa información.

Hay que distinguir entre fichero y tratamiento. El fichero es la mera acumulación de los datos de carácter personal que deberá manifestarse en un soporte informático o no automático en el que los datos estén organizados de acuerdo a un criterio lógico, por ejemplo, por orden alfabético. Es decir que haya una entrada para acceder a los datos.

El tratamiento se refiere a las actuaciones u operaciones que se realizan con los datos. El tratamiento hace referencia a una actividad concreta con los datos.

- un elemento formal: el inicio del tratamiento se realiza por una autorización legal o por el consentimiento. El art. 6.1 LOPD determina que es necesario el consentimiento por parte del interesado cuando tenga por único objeto el tratamiento de los datos personales.

Como regla general, la forma en la que se otorga el consentimiento no es esencial para el nacimiento de la relación, es decir no se exige una forma concreta por la ley. Sin embargo, la ley exige que el consentimiento sea expreso cuando se trata de datos especialmente protegidos y que sea expreso y otorgado por escrito en el caso de los datos relativos a la ideología, afiliación sindical, religión o creencias.

En derecho se admiten tres formas de otorgar el consentimiento: expresa, presunta y tácita. El consentimiento expreso puede hacerse por escrito, mediante comunicación telemática o por cualquier medio. Implícito o presunto cuando el consentimiento se deduce de los actos del interesado, por ejemplo cuando rellenamos un formulario. Tácito cuando se deduce por la falta de actuación del interesado, por ejemplo cuando las compañías telefónicas utilizan los datos para promoción y publicidad de sus productos cuando concurre el silencio de los interesados.

La Agencia de protección de datos (APD) ha admitido las tres formas de otorgar el consentimiento, por cualquier medio admitido en derecho.

No será preciso el consentimiento en los siguientes casos (art. 6.2 LOPD):

- los tratamientos mantenidos por las administraciones públicas para el ejercicio de sus competencias
- el tratamiento de datos relativos a las partes de un contrato o precontrato de una relación negocial, administrativa o laboral que sean necesarios para su cumplimiento.
- el tratamiento para proteger un interés vital del interesado.
- el tratamiento de los datos que se hallen publicados en fuentes accesibles al público. Si bien el afectado deberá ser informado con posterioridad de la existencia del tratamiento y su finalidad, con la posibilidad de oponerse al tratamiento si existen motivos fundados y legítimos relativos a una situación personal.

5.2 El contenido del tratamiento de datos de carácter personal: derechos y obligaciones de las partes

5.2.1 Derechos y obligaciones del responsable del tratamiento

1. Deber de inscripción en el Registro General de Protección de Datos (RGPD)

El Registro general de protección de datos es un órgano de la APD que tiene por objeto la inscripción de los ficheros de titularidad de las Administraciones Publicas, los ficheros de titularidad privada, las autorizaciones establecidas en la ley respecto de las transferencias internacionales de datos, los códigos éticos, así como los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición. La inscripción en el registro es declarativa a efectos del funcionamiento del tratamiento, simplemente es necesaria para cumplir la obligación legal y no incurrir en las correspondientes sanciones.

2. Derecho de uso de los datos una vez obtenido el consentimiento

El responsable del tratamiento puede obtener los datos de carácter personal de dos tipos distintos de fuentes:

a) del propio interesado, de forma que en el mismo momento en que obtenga los datos debe obtener el consentimiento para incluirlos en un tratamiento.
b) De cualquier otra fuente de información en cuyo caso debe informar al afectado del hecho de haber recibido la información, la procedencia de ésta y la finalidad de su tratamiento dentro de los tres meses siguientes o antes de realizar la primera cesión de los datos. La ley en este supuesto permite el tratamiento de los datos por el responsable sin otra obligación de la de informar en el plazo de tres meses desde que se inicio el tratamiento acerca de dicha circunstancia y la atención al derecho de cancelación para que pueda ejercerse por el

interesado.

3. Deber de información sobre el tratamiento

En la recogida de los datos será requisito para la validez del consentimiento que de modo previo e inequívoco se advierta al interesado: de la existencia de un fichero automatizado, de la finalidad del mismo, de los destinatarios de la información, del carácter obligatorio o facultativo de sus respuestas a las preguntas planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad y dirección del responsable del fichero.

Cuando se utilicen cuestionarios u otros impresos para la recogida figurarán las advertencias señaladas en los puntos anteriores.

4. Obligaciones respecto de la calidad de los datos

La calidad de los datos exige que "los datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido". Esta obligacion no permite que se puedan incluir en el tratamiento datos que no sean necesarios para atender a la finalidad a la que se autoriza.

La calidad de los datos establece una serie de obligaciones:

- Si los datos han dejado de ser necesarios o adecuados para la finalidad para la que han sido recogidos, nace la obligación de cancelar los datos innecesarios.
- Se establece en la ley la obligación de adecuación de los datos a la finalidad autorizada, es decir, a la actividad genérica a que se destinan los datos objeto de tratamiento. Sin embargo, no será incompatible que posteriormente se destinen a un tratamiento con fines históricos, estadísticos, o científicos
- Los datos deberán ser exactos y puestos al día respondiendo con veracidad a la situación actual del afectado. Si no son exactos o están incompletos deben ser cancelados o sustituidos por los correctos por efecto del deber de actualización y rectificación de los datos.
- En cuanto a las obligaciones de organización, se exige que los datos sean almacenados de forma que permitan el ejercicio del derecho de acceso. No se establece una organización concreta, se obliga a cualquiera que sea la estructura del tratamiento el afectado pueda ejercer su derecho de acceso.
- Por último se establece la prohibición de recogida de datos por medios fraudulentos, desleales o ilícitos.

5. Adopción de las medidas de seguridad

El responsable de los datos deberá adoptar las medidas necesarias para mantener la seguridad de los datos, al tiempo que está obligado a evitar la alteración, la pérdida y el acceso no autorizado.

Esta obligación legal se ha desarrollado reglamentariamente mediante el RD 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal. El sistema de seguridad se estructura en tres niveles:

- nivel básico: se aplica a todos los tratamientos de datos, con independencia de su contenido, tamaño o finalidad. Las medidas de este nivel básico son las mínimas que deben establecerse para cualquier tratamiento. La principal de estas medidas es la que consiste en la elaboración de un documento de seguridad por el responsable del tratamiento.

- nivel medio: se exige si los ficheros conforman un perfil de la persona por incluir datos relativos a la infracción de normas administrativas, penales, tributarias o servicios financieros. Las medidas principales son la obligación de nombrar un responsable de seguridad, la obligación de realizar una auditoria del sistema de seguridad y la llevanza de un registro de incidencias

- nivel alto: se exige si los ficheros contiene datos de ideología, religión, creencias, salud o vida sexual así como los que contengan datos con fines policiales sin consentimiento de las personas afectadas. Las medidas cualificadas de seguridad consisten en el cifrado de la información, el registro de accesos y la obligación de conservar copias de seguridad.

6. Deber de secreto

La obligación del deber de secreto afecta al responsable del fichero y demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal, incluso después de haber finalizado la relación con el titular o el responsable del fichero.

7. Prohibición de la cesión de los datos

Sólo podrá realizarse la cesión de los datos con el consentimiento previo del afectado y para el cumplimiento de la finalidad previamente determinada del fichero.
Será nulo el consentimiento cuando no conste la finalidad a la que se destinaran los datos o el tipo de actividad de aquel a quien se pretendan comunicar. Además, el cesionario se obliga, por la sólo recogida de los datos, a cumplir todas las disposiciones de la Ley.

Hay una serie de excepciones a la exigencia del consentimiento previo:

a) Cuando la cesión está autorizada en una Ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. en este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

8. Deber de comunicar la primera cesión de los datos

El responsable del fichero deberá informar de a los afectados de la primera cesión de los datos en cualquier supuesto indicando la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. La doctrina ha criticado esta obligación, por entender que conforme a la Directiva debe cumplirse esta obligación sólo en los casos en que el interesado no conozca la existencia del tratamiento.

Se excepciona esta obligación en los casos de cesiones entre las Administraciones públicas y el destinatario sea el ministerio fiscal, jueces y tribunales, defensor del pueblo y tribunal de cuentas.

9. Derecho a la autonomía en la organización: el encargado del tratamiento.

La Ley no exige que sea el responsable del tratamiento el que realice dicho tratamiento. De modo que el responsable del tratamiento puede encargar a un tercero la gestión del tratamiento a través de un contrato de arrendamiento de servicios.

5.2.2 Derechos y obligaciones del interesado o afectado

Los derechos a que se hace referencia a continuación tienen carácter personalísimo, por lo que sólo pueden ejercerse por parte del afectado. Podrá no obstante actuar su representante legal cuando el afectado se encuentre en situación de minoría de edad o esté declarado incapaz para el ejercicio de sus derechos.

1. Derecho a no soportar valoraciones automáticas.

Se otorga al afectado el derecho a impugnar tanto los actos administrativos como las decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea una interrelación de datos automatizados de carácter personal que ofrezca una definición de sus características o personalidad.

2. Consulta al Registro General de Protección de datos

Se trata del derecho de los interesados a consultar e1 Registro General de Protección de Datos, donde consta toda la información de las características de los tratamientos: la existencia de los ficheros o tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento para hacer posible el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El Registro es una fuente de información y de consulta pública y gratuita.

En el Registro General queda inscrita una descripción de los ficheros que tienen la obligación legal de inscribir. Por tanto, se puede averiguar mediante consulta al Registro información de aspectos concretos de los ficheros, tales como su finalidad, estructura, identidad del responsable del tratamiento, ubicación, cesiones previstas..., pero no contiene los datos de carácter personal que se incluyen en el tratamiento.

3. Derecho de acceso

Se regula el derecho del afectado a solicitar obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento al responsable del mismo sobre el origen de sus datos así como las comunicaciones realizadas o las que se prevean.

El derecho de acceso sólo puede ejercerse a intervalos de doce meses, salvo que el afectado acredite un interés legítimo antes de que transcurra dicho plazo.

El procedimiento para ejercitar este derecho, que consiste en las siguientes fases:

a) Solicitud o petición dirigida al responsable del fichero, que tiene el plazo de un mes para resolver.
b) Caso de acceder a la solicitud, se lo notificará al afectado y le dará un plazo de 10 días para ejercer su derecho a contar desde ese momento.
c) Caso de desestimar la solicitud, cabe reclamación ante la Agencia de Protección de Datos

4. Derecho de rectificación y cancelación

Si los datos no se ajustan a lo dispuesto en esta ley o que se encuentran en un fichero son inexactos, erróneos o incompletos, el afectado podrá exigir que el responsable cumpla con la calidad de los datos a través de su derecho de rectificación, o cancelación en su caso.
El art. 16 LOPD establece que el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación en el plazo de 10 días. El interesado tendrá que acreditar que el dato es erróneo o incompleto y la corrección que debe hacerse. El responsable está obligado a atender la cancelación de los datos sin necesidad de que se dén requisitos especiales. Por otro lado, el responsable no podrá exigir compensación alguna por la

rectificación o cancelación de los datos de carácter personal inexactos.

El derecho de cancelación es el derecho del interesado a que se excluyan del tratamiento datos de carácter personal ya sea por erróneos o por no interesarle que se sometan a tratamiento.

5. Derecho de oposición

Los casos en que no sea necesario el consentimiento, y siempre que la ley no disponga otra cosa, el afectado podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

El derecho de oposición consiste en la negativa a la continuación del tratamiento o al rechazo a las finalidades concretas del tratamiento y la cancelación genérica de los datos respecto de los datos que pudieran estar sometidos al mismo. Los interesados tendrán derecho a oponerse, previa petición y sin gastos al tratamiento de los datos que les conciernan, cancelandose las informaciones que contengan por su simple solicitud

6. Tutela de la Agencia de Protección de Datos.

El interesado tiene un derecho de reclamación ante la Agencia de Protección de datos, en virtud del cual solicita la tutela de sus derechos y puede acudir a la Agencia para cualquier actuación contraria a la ley. Para ello, dispone de dos procedimientos:

1. El procedimiento de tutela de derechos tiene como finalidad garantizar el ejercicio efectivo de los derechos de acceso, rectificación, cancelación y oposición del afectado. El procedimiento se divide en tres fases:

A) la fase de iniciación: El procedimiento se inicia mediante escrito del afectado expresando con claridad el contenido de la reclamación y los preceptos de la Ley Orgánica que se consideran vulnerados.
B) La fase de audiencia: Se dará traslado de la misma al titular del fichero para que en el plazo de quince días formule las alegaciones que estime pertinentes.
C) fase de resolución: la Agencia de Protección de Datos resolverá la reclamación en el plazo máximo de seis meses dando traslado de la misma a las partes, una vez realizadas las acciones que estime pertinentes.

2. Procedimiento sancionador

Los responsables de los ficheros están sujetos al régimen sancionador establecido en la Ley Orgánica. Existe una serie de comportamientos que se califican como infracciones leves, graves y muy graves.

El procedimiento sancionador se iniciará siempre de oficio mediante acuerdo del Director de la Agencia de Protección de datos, bien por denuncia de un afectado o afectados o

por propia iniciativa. El régimen de infracciones y sanciones se enumeran en el ANEXO II (art. 44 y 45 de la Ley Orgánica).

7. Derecho de indemnización.

Si los interesados han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la presente ley por el responsable o por el encargado del tratamiento, tienen derecho a ser indemnizados.

La responsabilidad patrimonial se reclamará por vía contencioso administrativa cuando se trate de los ficheros de titularidad pública, o bien ante los Tribunales ordinarios para los ficheros de titularidad privada.

5.3 Tratamientos especiales

La ley regula los siguientes tratamientos sectoriales bajo una doble categoría:

1. los ficheros de titularidad pública, entre los que regula el tratamiento de los ficheros de las Fuerzas y Cuerpos de la Seguridad del Estado

2. los ficheros de titularidad privada, en los que regula los siguientes ficheros específicamente:
   - ficheros de solvencia patrimonial y de crédito
   - tratamientos con fines de publicidad y de prospección comercial
   - datos incluidos en fuentes de acceso público
   - tratamientos con fines sanitarios
   - tratamientos con finalidad histórica, estadística o científica
   - datos especialmente protegidos
   - tratamientos con finalidad del ejercicio del derecho a la información
   - tratamientos por organizaciones religiosas
   - tratamientos realizados por las organizaciones no gubernamentales
   - supuesto de la fusión y escisión empresarial
   - tratamiento no automatizado.

1. Ficheros de titularidad pública

Son aquellos cuyo titular es una Administración Pública. Se estipula que su creación, modificación o supresión solamente podrá llevarse a cabo "por medio de disposición general publicada en el Boletín Oficial del Estado o en el Diario Oficial correspondiente". En esa disposición se deberá indicar la finalidad del fichero, las personas o colectivos sobre las que se pretende obtener datos, los usos previstos para el mismo, el procedimiento de recogida de datos, la estructura básica del fichero, las cesiones de datos que se prevean, los órganos de la Administración responsables del fichero y el servicio de la Administración ante el que se puedan ejercitar los derechos de acceso, rectificación y cancelación.

Los artículos 21 y 24 dedicados a la comunicación de datos entre las administraciones públicas y a las excepciones de los derechos de los afectados respectivamente, han sido objeto de varios recursos de inconstitucionalidad que han sido resueltos por la STC 292/2000 de 30 de noviembre de 2000:

La STC 292/2000 de 30 de noviembre declara nulos por ser inconstitucionales dos preceptos de la ley:

1. El artículo 21 establece como regla general que los datos personales no serán comunicados de unas administraciones a otras para el ejercicio de competencias diferentes o que versen sobre materias distintas "salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación de un fichero o por disposiciones de superior rango que regule su uso". Este inciso se ha declarado inconstitucional por entender que permite que por reglamento se pueda limitar el derecho fundamental a la protección de datos personales, limite que sólo puede establecerse por una norma con rango de ley y siempre que se justifique en la protección de otros derechos constitucionales.
2. El artículo 24 establece entre otras excepciones:

- que el ciudadano no será informado en la recogida de datos, cuando la información impida o dificulte gravemente el cumplimiento de las funciones de verificación y control de las administraciones públicas

El Tribunal Constitucional declara nulo este precepto por entender que abre un espacio de falta de seguridad jurídica por dos motivos: uno, los supuestos en que se limita el derecho fundamental de la protección de datos han de establecerse por ley (art. 53.1), ley que ha de precisar y justificar con exactitud los limites de este derecho y no puede trasladar esta función a la Administración, en definitiva, tales restricciones no pueden basarse en la actividad de la Administración Segundo, la expresión " funciones de control y verificación" permitiría a la Administración en todos los casos en los que necesite datos personales de alguien ejercer esta potestad ya que no se han fijado los casos en los que concurre la necesidad de control y verificación.

- que no serán de aplicación los derechos de acceso, rectificación y cancelación si ponderados los intereses en presencia resultase que esos derechos deben ceder ante razones de interés publico o ante intereses de terceros más dignos de protección.

El Tribunal Constitucional lo declara inconstitucional porque el responsable del fichero podría negar el ejercicio de estos derechos a un ciudadano por vía administrativa sin establecer cuales pueden ser esos intereses no las circunstancias en las que puede restringir el derecho a la protección de los datos de carácter personal.

- *Ficheros de las Fuerzas y Cuerpos de la Seguridad del Estado.*

Dentro de la categoría de los ficheros de titularidad pública, la ley regula los ficheros de las Fuerzas y Cuerpos de la Seguridad del Estado.

La recogida y tratamiento de los datos personales se podrán recoger, sin consentimiento del afectado, "aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales". Asimismo, la recogida en estas condiciones de los que hemos llamado "datos sensibles", podrá hacerse "exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta". La cancelación de estos datos se realizará "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

La ley introduce una garantía para el interesado que consiste en el posible control de la legalidad de la actuación administrativa y la obligación de resolver las pretensiones formuladas por los interesados que corresponden a los órganos jurisdiccionales.

Continúan las excepciones y limitaciones a los derechos, al expresar la LOPD que los responsables de los ficheros de las Fuerzas y Cuerpos de Seguridad y los de la Hacienda Pública podrán denegar el ejercicio de los derechos de acceso, rectificación y cancelación cuando ello obstaculice las actuaciones administrativas tendentes a asegurar, para los primeros, la defensa del Estado, la seguridad pública o las necesidades de la investigación, y para los segundos, el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Se establece no obstante que el afectado al que se le deniegue el ejercicio de tales derechos podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente en cada Comunidad Autónoma en el caso de ficheros mantenidos por los Cuerpos de Policía propios de estas, o por las Administraciones Tributarias Autonómicas, quienes deberán asegurarse de la procedencia o no de la denegación.

2.Los ficheros de titularidad privada

La LOPD permite la creación de ficheros de titularidad privada que contengan datos de carácter personal cuando sea necesario para el objetivo de la actividad o el logro de la persona o empresa y siempre que se respeten las garantías establecidas en la ley

La persona física o jurídica que haya creado un fichero deberá notificarlo previamente a la APD, así como los cambios posteriores que se produzcan en la finalidad del fichero automatizado, en su responsable. El fichero será objeto de inscripción en el RPD

Como requisito se exige que el responsable del fichero informe al interesado de la primera cesión de los datos.

En cuanto al funcionamiento de los ficheros hay que hacer una referencia expresa a los *códigos tipo* que puedan establecer, mediante acuerdos entre ellos, los responsables de los ficheros privados para determinar pautas organizativas y funcionales uniformes que abarquen tanto los aspectos sustantivos de su actividad (las condiciones de organización, régimen de

funcionamiento, procedimientos aplicables y las garantías para el ejercicio de los derechos de las personas) como los instrumentales, a propósito de la seguridad del entorno o de los programas y equipos. Mediante esta técnica, la LOPD ha querido dejar el espacio suficiente para que se incardinen en el sistema de protección de datos estas normas fruto de la autonomía privada. Por ello, el art. 32 ordena su depósito o inscripción en el Registro General de Protección de Datos y habilita a sus encargados para denegarla cuando, a su juicio, no se ajusten a la LOPD o a lo dispuesto en el RD 1720/2007 Estos códigos tienen "el carácter de códigos deontológicos o de buena práctica profesional".

Dentro de esta categoría , la ley dedica una atención especial a:

- *Los datos incluidos en fuentes accesibles al público.*

Se trata de los datos que se encuentren en el censo promocional o en las listas de personas pertenecientes a grupos profesionales que se limitarán a la finalidad a que se destina cada listado.

Se exige siempre el consentimiento del afectado para recabar los datos, al mismo tiempo que ese consentimiento puede ser revocado. Se reconocen los derechos de información, de acceso, de rectificación, de cancelación, y toda esa lista que ya hemos enumerado. Incluyendo, como es natural, un control del interesado en la posibilidad de cesión de los datos, que debe ser con su total consentimiento.

- *Ficheros de solvencia*

Deben distinguirse dos supuestos claramente diferenciados:

1. Ficheros que contienen información sobre solvencia patrimonial y crédito de carácter positivo, es decir, que hace referencia a las posibilidades económicas y financieras de una persona física.
Sólo podrán obtenerse los datos personales de esta clase de ficheros:
de fuentes accesibles al público,
de informaciones facilitadas por el afectado,
de informaciones consentidas por el afectado.
2. Ficheros cuya finalidad es el almacenamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias. La notificación de la inclusión de datos personales en el fichero se efectuará en el plazo máximo de 30 días, informando al afectado de su derecho a recabar información sobre los datos recogidos en el fichero.

En este supuesto nos encontramos ante dos ficheros diferentes; de un lado, el fichero del acreedor, del que provienen los datos, y ,de otro, el fichero que almacena los datos sobre cumplimiento de obligaciones dinerarias y que presta información en esta materia.

Cuando el interesado lo solicite, el responsable del fichero le comunicará sus datos y deberá facilitar las evaluaciones y apreciaciones que se hayan comunicado sobre el afectado en los

últimos seis meses, así como el nombre y dirección de los cesionarios.

Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica, que se refieran como máximo a los 6 últimos años, a partir del momento de la inclusión del dato personal desfavorable en el fichero y, en todo caso los datos de carácter personal registrados deberán responder a la situación actual de éstos

- *Marketing directo: tratamientos con fines de publicidad y prospección comercial.*

Aquí, además de ofrecer la garantía al afectado de ser dado inmediatamente de baja cuando lo desee y el derecho a conocer de donde se han obtenido los datos, restringe las fuentes de las que pueden obtener información personal los responsables de este tipo de ficheros. En efecto, quienes se dediquen a recopilar direcciones, repartir documentos, publicidad o venta directa u otras actividades análogas sólo podrán utilizar listas tratadas informáticamente de nombres o direcciones, cuando los mismos procedan de listas accesibles al público o si se los facilita el afectado.

La prestación de servicios o "0utsourcing" consiste en la prestación por cuenta de terceros de servicios de tratamiento automatizado de datos de carácter personal.

La LOPD incluye la prestación de servicios en el art. 12 titulado acceso a los datos por cuenta de terceros

La prestación de servicios por cuenta del responsable del tratamiento responde a las siguientes características:

- no se considera comunicación de datos
- debe estar regulada por un contrato escrito, o por una forma que permita acreditar su celebración y contenido y en el que debe tratar los datos conforme a las instrucciones del responsable del tratamiento.
-Los datos se aplicarán o se utilizarán con el fin que figure en el contrato
- se prohibe cederlos ni siquiera para su conservación, a otras personas.

De hecho, la LOPD les impide mantenerlos una vez cumplida la prestación contractual, ya que les obliga a destruirlos en ese momento o a devolverlos al responsable del fichero.

- *Datos especialmente protegidos*

Los datos referentes a ideología, afiliación sindical, religión o creencias tienen una protección máxima en la ley. Nadie podrá ser obligado a declarar sobre estos datos, salvo que el afectado consienta expresamente y por escrito. Además, existe una obligación de advertir al interesado su derecho a no prestar su consentimiento.
Los datos que se refieran al origen racial, salud o vida sexual reciben una protección media. Sólo podrán recabarse cuando:

- por razones de interés general lo disponga una ley
- o el afectado consienta expresamente. (por escrito, salvo otra fórmula probatoria).

Además se refuerza su protección por una prohibición de crear o mantener ficheros con la finalidad exclusiva de almacenar datos que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico y vida sexual.

La ley prevé una regla especial según la cuál sin el consentimiento sólo podrán ser objeto de tratamiento datos sobre ideología, afiliación sindical, religión, creencias, salud, vida sexual y origen racial cuando sean absolutamente necesarios para los fines de una investigación concreta realizada por las Fuerzas y Cuerpos de Seguridad.

Por otro lado, hay datos especialmente protegidos por sus propias normas reguladoras como aquellos relativos a comisión de infracciones penales o administrativas sólo podrán incluirse en los ficheros públicos por las Administraciones competentes de acuerdo con lo previsto en las normas reguladoras.

5.4 Especial referencia al movimiento internacional de datos

La transferencia de datos personales de un Estado a otro es un tema de especial atención en las leyes de protección de datos. Todos los principios y derechos reconocidos y recogidos en las mismas se verían seriamente amenazados si no se establece un control que marque unos límites de garantía y seguridad en la transmisión telemática, o en la transferencia de los datos personales cruzando fronteras. Por otra parte, la transmisión e intercambio de datos personales entre distintos países, es necesaria para la evolución y el ejercicio de actividades económicas, así como garantía y respeto a la libre circulación de personas y cosas en beneficio de las relaciones sociales, culturales y económicas entre los pueblos.

Sobre esto la LOPD establece la prohibición de transferir temporalmente o definitivamente datos de carácter personal con destino a países que no cuenten con un sistema similar de protección salvo que, además de observarse lo dispuesto en ella, se obtenga autorización del Director de la Agencia de Protección de Datos si se obtienen garantías adecuadas. El carácter adecuado de nivel de protección que ofrece el país de destino se evalúa por la Agencia de Protección de Datos.

La LOPD establece un régimen de excepciones muy detallado, siguiendo la Directiva Comunitaria.

5.5 Extinción del tratamiento

El tratamiento de los datos se extingue por su cumplimiento (cumplimiento de su finalidad), por acuerdo de las partes, por resolución unilateral instada por una de ellas o por nulidad del contrato.

La extinción del tratamiento se materializa mediante la cancelación de los datos. La ley exige el inmediato bloqueo de los datos, de modo que los datos cancelados no puedan utilizarse para otra finalidad. También podrá realizarse por el borrado o destrucción de los datos como mediante la despersonalización de los datos.

5.6 Régimen de infracciones y sanciones

Se fija en la LOPD un régimen sancionador al que estarán sometidos los responsables de los ficheros y los encargados de los tratamientos, estableciéndose, en cuanto a procedimientos y sanciones, unas especialidades cuando se trate de ficheros de los que sean responsables las Administraciones públicas.

Las infracciones se califican como leves (art. 44.2), graves (art. 44.3) y muy graves (art. 44.4), estableciéndose multas que van desde las cien mil pesetas a los cien millones, graduándose la cuantía de acuerdo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas.

Respecto a la prescripción, la infracciones prescribirán a los tres años las muy graves, a los dos las graves y al año las leves, comenzándose a contar desde el día en que la infracción se haya cometido.

5.7 El procedimiento sancionador

El procedimiento sancionador queda establecido por el RD 1720/2007, regulándose en el mismo las distintas fases de este procedimiento.

La potestad sancionadora la ejerce la Agencia de Protección de Datos y contra sus resoluciones se podrá interponer recurso contencioso-administrativo.

En los supuestos constitutivos de infracción muy grave, o de utilización o cesión ilícita de datos que atenten contra los derechos fundamentales, el Director de la A.P.D. podrá requerir a los responsables de los ficheros, tanto públicos como privados, la cesación de la utilización o cesión ilícita de los datos. Si se desatiende el requerimiento, se podrán inmovilizar los ficheros mediante resolución motivada

6. La Agencia de Protección de Datos.

Es el órgano de fiscalización y control que actúa con independencia de las Administraciones Publicas en el ejercicio de sus funciones. La APD es un ente de Derecho público con personalidad jurídica propia y plena capacidad pública y privada. Su régimen jurídico se regula por la LOPD y su propio estatuto aprobado por el RD 428/1993, de 26 de marzo, y modificado por el Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de

marzo (BOE de 5 de noviembre de 2008).

Composición:

La APD se compone de los siguientes órganos:

- el Director: que dirige la Agencia y ostenta la representación de la APD. El Director de la Agencia se nombra por el Consejo Consultivo mediante Real Decreto, por un período de cuatro años. El director ejercerá sus funciones con plena independencia y objetividad.

- El Consejo Consultivo es un órgano asesor del Director de la Agencia que estará compuesto por representantes de diversas instancias tanto públicas como privadas: un diputado, un senador, un representante de la administración central, un representante de la administración local, un experto en la materia, un representante de consumidores y usuarios y un representante del sector de ficheros privados.

Funciones de la Agencia y de su Director

Destacan como funciones propias:

- velar por el cumplimiento de la legislación sobre la protección de datos y controlar su aplicación en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos
-atender las peticiones y reclamaciones formuladas por las personas afectadas,
-proporcionar a las personas información sobre sus derechos sobre esta materia,
-ejercer la potestad disciplinaria,
-ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos y otras muchas que, en definitiva, tienden a velar por el cumplimiento de la legislación sobre protección de datos,
- redactar una memoria anual y remitirla al Ministerio de Justicia.

Además, cuando se dé el caso de infracción muy grave, de forma que se estén utilizando o cediendo los datos personales atentando gravemente contra los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, además de ejercer la potestad inspectora y sancionadora, el Director de la Agencia de Protección de Datos podrá requerir a los responsables de los ficheros la cesación de esa ilícita utilización o cesión de datos, pudiendo, en caso de no ser atendido en su requerimiento, inmovilizar los ficheros.
La Agencia tiene una potestad de inspección en el ejercicio de sus funciones, según la cuál, las autoridades de control podrán inspeccionar los ficheros y recabar las informaciones necesarias para el cumplimiento de sus atribuciones. Las autoridades que examinen los datos tienen la obligación legal de guardar secreto sobre las informaciones que conozcan en el ejercicio de sus funciones. Además podrán solicitar el envío de documentos t datos, examinarlos en el lugar en que estén depositados y acceder a inspeccionar los equipos físicos y lógicos utilizados en el tratamiento de los datos.

Las resoluciones que adopte la Agencia podrán ser recurridas ante la jurisdicción contencioso-administrativa.

Integrado en la Agencia, se crea el *Registro General de Protección de Datos* donde serán objeto de inscripción (art. 38) los ficheros automatizados de que sean titulares las Administraciones públicas, los ficheros automatizados de titularidad privada, los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información y los códigos tipo y las autorizaciones a que se refiere la ley. Su organización y estructura está contenida en los artículos 23 a 26 del RD 428/1993, de 26 de marzo, y modificado por el Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos.

Los órganos correspondientes de las CCAA tendrán la condición de órganos de control, y podrán ejercer determinadas funciones de la Agencia de Protección de datos cuando se trate de ficheros de carácter personal creados o gestionados por las comunidades autónomas y por la Administración local de su ámbito territorial.

Actualmente las Comunidades Autónomas están creando sus propias Agencias de Protección de Datos (Madrid, Cataluña, etc.). Se entiende que dichas agencias refuerzan a la autoridad de control nacional y la apoyan en los trabajos de cohesión y armonización de la Ley en todo el territorio del Estado.