# EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

# 1ª EDICIÓN

## MÓDULO 1.

## EL DERECHO A LA PROTECCIÓN DE DATOS


**Autores:**

- **Artemi Rallo Lombarte.** Director de la Agencia Española de Protección de Datos. Catedrático de Derecho Constitucional.
- **Ricard Martínez Martínez**. Coordinador del Área de Estudios de la Agencia Española de Protección de Datos. Profesor de Derecho Constitucional.
- **Agustín Puente Escobar.** Abogado del Estado-Jefe del Gabinete Jurídico de la Agencia Española de Protección de Datos.
- **Irene Agúndez Lería.** Abogada del Estado en la Agencia Española de Protección de Datos.


AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FUNDACIÓN CEDDET

**Con la colaboración de:**

MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

aecid

Fundación Carolina

# ÍNDICE

## INTRODUCCIÓN Y OBJETIVOS

## INTRODUCCIÓN Y OBJETIVOS

El Módulo Primero contiene tres aspectos básicos para comprender el derecho fundamental a la protección de datos y su configuración jurídica. De un lado se tratamiento de un instituto jurídico cuya garantía se encomienda, en el ámbito europeo, a autoridades independientes conformando un modelo de tutela altamente especializada.

Por otra parte, pese a su relativa juventud se trata de un derecho caracterizado por una evolución sustancial de la mano de las tecnologías de la información y de las comunicaciones. Además, aún cuando el bien jurídico protegido pueda resultar bastante homogéneo en todos los países no puede decirse lo mismo de la evolución normativa y jurisprudencial que permite diferenciar, como en tantas otras cosas, un modelo europeo basado en la regulación y en el reconocimiento específico del derecho fundamental a la protección de datos de un entorno norteamericano en el que prima la idea de privacidad y la autorregulación.

Por último, se estudian los elementos básicos del derecho fundamental a la protección de datos.

Entre los objetivos del módulo pueden destacarse:

- Conocer la evolución histórica del derecho a la vida privada y del derecho a la protección de datos.
- Ser capaces de verificar su caracterización en el contexto europeo y conocer los aspectos diferenciales respecto del modelo norteamericano.
- Dominar los aspectos básicos de la protección de datos.
- Conocer los derechos de acceso, rectificación y cancelación.
- Conocer los elementos que caracterizan a la Agencia Española de Protección de Datos como autoridad independiente ordenada a la tutela del derecho fundamental a la protección de datos.

# 1. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AUTORIDAD INDEPENDIENTE

## 1.1 Rasgos básicos

Durante las últimas décadas, la importancia del fenómeno informático se ha proyectado en ámbitos diversos y, entre ellos, han merecido especial atención sus efectos sobre los derechos fundamentales y, particularmente, sobre el personalísimo derecho a la intimidad. La potencialidad ilimitada del tratamiento informático, el fácil acceso a su información o su capacidad de transmisión se enmarcan en una fiebre informática que amenaza claramente la garantía de estos derechos y que exige de Autoridades independientes que los preserven frente a las agresiones procedentes tanto de lo privado como de lo público; instituciones independientes que lo sean, además, de los Gobiernos (titulares, por lo demás, de buena parte de los ficheros capaces de protagonizar tal agresión). De ahí que la creación de estas Administraciones independientes se haya convertido en una demanda de carácter internacional. Así, la Carta de los derechos fundamentales de la Unión Europea afirma en su art. 8 el derecho de toda persona a la protección de datos de carácter personal que la conciernan; a que dichos datos sean tratados de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada; y a acceder a los datos que le conciernan y a su rectificación. Finalmente, dicho precepto encomienda el respeto de estas normas "a una autoridad independiente".

La Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal, creó la Agencia Española de Protección de Datos (AEPD) - norma derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que reproduce, básicamente, el estatuto anterior de la AEPD -. La AEPD tiene por objeto garantizar y proteger, en lo concerniente al tratamiento de datos personales, las libertades públicas y los derechos fundamentales y, en particular, los derechos al honor y a la intimidad personal y familiar.

La AEPD es un ente de derecho público, con personalidad jurídica propia, plena capacidad pública y privada, "que actúa con plena independencia de las

Administraciones públicas en el ejercicio de sus funciones", con un Estatuto propio (cuya aprobación corresponde al Gobierno), con personal adscrito, con patrimonio propio, que elabora su anteproyecto de presupuesto (que es integrado por el Gobierno en los Presupuestos Generales "con la debida independencia") y cuyas resoluciones agotan la vía administrativa.

La dirección y representación de la AEPD corresponde a su Director - auténtico órgano unipersonal de gobierno -, que es nombrado por el Gobierno, previa comparecencia e informe del Congreso de los Diputados, por un período de cuatro años con dedicación exclusiva en dicho cargo, pero que no puede ser cesado discrecionalmente por el Ejecutivo (salvo por causas tasadas como el incumplimiento grave de sus obligaciones, incapacidad sobrevenida, incompatibilidad o condena por delito doloso) ni puede someterlo a instrucciones en el desempeño de sus funciones (pues deberá ejercerlas "con plena independencia y objetividad").

Paralelamente, se contempla la existencia en el seno de la AEPD de un Consejo Consultivo "singular" que, por un lado, asesorará al Director y, por otro, le formulará propuestas (debiendo necesariamente el Director oír al Consejo Consultivo cuando le formule dichas propuestas). Dicha función informativa se concreta, además, en la exigencia legal de que el Consejo emita informe previo a la decisión gubernamental de cese del Director por las causas tasadas referidas. El Director es nombrado por el Gobierno "de entre quienes componen el Consejo Consultivo" e integran dicho Consejo Consultivo: un Diputado, propuesto por el Congreso de los Diputados; un Senador, propuesto por el Senado; un representante de la Administración General del Estado, designado por el Gobierno; un representante de la Administración Local, propuesto por la Federación Española de Municipios y provincias; un miembro propuesto por la Real Academia de la Historia; un experto en la materia propuesto por el Consejo de Universidades; un representante de los consumidores y usuarios; un representante de cada Comunidad Autónoma con agencia de protección de datos; y un representante del sector de ficheros privados.

A la AEPD corresponde una genérica competencia para velar por el cumplimiento de la legislación sobre protección de datos, controlando su aplicación - así como los movimientos internacionales de datos - y por la publicidad de la existencia de ficheros de datos de carácter personal. Dicho ámbito competencial se vio notablemente incrementado tras la reforma legislativa operada por la Ley Orgánica

15/1999 - en virtud de la cual se adaptó el régimen español a la Directiva 95/46/CE- extendiéndose a los ficheros no automatizados e incrementándose la protección de los afectados.

En el ejercicio de sus competencias, las potestades de la APD se expanden al ámbito *informativo* (remite una Memoria anual al Ministerio de Justicia; comunica al Defensor del Pueblo sus actuaciones y resoluciones relativas a ficheros públicos incursos en infracción); *normativo* (dicta las instrucciones precisas para adecuar los tratamientos a la legislación vigente; informa preceptivamente los proyectos de disposiciones generales que desarrollen la ley); *resolutorio* (requiere a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para su adecuación a la ley y ordena el cese de comportamientos contrarios a la normativa vigente y la cancelación de los ficheros; podrá requerir de las Comunidades Autónomas la adopción de medidas correctoras de actuaciones autonómicas que vulneren la ley; inmovilizará ficheros); *supervisor* (recaba de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones); *inspector* (podrá inspeccionar los ficheros regulados por la ley recabando cuanta información precise para el cumplimiento de sus cometidos, solicitando la entrega de documentos o datos; podrá inspeccionar los equipos físicos y lógicos utilizados) y de *coordinación* interinstitucional (el Director podrá convocar regularmente a los órganos de las Comunidades Autónomas a efectos de cooperación institucional y de coordinación de criterios o procedimientos de actuación).

Pero, sin lugar a dudas, mayor significación merece la potestad sancionadora de la APD que se proyecta sobre los responsables de ficheros y encargados de tratamientos mediante un amplio catálogo de infracciones leves, graves y muy graves. No menos trascendentes resultan las sanciones que generan dichas infracciones y, además, si la infracción atañe a las Administraciones públicas, el Director de la APD podrá proponer la iniciación de expedientes disciplinarios.

En consecuencia, la AEPD constituye una Administración independiente cuyas singularidades merecen resaltarse. La AEPD es la primera y, hasta la fecha, única Administración independiente española destinada específicamente a la protección de un derecho fundamental como lo es la protección de datos de carácter personal.

Además, esta Administración independiente no toma ejemplo de ninguna institución referente del ámbito anglosajón. El modelo norteamericano de garantía de la privacidad frente al tratamiento de datos personales difiere notablemente del secundado en muchos países europeos. En Estados Unidos, no existe una *Independent Agency* específicamente creada para tal objeto. En Europa, sin embargo, existe ya una cierta tradición en la creación de instituciones singulares destinadas a proteger los derechos fundamentales frente al tratamiento informático de datos personales. De hecho, ha sido en Francia donde ha querido encontrarse el modelo sobre el que el legislador español creó la AEPD ejemplificado en la *Commission Nationale de l´Informatique et des Libertés* (CNIL). Esta Administración independiente francesa fue creada por la Ley de 6 de enero de 1978 para velar por el respeto a la ley informando a los ciudadanos de sus derechos y obligaciones y controlando las aplicaciones de la informática en los tratamientos de las informaciones personales. La CNIL está compuesta por diecisiete miembros (designados por un período no revocable de cinco años): dos diputados y dos senadores designados por sus Asambleas respectivas; seis miembros de Altas jurisdicciones como el Consejo de Estado, el Tribunal de Casación y el Tribunal de Cuentas, designados por sus respectivas asambleas generales; dos miembros del Consejo económico y social; tres personalidades nombradas por el Presidente de la República; y dos personalidades cualificadas por sus conocimientos en el ámbito de la informática designados por el Primer Ministro a propuesta de los Presidentes de cada Asamblea parlamentaria. La CNIL goza de plena independencia y no está adscrita a ningún Ministerio ni sometida a instrucción gubernamental alguna. Unicamente, un Comisario que representa al Primer Ministro puede requerir de la Comisión una nueva deliberación sobre determinados asuntos. Los amplios poderes de la CNIL se traducen en singulares facultades de investigación, asesoramiento, propuesta, normativas y de decisión autónoma - en notable paralelismo con las confiadas a la AEPD con la excepción significativa del notable poder sancionador que a ésta sí se le confiere -.

Por último, resulta obligado constatar y reconocer el prestigio y autoridad logrados, en la práctica, por la AEPD como auténtica Administración independiente del Gobierno a lo largo de su reciente historia y muchos son los ejemplos que permiten sostener tal aseveración.

## 1.2 Breves consideraciones adicionales

### 1.2.1 Sobre la potestad normativa de la AEPD

El art. 97 CE (Constitución Española) proclama que "El Gobierno ejerce la potestad reglamentaria de acuerdo con la Constitución y las leyes". A la vista de dicha previsión constitucional es fácil entender que no haya resultado pacífico conferir potestad reglamentaria a Administraciones independientes como la AEPD. La realidad de nuestros días impone, sin embargo, la necesidad de extender el ejercicio de la potestad reglamentaria y, en concreto, la APD goza de la potestad de emitir las instrucciones precisas para adecuar los tratamientos a la legislación vigente.

La asignación legislativa de potestad reglamentaria a la AEPD permite advertir de la emergencia de un auténtico sub-ordenamiento autónomo cuya integración ofrece, ciertamente, una complejidad y riesgo relevantes que anima a un tratamiento prudente y restrictivo de tal facultad. Ni el art. 97 CE impide dotar a la AEPD de poderes normativos propios ni resulta cuestionable la necesidad de conferirle dicha facultad para garantizar su funcionamiento y preservar su independencia. Si las voces más críticas no niegan esta posibilidad, sí advierten, sin embargo, de que ello ha de hacerse cautelosamente pues, si bien la potestad reglamentaria del Gobierno goza de carácter originario y queda directamente imbricada en la ley y la Constitución, la potestad reglamentaria derivada de la AEPD proviene del legislador que confiere una potestad reglamentaria "auténticamente independiente"; por ello, el límite en su ejercicio queda dibujado por el marco legal que la conforma y a la jurisdicción ordinaria corresponde salvaguardarlo.

### 1.2.2 Sobre el control parlamentario

El art. 66 CE encomienda a las Cortes Generales "el control de la acción del Gobierno" pero lo cierto es que éste no ostenta facultad directiva alguna sobre la AEPD por lo que se rompe el encadenamiento lógico Parlamento-Gobierno-Administración sobre el que se asientan los principios de confianza y responsabilidad sobre los que se sustenta, a su vez, el principio democrático.

Lo cierto es que ningún espacio público puede quedar vedado a la acción de vigilancia, información, discusión y valoración política en sede parlamentaria. No en vano, la práctica parlamentaria evidencia la existencia de mecanismos específicos que posibilitan el ejercicio de esta modalidad de control parlamentario. De hecho, se

ha consolidado la práctica parlamentaria de dirigir los instrumentos de control (singularmente, preguntas parlamentarias) que afecten a la AEPD directamente al Gobierno. Además, los singulares mecanismos de relación directa Parlamento-AEPD previstos en la legislación específica (por ejemplo, la presentación de informes periódicos) permiten no sólo una acción exclusivamente informativa sino, también, de valoración y control político.

Ahora bien, si se identifica el control parlamentario con la exigencia de responsabilidad política, lo cierto es que el Parlamento sólo puede exigir responsabilidad política al Gobierno de su "acción"; de forma que, si el Gobierno no ostenta dirección alguna sobre la AEPD no cabe atribuirle responsabilidad política en ese ámbito. Sin embargo, si bien se establece un estatuto de inamovilidad e independencia del Director de la AEPD, lo cierto es que al Gobierno se le atribuye una amplia discrecionalidad para su nombramiento. Por ello, del acto mismo de su designación se deduce una imputación de responsabilidad política para el Gobierno.

Nada repugnaría más al principio democrático que admitir la existencia de espacios públicos exentos de control parlamentario. Ciertamente, la fragmentación de lo público operada durante las últimas décadas ha generado un notorio desconcierto sobre los instrumentos tradicionales de verificación de las funciones parlamentarias clásicas. No existe margen de duda a la exigencia constitucional de someter la acción de la AEPD al control del Parlamento. Cuestión distinta será la dificultosa articulación de mecanismos que aseguren su adecuada inserción en la estructura constitucional y que superando las tradicionales técnicas de sometimiento gubernativo-administrativo preserven la función parlamentaria de control.

Por un lado, resultará indispensable reafirmar la pervivencia de los instrumentos ordinarios de control parlamentario. La articulación constitucional del sistema parlamentario de gobierno y los Reglamentos de las Cámaras amparan la demanda de información y el control gubernamental. No obstante, el alcance, extensión y contenido del control parlamentario dependerá en última instancia del legislador y de cómo contribuya a delimitar las relaciones Parlamento-Gobierno-AEPD y Parlamento-AEPD. Lo cierto es que cuando el Parlamento ha tratado de recabar información de la actividad de la AEPD a través del Gobierno no se han planteado significativos conflictos. En consecuencia, en la práctica, el problema no reside tanto en la ausencia de instrumentos para realizar dicha fiscalización parlamentaria como en el insuficiente uso que de ellos se haga a causa del desconcierto que todavía sigue

provocando su existencia y, en particular, su peculiar inserción en el esquema de poderes del Estado.

Menos sencillo de resolver resulta el interrogante relativo a la responsabilidad política que sigue ostentando el Gobierno y su exigibilidad por el Parlamento. Como posición de principio, parece harto cuestionable que de la actuación de la AEPD pueda derivarse responsabilidad política de los responsables de Departamentos ministeriales con los que ésta se relaciona. Una correcta aproximación al análisis de esta cuestión exige atender a experiencias comparadas de singular interés en el tema que nos ocupa, y ajustar el juicio a los exactos términos legales en los que se diseña el modelo concreto de relaciones Parlamento-Gobierno-AEPD.

Es un principio insoslayable del régimen parlamentario que el ejercicio de todo poder público conlleva la responsabilidad política ante el Parlamento. Dicha responsabilidad ministerial resultará inesquivable y derivará directamente de la designación de los altos cargos -independientemente del grado de autonomía de que gocen, con posterioridad, en su acción administrativa-. La designación o no de cargos administrativos constituirá la clave de bóveda del sistema de responsabilidad política ministerial. Así, el Gobierno designa casi con absoluta libertad al Director de la AEPD lo que, de entrada, debiera permitir imputarle la plena responsabilidad política. Sin embargo, el estatuto de inamovilidad que le es predicable lo equipara ampliamente con el modelo profesionalizado y nos ubica, más bien, en un nivel de exigencia de atenuada responsabilidad *in vigilando* . Y, en cualquier caso, el Gobierno tiene notablemente debilitadas sus facultades sobre la actividad cotidiana de la AEPD lo que, necesariamente, matiza la posibilidad de imputación de responsabilidad política. Por último, no resulta baladí recordar que quien tiene la facultad de exigirle responsabilidad política (el Parlamento) interviene en el proceso de designación (de forma, ciertamente devaluada) dándose, en consecuencia, la paradoja de que el Parlamento no podrá imputar *in toto* la responsabilidad política del nombramiento al Gobierno pues él mismo participó en el proceso de designación. En conclusión, al Gobierno le es atribuible la responsabilidad política del nombramiento de forma graduada y proporcional a su mayor o menor libertad de decisión en la designación.

Ahora bien, resultando innegable que nos hallamos ante un debilitamiento de la función parlamentaria de control sobre la acción del Gobierno es imprescindible superar los procedimientos tradicionales de articulación del control intensificando el control parlamentario directo sobre la AEPD. No debiera causar recelo - ni doctrinal

ni político - la posibilidad de que el Parlamento articulase intensamente una relación directa con la AEPD pues, no en vano, podrían alcanzarse muy deseables objetivos. Así lo ha entendido el legislador al contemplar la existencia de mecanismos específicos de control directo sobre la AEPD por parte del Parlamento como, por ejemplo, cuando se preceptúa la remisión al Parlamento de la memoria anual de actividades de la AEPD.

### 1.2.3 Sobre la imparcialidad reforzada por un garantista sistema de incompatibilidades

La Constitución matiza los efectos del art. 97 CE al disponer que 'la Administración Pública sirve con objetividad los intereses generales' (art. 103.1 CE), esto es, que el apoderamiento gubernamental sobre la Administración no implica la disponibilidad absoluta del Gobierno sobre ésta sino que dicho precepto consagra el principio de neutralidad de la Administración (STC 77/1985). Lo que, en principio pudiera parecer incompatible (conciliar la dirección política del Gobierno con la objetividad y profesionalidad de la Administración), no lo es, en la práctica, pero sí aboca a una tensión entre la dirección política del Gobierno y la exigencia de una actuación administrativa objetiva, neutral y sometida a la ley y al Derecho. La dificultad para conciliar ambos mandatos constitucionales reside, obviamente, en el fundamento democrático de la actuación administrativa: el sometimiento a la dirección política del Gobierno suple el déficit de legitimidad democrática del que adolece la Administración por su propia naturaleza instrumental; por contra, un cierto alejamiento del Gobierno constituye *conditio sine qua non* para garantizar la objetividad de la Administración entendida como neutral políticamente, esto es, al servicio de los intereses generales -entendidos éstos como los que defina sucesivamente el Gobierno de turno legitimado democráticamente por las mayorías parlamentarias -.

Si la Administración sirve con objetividad los intereses generales y, en consecuencia, dicha exigencia limita los poderes directivos de la Administración, ¿qué sentido tiene crear Autoridades independientes como la AEPD desvinculadas del Gobierno para que gestionen ámbitos administrativos con independencia, neutralidad política, objetividad y sin obedecer a intereses políticos partidistas?. Si la Constitución española obliga a todas las Administraciones a servir con 'objetividad' los intereses generales y a organizar todo el sistema de función pública con arreglo a reglas que garanticen la 'imparcialidad' de los funcionarios en el ejercicio de sus

funciones, ¿cabe que unas Administraciones sean más objetivas y neutrales que otras por razón de la función que desempeñan o todas deben serlo por igual?. ¿Acaso determinadas funciones o servicios públicos exigen garantías especiales contra el Gobierno en tanto en cuanto en ellas la objetividad y la imparcialidad no se respeta?.

Lo cierto es que en la objetividad administrativa ha querido verse una manifestación del principio de igualdad, esto es, de la interdicción de la arbitrariedad administrativa y, por ello, conviene insistir en que un organismo independiente como la AEPD no constituye una manifestación reforzada de la objetividad administrativa constitucionalmente exigida en el art. 103.1 CE sino expresión de la voluntad del legislador de limitar el poder gubernamental restringiendo su ámbito de dirección administrativa.

No obstante, la imparcialidad de la Dirección de la AEPD adquiere una significación especial frente a la que resulta predicable del resto de funcionarios públicos en el ejercicio de sus funciones. La independencia de esta Autoridad y su poder para regular determinados sectores socio-económicos hace emerger el fantasma de lo que tradicionalmente se ha dado en denominar *la captura del regulador* por parte de los sectores regulados. Esto es, resulta real el peligro de que se acabe sucumbiendo a los deseos de los sectores socio-económicos a los que, teóricamente, deben imponerse mediante diversos mecanismos de influencia. A evitar tal riesgo, va destinado un estricto y garantista sistema de incompatibilidades al que se le somete durante el ejercicio del cargo y no sólo: también, durante un tiempo futuro que impida dicha colisión entre los intereses particulares y los generales. Así, le resulta aplicable un régimen de dedicación absoluta y el sistema de incompatibilidades propio de los altos cargos de la Administración del Estado) que, incluso, se prorroga, *pro futuro*, durante los dos años posteriores al cese.

### 1.2.4 Sobre el nombramiento gubernamental del Director de la AEPD

El Director de la AEPD es nombrado por el Gobierno, previa comparecencia e informe del Congreso de los Diputados, de entre los miembros del Consejo Consultivo de la Agencia.

La tímida intervención parlamentaria prevista legalmente en el proceso de designación del Director de la AEPD tiene una relevancia limitada pues en nada condiciona jurídicamente la decisión gubernamental de nombramiento. Y, desde

luego, muy lejos queda esta limitada participación parlamentaria de su auténtico significado en el sistema constitucional norteamericano que ha dado carta de naturaleza a las Administraciones independientes. La exigencia de ratificación senatorial de los candidatos presidenciales para integrar las *Independent Agencies* formalmente constituye un auténtico contrapeso y límite a las facultades presidenciales, esto es, una expresión de los *checks and balances* que caracterizan el sistema constitucional norteamericano.

Tampoco nuestro sistema contempla mecanismos garantizadores de la pluralidad ideológica en el seno de la AEPD dada la naturaleza unipersonal y no colegiada del órgano directivo. Por el contrario, en el modelo norteamericano, al prescribirse la imposibilidad de que el nombramiento recaiga en miembros del mismo partido político en número superior a la mitad más uno de sus integrantes, el nombramiento presidencial puede recaer en miembros del otro partido político, necesariamente, cuando se supera el cupo del propio partido. No obstante, este monopolio gubernamental en el nombramiento del Director no significa que el mismo no se vea sometido a ciertos límites como la existencia de un mandato temporal fijo.

Por lo demás, la legislación vigente no impone cualidad específica, personal o profesional, al Director de la AEPD. Sin embargo, estamos ante el ejemplo, teóricamente, más restrictivo de la facultad gubernamental de designación pues su ley reguladora prescribe que deberá surgir de entre quienes componen el Consejo Consultivo - recuérdese: un Diputado, propuesto por el Congreso de los Diputados; un Senador, propuesto por el Senado; un representante de la Administración Central, designado por el Gobierno; un representante de la Administración Local, propuesto por la Federación Española de Municipios y provincias; un miembro propuesto por la Real Academia de la Historia, propuesto por ella; un experto en la materia propuesto por el Consejo Superior de Universidades; un representante de los consumidores y usuarios; un representante de cada Comunidad Autónoma con agencia de protección de datos; y un representante del sector de ficheros privados- . Restricción meramente teórica si, como resulta intuible, el nombramiento recaerá en el representante de la Administración General del Estado que al mismo Gobierno compete designar. En este caso, la decisión gubernamental gozará de absoluta discrecionalidad.

Un límite cierto al poder gubernamental de nombramiento del Director de la AEPD y, al mismo tiempo, una garantía sustancial del estatuto de imparcialidad residiría

tanto si se diferenciara con el mandato gubernamental (en principio, cuatro años) como si se limitara la capacidad gubernamental para su renovación en el cargo. Pero lo cierto es que el Director de la AEPD es nombrado por un período de cuatro años y no se prohíbe la renovación del mandato. En consecuencia, las reglas que atañen a la prolongación de mandato o la renovación del mismo resultan inexistentes. Lo que no significa que tenga necesariamente que coincidir el mandato del Director con el del Gobierno. Lo que atenúa, en verdad, la previsible crítica fundada en la coincidencia de mandatos. La posibilidad de renovación tampoco contribuye a forjar escrupulosamente su estatuto de independencia pues con ello se debilita seriamente la libertad de criterio.

### 1.2.5 Ausencia de remoción gubernamental discrecional y causas tasadas de cese: la inamovilidad como principal restricción a la potestad directiva del Gobierno

La más relevante restricción del poder directivo del Gobierno sobre la AEPD reside en la imposibilidad de cesar discrecionalmente a su Director. El instrumento legal de verificación de dicha prohibición de cese discrecional descansa sobre la existencia de un elenco de causas tasadas de cese: renuncia voluntaria, expiración de mandato, incapacidad permanente para el ejercicio de su función, falta de diligencia o incumplimiento grave de sus obligaciones, incompatibilidad sobrevenida o procesamiento por delito doloso.

Como se observará, existen causas de cese que atañen exclusivamente a la voluntad o personalidad del sujeto que integra la Autoridad (por ejemplo, la renuncia voluntaria) o responden a circunstancias y condiciones de naturaleza objetiva (por ejemplo, la finalización del mandato, el procesamiento o la incompatibilidad sobrevenida). En estos supuestos, resulta imposible una intervención gubernamental que, de alguna manera, pretenda afectar la inamovilidad garantizada. Sin embargo, de entre las causas tasadas de cese, alguna de ellas adolece de una ambigua formulación que permite interpretaciones diversas: en concreto, el "incumplimiento grave de las obligaciones del cargo". De ahí que adquiera notable relevancia el procedimiento establecido para ejecutar el cese por la causa referida -máxime cuando el cese formal compete al Gobierno-. En este sentido, el cese del Director de la APD requerirá que el Consejo Consultivo emita informe previo a la decisión gubernamental de cese.

Resulta intuible que el denominado "incumplimiento grave de obligaciones" podría amparar una intervención gubernamental que burlara la voluntad del legislador de garantizar escrupulosamente la inamovilidad del Director de la AEPD. Sin embargo, existen en el ordenamiento garantías suficientes para impedir tal intento como la exigencia legal de que al cese gubernamental le preceda un informe del Consejo Consultivo o, en última instancia, el hecho de que cualquier decisión arbitraria estará sometida al pertinente control judicial conforme a parámetros jurídicos que permitan delimitar la referida causa de cese.

### 1.2.6 Sobre el alcance jurídico de la afirmación legal expresa de "independencia"

El legislador ha querido atribuir expresamente a la AEPD "plena independencia de las Administraciones públicas en el ejercicio de sus funciones". Singularmente, esta genérica regla se manifiesta en que el Gobierno no podrá someter al Director de la AEPD a instrucciones en el desempeño de sus funciones pues debe ejercerlas "con plena independencia y objetividad".

¿Cuál es el significado y alcance de dichas proclamas legales?. En primer lugar, estas manifestaciones del legislador poco contribuyen a delimitar la naturaleza y concepto de esta Autoridad y, en última instancia, el estatuto real de independencia derivará de la regulación concreta y del elenco de mecanismos e instrumentos jurídicos que persigan garantizarla.

Respecto de la específica prohibición impuesta al Gobierno de cursar instrucciones a la AEPD, resulta dudosa la efectividad de dicha prescripción legal. Ciertamente, una hipotética actuación gubernamental de tal naturaleza formalizada conforme a los instrumentos jurídicos habitualmente utilizados por los órganos administrativos jerárquicamente superiores para instruir la actuación de los inferiores vulneraría el mandato legal y sufriría un vicio de nulidad.

### 1.2.7 Sobre el control judicial directo: personalidad jurídica propia y agotamiento de la vía administrativa

Si bien es cierto que, en un intento racionalizador de la compleja estructura administrativa, la LOPD establece que la AEPD se relacionará con el Gobierno a través del Ministerio de Justicia, lo más cierto es que le otorga personalidad jurídica propia y plena capacidad de obrar. Esto es, el ordenamiento permite a la AEPD

ejercer en el tráfico jurídico con personalidad propia y sin dependencia de instancias gubernamentales.

Sin lugar a dudas, la principal manifestación de la independencia jurídica de la AEPD frente al resto de la Administración y, en concreto, frente al Gobierno, reside en el control judicial directo. Esto es, las resoluciones del Director de la AEPD agotan la vía administrativa y son directamente recurribles ante la jurisdicción ordinaria sin necesidad de recurso previo ante determinado órgano ministerial o gubernamental. Sin personalidad jurídica propia y revisión judicial directa de sus actos administrativos, resultaría difícilmente reconocible una Administración independiente como la AEPD.

### 1.2.8 Sobre la autonomía presupuestaria, patrimonial y financiera

La independencia de un ente administrativo vendrá determinada, necesariamente, por el libre y autónomo disfrute de recursos materiales suficientes para el desempeño de las funciones que legalmente tenga atribuidas. A mayor disponibilidad de éstos, menor dependencia gubernamental y mayor libertad en la toma de decisiones. Autonomía que no lo será sólo respecto de instancias gubernamentales sino, también, respecto de los sectores regulados. No debe olvidarse, por ejemplo, que, en Estados Unidos, la asignación y control presupuestarios son, respectivamente, instrumentos para la injerencia del Ejecutivo y del Congreso en las *Independent Agencies*. La ausencia de recursos económicos propios, históricamente, ha permitido una cierta dependencia de los sectores económicos regulados.

Desde la perspectiva presupuestaria, se reconoce legalmente que el Presupuesto de la AEPD será integrado por el Gobierno en los Presupuestos Generales "con la debida independencia". Sin duda, se reconoce autonomía plena para elaborar el anteproyecto de sus presupuestos económicos pero los interrogantes surgen sobre el grado de vinculación que esta propuesta presupuestaria genera en el Gobierno. Aunque la obligación legal atribuida al Gobierno de integrar ("con la debida independencia") en su proyecto de Presupuestos el anteproyecto elaborado parece presuponer que éste no será alterable por aquél y que deberá remitirse intacto al Parlamento, no resulta imaginable, que pueda formularse una propuesta presupuestaria con absoluta libertad e imponer al Gobierno la obligación de respetarla y adjuntarla, sin revisión alguna, al proyecto de Presupuestos. Y ello por cuanto es al Gobierno, en exclusiva, al que la Constitución atribuye la potestad de

iniciativa presupuestaria y, en general, un poder de dirección política que le faculta, en lo económico-presupuestario, para diseñar, cuanto menos, unas directrices básicas, comunes al conjunto de departamentos administrativos, de las líneas presupuestarias a las que, necesariamente, se sujetará la AEPD.

La legislación vigente no sólo no impone una financiación exclusivamente pública de la AEPD sino que contempla, además, mecanismos de financiación propia derivados de las sanciones económicas impuestas. A ello se une la asignación y disfrute de un patrimonio propio. Si en principio parecen muy limitadas las facultades autónomas en materia presupuestaria, patrimonial, de financiación y recursos humanos, lo cierto es que se intuye una indiscutible tendencia hacia el reforzamiento de este ámbito de autonomía con el fin de restringir la dependencia gubernamental y de evitar la influencia de los sectores regulados.

# 2. HISTORIA DEL DERECHO A LA VIDA PRIVADA Y EL DERECHO A LA PROTECCIÓN DE DATOS.

## 2.1 El derecho a la vida privada: Estados Unidos.

El punto de partida de cualquier análisis sobre el derecho a la protección de datos debe tener en cuenta el nacimiento del derecho a la vida privada en la doctrina norteamericana. Su formulación teórica se debe a los juristas norteamericanos Warren y Brandeis.

Warren y Brandeis señalaron que el «Common Law» garantiza a cada persona el derecho a decidir hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones» y trasladan la tutela del derecho a la intimidad desde el plano de la propiedad al ámbito del derecho a la personalidad:

«el principio que tutela los escritos personales y cualquier otra obra producto del espíritu o de las emociones es el derecho a la intimidad, y el derecho no necesita formular ningún principio nuevo cuando hace extensivo este amparo a la apariencia personal, a los dichos, a los hechos y a las relaciones personales, domésticas o de otra clase».

A continuación, y para finalizar su trabajo, Warren y Brandeis indican que el derecho a la intimidad no es un derecho ilimitado y elaboran un cuerpo doctrinal que ha llegado intacto hasta nuestros días. Señalan que la intimidad no impide la publicación de aquello que posea un interés público o general, atendiendo además a la condición pública o privada del sujeto sobre el que verse la noticia y matizan este último extremo en el sentido de reconocer que hasta los hombres públicos tienen el derecho a ver protegida una parte de su vida privada. En segundo lugar, la tutela de la vida privada no excluye la publicación de determinados asuntos si se trata de informaciones sobre hechos o manifestaciones producidas ante instituciones o corporaciones públicas etc. Warren y Brandeis atienden también a las circunstancias en que se produce la vulneración en función del medio y el grado de publicidad. Por otra parte prestan atención a la conducta del afectado y consideran que su derecho a la intimidad decae con la publicación de los hechos

por el mismo o con su consentimiento. Finalmente consideran la imposibilidad de alegar en el campo de la intimidad la exceptio veritatis y la ausencia de malicia.

Esta concepción evoluciona en el ámbito norteamericano identificando, en el plano civil, la presencia de cuatro "torts" en el derecho a la vida privada. Estas cuatro categorías de "tort" son la intrusión en la soledad o retiro, o en los asuntos privados, la difusión publica de hechos privados, la información que da una imagen falsa del afectado ante los ojos del público –o "False Light"-, y, por último la apropiación en beneficio propio de la imagen o el nombre ajenos.

En el ámbito norteamericano, la evolución doctrinal del derecho a la vida privada ha girado en torno a dos polos. La de aquellos que distinguen netamente dos ámbitos de juego para el derecho a la vida privada: 1) aquél en el que actúa como límite a la actuación de los poderes públicos sometidos en su actuación a los límites que imponen la Constitución y determinadas normas; 2) el plano de las relaciones privadas que se regirían por el principio de autonomía de la voluntad y donde juega un papel determinante la autorregulación corporativa. Por el contrario, otros autores critican el paradigma dominante de la privacy-control basada en la autonomía del individuo y en el principio del consentimiento, a partir de las consecuencias de las tecnologías de la información y las comunicaciones y de las prácticas existentes en Internet para la vida privada. Estos últimos reclaman un modelo normativo similar al Europeo.

EN RESUMEN:

En Estados Unidos

- No se utiliza prácticamente la idea de Data Protection tanto como el de Right to Privacy.
- El derecho a la vida privada se ha configurado y definido por la jurisprudencia del Tribunal Supremo.
- Existe una regulación general, la Privacy Act de 1974, y multitud de regulaciones sectoriales.
- En las relaciones privadas rige el principio del consentimiento y las prácticas de autorregulación con una regulación más débil que la europea.

## 2.2 El Derecho a la intimidad.

En el ámbito europeo se habla de right to privacy, vié privée, riservatezza o derecho a la intimidad. Habitualmente se encuadra el derecho a la intimidad en una concepción individualista que lo configura como un derecho de defensa, o una libertad negativa perteneciente al status libertatis. Se trata de proteger una "esfera privada", de la cual el individuo puede libremente excluir a terceros o impedir intromisiones. Alcanza al círculo de relaciones personales del titular y al marco físico de la vida social, en la que éstas se desarrollan con voluntad de permanecer en el anonimato y con solo el conocimiento de quienes en ellas participan. Así concebida, esta es una "intimidad preinformática", que no puede cubrir las repercusiones derivadas de las tecnologías de la información.

Se trata de un derecho fundamental vinculado a la dignidad humana y al libre desarrollo de la personalidad que en el ámbito europeo ha encontrado acomodo en el art. 8 del Convenio Europeo de Derechos Humanos, ha sido reconocido jurisprudencialmente en Alemania e Italia y, en algunas constituciones recientes como la española de 1978. En la práctica, en algunos ordenamientos como el

español, el derecho a la intimidad y el derecho a la protección de datos juegan roles diversos. El derecho a la intimidad se ordena a proteger las manifestaciones privadas de la personalidad del ser humano mientras que, como veremos después, el derecho a la protección de datos pose un objeto mucho más amplio. Por ello, la intimidad juega su papel en el ámbito de los conflictos vinculados a la revelación de secretos y en las intromisiones en la vida privada provenientes, generalmente de los medios de comunicación.

En resumen

a) El derecho a la intimidad tutela la esfera privada, el ámbito íntimo de los sujetos.

b) Se diferencia del derecho fundamental a la protección de datos en que éste último tutela respecto de cualquier tratamiento de datos personales.

## 2.3 El nacimiento y evolución del derecho a la protección de datos.

Las primeras normas sobre protección de datos nacen en Europa en los años setenta. Es la época de consolidación de la informática como herramienta de gestión. en aquellos momentos, sólo los estados, ciertas entidades, -como algunas universidades-, y las grandes empresas y corporaciones tenían capacidad para disponer de computadores. Ello generó un cierto recelo ante la capacidad del Estado de procesar y utilizar sin límite aparente alguno la información de los ciudadanos. A ese recelo responde sin duda la redacción del art. 18.4 de la Constitución Española o de la prohibición del uso de un número de identificación único por el art. 35 de la Constitución Portuguesa de 1976.

Esta inquietud era compartida en el seno del Consejo de Europa entre cuyas aportaciones deben citarse la Resolución núm. 509 del Consejo de Europa sobre los derechos humanos y los nuevos logros científicos y técnicos, de 31 de enero de 1968 y dos Resoluciones del Comité de Ministros, la R (73) 22 y la R (74) 29,

referidas a la protección de datos en los sectores privado y público respectivamente. Con este primer paso se llevaba a cabo un intento inicial de aproximación de las legislaciones de los Estados miembros en tres puntos: 1) en la fijación de los principios de publicidad sobre la existencia de ficheros; 2) en la existencia de autoridades garantes de la aplicación de las normas y los derechos de los ciudadanos y, 3) en la extensión del ámbito de aplicación de las leyes de protección de datos tanto al sector público como al privado. En aquel momento sólo algunos países europeos habían desarrollado normas sobre protección de datos, la República Federal Alemana y Suecia, siendo acompañadas de algún esfuerzo en Estados Unidos.

A estas leyes de protección de datos de la primera generación, les sucede una segunda. Con ella el legislador se enfrentaba al crecimiento significativo de la capacidad de almacenamiento y procesado. El objetivo será fijar un conjunto de condiciones que, de modo preventivo, garanticen los derechos de los ciudadanos. La doctrina sitúa en esta segunda generación a las constituciones Española y Portuguesa aunque, ciertamente, es la segunda en su art. 35 la que presenta una regulación más sistemática y reconocible:

> «1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización.
>
> 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.
>
> 3. Se prohíbe atribuir un número nacional único a los ciudadanos».

En estas normas comienza a atribuirse derechos de información, acceso, rectificación y cancelación, se regula la tutela de los mismos y principios como el la calidad de los datos que definen el modo en que los datos deberán ser tratados.

Las normas y resoluciones del Consejo de Europa antes citadas allanaron el camino a una tercera generación que, de la mano del Convenio del Consejo de Europa, de 28 de enero 1981, para la protección de las personas con respecto al

tratamiento automatizado de datos de carácter personal, -también denominado Convenio núm. 108-, conducirá a la aparición de un acervo común europeo. Este Convenio define el contexto de protección de la privacidad en relación con las tecnologías de la información y las comunicaciones. El mismo surgió de la necesidad de profundizar en la protección de los derechos de los individuos en relación con el uso de la informática, en especial en lo relativo a la vida privada, protegida por el artículo 8.1 del Convenio Europeo de Derechos Humanos. Además, se debía hacer compatible esta tutela jurídica con la libertad de circulación de la información, y, por último, se consideraba necesario establecer un mínimo denominador común entre las legislaciones de los futuros Estados signatarios que permitiese facilitar el flujo internacional de datos.

El Convenio, posee tres partes claramente diferenciadas: las disposiciones de Derecho sustantivo, en forma de principios básicos; las reglas especiales referentes a los flujos internacionales de datos; y unos mecanismos de auxilio mutuo y consulta de las Partes. La norma define un modelo de regulación estructurado en varios pilares básicos:

- Una definición clara de los principios que deben regir el tratamiento de los datos personales, estructurado en torno al principio de calidad (legitimación y legalidad del tratamiento, adecuación y veracidad de los datos, uso limitado a la finalidad, proporcionalidad de los tratamientos), el secreto o la seguridad.

- La atribución de derechos de información en la recogida, acceso, rectificación, cancelación y oposición.

- Un régimen específico para datos cuya especial naturaleza los hace susceptibles de ser utilizados con fines discriminatorios, o afectan a lo más recóndito de nuestra intimidad (origen racial, opiniones políticas, convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual).

- El Convenio tasa las excepciones que los estados pueden establecer a su régimen en razón de la protección de la seguridad del Estado, de la seguridad pública, de los intereses monetarios del Estado o para la represión de infracciones penales, así como para la propia protección de la persona concernida y de los derechos y libertades de otras personas.

- Se fija un modelo de tutela administrativa encomendada a autoridades independientes sin perjuicio de la tutela jurisdiccional.

El Convenio 108 da lugar a las llamadas normas de tercera generación que se caracterizan por dos elementos. Por una parte, plantean un modelo definido y estructurado que abarca los tres elementos esenciales en todo: tratamiento, las condiciones de legitimación para el tratamiento, los principios que deben regirlo y la garantía de los derechos. En segundo lugar, fijan un conjunto de reglas que aseguran el flujo de datos en los distintos sectores de actividad.

Finalmente cabe señalar que la norma comunitaria de referencia es la Directiva 95/46/CE que será ampliamente considerada a lo largo de los distintos módulos.

Por último, es conveniente tener en cuenta que la evolución de las tecnologías de la información definen un nuevo escenario con características específicas:

a) Configuran un escenario global, trasnacional.

b) Las redes sociales y en el futuro inmediato la Internet de los objetos, plantea nuevos problemas para la protección de la privacidad: análisis del comportamiento de los internautas, marketing viral, geolocalización etc…

c) El individuo se convierte en un agente activo "colgando" datos e informaciones de terceros.

d) La capacidad de control de internautas, generalmente desinformados es nula y su actitud se ha definido como "extimidad".

e) Determinados colectivos se encuentran en riesgo y singularmente lo menores.

Por ello la protección de datos personales debe superar la barrera nacional y europea. A estos problemas trata de hacer frente la «Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal» aprobada en Madrid por la 31 Conferencia Internacional de Autoridades de Protección de datos y Privacidad.

EN RESUMEN

- El derecho fundamental a la protección de datos surge a partir de los años 70 y se desarrolla a través de tres generaciones de leyes.
- El Convenio 108 es la norma que marca un hito fundamental en el nacimiento del derecho fundamental a la protección de datos en Europa.
- Se reconocen los derechos de información, acceso, rectificación y cancelación. Se finan los principios rectores para el tratamiento (calidad, seguridad y secreto) y se define un modelo de tutela administrativa.
- La Directiva 95/46/CE abre la legislación comunitaria.
- Hoy nos enfrentamos a nuevos retes en el ámbito de las redes sociales y la Internet de los objetos

## 2.4 El derecho a la protección de datos.

En el contexto europeo la protección de datos personales ha alcanzado un rango de derecho fundamental. Esta evolución se ha producido paralelamente en el ámbito del Consejo de Europa, en la Unión Europea y en la jurisprudencia constitucional de los Estados Miembros. Ello hace particularmente difícil el realizar una exposición lineal y sistemática, por lo que se optará por la exposición separada de cada uno de los ámbitos.

### 2.4.1 La sentencia del Tribunal Constitucional Federal Alemán en el caso de la Ley del Censo de Población.

Puede afirmarse que el perfil constitucional del derecho a la protección de datos nace con la jurisprudencia dictada por el Tribunal Constitucional Federal Alemán (TCFA) en la sentencia sobre la Ley del Censo. Diversos de sus preceptos podían vulnerar el derecho al libre desarrollo de la personalidad y a la dignidad humana y el derecho a la libertad de expresión, y planteaban problemas en sus garantías procesales.

El TCFA construyó su argumentación sobre el derecho general de la personalidad, partiendo de dos argumentos iniciales: 1) que en « la clave de bóveda del ordenamiento de la Ley Fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre», y a cuya protección se encamina este derecho de la personalidad; y, 2) que, precisamente por influjo de la «evolución moderna y de las nuevas amenazas que lleva aparejadas para la personalidad cobra (este derecho) significación especial».

El derecho general de la personalidad comporta la atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida. Para el TCFA:

> «la autodeterminación del individuo presupone -también en las condiciones de las técnicas modernas de tratamiento de la información- que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada.»

Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación. Para ilustrar sus argumentos el Tribunal plantea un ejemplo muy gráfico:

> «Quién sepa de antemano que su participación en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrán

derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales (artículos 8.° y 9.° de la Ley Fundamental). Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos».

La consecuencia de este razonamiento es el reconocimiento jurisprudencial de un derecho fundamental a la autodeterminación informativa que ofrece protección frente a la recogida, el almacenamiento, la utilización, y la transmisión ilimitada de los datos de carácter personal y «garantiza la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y la utilización de sus datos personales».

De la argumentación del TCFA se deduce con claridad que el tratamiento automatizado de datos personales puede repercutir no sólo sobre la libertad individual sino también sobre el interés público, o bien público, en la medida en que la libertad individual es presupuesto básico de la convivencia democrática. El pronunciamiento del Tribunal Constitucional Federal alemán abre así una nueva vía para la tutela de los derechos fundamentales frente a las repercusiones asociadas al uso de las tecnologías de la información y las comunicaciones.

### 2.4.2 La jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el artículo 8 del CEDH. Criterios de interpretación.

El análisis de la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) permite afirmar sin ningún género de dudas que nos encontramos ante un derecho de amplio recorrido. En este sentido la Corte ha sido muy flexible en su interpretación. De este modo ha venido a cobijar en el artículo 8 el derecho a la personalidad en sus múltiples manifestaciones. Así, el Tribunal ha extendido la aplicación del precepto al desarrollo del ser humano en el entorno familiar. Ha asumido la necesidad de mantener la relación familiar cuando decisiones de naturaleza administrativa en aplicación de normas sobre extranjería amenazaban al demandante con el desarraigo o ha considerado al amparo de la vida privada y familiar la libertad de fijar y habitar la residencia familiar y la defensa del medio ambiente doméstico frente a la contaminación.

En el plano individual la labor de la Corte ha ido consolidando la libertad e identidad sexuales. Por otra parte, el TEDH ha aunado en sus decisiones tradición y modernidad. Ha resuelto aplicando el artículo 8 los conflictos tradicionales relativos a la protección del domicilio y la correspondencia. Pero a la vez, ha aprovechado la maleabilidad del derecho a la vida privada para hacer frente a los retos planteados desde el ámbito de las tecnologías de la información y las comunicaciones. Por último, lejos de quedarse anclado en una noción puramente reactiva del derecho a la privacidad como escudo protector frente a las intromisiones de los poderes públicos ha alentado una doctrina orientada a que el ciudadano pueda exigir del Estado prestaciones positivas derivadas de su derecho a disfrutar de la vida privada.

Por tanto, el Tribunal Europeo de Derechos Humanos ha apostado por una concepción muy amplia de la vida privada y familiar y ha desarrollado una intensa labor en la interpretación que permite distinguir o clasificar las sentencias en distintas líneas argumentales.

Aun que hay algunos casos donde la cuestión se plantea, como Leander[1] o Gaskin[2] es en Z contra Finlandia[3] donde se aborda la relación de los datos de carácter personal con el derecho a la vida privada. En concreto se trata del uso de datos médicos de la demandante en el marco de un proceso judicial contra su esposo por un delito de violación, agravado por el hecho de ser seropositivo. El Tribunal finlandés debe establecer el origen de la enfermedad y el momento en que se contrajo y en la medida en que la fuente de contagio del enjuiciado resulta ser la propia esposa, y ante la negativa de ésta a testificar contra el marido, se requiere al personal facultativo que la atendió para que declare y presente el correspondiente historial clínico. Esta información acaba trascendiendo a los medios de comunicación a pesar del carácter secreto del proceso.

Se trataba de determinar si las declaraciones de los médicos supusieron una ingerencia en la vida privada de la demandante y en establecer si la publicación de la sentencia afecta a la vida privada. La Corte se aproxima a estas cuestiones desde una perspectiva centrada en la protección de datos como elemento integrado en el artículo 8 del Convenio y a partir de la Recomendación (89) 14 del

[1] Leander c. Suede, Serie A núm. 116 (1987).
[2] Gaskin c. Royaume-Uni Serie A núm.160 (1989).
[3] Z c. Finlande Recueil 1997-I (1997).

Consejo de Europa sobre las incidencias éticas de la infección por VIH en el marco sanitario y social[4]. El TEDH equipara la protección de la vida privada con las previsiones de distintos artículos del Convenio 108 del Consejo de Europa.

El Tribunal afirma que las legislaciones nacionales para proteger los datos médicos cumpliendo con el artículo 8 del Convenio de Roma deben respetar las previsiones del Convenio 108 del Consejo de Europa. Por tanto, y a pesar de no realizar una afirmación expresa en tal sentido, el Tribunal Europeo de Derechos Humanos viene a equiparar la tutela de la vida privada que ofrece el artículo 8 del CEDH con la aplicación material de las previsiones del Convenio 108, y por tanto a integrar la protección de datos como una faceta de otra categoría más general.

En M. S. contra Suecia[5] se enjuicia una comunicación de datos desde una clínica ginecológica a una Administración en la tramitación de un procedimiento de reconocimiento de pensión por invalidez profesional. El Tribunal considera que el artículo 8 es aplicable al caso y concluye que ha habido injerencia en el uso de los datos si bien, como es habitual en la actuación de la Corte, procede a examinar si se trata de una injerencia justificada a la luz de las excepciones del Convenio. Y aplica el test de proporcionalidad destacando la importancia de los datos personales de carácter médico tanto desde el punto de vista de la protección de la vida privada como desde la perspectiva de la relación de confianza que integra las relaciones entre el paciente y su médico. En este supuesto, atendida la legislación sueca y las circunstancias del caso, se considera que se trata de una injerencia justificada.

En el asunto Amman[6] se considera un supuesto de ejercicio del derecho de acceso a un expediente policial protegido por el secreto de estado. En este caso el Tribunal reafirma su doctrina sobre la incardinación de la protección de datos en el ámbito del artículo 8 del Convenio. Y continúa inmediatamente planteando una concepción amplia de la vida privada que abarca la protección de datos personales.

[4] Recomendación núm. R (89) 14, de 24 de octubre, del Comité de Ministros a los Estados miembros, sobre las incidencias éticas de la infección por VIH en el marco sanitario y social. Véase también la Recomendación núm. R (97) 15, de 13 de febrero de 1997, relativa a la protección de los datos médicos.
[5] M.S. c. Suède, Recueil 1997-IV (1997).
[6] Amann C. Suisse Recueil des arrêts et décisions 2000-II 16 février 2000.

Finalmente en el asunto Rotaru[7] el Tribunal Europeo de Derechos Humanos retoma y consolida el conjunto de los pronunciamientos dictados en los asuntos Leander, Z contra Finlandia y Amman. En el caso, el demandante cuestiona la posesión por parte del Servicio Rumano de Información de un fichero que contenía datos personales sobre su pasado político. La Corte reafirma su postura y considera que el tratamiento de datos personales esta incluido en el bien jurídico protegido por el artículo 8 del Convenio, puesto que el precepto tutela aspectos que exceden del ámbito de la intimidad concebida en sentido estricto y se extiende al ámbito definido por el Convenio núm. 108 del Consejo de Europa.

### 2.4.3 El derecho a la protección de datos en el acervo comunitario.

El análisis del derecho a la protección de datos en la Unión Europea obliga a examinar tres niveles normativos distintos: a) el Derecho originario y derivado propiamente dicho. B) la Jurisprudencia del Tribunal de Justicia y c) las normas de naturaleza pseudoconstitucional.

#### 2.4.3.1 Derecho originario y derecho derivado: las directivas comunitarias.

La primera referencia específica en una norma de Derecho Originario al derecho a la protección de datos se encontraba en el antiguo artículo 286 de la versión consolidada del Tratado de la Comunidad Europea

Para estudiar esta materia hay que tener en cuenta las sucesivas directivas que se han dictado. La primera, y referente de las sucesivas directivas es la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio 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. La norma, que se inserta en la tradición de protección de la vida privada del Convenio Europeo de Derechos Humanos y en la del Convenio 108, persigue dos objetivos fundamentales: tutelar la intimidad y el resto de los derechos fundamentales y garantizar el flujo de datos entre los Estados miembros para impedir que «las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales» afecte al ordenado funcionamiento del mercado único.

[7] Rotaru c. Roumanie, Recueil 2000-V (2000).

La Directiva contempla la realidad tecnológica con amplitud de miras abarcando cualquier tipo de información personal y en cualquier formato incluidos aquellos que integren información estructurada en soporte papel, o información consistente en imágenes y sonidos.

El núcleo central de la protección otorgada por la Directiva se basa en el consentimiento, en la garantía de la autodeterminación individual, sin perjuicio de la existencia de supuestos en los que una habilitación legal, los derechos e intereses legítimos de terceros o el propio interés vital del titular de los datos, habiliten para un tratamiento de datos sin consentimiento.

El siguiente esfuerzo comunitario en la regulación de las tecnologías de la información se desarrolló con la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Esta Directiva se identifica como complemento de la Directiva 95/46/CE en lo que afecta a la tutela de la intimidad y a la regulación del tratamiento de datos personales en el ámbito de las comunicaciones y por ello le atribuye carácter supletorio.

La Directiva pretende afrontar los retos planteados por las nuevas redes digitales y los servicios que prestan, incluida la televisión interactiva y el vídeo bajo demanda, y hacerlo garantizando los derechos de los ciudadanos. La norma establece las condiciones que faciliten un anonimato controlado en ámbitos como la facturación, en la identificación de las líneas, fijando las condiciones para que el abonado decida hacer pública su información en la guía o garantizando el derecho a la intimidad en su dimensión más tradicional de derecho a no ser molestado.

Posteriormente, se dictó la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. La Directiva 2002/58/CE pretende abarcar, Internet y los nuevos servicios asociados a la telefonía digital y tiene en cuenta nuevas tipologías de datos personales asociados a la movilidad individual y a la localización a través de los dispositivos móviles. Por otra parte, la exposición de motivos define el ordenador como un ámbito de intimidad tutelado por el Derecho y deben ser protegidos frente a intromisiones no deseadas. Debe subrayarse que la Directiva considera que los datos de trafico en las comunicaciones, incluidos los relativos al establecimiento de las mismas, pertenecen

a la vida privada de los usuarios y se hallan protegidos por el secreto de las comunicaciones de modo que sólo podrán utilizarse con fines técnicos y de facturación requiriéndose el consentimiento para cualquier otro tipo de uso.

Esta Directiva se adaptó a los tiempos. Así se previó la posibilidad de prestar el consentimiento en un entorno web, se aludía a las guías de abonados online y a las guías de búsqueda inversa y entre las posibilidades para rechazar mensajes comerciales no solicitados se incluyeron los "SMS" -short message service-, hoy día omnipresentes.

A continuación la Directiva 2006/24/CE, de 21 de febrero de 2006, del Parlamento Europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE, abordó el espinoso tema de la conservación de estos datos.

Esta norma establece una obligación de conservación de los datos de tráfico y localización para proporcionarlos «a las autoridades nacionales competentes y, en casos específicos, de conformidad con la legislación nacional, con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como el terrorismo y la delincuencia organizada». Establece los periodos de conservación de los datos por un periodo que podrá ir de 6 meses a dos años permitiendo a su vez ampliar el plazo de modo limitado, a los Estados miembros.

Desde el punto de vista del tratamiento y control de la información personal cabe referirse a la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Esta Directiva regula el uso de datos personales para el envío de correo comercial, dejando a los Estados la libertad de elegir entre el empleo de sistemas que requieren el consentimiento expreso para recibir información (opt-in) o bien la solicitud de ser incluidos en listas de exclusión (opt-out).

Finalmente la reciente Directiva 2009/136/CE [8] ha venido a modificar la Directiva 2002/58 mediante la introducción de previsiones relativas a la seguridad de los

[8] Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al

datos en el sector de las telecomunicaciones, y la notificación al afectado de las quiebras de seguridad cuando puedan afectar negativamente a la intimidad o a los datos personales de un abonado o particular, salvo que el proveedor haya probado a satisfacción de la autoridad competente que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad.

Además regula el uso de dispositivos que, como las cookies, se instalan en el ordenador de los usuarios. Por último se aborda el envío de mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación.

#### 2.4.3.2 La doctrina del TJCE.

La jurisprudencia relacionada con las tecnologías de la información no es muy abundante. Las sentencias más relevantes en materia de protección de datos son las dictadas en el 6 de noviembre de 2003, asunto Bodil Lindqvist (asunto C-101/01), la sentencia dictada el 20 de mayo del mismo año con motivo del los asuntos C-465/00, C-138/01, C-139/01 y C-465/00, y la Sentencia del Tribunal de Justicia dictada en los asuntos acumulados C-317/04 y C-318/04. En está última se anula la decisión del Consejo relativa a la celebración de un acuerdo entre la Comunidad Europea y los Estados Unidos sobre el tratamiento y la transferencia de datos personales y la decisión de la Comisión relativa al carácter adecuado de la protección de estos datos

La primera de ellas trae su causa del caso de la la Sra. Lindqvist, que mantenía una página de información parroquial en la que llegó a informar sobre el estado de salud de un miembro de la comunidad. El TJCE identifica la presencia de un tratamiento de datos de carácter personal:

> «25. En cuanto al concepto de «tratamiento» de dichos datos que utiliza el artículo 3, apartado 1, de la Directiva 95/46, éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales».

tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n o 2006/2004 sobre la cooperación en materia de protección de los consumidores

> Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole».
>
> El TJCE consideró aplicable la directiva al citado tratamiento.

En la segunda de las sentencias citadas se discutía la conformidad con la Directiva de las comunicaciones de datos previstas por el artículo 8 de la Ley Federal Constitucional sobre la limitación de la retribución de funcionarios públicos, BGB. I 1997/64. En los fundamentos jurídicos del fallo núms. 65 y ss. El TJCE viene a afirmar la vigencia de los principios de finalidad, calidad de los datos y consentimiento señalando la existencia de intereses públicos que justifican comunicaciones de datos sin consentimiento.

En la última de las sentencias señaladas se enjuiciaba la adecuación de las medidas adoptadas para colaborar en la lucha antiterrorista con Estados Unidos. La Comisión consideró que se daba un nivel adecuado de protección en el tratamiento de estos datos y el Consejo adoptó una Decisión por la que aprobaba la celebración de un Acuerdo entre la Comunidad Europea y Estados Unidos sobre el tratamiento y la transferencia de los datos de los PNR por las compañías aéreas establecidas en el territorio de los Estados miembros.

El Tribunal de Justicia concluye que la Decisión de la Comisión sobre el carácter adecuado de la protección no está comprendida en el ámbito de aplicación de la Directiva 95/46/CE dado que se refiere a un tratamiento de datos personales que está excluido de ésta[9].

#### 2.4.3.3 Los textos "constitucionales" comunitarios.

El primer reconocimiento expreso del derecho a la protección de datos se produjo en la Carta Europea de Derechos Fundamentales. Este texto carecía de virtualidad jurídica pero incorporó por primera vez una Declaración de derechos técnicamente reconocible como tal, ofreciendo un referente interpretativo directo fruto del Consenso de los Estados. En lo que afecta a las tecnologías de la información la

[9] Existen otras sentencias que pueden consultarse en el apartado de documentación del website de la AEPD. (http://www.agpd.es/portalweb/canaldocumentacion/sentencias/index-ides-idphp.php)

Carta es consciente de la necesidad de «reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos».

A los efectos de este curso es el artículo 8 que recoge lo dispuesto por el artículo 286 del Tratado de la Comunidad Europea y la Directiva 95/46/CE. Por supuesto, también se invocan como fuentes de inspiración el artículo 8 del CEDH y el Convenio 108.

Los derechos que se vienen comentando fueron incorporados a la fracasada Propuesta de Tratado por el que se instituye una Constitución para Europa y, finalmente se han incorporado dos artículos tras el Tratado de Lisboa a la Versión Consolidada de los Tratados. El primero se sitúa en el plano del funcionamiento de las instituciones pero con eficacia en todo el Derecho Comunitario:

> «Artículo 16
>
> (antiguo artículo 286 TCE)
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.
>
> Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea».

Y en el ámbito de la política exterior y de seguridad común:

> «Artículo 39

> De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes».

Con ello se cierra la definitiva consolidación en el contexto de la unión Europea del derecho a la protección de datos.

## 2.5 El derecho fundamental a la protección de datos en España.

La técnica de protección de datos tiene por objeto garantizar que el individuo tenga la capacidad de ejercer un control real sobre su información. En Espña adquiere una dimensión constitucional. Así, según dispone el art. 18.4 de la Constitución Española:

> «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».

Para entender correctamente los problemas que suscita la protección de datos personales debemos partir del concepto de información personal y ser capaces de diferenciar entre intimidad, vida privada y protección de datos. La protección de datos se diferencia del derecho a la intimidad por atribuir al individuo facultades de control sobre todos sus datos personales con independencia de la naturaleza de éstos, y por requerir de cauces procedimentales para obtener prestaciones positivas a cargo del Estado o de los particulares.

El contenido de éste derecho ha sido concretado por el Tribunal Constitucional a lo largo de distintas sentencias, desde la STC 254/1993, que han ido consolidando su doctrina. La más relevante, por cuanto desarrolla completamente el derecho es la

sentencia 292/2000 que lo consolida de modo definitivo como un derecho fundamental dotándolo de plena autonomía respecto del derecho a la intimidad:

> «el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).
>
> Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran».

El Tribunal Constitucional cierra su argumentación definiendo el objeto de protección del derecho a la protección de datos que alcanza:

> «a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo»(FJ 6).

En el mismo fundamento se describe, ahora si de modo integral, el contenido del derecho fundamental a la protección de datos que incluye un haz de garantías y facultades que se traducen en determinadas obligaciones de hacer para la Administración Pública, pero por extensión para cualquier responsable de un fichero, y correlativos derechos para el administrado. Concretamente el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el derecho a la protección de datos atribuye un poder de disposición sobre los datos personales[10].

EN RESUMEN

[10] La jurisprudencia del Tribunal Constitucional se encuentra en las SSTC 254/1993, 143/1994, 11/1998, 144/1999, 290/2000, 292/2000, 202/1999, 203/2001, 123/2002, 14/2003, 153/2004, 68/2005, 233/2005 y 114/2006

- El derecho fundamental a la protección datos es un derecho consolidado en Europa tanto en los Tratados Constitutivos y Directivas de la UE, como en el sistema del Consejo de Europa.
- Las constituciones y la jurisprudencia de los tribunales constitucionales de algunos Estados miembros han consolidado el derecho fundamental a la protección de datos.
- El derecho a la protección de datos personales se configura como un derecho de control sobre la información personal pública o privada.

# 3. CONCEPTOS BÁSICOS Y ALCANCE DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

## 3.1 Concepto de dato personal y titular del derecho

El objeto de las normas de protección de datos es la garantía y salvaguarda de los derechos fundamentales de las personas en relación con el tratamiento de sus datos de carácter personal.

De este modo, la determinación de qué ha de ser considerado como dato personal resulta esencial para poder establecer el ámbito de protección y garantía derivado del derecho fundamental

La mayoría de las normas de protección de datos definen dato personal como:

***Cualquier información concerniente a una persona física identificada o identificable***

Así, son dos los elementos básicos para establecer una definición de lo que es dato personal

- Debe tratarse de información personal que permita identificar al titular del derecho.
- Sólo son titulares del derecho, en la mayoría de los sistemas, las personas físicas.

**¿Cuándo cabe entender que la información permite la identificación de la persona?**

Ante todo, debe considerarse que el término "información" ha de entenderse en su sentido muy amplio. Hasta época reciente esa información asociada a una persona solía aparecer recogida de forma escrita o referirse a aspectos esenciales relacionados con la persona, sus características, preferencias, opiniones, propiedades, etc.

Sin embargo, actualmente es posible que existan bases de datos que únicamente contengan una imagen, un sonido o una huella digital.

**La información, por tanto puede ser numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.**

Para dar respuesta a la pregunta que se ha planteado será necesario analizar la posible vinculación entre una información aislada y la persona a la que esa información se refiere, pudiendo haber varios grados de "identificabilidad":

- Una lista con los nombres y direcciones de personas contendrá lógicamente datos personales.
- Pero también serán datos personales los incluidos en una lista que sólo contenga el número de identificación o cédula de esas personas.
- ¿Y si la lista se refiere únicamente a direcciones postales sin incluir más información?
- ¿Y también lo será una lista de direcciones de correo electrónico? ¿Y de direcciones IP de usuarios?

La respuesta a las preguntas que acaban de plantearse exige determinar cuándo una persona puede ser identificable a través de una determinada información que le concierne. A tal efecto, puede considerarse como persona identificable:

***Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.***

De este modo, para que quepa considerar una información como dato de carácter personal deberá analizarse esa vinculación a la persona a la que la información se refiere y si resulta más o menos complejo llevar a cabo esa identificación. Así:

- Un número de identificación o de cédula tiene por objeto precisamente identificar a la persona y además es sencillo lograr esa identificación mediante una búsqueda en Internet, por lo que es un dato personal.

- Una dirección postal podrá ser considerada un dato personal del propietario de la vivienda, dado que podrá asociarse al mismo mediante la consulta al Registro de la Propiedad.

- Existen casos más complejos, como los del correo electrónico, la dirección IP o el número de Teléfono, en que habrá que valorar la información derivada del propio dato y si la vinculación a la persona puede llevarse a cabo por quién tiene el dato en su poder.

  No cabe duda que una dirección de correo electrónico del tipo nombre.apellido@empresa.com será un dato personal.

  Tampoco hay dudas de que la dirección IP asignada a un usuario por su operador será un dato personal para dicho operador.

  Pero en otros casos la solución será más complicada y deberá analizarse caso por caso, a fin de evaluar si estamos ante un dato personal. Por ejemplo, cuando una empresa sólo tenga una lista de números de teléfono que no puedan ser consultado en una guía o cuando las direcciones de correo de que disponga sean del tipo xxnn33x@gmail.com o spiderman@hotmail.com.

**¿Cuándo cabe entender que la información se refiere a personas físicas?**

La respuesta a esta cuestión aparentemente resulta sencilla. Todos conocemos la diferencia entre una persona física y una persona jurídica. Sin embargo existen casos en que pueden plantearse dudas, dado que la información se vincula más a una actividad económica o al trabajo que desempeña la persona física que a ella misma.

Así nos podemos plantear varias cuestiones:

- ¿Son datos referidos a personas físicas los que se limiten a indicar el volumen de facturación de una empresa individual no constituida como sociedad?

- ¿Y otros datos adicionales que permiten identificar a esa empresa y distintos de los que identifican al empresario?

- ¿La información de mi tarjeta de visita contiene datos de carácter personal?

La solución a estas preguntas puede diferir en los distintos países. Algunos incluso consideran datos personales a las informaciones referidas a personas jurídicas.

En España, las normas de protección de datos han establecido algunos criterios en cuya virtud ciertos datos, aún asociados estrictamente a una persona física no son considerados datos personales. Así:

- ***Los datos relativos a empresarios individuales, cuando únicamente hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.***

- ***Tampoco se aplican las normas de protección de datos cuando los tratamientos se limiten a incorporar los datos de las personas físicas que presten sus servicios en une empresa, siempre que esos datos consistan únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.***

Para que operen estas reglas será necesario que la información tratada lo sea con una finalidad básicamente empresarial, es decir, que quien trata dato únicamente pretenda relacionarse con la empresa individual o con aquélla otra en que el interesado trabaje, pero no exista voluntad de tratar los datos con la finalidad de contactar directamente con es persona. Dicho de otra forma, el tratamiento será lícito en las relaciones "business to business" pero no en las "business to consumer".

> De este modo, si una persona o una empresa tiene un fichero de "personas de contacto" con la única finalidad de dirigirse a personas de otras organizaciones para mantener una relación con esa organización y únicamente se tratan los datos que se

han enumerado, no sería de aplicación la legislación de protección de datos.

Por ejemplo, si una empresa proveedora tuviera un fichero con los datos de los directores del departamento de compras de sus empresas clientes.

Si por el contrario, lo que se pretendiese fuera captar como clientes a esas personas, siendo precisamente el puesto en que trabajan un criterio para segmentarlas (por ejemplo, para ofrecer a altos directivos un producto financiero) , sí serán aplicables las normas de protección de datos.

La última cuestión que debe resolverse en este momento es la de **si las personas fallecidas son titulares del derecho fundamental a la protección de datos o si este derecho se extingue con la muerte**.

Como regla general en los países cuyo derecho civil es heredero del Código de Napoleón (lo que sucede en la mayor parte de los países de la Comunidad Iberoamericana), el derecho a la protección de datos, como derecho de la personalidad, se extingue con la muerte de las personas.

Sin embargo, hay que tener en cuenta que el que una persona fallecida no sea titular del derecho no implica que puedan seguir tratándose sus datos, dado que ese tratamiento puede causar un perjuicio a su honor, cuyo resarcimiento puede reclamarse por sus herederos. Además, mantener el tratamiento de los datos de una persona que ha fallecido puede dar lugar a otros perjuicios a sus familiares, difíciles de evaluar.

- ¿Puede mantenerse el dato de un fallecido que no cumplió con todas sus deudas en un "bureau de crédito", cuando es la herencia o son los herederos los deudores?

- ¿Resulta razonable que los herederos de un fallecido sigan recibiendo publicidad dirigida a esa persona? ¿o que reciban una llamada en que se felicite al difunto por su cumpleaños?

La respuesta a estas preguntas es lógicamente negativa. Si los fallecidos no tienen derecho a la protección de datos, quienes tratan sus datos deben además actualizarlos para que o persista ese tratamiento.

Para evitar esas situaciones algunos sistemas como el español han establecido una regla que permite a quien está tratando los datos saber que ya no procede ese tratamiento. Así, en el Reglamento de desarollo de la Ley española se dice lo siguiente:

***Este Reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos***

Además, debe tenerse en cuenta que:

- En ocasiones, los herederos o, en su caso los legatarios, tendrán derecho a conocer los datos del fallecido que estén siendo tratados precisamente por ostentar esa condición. Por ejemplo, a fin de conocer el caudal hereditario o la cuantía y circunstancias del legado.

- La normativa sanitaria suele reconocer el derecho de los familiares a acceder a la historia clínica de los pacientes en cuanto dicho acceso puede, por una parte, dar lugar al ejercicio de determinadas acciones y, por otra, permite a los familiares conocer determinados datos que pueden influir en su propia salud, al compartir una misma línea genética.

**EN RESUMEN**:

- Los datos personales pueden referirse a información de muy diversa índole y en diversos tipos de soporte.
- La persona a la que los datos se refieren deberá resultar identificable para que nos encontremos ante datos personales.
- Los datos personales se refieren a personas físicas no fallecidas; pero existen ciertas especialidades en relación con los empresarios individuales y las "personas de contacto" en que deberá tenerse en cuenta la finalidad para la que se tratan los datos

## 3.2. Conceptos de fichero y tratamiento.

En España, las normas de protección de datos se aplican a los datos personales incorporados a un soporte físico susceptible de tratamiento. De este modo, para que dichas normas sean de aplicación no basta con que "tengamos" un dato personal, sino que será necesario que el mismo sea susceptible de ser tratado.

- ¿El mero conocimiento de una información personal está sometido a las normas de protección de datos?
- ¿Si mantengo la información en hojas de papel sin ordenar estoy sometido a las normas de protección de datos?
- ¿Y si las mantengo en una base de datos en mi ordenador, o simplemente en una hoja de Excel?
- Si los datos están en papel ordenados por el nombre de las personas o por un índice que mantengo en un documento de mi ordenador, ¿se me aplican las normas de protección de datos?

La respuesta a estas preguntas puede depender del sistema en el que estemos. No obstante existen unos criterios básicos uniformes que nos permitirán determinar si estamos o no sometidos a las normas de protección de datos.

En primer lugar, para que esas normas sean aplicables es necesario que exista un tratamiento de datos personales. Por tratamiento de datos cabe considerar:

> ***Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias***

Este concepto, como puede comprobarse, es omnicomprensivo, dado que prácticamente cualquier operación relacionada con un dato de carácter personal puede encajar en el concepto de tratamiento. Por tanto, dicho concepto no es suficiente para establecer una delimitación clara de las normas de protección de datos.

El derecho a la protección de datos, como se ha señalado en otros lugares, surge para proteger la intimidad del individuo frente a la intromisión que puede suponer el uso de la informática. Así se recoge en distintos instrumentos normativos e incluso en algunos textos constitucionales como el español:

> Según el artículo 18.4 de la Constitución Española "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".

Esta protección del individuo frente a la informática, aun cuando el ámbito del derecho fundamental a la protección de datos haya aumentado en la actualidad para convertirse en un derecho fundamental independiente y autónomo de la intimidad personal y familiar, puede ser tenido en cuenta para delimitar el alcance de los tratamientos que deberán someterse a las normas de protección de datos. De este modo:

- Siempre que el tratamiento de los datos implique el uso de la informática, es decir, cuando dicho tratamiento sea "automatizado", el individuo deberá ser protegido por la norma.

  Así, cuando tenemos un documento en un procesador de texto o una hoja de cálculo en que se contienen datos personales, por

ejemplo para hacer etiquetas, estamos sujetos a las normas de protección de datos.

Lo mismo sucederá si tenemos diversos ficheros referidos a personas distintas en una carpeta de nuestro sistema.

Igual sucederá en caso de guardar en nuestro ordenador fotografías o registros de voz de nuestro personal o si a través del mismo accedemos a las imágenes recogidas por una webcam instalada para proteger nuestras oficinas (en este punto, debe tenerse en cuenta lo que se indicará después sobre el tratamiento de datos para fines personales o domésticos).

- Cuando el tratamiento no sea automatizado, deberá tenerse en cuenta el grado de injerencia en el derecho a la protección de datos derivado de ese tratamiento.

Surge así el concepto de fichero como complementario del de tratamiento para delimitar objetivamente el ámbito de aplicación de las normas de protección de datos. Puede definirse como tal:

***Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.***

Debe tenerse en cuenta que el concepto de fichero no debe considerarse necesariamente vinculado al de "base o banco de datos". Generalmente una base de datos es un fichero, pero existen casos en que el concepto legal de fichero engloba a distintas bases de datos que, incluso pueden no estar interconectadas. En este caso, para determinar si nos encontramos ante un fichero deberemos tener en cuenta la estructura de las distintas bases de datos, el motivo por el que se crearon y la finalidad que pretenden cumplir.

Así, por ejemplo, si una compañía de salud es dueña de distintos hospitales, gestionando sus recursos y en cada uno de ellos existe una base de datos en que se incorporan los datos del historial clínico de cada hospital, podremos considerar que

existe un único fichero de historiales clínicos de la compañía, a pesar de que existan "distintas" bases de datos localizadas en cada uno de los hospitales.

El concepto de fichero resulta especialmente importante en caso de que no nos encontremos ante un tratamiento automatizado de datos, puesto que en este caso las normas de protección de datos tienden a delimitar su ámbito de aplicación únicamente a los supuestos en que los datos no tratados automatizadamente se incorporen a un fichero. Por fichero no automatizado puede entenderse:

***Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica***

El requisito esencial para que un conjunto de datos no tratados automatizadamente sea un fichero no automatizado ese conjunto se encuentre estructurado y que los criterios en que se basa esa estructuración se refieran a personas físicas a las que la información se refiere.

- El conjunto de carpetas de asuntos de un abogado será un fichero no automatizado, en cuanto pueda acceder a la información de un asunto a partir de la identificación de su cliente.

- También lo serán las capetas en las que un médico guarda las historias clínicas de sus pacientes.

Generalmente, esas carpetas estarán asociadas a un índice generado informáticamente que permitirá identificar una carpeta numerada por la referencia a una persona.

Pero existirán otros casos en los que no es fácil determinar a primera vista si un conjunto de informaciones tiene o no la consideración de fichero

En estos últimos casos lo fundamental es analizar si el criterio de estructuración permite acceder a la información de una persona con un criterio sencillo referido a la misma.

> Si las carpetas están ordenadas conforme al número de identificación del interesado cabrá entender que hay un fichero.
>
> También es posible entender que hay fichero si las carpetas están ordenadas por fechas de nacimiento, dado que este dato es fácilmente accesible.

Sin embargo hay casos en que el criterio de estructuración no permite acceder fácilmente a la información referida a una persona concreta. En ese caso cabrá considerar que no hay fichero y si no existe un tratamiento automatizado de datos no serían aplicables las normas de protección de datos personales.

> En España, el Tribunal Supremo ha considerado que los Libros de Bautismo de la Iglesia Católica, cuando no hay un tratamiento automatizado de la información sobre el bautismo, no están sometidos a la legislación de protección de datos. Entiende el Tribunal Supremo que no es fácil acceder a la información de un bautizado, porque la estructura del libro exige conocer la fecha concreta en que una persona se bautizó y la parroquia en que fue bautizado, por lo que el Libro no encaja en el criterio general de fichero no automatizado.

Hechas estas consideraciones, existen supuestos en los que aún produciéndose un tratamiento automatizado de datos personales o existiendo un fichero, automatizado o no, con los mismos, las normas de protección de datos no son aplicables.

a) En algunos casos esta exclusión puede basarse en que la propia normativa reguladora de un concreto fichero establece un sistema integral de protección de datos relativo al mismo. Así podría suceder, por ejemplo, en relación con determinados registros públicos, el censo electoral o el padrón de habitantes, las historias clínicas u otros supuestos.

Sin embargo en estos casos, las normas de protección de datos deben ser tenidas en cuenta, completando el régimen especial de estos ficheros y garantizando que esas especialidades no supongan una excepción inadecuada del régimen general de garantías del derecho fundamental. Generalmente este objetivo se logra mediante la aplicación supletoria de las normas de protección de datos a cada fichero concreto.

b) En otros casos existe una razón de interés público que justifica el establecimiento de excepciones concretas a la aplicación general de las normas de protección de datos. En estos casos, se trata de una limitación de un derecho fundamental fundada en la existencia de otros derechos dignos de protección.

Por ejemplo, en el derecho comunitario europeo la Directiva de Protección de Datos prevé que algunas de sus disposiciones no serán aplicables a determinados ficheros cuando tal limitación constituya una medida necesaria para la salvaguardia de: la seguridad del Estado; la defensa; la seguridad pública; la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; un interés económico y financiero importante, incluidos los asuntos monetarios, presupuestarios y fiscales; una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública; g) la protección del interesado o de los derechos y libertades de otras personas.

Siguiendo esta regla, las normas de protección de datos actualmente vigentes excluyen de su aplicación las materias clasificadas u objeto de inteligencia militar.

c) Por último, existen otros supuestos en los que la exclusión de la aplicación de las normas de protección de datos tiene su fundamento en el adecuado desarrollo de las relaciones sociales, de amistad o familiares, dado que la aplicación de estas normas no puede implicar una interferencia en la esfera privada de las personas.

De este modo, se excluyen habitualmente de la aplicación de las normas de protección de datos los tratamientos de datos o ficheros mantenidos en el ámbito de las relaciones personales o familiares de un individuo. En España, la Ley Orgánica de Protección de Datos dispone que la misma no se aplica:

***A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, definiendo como tales los relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares***

Así las normas de protección de datos no se aplicarían, por ejemplo, al uso de datos de un grupo de compañeros de universidad para preparar una cena o un viaje (no obstante, sí se aplicarían estas normas para el restaurante o la agencia de viajes que organice el evento, dado que en este caso el tratamiento no se realizaría en el ámbito de la vida privada).

Tampoco se aplicarían las normas de protección de datos a la libreta de direcciones, correos electrónicos o números de teléfono de nuestros amigos o familiares.

**EN RESUMEN:**

**-** Las normas de protección de datos se aplicarán a:

**-** Los tratamientos automatizados de datos

**-** Los tratamientos no automatizados si los datos se incorporan a un fichero.

- Existirían determinados tratamientos y ficheros excluidos de la legislación de protección de datos, siendo esta excepción aplicable en general a los tratamientos relacionados con la vida privada y familiar.

## 3.3 El responsable del fichero o del tratamiento y el encargado del tratamiento

Una vez delimitado el ámbito objetivo de aplicación de las normas de protección de datos, es preciso hacer referencia a los sujetos que resultan obligados por esas normas by que junto con el afectado o interesado al que los datos se refieren (y, en consecuencia, titular del derecho), constituyen los sujetos a los que se dirigen las normas reguladoras del derecho fundamental.

Tanto el responsable del fichero o del tratamiento como el encargado del tratamiento están relacionados con las actividades de tratamiento a las que nos hemos referido con anterioridad, pero su relación con dicho tratamiento diferirá como consecuencia del distinto poder de decisión y disposición sobre las operaciones de tratamiento.

Además, ambos resultarán sujetos obligados por las normas de protección de datos, de forma que las autoridades de control estudiadas también con anterioridad podrán ejercer sus competencias en relación con todos ello.

***Se considera responsable del fichero o del tratamiento a la persona física o jurídica, de naturaleza pública o privada que, sola o en compañía de otros responsables, decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.***

Esta definición permite, en primer lugar delimitar quiénes podrán ser considerados responsables del fichero o del tratamiento. Este responsable podrá ser:

- Una persona física que trata datos al margen de sus actividades meramente personales o familiares.
- Una persona jurídica (empresa, fundación, asociación, ONG…)
- La Administración Pública. En ese caso la responsabilidad podrá recaer en la propia Administración, como persona jurídica o en un órgano de la misma o en una entidad pública con personalidad jurídica propia.

  Así, podrá ser responsable del fichero o del tratamiento, en el caso de la Administración, una Municipalidad o una empresa municipal o un órgano de esa municipalidad. La decisión de

quién sea responsable dependerá del grado de autonomía del mismo para decidir sobre la finalidad, contenido y uso del tratamiento.

En ocasiones es posible que esta facultad decisoria pueda recaer sobre varios responsables simultáneamente. Así puede suceder en el caso de los llamados "ficheros comunes" en que existe un solo conjunto estructurado de datos personales mantenido en una única base de datos al que aportan información varias entidades, teniendo cada una la condición de responsable en relación con la información aportada.

En España un supuesto típico de esta pluralidad de responsables se da en los llamados "sistemas de información" del sector público (por ejemplo, en el ámbito de la medicina pública o de las políticas públicas de empleo). En ocasiones estos sistemas se estructuran mediante la información facilitada al sistema común por el órgano competente de cada Comunidad Autónoma, que será responsable en relación con esa información, gestionándose generalmente el sistema por la Administración del Estado, que asimismo será responsable del fichero.

Como se ha dicho, lo que caracteriza al responsable es su capacidad de decisión sobre los fines y usos del tratamiento, así como sobre su contenido. Ello exige hacer dos precisiones importantes:

- El responsable no deja de tener esa condición por el hecho de que, en ocasiones, una Ley le obligue a realizar el tratamiento de los datos de una determinada manera o que dicho tratamiento deba referirse a determinados datos concretos

Así, por ejemplo, el hecho de que un centro sanitario esté obligado a la llevanza de las historias clínicas de sus pacientes con un contenido y con una estructura que en muchos sistemas

viene impuesta por las leyes sanitarias no implica que ese centro pierda su condición de responsable, dado que el poder de decisión tiene como punto de partida el hecho de que se ha tomado la decisión de desarrollar esa actividad.

Del mismo modo, el hecho de que un empresario deba tratar al hacer la nómina de sus empleados, dato tales como la retención a pagar a la Administración Fiscal o la cuota que haya de abonarse a la Seguridad Social no altera el hecho de que ese empresario sea responsable del fichero de nóminas

- En ocasiones, es posible que el responsable no realice materialmente el tratamiento de los datos, bien porque éste se lleve a cabo por un encargado del tratamiento, al que nos referiremos inmediatamente, bien porque coexistan las figuras del responsable del fichero y el responsable del tratamiento. Vamos ahora a referirnos a este supuesto.

  En los llamados "bureaus de crédito", por ejemplo, existen dos entidades vinculadas a la realización de un concreto tratamiento relacionado con el impago de una deuda: la entidad acreedora, que facilita el dato al "bureau" y la entidad titular y responsable del fichero en que consiste el "bureau". Si bien la segunda será, obviamente, responsable del fichero, la primera es la que deberá velar porque se cumplan los principios de protección de datos en relación con la información que ha sido facilitada. Así, esta entidad, que no realiza materialmente el tratamiento del dato de la deuda en el "bureau", deberá responder porque la información sea exacta, la deuda exista, no se hayan cumplido los plazos legalmente previstos para que opere el "derecho al olvido", etc.

  Igualmente, en el ámbito de la publicidad no es extraño que las entidades anunciantes acudan a los denominados "listbrokers". Estas empresas son titulares de diversas bases de datos, cuya información, lógicamente, deberá haber sido obtenida de forma lícita. El anunciante determina los parámetros que deberá reunir

la muestra a la que habrá de dirigirse la publicidad, en ocasiones con un detalle tal que la muestra queda limitada a un número muy concreto y reducido de destinatarios, aunque en ningún momento ese anunciante accede a la base de datos para saber quiénes son los concretos destinatarios.

En estos casos, la jurisprudencia de algunos países, como España, ha reconocido la necesidad de diferenciar entre el responsable del fichero (o titular de la base de datos) y el responsable del tratamiento (que efectivamente decide las operaciones concretas de tratamiento en un supuesto concreto). Así, la Sentencia de 5 de junio de 2004 del tribunal Supremo español, reiterando los argumentos de la sentencia recurrida ante el mismo en casación, decía lo siguiente:

*"Se desprende asimismo de los repetidos apartados del art. 3, como ya se ha manifestado, la diferenciación de dos responsables en función de que el poder de decisión vaya dirigido al fichero o al propio tratamiento de datos.* ***Así, el responsable del fichero es quien decide la creación del fichero y su aplicación, y también su finalidad, contenido y uso, es decir, quien tiene capacidad de decisión sobre la totalidad de los datos registrados en dicho fichero. El responsable del tratamiento, sin embargo, es el sujeto al que cabe imputar las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica****. Se trataría de todos aquellos supuestos en los que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento."*

Junto con el responsable, el otro sujeto obligado por las normas de protección de datos es el encargado del tratamiento.

***Por encargado del tratamiento puede entenderse la persona física o jurídica, pública o privada que sola o junto con otras trata datos como consecuencia de la prestación de un servicio contratado por el responsable del fichero o del tratamiento, de forma que únicamente accede a los datos en nombre y por cuenta de aquél.***

Así son servicios típicos de un encargado del tratamiento los realizados, por ejemplo, por un "call center" con el que un responsable contrata la prestación del servicio de atención a sus clientes, los prestados por una empresa que aloja los datos tratados por el responsable en un servidor o los que desarrolla una empresa que ejecuta una campaña publicitaria contratada por un anunciante cuando ésta le facilita su fichero de clientes para su realización.

Los servicios prestados por el encargado del tratamiento, por otra parte, pueden suponer distintos tratamientos de datos que se caracterizarán por la nota común de que siempre serán desarrollados por cuenta del responsable, no siendo el encargado más que un prestador de servicios. Así, el encargado podrá tener como misión recoger los datos en nombre del responsable, conservarlos, facilitarlos a un tercero en nombre del responsable, atender también en su nombre los derechos de acceso, rectificación, cancelación u oposición, organizar y estructurar el contenido de la base de datos, etc.

De lo que se ha indicado se desprenden varias consecuencias:

- El encargado del tratamiento siempre tratará los datos como un mero prestador de servicios del responsable, y nunca podrá emplear los datos en nombre propio.

- El margen de actuación del encargado deberá quedar delimitado en el documento en que se plasme su relación de servicios con el responsable y nunca podrá exceder de la misma.

- Por todo ello, el encargado, en relación con los interesados, siempre actuará como prestador de servicios en nombre del responsable y nunca tratará los datos para establecer un vínculo directo, en su propio nombre, con el afectado, dado que entonces sería responsable y no encargado.

Piénsese, por ejemplo, en el siguiente supuesto: una aseguradora de vehículos firma un acuerdo con una entidad emisora de tarjetas de pago de combustible a fin de que se extienda una tarjeta a nombre de sus asegurados. Para ello, la empresa firma un contrato de prestación de servicios en que se señala que la entidad emisora de las tarjetas es encargada del

tratamiento de la aseguradora. Sin embargo, cuando los asegurados pagan el consumo de gasolina con la tarjeta es esa empresa emisora la que factura a los usuarios y la que efectúa a su nombre los correspondientes cargos en la cuenta asociada a la tarjeta. En este caso, la empresa emisora no es encargada sino responsable del tratamiento, manteniendo una relación directa y en nombre propio con los usuarios. La consecuencia será que la entidad aseguradora ha cedido a la entidad emisora de la tarjeta los datos de sus asegurados, debiendo existir legitimación suficiente para ello, sin que dicha legitimación se pueda encontrar simplemente en la firma de un contrato de prestación de servicios.

Para que pueda considerarse que nos encontramos ante un encargado del tratamiento será necesario, además de atender a la propia naturaleza de la actividad desarrollada por aquél, que exista una clara acreditación de que la actividad del encargado consiste únicamente en la prestación de un servicio al responsable. Por este motivo, la mayor parte de los sistemas normativos de protección de datos exigen que la relación entre el responsable y el encargado se encuentre debidamente documentada, generalmente a través de un contrato escrito, en que se especifiquen con claridad:

- Los servicios que deberá prestar el encargado, siempre por cuenta del responsable.
- El compromiso del encargado de no utilizar los datos para una finalidad distinta de la que justifica el encargo.
- Que concluido el encargo no conservará ni utilizará los datos, devolviéndolos al responsable o destruyéndolos.

  No obstante, en ocasiones, el encargado podrá conservar los datos, aunque sin tratarlos, a fin de garantizar que pueda responder o "rendir cuentas" adecuadamente al responsable durante los períodos legalmente previsto para esa redición de cuentas.

- Que el encargado no facilitará en ningún caso los datos a un tercero (a menos que sea esa comunicación, en nombre del responsable, uno de los tratamientos objeto de la prestación de servicios).

Por ejemplo, una entidad que preste al responsable un servicio integral de asesoramiento fiscal o laboral y emita en su nombre las nóminas de sus empleados facilitará a las autoridades fiscales y de seguridad social en nombre del empresario y como parte del encargo los datos referidos a los pagos a Hacienda y a la Seguridad Social.

- Que el encargado se compromete a adoptar en relación con el tratamiento que lleva a cabo las mismas medidas de seguridad que debería implantar el responsable en caso de hacerlo él mismo.

**EN RESUMEN**

- Los sujetos obligados en materia de protección de datos son el responsable del fichero o del tratamiento y el encargado del tratamiento.

- El responsable se caracteriza por tener un poder de decisión sobre la realización del tratamiento, su finalidad, contenido y uso.

- En ocasiones este poder de decisión podrá no implicar necesariamente el acceso a los datos, pudiendo distinguir entre el responsable del fichero y el responsable del tratamiento

- El encargado del tratamiento carece de ese poder de decisión y deberá actuar en todo momento, como prestador de servicios que es, en nombre y por cuenta del responsable que le contrate.

## 3.4 Ámbito territorial de aplicación de las normas de protección de datos

Una vez delimitado quién es el titular del derecho a la protección de datos, cuál es el objeto de la garantía otorgada por las normas que la regulan y quiénes son los obligados por dichas normas, es preciso determinar cuál será la norma nacional reguladora del derecho fundamental que será de aplicación en cada caso, lo que no siempre resulta sencillo en un mundo globalizado como el actual. Así, será preciso delimitar la Ley aplicable al tratamiento en supuestos como los siguientes:

- El llevado a cabo por un call center ubicado en el Estado A que presta servicio a los clientes de un responsable, cuando tanto la sede de ese responsable como los clientes están situados en el Estado B.
- El llevado a cabo por la sucursal de ese mismo responsable situada en el Estado A.
- El efectuado por un proveedor de servicios de Internet cuya sede social está en A y que presta servicios a usuarios situados en B
- El derivado de una encuesta que realiza una empresa situada en A respecto de los hábitos de consumo de los ciudadanos del Estado B.
- El tratamiento de datos realizado por un buscador de Internet, ubicado en A que, por una parte, introduce en los terminales de los usuarios situados en el Estado B dispositivos invisibles ("cookies") para perfilar sus búsquedas y, por otra, recoge información de los servidores situados en el Estado C para indexar las búsquedas sobre toda la web.

Como puede comprobarse, la respuesta a estas cuestiones no resulta en todos los casos sencilla, pudiendo tenerse en cuenta para la determinación de la Ley aplicable diversos criterios, entendiendo aplicable:

- La Ley del lugar en que esté la sede principal del responsable.
- La Ley del lugar en que se encuentre el establecimiento del responsable en que se realiza el tratamiento.
- La Ley nacional del interesado.

- La Ley en que se encuentren los medios o "equipamiento" empleados para el tratamiento.

De entre estas posibles soluciones, las legislaciones han optado, por lo general por las referidas al lugar de ubicación del establecimiento o, en su defecto, del "equipamiento" o medios empleados para el tratamiento.

Así, por ejemplo, el artículo 4 de la Directiva Comunitaria de Protección de Datos dispone lo siguiente:

***1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:***

***a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;***

***b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;***

***c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.***

***2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.***

Si bien las reglas establecidas en este precepto tienen específicamente en cuenta la existencia de la Unión Europea, lo que afecta a la determinación de la Ley aplicable

en caso de empresas ubicadas en varios Estados Miembros, sus criterios son los seguidos por otras legislaciones nacionales extracomunitarias. De este modo, los criterios de aplicación de la Ley serían los siguientes:

**a) Ubicación del establecimiento del responsable en que se lleve a cabo el tratamiento**

A estos efectos, lo relevante no sería determinar la sede principal del responsable, sino del establecimiento del responsable en cuyo marco de actividad se realiza el tratamiento. De este modo, por ejemplo, el tratamiento llevado a cabo por una sucursal en un país distinto a aquél en que se encuentra la sede social se sometería a la legislación del Estado de situación de la sucursal y no al de la Sede.

Por ejemplo, el tratamiento llevado a cabo en España por la sucursal de una entidad bancaria o aseguradora extranjera que no ha creado una filial en España estaría sometido a la Ley española.

Una segunda consecuencia de la aplicación de este criterio será la de que el tratamiento efectuado por un encargado del tratamiento será la que resultaría aplicable si dicho encargado no existiera. De este modo, la legislación aplicable al tratamiento sería la del establecimiento del responsable por cuenta del cual se lleva a cabo la prestación de servicios.

Así, el "call center" de una empresa española estará sometido en lo referente al tratamiento de sus datos a la Ley española. Del mismo modo, el tratamiento llevado a cabo por el servidor en que se almacenen los datos de los que es responsable una empresa española estará igualmente sujeto a la Ley española.

Es importante, no obstante efectuar dos precisiones en relación a las reglas que acaban de indicarse:

- En primer lugar, en el ámbito de la Unión Europea esta regla se aplica cuando tanto el responsable como el encargado están ubicados en un

Estado Miembro, dado que si el responsable es extracomunitario se considera de aplicación al tratamiento la legislación del encargado en virtud del segundo criterio que veremos inmediatamente.

- En segundo lugar, incluso cuando ambas empresas se encuentran en la Unión Europea, la regla general queda exceptuada en un punto: serán de aplicación al tratamiento las normas de seguridad exigibles por la Ley del Estado en que se encuentre el encargado del tratamiento.

**b) Ubicación de los "medios" o "equipamiento" empleados para el tratamiento**

Cuando el criterio de la ubicación del establecimiento del responsable no es suficiente, y en particular en el ámbito de la Unión Europea cuando dicho establecimiento no está en el territorio de la Unión, el segundo criterio delimitador de la legislación aplicable será el de la ubicación del equipo ("equipment" en la versión inglesa de la Directiva) utilizado para llevar a cabo el tratamiento.

De este modo, si dicho equipo está ubicado en un determinado Estado de la Unión Europea es la legislación de ese Estado la aplicable al tratamiento.

La interpretación del concepto de "medios" o "equipamiento" no es clara, aunque existen diversos documentos que la han analizado con detalle. Así, por ejemplo, se ha entendido que ese equipo es el terminal del usuario/interesado/titular del derecho si el responsable instala en el mismo una cookie.

En todo caso, será necesario que esos medios o equipamiento no se empleen únicamente con fines de mero tránsito, como sucedería, por ejemplo, en el caso de una red pública de comunicaciones electrónicas cuando ni el origen ni el destino de la comunicación estén ubicados en el país en cuestión.

En estos supuestos, dado que el responsable no se encuentra ubicado físicamente en el Estado en que se encuentran los medios empleados para el tratamiento, será necesario que el mismo cuente con un representante en el Estado en que estén situados los mencionados medios. Este representante podrá ser un encargado del tratamiento (que podría estar gestionando estos medios), un representante comercial o una sucursal de la empresa responsable.

**EN RESUMEN:**

**-** La delimitación de la legislación aplicable a un tratamiento resulta imprescindible en un ámbito marcado por la globalización o fenómenos tales como Internet.

- En general, el criterio delimitador de la Ley aplicable es el del establecimiento del responsable en cuyo marco se desarrolle el tratamiento de los datos.

- Como criterio residual, si el tratamiento utiliza medios situados en un determinado Estado, será aplicable la Ley del Estado en que se encuentren dichos medios.

## 3.5 Otros conceptos básicos en materia de protección de datos

Hasta ahora hemos visto las definiciones esenciales a tener en cuenta para delimitar el alcance y garantías previstos en las normas de protección de datos (incluyendo conceptos como los de datos personal, interesado, tratamiento, fichero, responsable del fichero, responsable del tratamiento o encargado del tratamiento).

A continuación se va a hacer referencia a un pequeño glosario de términos que igualmente deberán ser tenidos en cuenta al afrontar el estudio de los principios y normas de protección de datos, sin perjuicio de que el estudio detallado de su aplicación y consecuencias corresponda llevarlo a cabo en otros lugares y momentos del curso:

- **Dato disociado**: aquél que no permite la identificación de un afectado o interesado.

- **Procedimiento de disociación**: Todo tratamiento de datos personales que permita la obtención de datos disociados.

- **Datos de carácter personal relacionados con la salud**: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

- **Consentimiento del interesado**: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

- **Cesión o comunicación de datos**: Tratamiento de datos que supone su revelación a una persona distinta del interesado. No obstante, el acceso a los datos por un encargado del tratamiento no se considerará cesión de datos.

- **Destinatario o cesionario**: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. El destinatario podrá ser a su vez responsable del tratamiento si el mismo se produce una vez recibidos los datos.

- **Transferencia internacional de datos**: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del un Estado (o en el ámbito de la Directiva Comunitaria, del Espacio Económico Europeo), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable.

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

- **Importador de datos personales**: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en

caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

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

# 4. LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN.

## 4.1 Introducción

La Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, reconoce de modo inequívoco la existencia de una derecho fundamental a la protección de datos de carácter personal, considera uno de los elementos esenciales del citado derecho el posible ejercicio por el afectado de los derechos de acceso, rectificación, cancelación y oposición.

Así recuerda la citada Sentencia que "*el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, F. 7)*"

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

Teniendo en cuenta la citada Sentencia y la Directiva Comunitaria se aprobó en el ámbito español la correspondiente Ley Orgánica[11] y su Reglamento de desarrollo, donde se regulan de forma detallada los derechos de Acceso, Rectificación, Cancelación y Oposición.

## 4.2 Disposiciones generales sobre el ejercicio de los derechos

### 4.2.1. Carácter personalísimo y ejercicio por medio de representante legal o voluntario

La configuración del derecho fundamental a la protección de datos como derecho de la personalidad, formando parte los derechos de acceso, rectificación, cancelación y oposición del haz de facultades que conforma el derecho fundamental, conduce necesariamente a la conclusión de que el ejercicio de tales derechos es personalísimo, debiendo precisamente ejercitarse por el afectado al que los datos se refieren.

Sin embargo, la consideración de un derecho de carácter personal no puede confundirse con la imposibilidad del ejercicio de los mismos por medio de representación.

En efecto, el ejercicio de los derechos a través de representante, legal o voluntario, no puede considerarse en modo alguno contrario a su carácter personalísimo, dado que los actos realizados por dicho representante han de reputarse llevados a cabo por el propio representado, siempre que concurran los requisitos necesarios para acreditar la validez de la representación. Por tanto, la interposición del representante, en la relación afectado-responsable en modo alguno desvirtúa el carácter directo de dicha relación y menos aún vulnera las exigencias derivadas de la regla que se ha venido citando.

[11] Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (en adelante LOPD) y el Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Este razonamiento, se manifiesta en la normativa española[12] que después de haber reiterado el carácter personalísimo de los derechos, posibilita su ejercicio a través de representante legal o voluntario.

En cuanto al ejercicio de los derechos a través de representante legal, podemos destacar en primer lugar los supuestos de incapacitación, en los que será preciso que la incapacitación se haya producido realmente, habiendo recaído la correspondiente sentencia de incapacitación. Por otro lado, respecto a los menores de edad, deben tenerse en cuenta las previsiones[13] que se contienen en cuanto a la posibilidad de que los menores de edad puedan prestar por sí mismos su consentimiento al tratamiento de los datos de carácter personal, permitiendo a los mayores de catorce años (en el ámbito español) otorgar su consentimiento para el tratamiento de los datos y para los menores de catorce años se requerirá el consentimiento de los padres o tutores.

En relación con el ejercicio de los derechos a través de representante voluntario, se permite esta circunstancia, siempre que exista, un apoderamiento expreso y, que se aporté la documentación acreditativa de la identidad del representado y de la representación expresamente conferida.

Incluso se permite que el apoderamiento se refiera al ejercicio de los derechos en relación con un determinado fichero o incluso en relación con un responsable del tratamiento concreto, sin que fuera necesario un apoderamiento específico para cada supuesto de ejercicio. Al propio tiempo, deberá denegarse la solicitud, cuando ésta sea formulada por persona destinta del afectado y no se acreditase que actúa en representación de aquél.

### 4.2.2 Condiciones generales para el ejercicio de los derechos. Caracteres de estos derechos

Existen tres características esenciales[14] que son exigibles en el ejercicio de los derechos que son; independencia, gratuidad y sencillez.

[12] Artículo 23.2 del Reglamento de desarrollo de la LOPD
[13] Artículo 13.1 del Reglamento de desarrollo de la LOPD
[14] Artículos 24 y 25 del Reglamento de desarrollo de la LOPD.

#### 4.2.2.1 Independencia

La normativa española dispone claramente que "*los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro*".

De este modo, lo que se manifiesta es que cualquier derecho puede ejercitarse sin necesidad de ejercitar previamente el derecho de acceso, cada derecho es independiente el uno del otro, de ahí que pueda instarse la rectificación de sus datos personales sin necesidad de, ejercitar previamente el derecho de acceso.

*Ej: en los supuestos en los que el responsable del fichero informe periódicamente al afectado de los datos sometidos a tratamiento, bien como consecuencia de la facturación periódica de un servicio (telefonía), y es en la factura donde se observa el error, el afectado podrá requerir que se rectifique, sin necesidad de ejercitar previamente el derecho de acceso.*

#### 4.2.2.2 Gratuidad

Continua la normativa señalando que "*deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición*", consagrando así las dos características que, junto con la independencia o autonomía, configuran el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

En cuanto a la gratuidad en el ejercicio de los derechos, dicho principio no aparece expresamente reconocido en las normas internacionales o comunitarias de las que trae causa en última instancia, la legislación española en la materia.

Así, el artículo 8 del Convenio 108 únicamente prevé que el ejercicio por el afectado de su derecho de acceso se deberá efectuar "sin demoras ni gastos excesivos", aclarando el apartado 53 de su memoria explicativa que la expresión "gastos" se refiere al coste del ejercicio para el afectado, no al conste real que la operación pueda implicar para el responsable. Esta fórmula se reproduce prácticamente por el artículo 12 a) de la Directiva 95/46/CE, que se refiere a esta cuestión únicamente en relación con el derecho de acceso, que deberá poder ejercitarse "libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos".

Sin embargo la Ley Orgánica de Protección de Datos fue clara al respecto señalando en el artículo 17.2, que "no se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación".

#### 4.2.2.3. Sencillez

Como ya se ha indicado, se impone que el medio que el responsable del fichero deberá poner a disposición del interesado para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, además de gratuito, sea sencillo.

Que el procedimiento sea sencillo, significa que no suponga un esfuerzo extraordinario poder ejercitarlo. Además el responsable del fichero deberá de asignar cauces para el ejercicio de los derechos.

De este modo, no puede ser similar el nivel de exigencia en los supuestos de ejercicio de los derechos ante grandes compañías prestadoras de servicios a un número sumamente grande de afectados o ante entidades cuya principal actividad consiste, precisamente, en el tratamiento de datos (por ejemplo, las responsables de ficheros de solvencia patrimonial y crédito o las dedicadas a actividades de publicidad y prospección comercial) que cuando el derecho se ejerce ante pequeñas empresas. En el primer supuesto, es probable que el número anual de solicitudes de acceso, rectificación, cancelación u oposición sea de varios millares; en el segundo, las solicitudes podrán ser meramente esporádicas y excepcionales.

Del mismo modo, en el primero de los supuestos enunciados es probable que la propia estructura organizativa del responsable del fichero incorpore un área concreta destinada a la tramitación de los procedimientos vinculados al ejercicio de los derechos o incluso mantenga una parcela específica de la organización que vele por el cumplimiento de la normativa de protección de datos. Por el contrario, en las pequeñas y medianas empresas no relacionadas directamente con el tratamiento de datos personales la organización será mucho más reducida y no existirán recursos humanos dedicados a la garantía del cumplimiento de esta legislación.

Incluso se ha llegado a preveer que en los supuestos en que el responsable del fichero o tratamiento dispongan de servicios de atención al público, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la

identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

No obstante la existencia de estos procedimientos, no impide que el afectado pueda ejercitar los derechos por cualquier otro medio, siempre que éste permita acreditar el envío y la recepción de la solicitud y ésta contenga todos los elementos necesarios, debiendo en estos casos el responsable del fichero o tratamiento atender la solicitud.

De lo expuesto podemos concluir que no será posible que el responsable pueda ampararse en motivos de orden burocrático, tales como la no utilización del canal puesto a disposición del ciudadano para el ejercicio de sus derechos, para proceder a una denegación de los mismos.

Si bien la única exigencia será que la solicitud efectuada por el interesado cumpla con los requisitos que impone la propia normativa, pudiendo acordarse la subsanación de no cumplirse tales exigencias.

### 4.2.3 Reglas de ejercicio

#### 4.2.3.1. Solicitud del interesado y su subsanación

El artículo 25.1 RDLOPD establece los requisitos que debería cumplir la solicitud de ejercicio planteada por el afectado, disponiendo lo siguiente:

*"Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:*

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

*El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.*

*b) Petición en que se concreta la solicitud.*

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

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

El problema se plantea, en los supuestos en los que el responsable del fichero ante el que se ejercitan los derechos manifieste no haber recibido la solicitud del interesado y éste afirme haberla realizado. En ese caso, el afectado deberá de aportar algún medio que permita acreditar la realización de la solicitud será necesaria para que una eventual solicitud de tutela de sus derechos ante la Autoridad de Protección de Datos pueda prosperar.

Una vez subsanada la solicitud puede entenderse que se inicia el plazo para resolver acerca de la solicitud formulada, pues hasta ese momento, el responsable no disponía de toda la información necesaria para poder atender adecuadamente a la solicitud. De este modo, sólo en el momento en que la solicitud reúne todos los requisitos legalmente establecidos para su formulación puede considerarse, en puridad, que comienza el plazo de que goza el responsable para resolver sobre la procedencia o improcedencia de lo solicitado.

#### 4.2.3.2 Decisión del responsable del fichero

Una obligación que se le impone al responsable del fichero o tratamiento, es que deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

El deber de respuesta al afectado operará incluso en los supuestos en que proceda la denegación del derecho. Así la Resolución de la Agencia Española de Protección de Datos (AEPD), de 25 de febrero de 2008 estima la tutela del derecho de acceso a ficheros de las fuerzas y cuerpos de seguridad formulada por un afectado, al considerar que, al margen de la cuestión de fondo, procederá contestar al afectado acerca de la solicitud formulada.

La AEPD ha sido especialmente exigente en el cumplimiento de este requisito formal, considerando procedente la estimación de las tutelas formuladas por falta de atención en plazo de los derechos de los afectados. Por último, en cuanto a la conservación por el responsable de la prueba acreditativa del cumplimiento de su deber de respuesta, se permite que utilice medios informáticos o telemáticos

pudiendo proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

#### 4.2.3.3 Ejercicio de los derechos ante un encargado del tratamiento

Como es sabido, junto con las figuras del responsable del fichero o del tratamiento, que deciden sobre la finalidad, contenido y uso del tratamiento, la LOPD se refiere a la del encargado del tratamiento, que define el artículo 5.1 i) del RDLOPD como "*la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio*", aclarando que "*podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados*".

La figura del encargado del tratamiento reviste una importancia creciente en materia de protección de datos, dado que en el marco en que nos encontramos es cada vez más frecuente la externalización de todo o parte de los servicios relacionados con el tratamiento de datos de carácter personal.

La regulación[15] de la figura del encargado del tratamiento es detallada y minuciosa y en ella se ha previsto que los afectados puedan ejercitar sus derechos ante el encargado del tratamiento, y éste debe ó dar traslado de la solicitud del responsable del fichero para que conteste, ó resolver directamente. Si bien, para que tenga lugar está última previsión será necesario que esta circunstancia se prevea en el contrato que regula la relación entre el responsable y encargado del tratamiento. Por este motivo, sería conveniente que en los contratos en que se acuerde la prestación de estos servicios se incluya protocolos que habiliten el traslado de las solicitudes al responsable con la debida celeridad.

[15] Artículo 12 de la Ley Orgánica 15/1999, y artículos, 20,21 y 22 del Reglamento.

### 4.2.4. Otras cuestiones relacionadas con el ejercicio de los derechos

#### 4.2.4.1 Límites al ejercicio de los derechos

Los Derechos Acceso, Rectificación, Cancelación y Oposición no son absolutos e ilimitados, sino que podrán modularse en determinados supuestos tales como la seguridad pública. Estas limitaciones traen causa de lo establecido con carácter general en el artículo 13 de la Directiva 95/46/CE, que permite a los Estados miembros excluir lo dispuesto en su artículo 12, referido a los derechos de acceso, rectificación, supresión y bloqueo *"cuando tal limitación constituya una medida necesaria para la salvaguardia de:*

a) *la seguridad del Estado;*

b) *la defensa;*

c) *la seguridad pública;*

d) *la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;*

e) *un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;*

f) *una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);*

g) *la protección del interesado o de los derechos y libertades de otras personas"*.

En desarrollo de la previsión comunitaria la propia LOPD establece en su artículo 2.2, reproducido por el artículo 4 del RDLOPD, determinadas exclusiones a su aplicación, haciendo especial referencia a los ficheros creados para la investigación del terrorismo y formas graves de delincuencia organizada. Al propio tiempo, la LOPD en su artículo 23 establece determinadas excepciones al ejercicio de los derechos, referidos a los ficheros de investigación policial y a los de inspección tributaria.

También existen otras normas con rango de Ley vienen a establecer determinadas restricciones al ejercicio del derecho de acceso, como son las normas reguladoras de

la prevención del blanqueo de capitales, a las que deberán añadirse las relacionadas con la prevención y bloqueo de la financiación del terrorismo o las relacionadas con la implantación de sistemas de videovigilancia, bien por las fuerzas y cuerpos de seguridad del Estado.

#### 4.2.4.2 Aplicación de normativa específica

No podemos olvidar que en determinados casos la rectificación o cancelación exija la interposición por parte del afectado de un recurso administrativo o jurisdiccional encaminado, precisamente, a determinar la efectiva exactitud del dato contenido en el fichero, sin que podamos utilizar los procedimientos previstos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Ejemplo; la cancelación de un asiento del Registro de la Propiedad no puede efectuarse a través del procedimiento previsto en la normativa de protección de datos de carácter personal sino que debe regirse por lo dispuesto en la normativa hipotecaria.

## 4.3 El derecho de acceso

### 4.3.1 Concepto, naturaleza y alcance de este derecho

El derecho de acceso se define como la posibilidad que "*el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos*".

Así, recuerda la Sentencia de la Audiencia Nacional de 14 de diciembre de 2006 que "*regula el art.15 de la LO 15/1999 el derecho denominado habeas data o habeas scriptum que consiste en que el afectado puede exigir al responsable del fichero una prestación de hacer consistente en la mera exhibición de sus datos y, en su caso, su rectificación o cancelación. Se trata de un derecho esencial en la materia que se encuentra recogido en el art.8.b) y c) del Convenio 108 del Consejo de Europa y 12 y 13 de la Directiva 95/46/CE. En relación con el tema que nos ocupa es interesante destacar que en relación con el art.8.b) del Convenio 108 la República Federal de Alemania hico una declaración consistente en afirmar que no era posible acceder a la petición de información «si el interesado no puede especificar adecuadamente su*

*petición». Por lo demás, es indiscutible que el derecho de acceso constituye núcleo esencial del derecho regulado en el art.18.4 de la Constitución (STC 292/2000)*".

De este modo, el derecho de acceso puede considerarse como la manifestación primigenia del derecho fundamental a la protección de datos, encontrándose regulado o jurisprudencialmente reconocido, bajo su denominación de derecho de "habeas data", incluso en aquellos ordenamientos en los que no existe una norma que de modo general y sistemático regule el derecho fundamental. Así sucede en la mayor parte de los Estados iberoamericanos, en los que no existiendo, salvo supuestos excepcionales, un derecho fundamental constitucionalmente reconocido a la protección de datos de carácter personal, si suele reconocerse en los textos constitucionales el derecho de ejercicio de la acción de habeas data, traducida en nuestro derecho como el ejercicio de los derechos de acceso, rectificación o cancelación. En este sentido, resulta interesante el análisis comparado efectuado en el Preámbulo del documento de Directrices para la Armonización de la regulación de protección de datos en la Comunidad Iberoamericana, aprobado por la Red Iberoamericana de Protección de Datos en el marco del V encuentro Iberoamericano de Protección de Datos, celebrado en Lisboa los días 8 y 9 de noviembre de 2007.

De este modo, el derecho de acceso aparece recogido expresamente en el último inciso del artículo 8.2 de la Carta de Derechos Fundamentales de la Unión Europea, según el cual "*toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación*".

No podemos olvidar que el derecho de acceso resulta correlativo del deber de informar al afectado, por cuanto se exige al responsable informar al afectado de "la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición", en el momento de la recogida de los datos personales.

El derecho de acceso permitirá al interesado conocer no sólo el hecho mismo del tratamiento, sino su extensión, en el sentido de conocer los datos tratados y las finalidades para las que se lleva a cabo el tratamiento, el origen de los datos y los cesionarios de los mismos.

Es conveniente destacar que el derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular al derecho de los ciudadanos al acceso de los archivos y registros públicos.

En efecto, el derecho de acceso, configurado por la Sentencia del Tribunal Constitucional 292/2000 como una de las facultades incluidas en el derecho fundamental a la protección de datos de carácter personal, resulta claramente diferenciado, incluso en su fundamento constitucional del derecho de acceso por los ciudadanos a los archivos y registros públicos. Así, mientras el primero de ellos forma parte integrante del derecho fundamental derivado del artículo 18.4 de la Constitución, el segundo trae causa del mandato impuesto a los poderes públicos por el artículo 105 b) de la propia Norma Suprema.

El alcance del derecho de acceso, permite al interesado obtener del responsable del tratamiento, información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento. Este alcance trae causa en la complementariedad existente entre el derecho de acceso y el derecho de los afectados a obtener información del Registro General de Protección de Datos acerca de los distintos ficheros inscritos en el mismo.

### 4.3.2 Procedimiento de ejercicio y otorgamiento del derecho

#### 4.3.2.1 La elección del modo de acceso

A la hora de elegir el modo de formalizarse el acceso se prevén determinados sistemas de consulta de fichero tales como;

a) Visualización en pantalla.

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

c) Telecopia.

d) Correo electrónico u otros sistemas de comunicaciones electrónicas.

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

Como puede observarse estas distintas alternativas van acorde con la evolución del estado de la técnica. De este modo, se pretende que la legislación de protección de datos mantenga el principio de neutralidad tecnológica, admitiendo la posible existencia de medios de respuesta no contenidos en la enumeración y que podrán ser puestos a disposición del afectado por el propio responsable del fichero.

Si bien la potestad decisoria relativa al modo de ejercitar el derecho de acceso recae sobre el propio interesado así lo ha reconocido la Audiencia Nacional en la Sentencia de 27 de octubre de 2006:

> *"La segunda razón de impugnación que invoca (…) es que no puede admitirse, como implícitamente sostiene la Agencia Española de Protección de Datos, que la legislación vigente reconozca a los interesados el derecho a solicitar a los responsables de los ficheros el acceso a sus datos por el medio que estimen oportuno, sino que muy al contrario faculta al responsable del fichero para poner en conocimiento del solicitante los datos personales obrantes en su base de datos a través de cualquiera de los medios previstos en el artículo 15 de la Ley Orgánica de Protección de Datos.*
>
> *Tampoco tiene aquí razón (…). Si releemos el art. 15, antes trascrito, comprobaremos que es el interesado que ejercita el derecho el que tiene la libertad de optar por el procedimiento que estime oportuno para recabar la información que le interesa. Precisamente el inciso 2 del precepto dice que la información podrá recabarse mediante...y recabar es obtener no facilitar. El que quiere obtener la información es el que puede optar (ese es el sentido del podrá de la norma), el que tiene libertad de elegir el medio para obtener la información (mediante dice el artículo)."*

Esta regla únicamente podrá exceptuarse en caso de que la configuración o implantación material del fichero o de la naturaleza del tratamiento impida atender el derecho del afectado a través del medio que él haya elegido libremente. En este caso, el responsable podrá poner a su disposición otro medio "*siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige*".

Así sucedería *por ejemplo en caso de que, dada la estructura del fichero, la visualización en pantalla de los datos del afectado que ejercita su derecho pudiera implicar el conocimiento por aquél de datos de terceros contenidos en el propio fichero. En ese caso será precisa una previa depuración de la información, de forma que el afectado sólo tenga acceso a sus propios datos, puesto que en caso contrario el ejercicio del derecho de acceso podría implicar una cesión al afectado de datos de terceros, resultando esa cesión contraria a lo exigido por la LOPD.*

Al tramitar la solicitud del ejercicio del derecho de acceso, el responsable deberá de cumplir con las medidas de seguridad a implantar sobre los ficheros de datos de carácter personal.

Ahora bien, es posible que el afectado, sobre el que, como se ha indicado recae el poder de decidir el medio a emplear para facilitar el acceso no acepte el medio propuesto por el responsable del fichero y opte por un procedimiento en que pueda existir un mayor riesgo para la seguridad.

Así, por ejemplo, en caso de que un centro sanitario ofreciese al interesado la posibilidad de remitirle la información contenida en su historia clínica a través de correo electrónico cifrado y él insistiese en que le fuera remitida por correo ordinario, el afectado no podrá exigir ningún tipo de responsabilidad al centro sanitario por el hecho de que durante el envío de la información se hubiera producido su pérdida o alteración o hubiera tenido lugar un acceso no autorizado a la misma.

Junto al poder decisorio del afectado que se le permite optar por un u otro medio de acceso, va ligado a que la elección de dicho medio no genere un quebranto económico al responsable, cuando con la elección de otro medio de menor coste, se materializa el acceso con las mismas medidas de seguridad. En estos casos si el afectado opta por este tipo de medios, el mayor gasto económico que genere al responsable del fichero, deberá satisfacerlo el afectado. En consecuencia, el poder de decisión no se traslada al responsable, que deberá limitarse a ofrecer ese medio alternativo, debiendo atender la solicitud por el medio elegido por el afectado, que habrá de satisfacer los gastos necesarios para ello.

#### 4.3.2.2 Otorgamiento del acceso

El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes[16] a contar desde la recepción de la solicitud. Puede darse el caso que la solicitud fuera estimada y el responsable no acompañase a su comunicación la información que se hará efectivo durante los diez días siguientes a dicha comunicación.

[16] El plazo de un mes es en la normativa española, artículo 29 del Reglamento

Es de obligado cumplimiento para el responsable responder la solicitud del afectado en el plazo señalado, aunque no dispongan de datos de carácter personal de los afectados.

El mero transcurso del plazo de un mes sin que el responsable del fichero conteste la solicitud formulada por el afectado hará nacer el derecho de éste a recabar la tutela de la Autoridad de Protección de datos, que, en caso de contestación tardía, amparará al afectado, estimando la tutela por motivos formales.

Por otra parte, el responsable del fichero deberá garantizar que la información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

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

#### 4.3.2.3. Causas de denegación del derecho de acceso

Existen determinados supuestos en que pueda denegarse el derecho de acceso, lo que constituye una restricción al ejercicio de una facultad propia de un derecho fundamental, por lo que la restricción debe fundamentarse en una Ley.

Así, son tres las posibles causas de denegación del derecho de acceso:

- El ejercicio reiterado del mismo en un plazo de doce meses sin justa causa, La existencia de una prohibición legal expresa en una norma interna o comunitaria.
- La existencia de una prohibición legal expresa de informar al afectado acerca del tratamiento de los datos, contenida igualmente en una norma legal o comunitaria.

En cuanto a la limitación temporal, la misma trae causa de lo dispuesto en el artículo

12a) de la Directiva 95/46/CE que prevé expresamente que el derecho de acceso reconocido al afectado podrá ejercitarse con una "periodicidad razonable".No obstante, como es lógico, en caso de que existan nuevas circunstancias que fundamenten la concurrencia de una justa causa o un interés legítimo en el afectado que justifique el ejercicio del derecho, el responsable no podrá en ningún caso denegar aquél al amparo de su ejercicio reiterado, prevaleciendo la garantía del derecho fundamental a la protección de datos.

Al limitar al afectado su ejercicio de derecho de acceso, el responsable del fichero deberá de informar al afectado de su derecho a recabar la tutela de la Autoridad de protección de datos.

## 4.4 Los derechos de rectificación y cancelación

### 4.4.1 Concepto, alcance y naturaleza

Los apartados b) y c) del artículo 12 de la Directiva 95/46/CE reconocen al afectado los derechos a obtener, la rectificación y cancelación de sus datos personales. Del mismo modo, el artículo 8 de la Carta de derechos Fundamentales de la Unión Europea reconoce el derecho del afectado a lograr la rectificación de los datos sometidos a tratamiento en su apartado 2.

Por eso serán rectificados o cancelados, los datos de carácter personal, cuando tales datos resulten inexactos o incompletos. Surgen así los derechos de rectificación y cancelación, como corolario a los principios de protección de datos, consagrados por el artículo 6 de la Directiva 95/49/CE .De este modo, si el tratamiento no se ajustase a esos principios, el responsable del fichero, que se encuentra obligado en todo caso a rectificar o cancelar los datos de oficio, podrá ser requerido por el afectado a que se produzca la rectificación o cancelación, subsanando así la vulneración de las normas de protección de datos y, en consecuencia, del derecho fundamental del afectado, derivadas del hecho de haberse incumplido los principios de calidad, y exactitud de los datos.

### 4.4.2 Procedimiento de ejercicio de los derechos

El procedimiento para el ejercicio de estos derechos, es semejante al procedimiento previsto para el ejercicio del derecho de acceso, si bien las diferencias son pocas y especialmente derivadas de la propia naturaleza de los derechos.

Por ello en a solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado". Por su parte, "en la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso".

En el derecho de rectificación, la necesidad de que la solicitud concrete la corrección que debe realizarse se fundamenta en que, el responsable del fichero parece legitimado para tratar el dato personal al que el derecho se refiere que, no obstante, no resulta acorde con la realidad. Por este motivo, el afectado debería indicar al responsable cuál es el dato que ha de ser rectificado y en qué modo el dato debe serlo, dado que el responsable puede desconocer esta circunstancia.

El fundamento del ejercicio del derecho de cancelación puede resultar más complejo en este punto. En efecto, nos encontramos ante una pluralidad de supuestos en que el dato tratado puede ser desde completamente irreal, debiendo suprimirse por una vulneración radical del principio de inexactitud, hasta inadecuado o excesivo para la finalidad que justifica el tratamiento. También es posible que la inadecuación del tratamiento sea sobrevenida, por haberse extinguido la finalidad que justificaba ese tratamiento, por ejemplo, por desaparecer la relación jurídica entre el responsable y el afectado que justificaba el tratamiento.

Así no cabe duda que el afectado deberá acreditar que el dato tratado es simplemente falso, mientras que en los otros supuestos que acaban de indicarse podrá ser suficiente la motivación del carácter excesivo del datos, del uso para una finalidad no admitida o incompatible con la que justificó su recogida o del mantenimiento en el tratamiento una vez cumplida plenamente la finalidad que lo justificó.

Por último en cuanto al plazo del que dispone el responsable para atender la solicitud es de diez días, en el ámbito español, debiendo de contestar tenga o no tenga datos del afectado. La brevedad del plazo deriva de la propia esencia de los derechos, pues

si están tratando datos de manera incorrecta o que deben de cancelarse lo lógico es que ese error se corrija cuanto antes, de ahí el plazo de diez días.

### 4.4.3 Efectos del otorgamiento

El artículo 12de la Directiva menciona las consecuencias del ejercicio de estos derechos "la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente directiva, en particular a causa del carácter incompleto o inexacto de los datos."

Así, la cancelación en el ámbito español[17] dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Por otra parte debe tenerse en cuenta que si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, para que también proceda a la rectificación ó cancelación. Pues de no garantizase la comunicación de la rectificación o cancelación por parte del responsable a los distintos cesionarios, podría darse el supuesto que el afectado tuviese que ir ejercitando sus derechos ante distintos responsables.

En cuanto al bloqueo de datos ha de ser considerado como la reserva de los datos necesaria para atender, en su caso, a las posibles responsabilidades derivadas del tratamiento o de la relación subyacente al mismo. Parece lógico la autoridad judicial o administrativa, que conozca cualquier contienda derivada del uso de los datos, pueda acceder al dato previamente sometido a tratamiento, de forma que pueda valorarse efectivamente las posibles responsabilidades exigidas por el afectado o por la propia autoridad judicial o administrativa.

*Así, por ejemplo, y ciñéndonos estrictamente a la normativa de protección de datos, debe ser posible a la Autoridad de Protección de Datos, ante una denuncia del afectado poder conocer durante cuánto tiempo y hasta qué momento el dato fue*

[17] Artículo 16.3 de la Ley Orgánica 15/1999.

*indebidamente tratado, a fin de en su caso exigir las responsabilidades derivadas de la vulneración de la legislación en la materia.*

### 4.4.4. Denegación del derecho

Existen también supuestos en los que podrán denegarse los derechos de rectificación y cancelación instados por el afectado.

Además de cuando lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

Es destacable que se denegará el acceso cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

Efectivamente, si el responsable puede proceder al tratamiento de los datos cuando así lo prevea una norma con rango de Ley o cuando sean necesario para el mantenimiento o cumplimiento de la relación jurídica que le vincula con el afectado y ha sido libremente aceptada por éste, no cabrá considerar sin más que pueda procederse a la cancelación de los datos solicitada por el afectado en tanto persistan esa obligación legal o la relación jurídica citada.

*Ejemplo puede resultar clarificador, el deudor de un banco, si solicita la cancelación de sus datos, el banco no podrá atenderla, pues al mantenerse la deuda viva, deberá seguir tratando sus datos, sólo podrá cancelarlos cuando la deuda haya sido debidamente satisfecha.*

Obviamente, el alcance de esta regla no puede ser considerado como absoluto; es decir, operará en tanto el dato sea exacto o en tanto el mismo no exceda de la finalidad (la relación jurídica o el deber legal) que justifica el tratamiento. En caso contrario, sí debería procederse a la cancelación del dato, permaneciendo el mismo bloqueado en los términos a los que nos hemos referido con anterioridad.

## 4.5 El derecho de oposición

### 4.5.1 Introducción y concepto

En la Directiva Comunitaria el Derecho de Oposición aparece regulado en los artículos 14 y 15 donde se recogen una pluralidad de supuestos. Estos supuestos tradicionalmente se han dividido en tres categorías, el derecho de oposición en sentido estricto, el derecho de oposición en los tratamientos relacionados con actividades de publicidad y prospección comercial y el derecho de oposición a las decisiones individuales automatizadas.

La doctrina recuerda que "el derecho de oposición ha sido definido como el derecho del interesado a negarse, por motivos legítimos, a que sus datos personales sean objeto de tratamiento". Ahondando en este concepto, se puede definir, como el derecho del afectado "a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo".

La primera consecuencia del derecho de oposición operará en los supuestos en los que el tratamiento de datos llevado a cabo por el responsable ante el que dicho derecho se ejercita es plenamente lícito conforme a las normas reguladoras del derecho fundamental a la protección de datos de carácter personal.

En la actualidad el derecho de oposición en sentido estricto se está demandando en relación con la oposición al tratamiento de la información personal a través de los motores de búsqueda en Internet, al ser una cuestión especialmente relevante, se va a tratar en otra parte del programa, por lo que no nos referiremos a ella, lo mismo ocurre con el derecho de oposición en los tratamientos automatizados con actividades de publicidad y prospección comercial, que se desarrollará en otra parte del programa.

A continuación analizaremos brevemente el derecho de oposición a las decisiones basadas únicamente en tratamientos automatizados, que se encuentra regulado en el artículo 15 de la Directiva Comunitaria. En el ámbito español[18] aparece bajo la rúbrica "impugnación de valoraciones".

La esencia de esta modalidad deriva que los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de

[18] Artículo 13 de la Ley Orgánica 15/1999

manera significativa, que se base únicamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito.

Por tanto se permite al afectado *impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento,* cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Respecto, a la impugnación, ésta deberá verificarse por los cauces que el ordenamiento tenga establecido para el acto resultante de la valoración. De este modo, si la decisión automatizada diera, por ejemplo, lugar a la adopción de un acto administrativo de gravamen para el afectado, aquél podrá invocar su nulidad a través de los recursos establecidos por las leyes administrativas, por haber sido vulnerado el derecho a las decisiones automatizadas.

Del mismo modo, si la valoración diera lugar a la resolución de un contrato o a su no celebración, el interesado podrá adoptar las acciones previstas en derecho para impugnar tal valoración o la decisión materialmente adoptada con conculcación de su derecho fundamental o para exigir las responsabilidades a que hubiera lugar como consecuencia de la adopción de esa decisión.

### 4.5.2 Excepciones

No obstante este derecho tampoco es absoluto e ilimitado, la propia Directiva reconoce la existencia de excepciones. La primera de las excepciones se refiere a los supuestos en que la decisión "se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado".

Para ello, será necesario además que concurran tres requisitos adicionales:

- Que se otorgue al afectado la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés.

- Que el responsable del fichero haya informado previamente al afectado, de forma clara y precisa, de que se adoptará este tipo de decisiones.

- Que el responsable procederá en todo caso a la cancelación de los datos en caso de que no llegue a celebrarse finalmente el contrato.

El primero de los requisitos exigidos viene a compensar el carácter automatizado y sin intervención humana de la decisión adoptada. En efecto, si aún siendo automática la decisión se otorga al afectado una suerte de "trámite de audiencia" en el que pueda alegar lo que estime adecuado en defensa de su derecho o interés, la decisión exigirá una intervención humana valorativa de las alegaciones efectuadas por el interesado, de forma que se evita el mero automatismo derivado de la mecánica adoptada en ese caso. De este modo, se reemplaza la exigencia de una necesaria intervención humana por una potencial intervención a instancia del afectado.

En segundo lugar, se exceptúa la adopción de este tipo de decisiones cuando las mismas estén autorizadas "por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado". La referencia a la Ley ha de entenderse igualmente efectuada a las normas de derecho comunitario que permitan la adopción de las valoraciones.

En todo caso, la norma habilitante deberá establecer medidas de garantía del derecho del afectado, como podrían ser nuevamente en el ámbito de la Administración Pública, las vinculadas a la posibilidad de revisión del acto adoptado en virtud de la valoración automatizada llevada a cabo.

### 4.5.3 Procedimiento para el ejercicio del derecho

No existen grandes especialidades relacionada con el ejercicio del derecho de oposición a las decisiones automatizadas, por lo que deberá estarse a las normas generales que hemos ido mencionando a lo largo del capítulo. En todo caso, el responsable deberá atender la oposición del afectado en el plazo más breve posible, en España[19] de diez días desde su solicitud y, en caso de estimarse, deberá cesar en el tratamiento de los datos vinculados a la valoración y decisión adoptadas.

[19] Artículo 35 del Reglamento de desarrollo de la LOPD

## BIBLIOGRAFIA

WARREN SAMUEL D. Y BRANDEIS LOUIS. «The right to privacy», *Harvard Law Rewiew*, vol. IV, núm. 5, 15-XII-1890. Existe traducción española: WARREN SAMUEL D. Y BRANDEIS LOUIS. *El derecho a la intimidad*. (Benigno Pendas y Pilar Baselga ed.). Civitas, Madrid, 1995.

## OTROS DOCUMENTOS

- «Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal»

http://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf.

- Guía del responsable de ficheros

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

- Dictamen 4/2007 sobre el concepto de datos personales

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_es.pdf

## RECURSOS

- Legislación:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/index-ides-idphp.php

- Jurisprudencia:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/index-ides-idphp.php