EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, 1ª EDICIÓN

MÓDULO 2.
PRINCIPIOS BÁSICOS DE LA PROTECCIÓN DE DATOS

Coordinador: José López Calvo

Autores: José López Calvo
Manuel García Prieto
Isabel Navarro Alonso
Angelina Lobato Lobato

Con la colaboración de:

ÍNDICE

Introducción y Objetivos

1. El equilibrio entre el derecho de protección de datos y otros derechos. Su contorno en los diferentes ámbitos. En concreto, libertad sindical, Internet, medios de comunicación, procesos de concurrencia pública. Supuestos reales.
- 1.1 Protección de datos versus libertad sindical
- 1.2 Protección de datos versus libertad de información
- 1.3 Protección de datos versus Transparencia Administrativa
- 1.4 Protección de Datos versus Servicios de la sociedad de la información
  - 1.4.1 Divulgación de datos no protegidos por deber de secreto
  - 1.4.2 Divulgación de datos sometidos a deber de secreto
  - 1.4.3 Buscadores
  - 1.4.4 Privacidad en las comunicaciones electrónicas
  - 1.4.5 Redes sociales (web 2.0)

2. Legitimación para el tratamiento: información y consentimiento.
- 2.1 El consentimiento
- 2.2 Excepciones a la regla del consentimiento
- 2.3 El consentimiento para el tratamiento de datos especialmente protegidos
- 2.4 Las relaciones con terceros
  - 2.4.1 Comunicaciones de datos personales
  - 2.4.2 El acceso a datos por cuenta de terceros

3. El principio de calidad de los datos: proporcionalidad, veracidad y finalidad. Cancelación, bloqueo y rectificación de oficio por el responsable.
- 3.1 Introducción
- 3.2 Proporcionalidad de los datos
  - 3.2.1 Datos adecuados, pertinentes y no excesivos
  - 3.2.2 Utilización de medios menos invasivos
- 3.3 Veracidad de los datos. Contenido del principio
  - 3.3.1 Supuestos que vulneran el principio de veracidad
- 3.4 Finalidad de los datos
  - 3.4.1 Finalidades determinadas, explícitas y legítimas
  - 3.4.2 Desvío de finalidad
  - 3.4.3 Deber de informar
- 3.5 Cancelación, bloqueo y rectificación de oficio por el responsable
  - 3.5.1 Cancelación de oficio y bloqueo de los datos
  - 3.5.2 Rectificación de oficio

4. La Tutela del Derecho fundamental a la protección de datos
- 4.1 Tutela de Derechos
  - 4.1.1 El ejercicio de estos derechos
    - 4.1.1.1 Ejercicio derecho de acceso
    - 4.1.1.2 Ejercicio derecho de rectificación
    - 4.1.1.3 Ejercicio del derecho de cancelación
    - 4.1.1.4 Ejercicio del derecho de oposición
  - 4.1.2 El procedimiento de tutela de derechos
    Gráfico 1

Gráfico 2
4.2 Inspección
4.2.1 Los poderes de inspección del cumplimiento de la normativa de protección de datos
4.2.1.1 La actuación de inspección "preventiva"
4.2.1.2 La actuación de inspección reactiva ante posibles infracciones
4.2.2 El procedimiento sancionador en materia de protección de datos
Gráfico 3
4.3 Tutela jurisdiccional

Bibliografía

INTRODUCCIÓN Y OBJETIVOS

Objetivos

En el presente módulo se analizan elementos esenciales referentes a protección de datos. Entre ellos se encuentra su carácter no absoluto. Se trata de un derecho que entra en conflicto con otros concurrentes y que requiere para su resolución un ejercicio de ponderación acerca de cual debe prevalecer en cada caso.

Junto a ello se desarrollan tres aspectos básicos del sistema: la legitimación para el tratamiento, que queda supeditada para los casos en que una ley no lo prevea por razones de interés general al previo consentimiento informado por parte del afectado. Junto a ello el principio de calidad (los datos deben ser adecuados y pertinentes) se configura como otra piedra angular del sistema y por último, los supuestos en que la comunicación y acceso por terceros es procedente.

Finalmente el sistema de protección de la privacidad no sería completo si no se establecieran instrumentos para sancionar o reparar los comportamientos en que se produce una infracción al derecho fundamental, circunstancia que también se analiza en el presente módulo haciendo referencia a los mecanismos disponibles: tutela o procedimiento sancionador.

1. EL EQUILIBRIO ENTRE EL DERECHO DE PROTECCIÓN DE DATOS Y OTROS DERECHOS. Su contorno en los diferentes ámbitos. En concreto, libertad sindical, internet, medios de comunicación, procesos de concurrencia pública. Supuestos reales.

El derecho a la protección de Datos reconoce el poder que cada persona debe tener de controlar la información que, sobre si mismo, una tercera parte puede tener, usar, almacenar o tratar. Refuerza el derecho de autodeterminar la información sobre uno mismo que se emite y desperdiga.

Esa es la razón por la que el "consentimiento personal" se erige como el pilar principal que condiciona todo tratamiento de datos. Datos como cuenta corriente, imagen, número de teléfono, dirección, IP, orientación sexual, tendencia política, creencia religiosa o e-mail son datos protegidos que se ubican en la esfera de privacidad personal cuya revelación debe estar precedida por el previo consentimiento de la persona afectada.

Sin embargo, como todo derecho, el derecho de privacidad entra en conflicto en ocasiones con otros derechos o bienes jurídicos concurrentes debiéndose en tal caso realizar una ponderación.

En ocasiones una ley prevé en beneficio público el uso de datos sin consentimiento. Los ejemplos son variados:

- para posibilitar la necesaria garantía de transparencia pública el legislador ha contemplado la obligada publicación en el diario Oficial de la obtención de una subvención pública o de un puesto de empleado público

- para el correcto funcionamiento institucional ha previsto la obligación de los colegiados de aportar datos a los colegios profesionales.

- El deber de ejercitar responsablemente la patria potestad prevalece sobre una eventual reivindicación de un menor para no comunicar a sus padres las calificaciones académicas

- para permitir al empleador ejercitar el derecho de vigilar la actividad del empleado puede tratar datos de sus empleados sin que, en el supuesto de que no se utilicen métodos desproporcionados, se pueda invocar por el trabajador su derecho a la privacidad. Esta previsión acarrea varias consecuencias:

- tras haberles informado previamente, podrán acceder y controlar el uso de su correo electrónico corporativo o sus accesos en Internet, podrá visualizarles por videocámara, implantar un sistema de control por huella digital o conocer su ubicación mediante sistemas de geolocalización.

- el servicio médico de la empresa podrá realizar controles de absentismo laboral sin consentimiento previo.

Si bien el empleador no tiene porque conocer datos de salud del empleado como excepción podrá conocer los datos de salud referentes a seguridad y prevención laboral que deben ser conocidos al afectar al correcto desempeño del puesto.

El legislador en estos casos ha decidido hacer prevalecer intereses generales u otros particulares que considera prevalentes sobre el poder de decisión que dispone cada persona sobre su propia privacidad soslayando el condicionamiento del consentimiento previo para tratar los datos.

Incluso el propio legislador puede decidir adoptar excepciones generales en la propia normativa de protección de datos como ha ocurrido en la ley española:

- considera de libre disposición los datos incluidos en determinadas fuentes como la prensa y las guías telefónicas.

- ha evitado someter al consentimiento el uso de datos en el marco de una relación negocial, laboral o administrativa. Como es lógico, la integración voluntaria en una relación jurídica limita la autodeterminación. Con efectos inherentes como que nadie puede oponer la privacidad como argumento para evitar la entrada de su jefe en el despacho o que la existencia de una relación con un abogado convierte en innecesario recabar el consentimiento de los clientes para el trato de sus datos.

Con ello no hace sino evidenciar que el derecho de protección de datos no es un derecho absoluto, trazar los perfiles que definen su espacio y los supuestos en que la privacidad cede frente a un interés prevalente

El legislador, consciente de que la sociedad no puede sostenerse sobre la construcción de infinidad de inaccesibles e incondicionales castillos de privacidad que rodeen a cada persona analiza en que supuestos debe ceder los datos y deben hacerse accesibles y a quien.

Pero también es posible que, sin intermediación de la ley o sin que la ley prevea una respuesta específica se produzca un conflicto del derecho de protección de datos con otro derecho que es necesario resolver.

Son múltiples los supuestos en los que el derecho de protección de datos cede o se concilia con otros bienes jurídicos protegidos actuando ambos derechos como contrapesos a eventuales extralimitaciones en un conflicto que es necesario ponderar en cada caso. El Organismo competente y los tribunales en su control posterior deben realizar una reflexión sobre el balance de derechos en los casos que se les presenta y a través de sus resoluciones delimitar los perfiles de los principios de protección de datos, resolviendo situaciones no siempre previstas explícitamente por el legislador Son varios los casos en los que la realidad plantea supuestos de conflictos que deben ser resueltos equilibradamente.

Sobre la principal catalogación de conflictos planteados y la justificación de la respuesta otorgada por la jurisprudencia y la Agencia Española de Protección de Datos se plantea el presente epígrafe.

Recuerde: El derecho de protección de datos no es absoluto. Su prevalencia o cesión deber ir precedido de un ejercicio de ponderación con otros derechos concurrente.

1.1 Protección de datos versus libertad sindical

De nuevo debe partirse de la consideración general de que los derechos fundamentales no son ilimitados, sino que, por el contrario, encuentran sus límites en los demás derechos fundamentales y bienes constitucionalmente protegidos

Incluye la actividad sindical el derecho a mantener informados a los miembros del sindicato en la empresa en todas las cuestiones que incidan de forma "directa o indirecta" o que puedan tener repercusión en las relaciones laborales. Esa transmisión de noticias de interés sindical, ese flujo de información entre el Sindicato y sus afiliados, entre los delegados sindicales y los trabajadores, según el Tribunal Constitucional "es el fundamento de la participación, permite el ejercicio cabal de una acción sindical, propicia el desarrollo de la democracia y del pluralismo sindical y, en definitiva, constituye un elemento esencial del derecho fundamental a la libertad sindical".

En consecuencia, el ejercicio de tales derechos puede mermar la protección de los datos de las personas afectadas. Tal conflicto se ha planteado en algunos casos resolviéndose de la forma que se ese expone a continuación:

- El ejercicio de la libertad sindical incluye el suministro por el empresario a los sindicatos de los correos corporativos de los empleados de una empresa para la realización de comunicaciones de forma ágil

- los sindicatos podrán remitir comunicaciones electrónicas de índole sindical a aquellos trabajadores que no se opongan manifestando su deseo de no recibirlas. Tal oposición no se podrá realizar en el periodo de elecciones sindicales en que el trabajador no podrá negarse.

- el derecho a la protección de los datos impide que los datos personales de un denunciante --nombre y apellidos-- se incluyan en una página de la Intranet corporativa de una empresa sin que medie su consentimiento inequívoco. No obstante, una nota informativa difundida por la Sección sindical del centro de trabajo, y en la que constan los datos de un denunciante, puede tener por finalidad la transmisión de noticias de interés sindical.

Carece de sentido –según manifiesta la Audiencia Nacional- informar sobre una querella criminal relativa a unos hechos surgidos con motivo de la actividad sindical, en el seno del propio sindicato, si no puede señalarse la persona contra la que se dirige para que los miembros del sindicato en la empresa puedan estar informados, conozcan y valoren, con todos.

Tal habilitación, no obstante, debe reconsiderarse en el caso de que se refiera a un trabajador sin responsabilidades sindicales. En tal caso, la información sindical se puede satisfacer habitualmente sin necesidad de identificar al trabajador.

- Otro de los elementos que confluye en la ponderación de los intereses es el ámbito de la difusión de la información contenida en la nota informativa que contenga datos. Es necesario tratar de manera diferente los supuestos de difusión que se han limitado estrictamente al ámbito de la empresa o centro de trabajo, en la página Intranet Corporativa, cuya difusión se limita a los trabajadores de dicha entidad financiera.

- El correcto desarrollo de la labor sindical permitirá el inicio de una campaña implicando a directivos de una empresa suministrando su e mail o móvil oficial. Sus funciones sindicales no le habilitarían para dar los datos particulares del directivo o directivos.

Recuerde: El derecho a la libertad sindical ha de prevalecer sobre el derecho a la protección de los datos personales cuando la acción sindical ampara la actuación del sindicato recurrente para divulgar entre los trabajadores de los centros los datos precisos, y únicamente necesarios, para el entendimiento de la noticia, teniendo un conocimiento cierto de la información relevante desde el punto de vista sindical.

1.2 Protección de datos versus libertad de información

La libertad de expresión otorgada a los medios de comunicación en el artículo 20 de la Constitución Española suele prevalecer en el supuesto de un eventual conflicto con el derecho a la privacidad invocado por personajes públicos esgrimiendo la protección de sus datos personales.

El art. 9 de la Directiva 95/46 bajo la rúbrica *"Tratamiento de datos personales y libertad de expresión",* dispone que*:*

"en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión".

En relación con esa cuestión, si bien la legislación española no contiene ninguna previsión específica encuentra una especialidad en la propia Constitución que en su art. 20 establece las garantías propias del derecho a la libertad de expresión reconociendo su prevalencia si se cumplen determinados requisitos.

La prevalencia de la libertad de información –señala nuestro Tribunal Constitucional- sobre los otros derechos de la personalidad constitucionalmente protegidos entre los que se encuentra el de protección de datos "alcanza el máximo nivel cuando la libertad es ejercida por profesionales de la información a través del vehículo institucionalizado de formación pública que es la prensa, entendida en su más amplia acepción (STC 29/2009 de 26 de enero)

El uso de datos personales en las noticias publicadas debe cumplir tres requisitos:

- ser un "hecho noticiable"

- ser veraz

- sea necesaria la publicación de los datos. Precisamente este tercer elemento ha dado lugar a varios resoluciones sancionadoras ratificadas por los tribunales:

· la STS 18 de febrero de 1999 estimó que si bien era un tema que interesaba a la opinión pública que dos internos de la prisión de Las Palmas que trabajaban en la cocina padecían sida no era necesario, puesto que no era noticiable, divulgar su identidad.

· el auto del Tribunal constitucional 155/2009 de 18 de mayo inadmitió a trámite un recurso de amparo contra una sanción administrativa de la AEPD impuesta por la publicación, sin su consentimiento, de los nombres y apellidos de los médicos y de los farmacéuticos que habían participado en una encuesta sobre uso y abuso de antibióticos. La prevalencia del derecho de comunicación a comunicar libremente información veraz sobre el de protección de datos dice el TC "resultaría de las circunstancias concretas de cada caso" para concluir que "el objetivo legítimo de informar podía haberse logrado por otros medios sin la referida invasión en la esfera personal de médicos y farmacéuticos".

En definitiva, las dos noticias serían igualmente creíbles sin la inclusión de los citados datos personales.

Mención aparte merece la eventual participación de un organismo administrativo como la Agencia Española de Protección de Datos –dada la premisa citada de la prevalencia de la libertad de información- sobre la relevancia o no de una noticia publicada en un medio y de la eventual prevalencia del derecho a la protección de datos del afectado. Debiendo destacarse el riesgo que supone una intromisión indebida por parte de la Administración en el contenido de las publicaciones de prensa, con peligros de censura administrativa, razón por la que debe rehuirse la realización de un ejercicio de ponderación que corresponde, en su caso, a los tribunales.

Cuestión diferente supone la obligación de los responsables del fichero –las fuentes de información- a someterse al secreto profesional. El dilema es ¿si se

conoce una conducta irregular en el ejercicio del puesto de trabajo en el que está sometido a secreto debe silenciarse? ¿y si se trata de una conducta que sin ser aparentemente irregular reviste trascendencia pública?

La persona vinculada por el secreto profesional no puede acercar al general conocimiento información y datos conocidos como consecuencia de su profesión. No obstante, de la experiencia de los conflictos planteados se deduce la concurrencia de elementos que deben tenerse en cuenta:

- la relevancia pública de la persona y del hecho noticiable

- el suministro de la información no por iniciativa propia sino en el contexto de una polémica pública que pudiera requerir clarificación o realizada a petición de parte (rueda de prensa, interpelación parlamentaria…)

- la necesidad de suministrar tales datos personales por resultar relevante para configurar la opinión pública o por referirse a conductas indebidas.

Recuerde: El derecho a la privacidad y el derecho de la sociedad a ser informada tiene su punto de encuentro en la prevalencia de la libertad de expresión ejercida por los medios de comunicación social sobre protección de datos.

1.3 Protección de datos versus transparencia administrativa

Los principios de transparencia y publicidad son esenciales para el correcto desarrollo de los procesos de concurrencia de los que derive el reconocimiento de derechos financiados con dinero público como plazas en colegios, ayudas, etc…

No obstante, la divulgación de la identidad y posibles datos adicionales de los beneficiarios –o de aquellos que superan trámites intermedios como exámenes- supone, como es obvio, una limitación de su privacidad trasladándose la información a la esfera pública.

Es necesario, por ello, hacer un análisis sobre la forma ideal de conciliar ambos derechos

Tal conflicto se ha manifestado, por ejemplo, en el caso de la concesión de plazas en colegios financiados con dinero público. Para la concesión de la plaza se suele realizar un proceso en el que tras una baremación de méritos se evalúan aspectos como los ingresos económicos, enfermedad o minusvalía o ubicación del domicilio familiar. ¿Se debe dar publicidad a tales datos de los concurrentes para garantizar la transparencia del proceso?

Si bien la publicación en tablón de anuncios de la puntuación referida a minusvalía – que no cabe duda de que contiene información sobre la salud del afectado – o la puntuación sobre enfermedad crónica del alumno supone una forma de garantizar los principios de transparencia y concurrencia competitiva más garantista con los principios de protección de datos que su publicación en Internet, o en un Boletín Oficial supone poner en conocimiento también de terceros no afectados por el proceso una información sobre la salud a la que no tiene porque acceder al no formar parte del proceso de concurrencia.

Es más adecuado al objeto de cumplimentar el derecho a concurrencia en igualdad de oportunidades, que el suministro de la información que contenga o de la que puedan derivarse datos de salud, renta u otros se realice únicamente previa petición de algún interesado.

Así, la publicación en el tablón de anuncios accesible a terceros no afectados poniendo a su disposición los restantes elementos del baremo junto al resultado final puede suponer la posibilidad de deducir por exclusión sin esfuerzo la valoración en materia de salud (discapacidad, enfermedad crónica,.....) u otros datos. En este caso se considera que deberá evitarse la publicación de las puntuaciones parciales y se pondrá cuadro valorativo parcial y expediente únicamente a disposición del interesado que lo solicite indicando el lugar donde los interesados podrán comparecer en el plazo que se establezca para el conocimiento íntegro de dichos actos deduciendo los posibles desacuerdos o comprobaciones en la forma indicada mediante acceso al baremo parcial y expediente por el interesado.

Como ha resumido algún artículo de prensa: información solo disponible en el despacho para los afectados.

Por contra, se considera adecuada la publicación en tablón de anuncios del resultado global de valoración al no deducirse de la misma información sensible.

Recuerde: La publicidad y equidad del proceso queda garantizada con la puesta a disposición de los involucrados en el proceso de la información relativa al resto de los concurrentes. No debe ponerse a disposición de terceros por ejemplo insertándolo en tablones de anuncios de acceso público.

La transparencia y la publicidad inherente a la actuación de las Administraciones en sus relaciones con los ciudadanos, así como el acceso a la información pública, que son exigencias constitucionalmente reconocidas como pilares del sistema democrático, deben acarrear la necesaria pero también la mínima divulgación de datos personales.

Y la solución al dilema se encuentra, como en el caso que se explicó antes relativo a la divulgación de datos sindicales en una Intranet, haciéndolos accesibles

únicamente a los interesados que participaban en el proceso de concesión de becas, ayudas públicas, plazas colegios concertados. Al colectivo afectado.

Es la misma solución que se aplica a la eventual divulgación en un tablón de anuncios de los deudores en una comunidad de propietarios. Solo podrán divulgarse en el ámbito de la comunidad al constituir el resto de los vecinos la esfera afectada sin que deba ponerse a disposición de terceros insertado en ubicaciones de libre acceso.

La publicación de datos personales en los boletines y diarios oficiales reviste trascendencia adicional en sus implicaciones sobre el derecho fundamental a la protección de datos. Convierte esta información en "fuente accesible al público" –y por lo tanto de libre uso- de acuerdo con la definición de las mismas contenida en la Ley Orgánica de Protección de Datos y multiplica exponencialmente su acercamiento al público debido a la combinación entre buscadores y publicación electrónica. Ha de tenerse en cuenta además que, entre los datos personales publicados en boletines y diarios oficiales, algunos de ellos son especialmente protegidos, como es el caso de las notificaciones de resoluciones sancionadoras o de las subvenciones vinculadas a datos de salud. De aquí que sea recomendable su limitación al máximo supeditando la inclusión a una previa previsión legal.

1.4 Servicios de la sociedad de la información

1.4.1 Divulgación de datos no protegidos por deber de secreto

En el caso de datos que aparecen en foros, blogs o vídeos, varias circunstancias deben tenerse en cuenta.

Por una parte la forma de aplicar el principio de consentimiento. Debe tenerse en cuenta que la realidad de Internet requiere realizar una interpretación del principio de consentimiento que evite su requerimiento con carácter previo, el cual paralizaría la red o la convertiría en una red profusa en vulneraciones legales al respecto de los datos de millones de personas, los cuales son, en muchas ocasiones, fácilmente accesibles mediante el uso de un buscador. Todo ello sin perjuicio de su derecho para negar su consentimiento para la permanencia de sus datos en Internet en el supuesto de que así lo considerara.

Junto a ello, frente a una denuncia sobre la inclusión de datos en la red sobre una persona debe tener en cuenta que cuando el Ordenamiento Jurídico ofrece varias soluciones, es necesario el agotamiento de fórmulas alternativas menos gravosas que las sancionadoras, por lo que se insta al afectado a ejercitar su derecho de cancelación. En el caso de que no se retiren los datos tras una actuación que la legislación española requiere que se haga con prontitud en diez días o no se justifiquen las razones para no hacerlo se abrirá un procedimiento de tutela de derechos -que se analiza en otra parte de este módulo- que tiene como objetivo reconocer en su caso el derecho, y por lo tanto reparar, no sancionar, no descartándose tampoco, si los datos persisten, acudir a la vía sancionadora.

En segundo lugar la relevancia pública o no de la persona afectada. Ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos podría suponer una insoportable barrera al

libre ejercicio de libertades de expresión a modo de censura previa no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse al ejercicio de las referidas libertades (por no resultar sus datos de interés público ni contribuir por tanto su conocimiento a forjar una opinión pública libre como pilar básico del Estado democrático) debe gozar de mecanismos reactivos amparados en derecho (como el derecho de cancelación de datos de carácter personal) que impidan su mantenimiento secular y universal en la red de su información de carácter personal.

Tal circunstancia no concurre en el caso de personajes públicos u objeto de hecho noticiable de relevancia pública. Así, se ha considerado que un alcalde tiene el deber de soportar la aparición en Internet de una fotografía de su vehiculo particular aparcado en zona prohibida sin que se haya instado a su supresión ni se haya iniciado procedimiento sancionador

La utilización del procedimiento sancionador No obstante, la inclusión de datos de personas carentes de relevancia pública en la red puede derivar en la aplicación directa de una sanción –sin la intermediación de un previo requerimiento de borrado- en el caso de que se refiera a datos sensibles o la inclusión revista especial gravedad. Así, la publicación de datos personales de especial sensibilidad (incluyendo videos) sin consentimiento previo del afectado derivaran en una imputación de tratamiento de datos sin consentimiento del afectado (precedente Lindqvist, SAN de 20/4/2009).

Por ejemplo, han derivado en sanciones administrativas los tratamientos de datos derivados de la inserción en youtube tanto de un video de un discapacitado como de un video grabado en una vía pública donde se ejerce la prostitución.

1.4.2 Divulgación de datos sometidos a deber de secreto

La aplicación directa de una sanción se interpreta también necesaria en el supuesto en que se produzca una divulgación en la red de información que debiera guardarse bajo secreto profesional. Uno de los principios de la protección de los datos es que el responsable del fichero o cualquiera que participe en el tratamiento se encuentra

obligado por secreto profesional. Su divulgación supone una conducta indebida. Tanto si se hace accesible depositando en la vía pública la documentación que contiene los datos como si se hace accesible a través de Internet.

Un caso especial de desvelamiento de secretos a través de la red es la divulgación en redes P2P de ficheros de organizaciones. En el historial de denuncias presentadas ante la Agencia consta la indebida divulgación de datos personales de clientes, empleados, miembros o pacientes.

Otro supuesto se encuentra en la publicación de datos personales previamente facilitados por el propio usuario a una organización, que sin el consentimiento de éste se difunden a través de la página web corporativa.

1.4.3 Buscadores

Los motores de búsqueda son complejos sistemas informáticos que indexan documentos almacenados en millones de servidores de páginas web (más comúnmente conocidos como servidores web), facilitando al usuario del servicio de búsqueda su inmediata localización, a través de determinadas palabras contenidas en los documentos buscados.

El índice de los motores de búsqueda se actualiza de forma dinámica a partir de la información obtenida por robots, que continuamente rastrean los servidores web públicamente disponibles en Internet, utilizando para ello la capacidad tecnológica de los propios servidores de la compañía, usualmente conocidos como "*arañas web*" o "*web crawlers*".

Los datos personales obtenidos por un buscador pueden afectar a la dignidad de la persona y pueden lesionar derechos de un tercero, por lo que la Agencia Española de Protección de Datos como órgano competente para velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, atendiendo a la reclamación formulada por el reclamante, puede requerir al responsable del tratamiento de los datos, la adopción de medidas necesarias para la adecuación del tratamiento.

Por ello debe estimarse la procedencia de evitar que el tratamiento por parte de un buscador tenga efectos no deseados con carácter permanente en contra de la voluntad del afectado.

Con frecuencia los buscadores en sus alegaciones, manifiestan que contestó a la petición del referido derecho de oposición indicando que no podían proceder a lo solicitado, debido a que las informaciones de los resultados de búsqueda se encuentran en páginas web de terceros cuyo acceso es público. Para eliminar contenido de los resultados necesitan la colaboración del webmaster.

2 situaciones principales pueden distinguirse:

a) El webmaster no puede cancelar. Es el caso de la publicación de datos personales en artículos insertados en prensa digital:

La publicación de una noticia en la versión digital de un diario se encuentra amparada por el artículo 20 de la Constitución Española que reconoce la libertad de expresión.

Pero la Ley no dispone que los datos personales del reclamante figuren en los índices que utiliza un buscador para facilitar al usuario el acceso a determinadas páginas, ni tampoco dispone que figuren en las páginas que un buscador conserva temporalmente en memoria "caché".

No existe, por tanto, una disposición legal en contrario respecto del ejercicio del derecho de oposición frente a los buscadores.

De acuerdo con lo anterior, se reconoce habitualmente la procedencia de excluir los datos personales del reclamante de los índices elaborados aunque frente a ello suele argumentar el buscador la imposibilidad de evitar la captación de la noticia si no es suprimida por la webmaster ya que los robots txt volverían a captarlo. La Agencia suele emplazar al buscador para que adopte y diseñe las medidas técnicas necesarias para evitar la indexación de manera autónoma.

No obstante aunque la publicación de una noticia en prensa se encuentra amparada en el derecho de libertad de expresión (art. 20 CE) el artículo 20 CE, se suele trasladar al medio de comunicación procedente la posibilidad de que acometan las medidas necesarias con el fin de evitar la indexación de los datos del interesado

que aparecen en el documento publicado en dicho Diario e impedir que sean susceptibles de captación por los motores de búsqueda de internet.

Lo mismo ocurre con la inclusión en Diarios Oficiales (indultos, sanciones administrativas, ayudas, edictos de juzgados, candidaturas elecciones, notificación sentencia de divorcio…) en que no cabe suprimir la versión en papel.

No procede la supresión del diario oficial pero si la cancelación evitando la indexación por los buscadores.

b) El webmaster puede cancelar.

Se estima la solicitud de tutela respecto al buscador para que adopte medidas para evitar la indexación.

Si el denunciante ha solicitado al webmaster la cancelación y no lo ha hecho se estima la tutela instando a que lo haga en el sentido que fue expuesto en el apartado 4.1.

1.4.4 Privacidad en los correos electrónicos

Dos aspectos principales deben resaltarse en lo que se refiere a privacidad en el ámbito de comunicaciones electrónicas que han tenido que ser analizadas como consecuencia de denuncias presentadas.

En primer lugar la concurrencia de publicidad contextual. El servicio de correo G-mail lleva asociada la recepción de publicidad no solicitada, relativa a productos y servicios relacionados con el contenido de los mensajes que visualiza el usuario en su bandeja. Por ejemplo, si el mensaje incluye palabras como "café" o "baloncesto" el usuario recibirá publicidad relacionada con tales conceptos.

Se ha debido resolver, tras una denuncia planteada por una asociación de consumidores, si el análisis del contenido de los mensajes suponía una intromisión indebida en la privacidad para concluir que el usuario registrado del servicio GMAIL presta un consentimiento expreso para el tratamiento de sus datos personales y para la asociación de publicidad personalizada, puesto que es la contrapartida para la prestación gratuita del servicio por lo que recae su consentimiento.

En segundo lugar la misma asociación de consumidores planteó el grado de garantía de confidencialidad del correo electrónico dimanante de los mecanismos de restablecimiento de contraseña a partir de una pregunta de seguridad.

El prestador del servicio analizado ofrecía dos opciones que permitían restablecer la contraseña de acceso, en el caso de que fuera olvidada. La primera de ellas consistía en recibir en un buzón alternativo de correo electrónico, que el usuario debe consignar en el momento del alta, un mensaje personalizado a través del cual el usuario podrá confirmar una nueva contraseña de acceso que sustituya a la que ha olvidado. La segunda opción consistía en contestar a una pregunta de seguridad, seleccionada también durante el alta, utilizando para ello la misma respuesta literal que se había registrado entonces.

Recordatorio: las opciones de restablecimiento de contraseña, unidas a una imprescindible concienciación conducían a otorgar un adecuado nivel de seguridad al acceso por parte de los usuarios.

1.4.5 Redes sociales (web 2.0)

El Grupo de Trabajo del artículo 29 (GT29), órgano consultivo europeo independiente establecido en virtud de la Directiva 95/46/CE, adoptó el 12 de junio de 2009 la Opinión 5/2009, sobre las redes sociales en línea. Este documento se centra en cómo el funcionamiento de los servicios de redes sociales (SRS) puede satisfacer los requisitos de la legislación sobre protección de datos de la Unión Europea.

En particular, en el documento se destaca cómo muchos usuarios de las redes sociales se mueven dentro de una esfera puramente personal, poniéndose en contacto con gente como parte de la gestión de sus asuntos personales, familiares o domésticos. Según destaca el GT29, la citada Directiva no impone las obligaciones de un responsable de datos a un individuo que procesa datos personales "*en el transcurso de actividades estrictamente personales o*

domésticas". Siguiendo este precepto, el GT29 estima que, con carácter general, en la mayor parte de las actividades realizadas por los usuarios de un SRS debe aplicarse lo que denomina "*exención doméstica*", en lugar de la normativa de protección de datos.

Ahora bien, en la Opinión se especifican así mismo tres supuestos en los que tales actividades no estarían cubiertas por la "*exención doméstica*". El primer supuesto se refiere a los casos en los que se utiliza el SRS como plataforma de colaboración para una asociación o una empresa. Si un usuario de SRS actúa en nombre de una sociedad o asociación, o utiliza el SRS principalmente como una plataforma para conseguir objetivos comerciales, políticos o benéficos, la exención no se aplica.En este caso, el usuario asume todas las obligaciones de un responsable de datos que está revelando datos personales a otro responsable de datos (el SRS) y a terceros (otros usuarios del SRS o, potencialmente, otros responsables de datos con acceso a los mismos). En estas circunstancias, el usuario necesita el consentimiento de las personas concernidas o algún otro fundamento legítimo dispuesto en la Directiva de Protección de Datos.

El GT29 expone que los prestadores del SRS deben garantizar la instauración de configuraciones por defecto gratuitas y que respeten la privacidad, restringiendo el acceso a los contactos seleccionados. En estas condiciones, cuando el acceso a la información del perfil se amplia hasta más allá de los contactos seleccionados, por ejemplo cuando se facilita el acceso al perfil a todos los miembros del SRS o cuando los datos son indexables por motores de búsqueda, el acceso desborda la esfera personal o doméstica. De igual manera, si un usuario toma una decisión informada de ampliar el acceso más allá de los "amigos" seleccionados, las responsabilidades inherentes a un responsable de datos se activan. Efectivamente, se aplicará el mismo régimen legal que cuando cualquier persona utiliza otras plataformas tecnológicas para divulgar datos personales en Internet. En varios Estados Miembros, la falta de restricciones de acceso (y así el carácter público) significa que la Directiva de Protección de Datos se aplica en el sentido de que el usuario de Internet adquiere responsabilidades de un responsable de datos. No obstante, el GT29 hace constar que, aunque la exención doméstica no se aplique, el usuario de SRS puede beneficiarse de otras exenciones como la exención con fines periodísticos o de expresión literaria o artística. En dichos casos, se ha de llegar a un equilibrio entre la libertad de expresión y el derecho a la privacidad.

Finalmente, el GT29 aborda un tercer escenario en que la "*exención doméstica*" no sería aplicable. Se trata de aquellos supuestos en los que es preciso garantizar los derechos de terceros, particularmente en relación con datos sensibles. No obstante se hace constar que, aun cuando se aplique la "*exención doméstica*", un usuario podría ser responsable de acuerdo con las disposiciones generales de la legislación civil o penal nacional en cuestión (por ejemplo, por difamación, responsabilidad civil extracontractual por suplantación de personalidad, responsabilidad penal).

En la Opinión se aclara el concepto de "*datos sensibles*". Así, los datos que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, la pertenencia a un sindicato o datos relativos a la salud o a la vida sexual se consideran sensibles. Los datos personales sensibles solo se pueden publicar en Internet con el consentimiento explícito del sujeto de datos o si el sujeto de datos ha hecho que los datos sean manifiestamente públicos él mismo.El GT29 expone que en algunos Estados Miembros de la UE, las imágenes de los sujetos de datos se consideran una categoría especial de datos personales, ya que se pueden utilizar para distinguir entre orígenes raciales/étnicos o pueden utilizarse para deducir las creencias religiosas o los datos sobre la salud. El GT29, en general, no considera que las imágenes en Internet sean datos sensibles, a menos que éstas se utilicen claramente para revelar datos sensibles acerca de los individuos.

En consecuencia, de conformidad con el criterio interpretativo mantenido por el GT29, es preciso que concurra alguno de los escenarios expuestos, en los que la "*exención doméstica*" no resulta de aplicación, para que sean aplicables los requisitos previstos en la LOPD.

Sin embargo, en el apartado 3.9 de la Opinión el GT29 aborda los derechos de los individuos afectados que, de acuerdo con las disposiciones expuestas en los artículos 12 y 14 de la Directiva 95/46/CE, deben respetar los SRS. Así, el GT29 concluye que los derechos de acceso, rectificación y cancelación no se limitan a los usuarios del servicio, sino a cualquier persona física cuyos datos se procesen. Los miembros y no miembros de los SRS deberán tener un medio de ejercitar tales derechosEn relación con las redes sociales, durante el año 2009 se recibieron en la AEPD 31 denuncias, además de 1 reclamación de tutela por desatención del derecho de cancelación.

El contenido de las denuncias fue el siguiente:

a) 13 fueron presentadas por docentes. De esas 13, 1 se refería a una supuesta suplantación de identidad, otra a la difusión de un documento suscrito por la denunciante y las otras 11 a la difusión en la red de fotografías tomadas en el entorno educativo, asociadas a distintos comentarios realizados por los alumnos.

b) 3 denuncias fueron presentadas por sendas personas cuya imagen (incluida en fotografías de grupo) había sido difundida a través de la red por un usuario sin el consentimiento de las afectadas.

c) profesores de una Universidad que vieron cómo, a través de un test, se difundía en la red social su imagen asociada a diversos comentarios injuriosos.

d) una organización de usuarios, por la difusión de promociones comerciales asociadas a sitios web que, utilizando técnicas supuestamente engañosas, facilitan la suscripción en servicios "*SMS-premium*".

e) una usuaria de la red cuya fotografía, captada de su propio perfil en la red social, había sido difundida a través de un SMS por otra usuaria (compañera de trabajo) a la que previamente había aceptado como amiga.

f) el ex trabajador de una compañía, por la suplantación de su identidad en la red social.

g) una usuaria de la red que, tras recibir en la red la solicitud de amistad de un usuario desconocido y aceptarla, descubrió que éste era el director de una compañía a la que había optado profesionalmente y que las intenciones de éste no eran exclusivamente profesionales.

De las citadas denuncias se archivarán 15 por no haberse constatado suficientemente los hechos denunciados o no ser aplicable la LOPD (datos no identificables). En la actualidad, se siguen tramitando 6 y el resto culminarán o han culminado en la apertura de un procedimiento sancionador.

2. LEGITIMACIÓN PARA EL TRATAMIENTO: INFORMACIÓN Y CONSENTIMIENTO

El concepto de tratamiento de datos es un concepto amplio y se encuentra recogido en diversas normativas y doctrina jurisprudencial. Entre otras, señalar la definición dada en la Directiva 95/46/CE, en la LOPD, en la norma que desarrolla la propia LOPD, así como la doctrina del TJCE en su sentencia de 6/11/2003.

Para lo que interesa en este capítulo, y siguiendo la definición que figura en el artículo 3.c) de la LOPD, se define tratamiento de datos como:

<<Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias>>.

También, en el informe final sobre Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Resolución de Madrid de enero de 2010, se define tratamiento como:

<<Tratamiento: cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión>>.

Obsérvese que la mera tenencia de datos de carácter personal (conservación) o la supresión o cancelación, se encuentran dentro del concepto de tratamiento.

Ejemplo 1º (expediente de la AEPD de referencia PS/00134/2008)

(https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2009/index-ides-idphp.php)

<< ANTECEDENTES: Con fecha dd/mm/aaaa, tuvo entrada en esta Agencia Española de Protección de Datos una denuncia de Don. B.García García (en lo sucesivo el denunciante) contra la empresa LEX Company.

La citada entidad, especializada en la publicación de resoluciones judiciales a través de su página web, publicó una sentencia judicial sin anonimizar los datos personales del denunciante.

En dicha publicación figuraban los siguientes datos del denunciante:

apellidos, DNI, y su domicilio, asociado a la condición de demandante en un proceso.

Tras la tramitación del correspondiente procedimiento sancionador, la AEPD resolvió lo siguiente al considerar que el tratamiento de los datos por dicha entidad carecía de consentimiento :

<< El Director de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a la entidad "LEX Company", una multa de 6.000 €, por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica. >>

La vertiente subjetiva del principio de tratamiento encuentra su fundamento en determinar *quién* está legitimado para llevar a cabo un determinado tratamiento de datos personales, así como los requisitos que debe cumplir.

Conforme a la normativa europea, recogida en la LOPD, está legitimado para realizar un tratamiento de datos personales tanto el *Responsable* como el *Encargado* del mismo. El encargado de tratamiento es aquél que trata los datos por

cuenta del responsable al que le presta servicios tratando los datos conforme a sus instrucciones. En este sentido, señalar que en el caso de producirse una cesión de datos a un tercero diferente del *Encargado* o que no ostente tal condición al decidir sobre la finalidad, uso y contenido de los datos el cesionario se convierte en un nuevo responsable, asumiendo, por tanto, las obligaciones y derechos propias tal figura.

Debe observarse, que tanto el *Responsable* como el *Encargado* pueden ser, indistintamente, personas jurídicas o físicas.

La figura del responsable en todo caso es fundamental, ya que sobre él se proyecta el conjunto de obligaciones vinculadas a los tratamientos de datos personales, en especial la obligación de informar previamente al afectado sobre el tratamiento de datos a realizar así como de recabar el consentimiento para el mismo.

Ejemplo 2º (expediente de la AEPD de referencia PS/00179/2009)

(https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2009/index-ides-idphp.php)

<< ANTECEDENTES : Con fecha dd/mm/aaaa, tuvo entrada en esta Agencia un escrito de Dña. C.C.C. antigua cliente del "Banco, S.A.", en el que denuncia a la entidad bancaria por haberle remitido a su domicilio información relativa a un determinado producto financiero, tratando para ello sus datos de carácter personal como son nombre y domicilio. Consta que los datos personales de la denunciante habían sido objeto de cancelación previa a petición de la misma. Además, la cancelación de los datos fue confirmada por la entidad bancaria>>.

Tras la tramitación del correspondiente procedimiento sancionador, la AEPD resolvió, al considerar que el consentimiento para el tratamiento de los datos de la denunciante por dicha entidad bancaria carecía de consentimiento al haber sido revocado, lo siguiente:

<<El Director de la Agencia Española de Protección de Datos
RESUELVE:

PRIMERO : IMPONER a la entidad Banco, S.A., por una infracción del artículo 6.1 de la LOPD, relativa a tratamiento sin consentimiento tipificada como grave en el artículo 44.3 d) de dicha norma, una multa de 60.101,21 € (sesenta mil ciento uno con veintiún céntimos de euro) de conformidad con lo establecido en el artículo 45 de la citada Ley Orgánica. >>

2.1 Información y consentimiento.

Para llevar a cabo un determinado tratamiento de datos personales se requiere que el *Responsable* de tal tratamiento cumpla obligatoriamente, y con carácter general, con determinados requisitos, como son:

a) deber de informar previamente al afectado, y

b) disponer del consentimiento del afectado.

Cumplidos estos dos requisitos por el *Responsable,* éste podrá trasladar la realización efectiva de un tratamiento concreto al *Encargado* de llevarlo a cabo.

En consecuencia, el *Encargado*, en el caso de existir, actuará siempre por cuenta del *Responsable.*

El *consentimiento* puede definirse como: <<Toda *manifestación de voluntad* (voluntad de un afectado que por sí sola es susceptible de producir el efecto deseado), *libre* (ausencia de coacción), *inequívoca* (que no de lugar a equívoco), *específica* (no genérica) e *informada* (conocimiento previo de las condiciones en la que se manifiesta la voluntad), mediante la que el interesado consienta el tratamiento de datos personales que le conciernen>>.

Respecto de los requisitos necesarios anteriormente citados, para que el otorgamiento del consentimiento para un determinado tratamiento sea válido, merece especial atención el requisito de disponer información previa al mismo.

Así, es evidente que el afectado que manifiesta la voluntad mediante la cual otorga el consentimiento para que sus datos personales sean tratados por el responsable que lo solicita, debe estar previamente informado sobre los pormenores de tal tratamiento. Al respecto, la legislación española determina cual es el mínimo de información que debe disponer el afectado.

Si no existe información previa, el consentimiento otorgado resultaría viciado y no sería válido, impidiendo realizar el tratamiento de datos para el que se solicitó.

Tal información suele facilitarse al afectado al que se le requiere sus datos a través de una *cláusula informativa*, que debe contener, como mínimo, los siguientes extremos:

a) *existencia de un fichero,*

b) *finalidad para la que se recaban,*

c) *destinatario de los datos*,

d) *identidad y dirección del responsable del tratamiento* o, en su caso, de su representante.

La nula o deficiente información sobre la finalidad para la que se recaban los datos es el origen, en la práctica, de que muchos tratamientos resulten sancionados.

Tal es el caso del tratamiento de datos con fines publicitarios. Si el responsable prevé en un futuro llevar a cabo una campaña publicitaria ajena al objeto del tratamiento para el que se otorgó el consentimiento, deberá informar de ello en el momento de la recogida o, en el caso de una situación sobrevenida, deberá recabar el consentimiento para ese nuevo tratamiento.

En el caso de que los datos no hayan sido recabados del propio afectado, éste deberá ser informado de forma expresa, precisa e inequívoca, además de los anteriores extremos, sobre el *contenido del tratamiento a realizar*, *procedencia de los datos y posibilidad de ejercitar sus derechos.* Por ejemplo cuando los datos provienen de fuentes accesibles al público (de libre disposición como las guías telefónicas) y se tratan con fines de publicidad. Sin embargo, en el caso analizado en el presente párrafo, como más adelante se explica, existen excepciones como

son que una norma de rango de ley así lo prevea o resulte imposible o exija esfuerzos desproporcionados facilitar tal información.

En consecuencia, todo tratamiento de datos personales requiere que previamente sea consentido por el afectado, en los términos antes expresados, con especial relevancia al derecho citado de información previa.

Una vez informado y otorgado el consentimiento, recae sobre el responsable la carga de probarlo, toda vez que no es admisible su presunción, tanto cuando se haya recabado de forma *expresa* como *tácita.*

Distinto es el caso en el que el consentimiento se recabó de forma *tácita*. En este supuesto el responsable se dirige al afectado informándole de los pormenores acerca del tratamiento de datos que solicita. Si una vez acreditada la recepción de la solicitud el afectado no contesta en un plazo determinado, se entenderá que *tácitamente* ha aceptado, en las condiciones informadas, y el responsable podrá iniciar el tratamiento de los datos así solicitados.

El problema más usual en el caso de *consentimiento tácito*, es el de acreditar que efectivamente el afectado ha recibido la carta de solicitud emitida por el responsable. Asimismo en caso de contestación negativa, que el responsable haya tenido conocimiento.

Discutible es también el plazo que el *responsable* debe esperar para considerar que el *afectado* acepta tácitamente el tratamiento. En la normativa española es de 30 días a contar desde que el afectado recibe la carta de solicitud al tratamiento.

Para finalizar este apartado, se debe señalar que todo consentimiento es revocable en todo momento y sin justificación alguna y debe poder solicitarse a través de un medio sencillo y gratuito ante el responsable del tratamiento o, en su caso, persona que actúe en su nombre.

Una vez revocado el consentimiento por el afectado, el responsable deberá cesar el tratamiento de los datos del afectado objeto de revocación. Además, cuando el responsable hubiera cedido los datos a terceros, deberá comunicar a los cesionarios tal revocación al objeto de que cesen, igualmente, el tratamiento que estén llevando a cabo.

Ejemplo 3º (expediente de la AEPD de referencia PS/00098/2009)

(https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2009/index-ides-idphp.php)

<< ANTECEDENTES: Con fecha dd/mm/aaaa, tuvo entrada en esta Agencia un escrito de D. E.E.E. (en lo sucesivo el denunciante) en el que declara que ha recibido un envío de publicidad no solicitada remitido por la entidad FINGES, SA, en el que *"no consta dirección alguna para ejercer los derechos que me reconoce la Ley Orgánica 15/1999"*>>.

Tras la tramitación del correspondiente procedimiento sancionador, la AEPD resolvió sancionar a la entidad FINGES, S.A. por infracción del artículo 5 de la LOPD, al considerar que el tratamiento de los datos por dicha entidad carecía de la información previa necesaria.

2.2 Excepciones a la regla del consentimiento.

No obstante lo anterior, se debe señalar que existen excepciones a la citada regla general sobre el consentimiento, tanto para la cesión como para el tratamiento de datos personales, tal y como se regulada detalladamente en el artículo 6.2 de la LOPD y en el artículo 10 del RLOPD.

El legislador decide en estos casos sobre el balance entre privacidad y libre difusión de información, trazando la línea que define los datos personales accesibles sin necesidad de recabar el consentimiento del afectado.

Así es cuando una norma de *rango legal, nacional o comunitaria,* exima del consentimiento de los afectados. El interés público hace soslayar la regla del consentimiento para usar los datos personales.

Esta eximente al consentimiento es habitual en muchos tratamientos de datos personales de los *ciudadanos* para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito exclusivo de sus competencias.

Tampoco es necesario el consentimiento cuando los datos tratados o cedidos por el responsable figuren en fuentes de acceso público y tenga un interés legítimo para su tratamiento y siempre que no se vulneren los derechos y libertades fundamentales del interesado. El legislador establece las fuentes de libre acceso como Boletines Oficiales, medios de comunicación social o guías.

Otra de las excepciones se produce cuando los datos personales tratados por el *Responsable/s* se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. En este caso, cada una de las partes podrá tratar los datos personales de la otra. Así, no tendría sentido que en una empresa el uso proporcional de los datos de los trabajadores quedara sometido a su previo consentimiento.

Tampoco será necesario el consentimiento del afectado, cuando el tratamiento de los datos por el *Responsable* tenga por finalidad proteger un interés vital, del afectado o de terceras personas, o resultar necesario para la prevención o diagnóstico médico o la gestión de servicios sanitarios.

Tampoco será necesario el consentimiento previo del afectado, cuando la comunicación de los datos tenga por destinatario determinadas Instituciones del Estado, como son el Defensor del Pueblo, fiscales y magistrados y Tribunal de Cuentas.

Mención especial merece el tratamiento de datos personales de los menores de edad, toda vez que requiriere la autorización de los padres o tutores si la edad del menor es inferior a catorce años. En caso contrario, la norma general es que el responsable podrá proceder al tratamiento de los datos con el consentimiento del menor.

Se debe señalar que la minoría de edad no supone una causa de incapacitación de las tasadas en la normativa civil común nacional. Por ello, tal circunstancia deberá ser analizada en cada caso concreto según la trascendencia del consentimiento prestado.

No obstante, en ningún caso, pueden recabarse del menor datos que permitan obtener información sobre lo demás elementos del grupo familiar. Sólo podrá

recabarse los datos identificativos del padre madre o tutor con la única finalidad de recabar la autorización para el tratamiento de los menores.

El tratamiento de los datos de menores ha sido abordado por el Grupo de Trabajo del artículo 29 de la mencionada Directiva 95/46, en el informe de fecha 18/01/2008.
(www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php).

Finalmente, se debe señalar que, en todo caso, será el responsable del tratamiento de los datos el obligado a acreditar que dispone del preceptivo consentimiento. En definitiva, es al responsable del tratamiento al que incumbe la carga de la prueba.

2.3 El consentimiento para el tratamiento de datos especialmente protegidos

Los datos personales especialmente protegidos son aquellos que afectan a la esfera más íntima del individuo. Por ello merecen que sean objeto de una especial protección. Tales datos están regulados, entre otras normas, en el Convenio número 108 del Consejo de Europa de 28/01/1981, Directiva 95/46/CE, y en la normativa española en la propia LOPD, artículo 7.

Deben diferenciarse dos tipos de datos personales especialmente protegidos:

a) aquellos relativos a la ideología, afiliación sindical, religión y creencias.

b) aquellos relativos al origen racial, a la salud y a la vida sexual.

Respecto del primer grupo de datos indicados, es necesario para su tratamiento el *consentimiento expreso y por escrito* del afectado. Para proceder al tratamiento de los datos personales referidos en segundo grupo, será necesario que así lo disponga una *norma de rango legal* o que el afectado consienta *expresamente*. Nótese que en este último caso, no requiere el consentimiento por escrito, pero sí excluye el *consentimiento tácito* para su tratamiento.

El plus de protección a que se someten este tipo de datos consiste, especialmente, en los requisitos necesarios para otorgar el consentimiento para su tratamiento, así como su máxima protección en el ámbito relativo a las medidas de seguridad de necesaria adopción para su custodia.

Por la cantidad de ficheros existentes conteniendo datos personales relativos a la salud, toda vez que el responsable de tal tipo de ficheros suele ser una autoridad sanitaria o bien, en el ámbito privado, un profesional o entidad sanitaria, se hace a continuación una breve mención a sus peculiaridades.

El concepto de salud es un concepto amplio. El apartado 5 de la Memoria Explicativa del Convenio 108 de Europa, define lo que considera *"datos personales relativos a la salud"*. También define tal concepto la Recomendación R(97)5, del Comité de Ministros del Consejo de Europa, y el propio Tribunal de Justicia de las Comunidades Europeas, Sala Pleno, de 6/11/2003, asunto C-101/2001 (Caso Lindqvist), así como la propia normativa española en su artículo 5.1.g) del reglamento que desarrolla la LOPD. En todas las definiciones se afirma que este tipo de datos comprende la información relativa a todos los aspectos de la salud pasada, presente y futura, tanto físicos como síquicos, de una persona, incluida la información genética.

Ejemplo 4º (expediente de la AEPD de referencia PS/00331/2007)

(https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2009/index-ides-idphp.php)

<< ANTECEDENTES : Con fecha dd/mm/aaaa, tiene entrada en esta Agencia un escrito de Doña G.G.G. (en lo sucesivo la denunciante), en el que denuncia que la entidad Aresa Seguros, S.A. (en lo sucesivo Aresa) cuenta con unos informes médicos suyos emitidos por el profesional que la trata en la actualidad y ajeno a dicha entidad. Dichos informes se refieren a una fecha anterior a la contratación de la Póliza de seguro médico suscrita con Aresa. La denunciante manifiesta no haber autorizado al facultativo de la entidad aseguradora para el tratamiento de sus datos.

Asimismo, denuncia que la interesada ha solicitado en distintas ocasiones a la aseguradora copia de dichos informes, habiéndosele denegado el acceso en varias ocasiones por considerar Aresa que era documentación interna de la misma. No obstante, con fecha 19 de diciembre de 2003, le remiten copia de uno de los informes con datos correspondientes al año 2000, asimismo, le comunican que dicha información ha sido proporcionada por el Doctor x.x.x. en virtud de un convenio existente entre ambos (entidad aseguradora y el doctor ajeno a la misma)>>.

Tras la tramitación del correspondiente procedimiento sancionador, la AEPD resolvió sancionar a la entidad aseguradora como al facultativo, al considerar que se había producido por parte de la aseguradora un tratamiento de datos especialmente protegidos sin consentimiento expreso de la interesada, así como una cesión inconsentida de datos especialmente protegidos por parte del facultativo que previamente la trataba.

2.4. Las relaciones con terceros.

Es una situación frecuente que en el marco de una relación negocial previamente establecida, los datos recabados por el responsable deban ser comunicados a terceros, bien porque la comunicación tenga por objeto la satisfacción de un interés legítimo del responsable o del cesionario, o bien por necesidades diferentes, como puede ser aquellas de índole privada.

El artículo 3.i) de la LOPD, define cesión de datos como *"toda revelación de datos realizada a una persona distinta del interesado".*

En todos los casos, la cesión de los datos por el responsable a una tercera persona deberá estar consentida por el afectado, autorizada por una norma de rango legal, o bien, que los datos figuren en fuentes de acceso al público y se tenga un interés legítimo para su tratamiento.

Sin embargo, también existen, en el caso de cesión de datos a terceros, excepciones a la regla general, tal y como se verá más adelante.

2.4.1 Comunicaciones de datos personales.

La cesión de datos por el responsable de los mismos (cedente) a terceros (cesionario) debe considerarse como un tratamiento cualificado de datos que requiere de unas mayores garantías, toda vez que los datos objeto de cesión salen de la esfera de seguridad del responsable extendiéndose el conocimiento de los mismos a personas diferentes a los que el afectado o titular de los datos no autorizó inicialmente. Tal y como ocurre en el caso del tratamiento, el consentimiento para la cesión será nulo cuando la información que se facilite al interesado no le permita conocer la finalidad a que se destinarán los datos.

En todo caso, la cesión de datos sólo será posible para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario con el previo consentimiento del afectado.

Sin embargo, será posible la cesión de los datos sin contar con el consentimiento del afectado en los siguientes supuestos:

a) Cuando la cesión esté consentida por ley

b) Cuando se trate de datos recogidos de fuentes accesibles al público

c) Que la cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte necesariamente la comunicación de los datos, limitándose en todo caso a la finalidad que la justifique.

d) Que la cesión que deba efectuarse tenga por destinatario determinadas instituciones determinadas por una norma de rango legal, como pueden ser, entre otras, el Ministerio Fiscal o los Jueces o Tribunales.

e) La cesión entre Administraciones Públicas siempre que tenga por objeto el tratamiento de datos con fines históricos, estadísticos o científicos, o bien hayan sido recabados por una Administración Pública con destino a otra y tal comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

f) Los datos especialmente protegidos en los términos establecidos el la LOPD. En el caso concreto de datos personales de salud, no será necesario el consentimiento del interesado, incluso a través de medios electrónicos, cuando se realice entre organismos, centros y servicios del Sistema Nacional de Salud para la atención sanitaria conforme dispone la normativa específica de atención sanitaria.

2.4.2. El acceso a datos por cuenta de terceros.

Un caso de especial trascendencia en la práctica comercial y empresarial es aquel en el que el responsable de los datos *encarga* a terceros para que lleve a cabo en su nombre tratamientos que son necesarios para la prestación del servicio al afectado o titular de los datos. La tercera persona que realiza el tratamiento necesario al responsable del fichero se denomina *"encargado"*, a la que ya hemos hecho referencia al principio del capítulo. Este tipo de acceso a datos por terceros (*encargados*) se encuentra legitimado en la citada Directiva 95/46/CE, artículo 2.5.

Al constituir realmente una comunicación de datos legalmente consentida y no conocida por el afectado toda vez que se halla en la creencia de que el tratamiento lo realiza el responsable al que otorgó su consentimiento, la norma impone tanto al *responsable* de los datos como al *encargado* de los mismos, una serie de requisitos singulares para que pueda llevarse a cabo sin vulnerar los derechos del afectado.

Conviene repetir en este momento la definición legal de *"encargado del tratamiento"* (Directiva 95/46/CE, artículo 2.e), y 17.2), y de idéntica forma la LOPD, artículo 3.g):

<<Encargado: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable>>.

Asimismo, en el informe final sobre Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Resolución de Madrid de enero de 2010, se define Prestador de servicios de tratamiento como:

<<Prestador de servicios de tratamiento: persona física o jurídica, distinta de la persona responsable, que lleve a cabo un tratamiento de datos de carácter personal por cuenta de dicha persona responsable>>.

La norma reglamentaria española es más explícita en la definición (RLOPD, artículo 5.1.i):

<<Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable 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. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados>.

Así, para asegurar que se cumplan los requisitos exigidos legalmente, el acceso a datos personales por tercero (encargado) deberá consolidarse en un contrato cuyo objeto son los datos personales a tratar y que habilite tal acceso por parte del encargado (prestador efectivo del servicio contratado).

Es el momento en exponer cuales son esos requisitos exigidos.

La Directiva 95/46/CE señala los siguientes (artículo 17.3):

- Que la realización del tratamiento por encargo deberá estar regulada por un contrato o acto jurídico que vincule inequívocamente al encargado con el responsable.

- Tal contrato dispondrá explícitamente que el encargado del tratamiento sólo actúa siguiendo las instrucciones del responsable.

- También dispondrá explícitamente las medidas de seguridad que el encargado debe asegurar.

Por su parte, la LOPD en su artículo 12.2), señala con más detalle estas exigencias, que deberán constar de forma explícita:

- La contratación del encargo se regulará en un contrato que deberá constar por escrito, o en alguna forma que permita acreditar su contenido.

- El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable, y no los utilizará con un fin diferente no los comunicará, ni siquiera para su conservación, a otras personas.

- En dicho contrato se estipularán las medidas de seguridad que el encargado está obligado a implementar en el tratamiento.

- Una vez cumplida la prestación contractual por el encargado, éste deberá destruir los datos objeto de tratamiento o devueltos al responsable.

- En el caso de que el encargado destine los datos con otra finalidad distinta a la que figure en el contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Por lo tanto, en ausencia de estas garantías, la comunicación de datos por el responsable al encargado del tratamiento no estará amparada por ley y requerirá, siguiendo la norma general anteriormente expuesta, el consentimiento previo del interesado.

Procede analizar por separado cada uno de los requisitos expuestos.

En primer lugar, debe existir un contrato formal, que si bien no requiere que sea escrito, deberá poder acreditarse su contenido. Se concluye, en consecuencia, que, toda vez que debe poder acreditarse su contenido, difícilmente podrá ser de otra manera diferente a su constancia por escrito.

En segundo lugar, el encargado deberá atenerse escrupulosamente a las instrucciones del responsable. De lo contrario será considerado responsable y deberá disponer del consentimiento del afectado para el tratamiento de sus datos personales.

En tercer lugar, el encargado deberá implementar en el tratamiento de los datos las mismas medidas requeridas para el responsable, tanto las de índole técnica como organizativa.

En cuarto lugar, una vez cumplida la prestación contractual, el encargado deberá destruir los datos objeto de tratamiento o los devolverá al responsable, de forma tal que tanto los datos originales comunicados por el responsable, como aquellos otros elaborados por el encargado, no pudiendo permanecer en ficheros del propio prestador del servicio. En este sentido, la norma reglamentaria que desarrolla la LOPD, aclara que no procederá la destrucción de los datos una vez cumplida la prestación del servicio cuando exista una previsión legal que exija su conservación, o que, en tanto puedan derivarse responsabilidades de su relación con el responsable, podrán permanecer, en este caso, debidamente bloqueados por el encargado.

En caso de incumplimiento de los términos del contrato por parte del encargado del tratamiento, se debe señalar que éste será considerado responsable del tratamiento adquiriendo las responsabilidades como tal, como es, entre otras, la de disponer del consentimiento del afectado para el tratamiento realizado, y responderá personalmente de las infracciones en que hubiera incurrido.

Se debe señalar que la figura de encargado del tratamiento no se refiere al personal propio adscrito al responsable de los datos, sino a tercera persona (física o jurídica) que trata los datos por cuenta y en nombre del responsable. Es decir, el responsable del tratamiento decide sobre las finalidades y usos de los datos y encomienda a una tercera persona y en su nombre (el encargado) la realización efectiva de tal tratamiento.

De no cumplirse los requisitos anteriormente señalados en la prestación de los servicios contratados, el acceso a los datos por el supuesto encargado deviene en tratamiento de datos sin consentimiento, y respecto del responsable que ha facilitado el acceso incurrirá en comunicación de datos sin consentimiento, infracciones grave y muy grave, respectivamente, según la normativa española (LOPD).

Dado que esta figura de *encargado del tratamiento* constituye un supuesto de excepción a la norma general, toda vez que implica una comunicación de datos sin necesidad de consentimiento ni informar previamente al afectado, ha de ser siempre interpretada de forma restrictiva.

Ejemplo 5º (expediente de la AEPD de referencia PS/00592/2008)

(https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2009/index-ides-idphp.php)

<< ANTECEDENTES: Ha tenido entrada en la Agencia Española de Protección de Datos con fecha dd/mm/aaaa, el escrito presentado por Dña. H.H.H. (en lo sucesivo la denunciante) en el que denuncia a las entidades CAJA LABORAL y BRECSAN, S.L., manifestando que:

"He recibido en el buzón de mi domicilio particular, carta sin franquear con nombre completo, con domicilio y piso remitida por CAJA LABORAL.

Con fecha de 16 de enero de 2007, me dirijo a la empresa BRECSAN, S.L. para solicitar aclaración de las fuentes accesibles al público en las que conste mi nombre y dirección completa; así como mostrar mi oposición a dicha fuente en la que consta mi nombre".

Por parte de la Inspección de Datos se le requirió a la afectada, para que remitiera la contestación dada por la sociedad BRECSAN a su solicitud. >>

Consta en los "HECHOS PROBADOS" de la Resolución del procedimiento sancionador, los siguientes:

<<PRIMERO.- La denunciante recibió en diciembre de 2006, un envío comercial en el constaban sus datos personales de nombre y apellidos y domicilio.

Asimismo se especifica que los datos han sido obtenidos de "fuentes accesibles al público" por BRECSAN, S.L. ante quién se podrá ejercitar los derechos. La entidad anunciada en el envío comercial es Caja Laboral Popular.

SEGUNDO.- En fecha de 16 de enero de 207, la denunciante solicita mediante carta certificada a la empresa BRECSAN la información a cerca de la procedencia de sus datos personales y muestra su

oposición a que sean utilizados los mismos. BRECSAN no contestó dicho requerimiento.

TERCERO.- Se acreditó por los servicios de Inspección de la Agencia Española de Protección de Datos, que en las guías "on-line" disponibles en Internet de los servicios de telecomunicaciones denominadas –paginas blancas y QDQ- figuran los datos de Dª H.H.H. asociados a un domicilio distinto del que figura en el envío publicitario.

CUARTO.- Caja Laboral Popular encargó sin constancia documental, a Unipost S.A. la realización de una campaña comercial en el mes de diciembre de 2006, efectuando los servicios de separación de bases de datos por determinados códigos postales, personalizar, manipulación, ensobrado y distribución.

QUINTO.- Unipost S.A. contrató con BRECSAN el alquiler de una base de datos para la realización de los servicios que le encargó Caja Laboral Popular. En el mencionado contrato no se recogen las previsiones del art. 12 de la LOPD.

SEXTO.- BRECSAN no ha acreditado el consentimiento para el tratamiento de datos personales de la denunciante en sus ficheros ni para la cesión de los mismos a terceras entidades. Tampoco que concurrieran circunstancia que permita tratamiento y cesión conforme os artículos 6.2 y 11.2 de la LOPD.

SEPTIMO.- Los datos personales de la denunciante resultaron tratados por Unipost, S.A. previa cesión de los mismos realizada por BRECSAN para la realización de una campaña publicitaria de productos de Caja Laboral Popular.>>

Tras la tramitación del correspondiente procedimiento sancionador, la AEPD resolvió sancionar a la entidad BRECSAN GESTION, S.L, por las infracciones de los arts. 11 (cesión) y 6 (tratamiento sin consentimiento) de la LOPD, tipificadas como muy grave y grave en los arts. 44.3 d) y 44.4 b) respectivamente, a la entidad Caja Laboral

Popular CC, por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3 d), y a la entidad UNIPOST, S.A., por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3 d).

Ejemplo 6º (expediente de la AEPD de referencia PS/000085/2006)

(https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2009/index-ides-idphp.php)

<< ANTECEDENTES: Con fecha dd/mm/aaaa, tuvo entrada en esta Agencia escrito de D. PMG (en lo sucesivo el denunciante) en el que denuncia que Asinco, S.A., con fecha 28/09/aaaa, le remitió a su domicilio, en la "*calle Río N, 1º B, 35111 Altos- Las Palmas*", un escrito reclamándole, en nombre de Banco General, el pago de una deuda, y que, con fecha 19/10/aaaa, le realizó una llamada telefónica a su línea de telefonía móvil nº NNNNNNNN reclamándole el pago de la citada deuda, sin que él haya facilitado a Banco General ni a Asinco, S.A., los datos del citado domicilio ni su número de teléfono.

Tras la tramitación del correspondiente procedimiento sancionador, la AEPD resolvió sancionar a la entidad ASINCO, SA, por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d), al considerar que dicha entidad trató los nuevos datos por ella recabados sin consentimiento del afectado:

Sin embargo, la Resolución de la Agencia Española de Protección de Datos fue impugnada ante los Tribunales de Justicia, resultando anulada y exonerada de responsabilidad la entidad imputada.

¿Por que resultó anulada la resolución de la AEPD y exonerada de responsabilidad a la entidad imputada (el encargado del tratamiento)?

El denunciante consideró que la entidad "encargada del tratamiento" de sus datos (Asinco, S.A.), se excedió cuando trató datos nuevos relativos a su dirección postal y teléfono, los cuales no habían sido suministrados por la entidad acreedora y responsable inicial de los datos, por lo que el

tratamiento de *"esos nuevos datos recabados"* carecía de consentimiento. A ASINCO, S.A., se le encargó la gestión del cobro de la deuda a partir del acceso a los datos que obraban en los ficheros del responsable (Banco General) y acreedor del denunciante, a través de un contrato de servicios articulado conforme al artículo 12 de la LOPD.

Sin embargo, recurrida la Resolución en sede judicial, se dictó sentencia en los siguientes términos:

> *"... Pues bien, el consentimiento inicialmente prestado para el consentimiento de unos concretos datos personales – un domicilio determinado y un número de teléfono – continúa proyectándose en el tiempo mientras permanece la relación contractual respecto de datos personales del mismo tipo que los que fueron proporcionados y autorizado su uso siempre que su tratamiento continúe siendo necesario para el cumplimiento o ejecución del contrato, como aquí ocurre."*

En definitiva, el afectado debiera haber actualizado los datos suministrados.

Se debe señalar que la esencia de una prestación de servicios, desde el punto de vista de la normativa de protección de datos, consiste en el siguiente flujo de datos:

1º.- El responsable dispone de los datos de sus clientes recabados con el preceptivo consentimiento informado.

2º.- El responsable, en un determinado momento, necesita realizar un tratamiento en el ámbito de la relación negocial que les vincula.

3º.- El responsable, bien por estrategia comercial o por necesidades técnicas u organizativas, se ve obligado a "subcontratar" con tercera entidad (encargado) un determinado tratamiento. En contrato suscrito entre el responsable y el encargado deberá incluir, además de las usuales en todo contrato, las cláusulas conforme dispone el artículo 12 de la LOPD.

4º.- Para ello, "comunica los datos de sus clientes" al encargado del nuevo tratamiento para que este lo lleve a cabo siguiendo unas estrictas

directrices impuestas por el responsable.

5º.- Una vez realizado el tratamiento, el encargado devuelve los datos inicialmente comunicados por el responsable así como aquellos que resultan del nuevo tratamiento.

6º.- Finalizada la relación entre el responsable y el encargado, éste último no puede disponer de cualquier dato, tanto los iniciales como los elaborados como consecuencia del tratamiento llevado a cabo.

El procedimiento sancionador incoado por la Agencia, tenía su fundamento en que "en el caso citado el "encargado" no se limitó a tratar los datos comunicados por el responsable, sino que se extralimitó del encargo al alimentar los datos iniciales con los suyos propios, resultado de investigar el nuevo domicilio y teléfono del deudor al objeto de localizarle y requerirle el pago de la deuda. En consecuencia, esos nuevos datos carecían de consentimiento para su tratamiento por parte del encargado".

La sentencia citada, consideró, sin embargo, que el consentimiento inicialmente otorgado al responsable para el tratamiento de los datos del cliente que resultó finalmente deudor, se "proyecta en el tiempo" y, en consecuencia, siempre y cuando los nuevos datos recabados por el encargado sean tratados para el cumplimiento de la ejecución del contrato suscrito entre el responsable y su cliente y sean necesarios para su cumplimiento, dicho tratamiento estará incluido en el ámbito del inicial consentimiento.

Por último, se debe señalar que el *encargado* del tratamiento encomendado por el *responsable* del mismo no podrá "subcontratar" con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable, salvo que hubiera obtenido de éste autorización para ello. Así se deduce a tenor de lo dispuesto en el artículo 12.2, último inciso, de la LOPD, donde señala que "*… el encargado del tratamiento… no los comunicará, ni siquiera para su conservación, a otras personas."* .

No obstante, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos, conforme dispone el artículo 21 del RLOPD:

a. Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

   Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b. Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c. Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

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

Además, si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Recuerde: El encargado de tratamiento presta servicios y trata los datos por cuenta del responsable del tratamiento. Esta vinculado contractualmente a seguir sus instrucciones y destruirlos o devolverlos. En caso contrario se convierte en responsable y el acceso en cesión que requiere consentimiento.

3. EL PRINCIPIO DE CALIDAD DE LOS DATOS: PROPORCIONALIDAD, VERACIDAD Y FINALIDAD. CANCELACIÓN, BLOQUEO Y RECTIFICACIÓN DE OFICIO POR EL RESPONSABLE

3.1 Introducción

El tratamiento de los datos de carácter personal requiere la adopción de una serie de garantías y el respeto de los principios que configuran el derecho a la protección de datos de carácter personal.

Estos principios generales definen las pautas a las que debe atenerse la recogida, tratamiento y uso de los datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información registrada como la congruencia y racionalidad de la utilización de los datos.

De entre estos principios destaca, por ser un principio fundamental, el principio de calidad de datos. Este principio ha de ser observado tanto en el momento de la recogida de los datos, dado que no podrán recogerse datos que no se adecuen a las exigencias derivadas del mismo, como en el posterior tratamiento que se realice de los datos y debe, asimismo, concurrir en el tratamiento de cualquier tipo de datos personales, sean de la naturaleza que sean.

¿Qué exigencias comporta este principio de calidad de datos?

En primer lugar, el tratamiento de los datos debe ser legítimo y leal, como recoge a nivel europeo la Directiva 95/46/CE. En consecuencia los datos deberán ser recogidos por medios lícitos, quedando prohibida la recogida de los datos por medios fraudulentos, desleales o ilícitos.

En segundo lugar, el cumplimiento del principio de calidad de datos conlleva la observancia de las siguientes obligaciones básicas:

- Proporcionalidad, que implica que sólo podrán recabarse aquellos datos que sean adecuados, pertinentes y no excesivos en relación con la finalidad para la que se hayan obtenido. Por ejemplo: sería excesivo recabar datos de orientación sexual para abrir una cuenta corriente.

- Veracidad, que exige que los datos sean exactos y actuales. P.ej.: imponer una multa de tráfico a una persona que ya no es propietaria del vehículo.

- Finalidad, que significa que los datos sólo podrán utilizarse para la finalidad o finalidades para las que hayan sido recabados. P. ej.: cargando en Internet imágenes de una cámara de video instalada por razones de seguridad.

Una adecuada comprensión del alcance de las citadas obligaciones exige el estudio de las mismas de forma detallada, y así se analizan a continuación.

3.2 Proporcionalidad de los datos

El principio de proporcionalidad en el tratamiento de los datos de carácter personal se encuentra vinculado a la finalidad, de este modo sólo podrán recabarse aquellos datos que sean necesarios para conseguir los fines que motivan su recogida.

A lo anterior ha de añadirse que el cumplimiento de la proporcionalidad exige que se opte, de entre los tratamientos que permitan conseguir los fines pretendidos, por el que menor incidencia tenga en el derecho a la protección de datos personales.

3.2.1 Datos adecuados, pertinentes y no excesivos.

El principio de proporcionalidad requiere el cumplimiento de las siguientes premisas:

- El dato que se recaba así como el tratamiento al que se somete dicho dato de carácter personal deberá ser adecuado a la finalidad que lo motiva.

- Asimismo, el dato que se recaba así como el tratamiento al que se somete deberá ser pertinente para conseguir la finalidad que legitima su tratamiento.

- No pueden recabarse datos o realizarse tratamientos que no sean necesarios para la finalidad que se persigue, es decir no pueden realizarse tratamientos excesivos.

De acuerdo con lo anterior, sólo pueden ser recabados y sometidos a tratamiento aquellos datos que sean necesarios para conseguir la finalidad legítima que se persigue, sin que sea lícito el tratamiento de los datos de forma abusiva.

Conviene recordar que este principio de proporcionalidad debe ser respetado tanto por las entidades privadas como por las Administraciones públicas, ya que éstas sólo podrán recabar datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades que tengan encomendadas.

En definitiva, en virtud de este principio, tal y como se desarrollará más adelante, el tratamiento de los datos ha de conectarse con la finalidad pretendida y deberá ser adecuado, pertinente y no excesivo en relación con aquella.

A modo de ejemplo puede citarse el supuesto analizado por la jurisprudencia española, en la Sentencia de fecha 16 de enero de 2008, dictada por la Audiencia Nacional, que declaró la confluencia de los citados elementos en la actuación de un centro médico que utilizó datos de salud concurriendo los siguientes datos fácticos:

Con motivo de la contratación de un préstamo hipotecario con una entidad bancaria, el interesado suscribió un seguro de vida. En el momento de la suscripción del seguro, el interesado cumplimentó una declaración de datos de salud en la que fue informado de que se le realizarían las siguientes pruebas médicas: examen médico, análisis de orina, electrocardiograma en reposo y análisis de sangre. Tras su aceptación, el interesado acudió a un centro medico para que le fueran realizadas las citadas pruebas médicas, entre ellas se le realizó la prueba de detección del SIDA sin que hubiera sido informado de forma expresa de la necesidad de su realización.

Se indica en la referida Sentencia que el análisis de sangre sobre la enfermedad del SIDA se realizó en el marco del contrato de un seguro de vida y considera que, si bien la expresión "análisis de sangre" utilizada para obtener el consentimiento del interesado, no revestía la concreción que resultaba exigible *por mor* del principio de calidad de datos, debía valorarse que es frecuente que se realice este tipo de análisis cuando se suscribe un seguro de vida, pues con él se busca una valoración de los riesgos que resulta adecuada a la finalidad pretendida y conocida por el interesado, por lo que concluye que este tratamiento fue adecuado, pertinente y no excesivo al existir entre la finalidad pretendida y la realización de la prueba del SIDA la necesaria coordinación.

3.2.2 Utilización de medios menos invasivos.

Ha de tenerse en cuenta que el principio de proporcionalidad supone que, siempre que resulte posible, deberán adoptarse los medios menos invasivos en la intimidad de las personas, con el fin de prevenir interferencias injustificadas en el derecho fundamental a la protección de datos y evitar tratamientos excesivos.

A nivel español, en cuanto a la proporcionalidad, nuestro Tribunal Constitucional ha tenido ocasión de referirse a ella en algunas de sus Sentencias, entre las que merece la pena destacar la Sentencia 207/1996 que determina que la proporcionalidad constituye «*una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales (...) viene determinada por la estricta observancia del principio de proporcionalidad*». Añade la referida Sentencia que «*para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el*

interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

De este modo, si la finalidad que se persigue puede ser conseguida mediante la realización de una actividad que no suponga un tratamiento de datos personales, sin que dicha finalidad se vea alterada o perjudicada, deberá optarse por dicha actividad, ya que todo tratamiento de datos personales supone, en mayor o menor medida, una limitación del derecho a la protección de datos personales.

En consecuencia, para evaluar el cumplimiento de la proporcionalidad deberá tenerse en cuenta si los fines perseguidos pueden alcanzarse del modo que menor incidencia tenga en el derecho a la protección de datos personales.

Para una mejor comprensión del principio aquí analizado se han seleccionado algunos informes dictados por la Agencia Española de Protección de Datos, en relación con el principio de proporcionalidad, en los que se analizan los supuestos de hecho sometidos a consulta y se extraen las conclusiones que a continuación se citan:

- Informe 90/2009

  (https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2009-0090_Proporcionalidad-en-el-tratamiento-de-datos-de-localizaci-oo-n.pdf)

La cuestión que se plantea en el mismo es si una empresa dedicada a prestar servicios de seguridad privada puede exigir a los escoltas que trabajaban para ella que lleven de forma continuada un terminal de telefonía, para que la empresa pueda conocer la localización geográfica del empleado, aunque no se encuentre de servicio.

Con carácter previo a determinar si el tratamiento de tales datos con la finalidad pretendida resultaba proporcional o no, se recoge en el informe que los datos de localización, ya que permiten conocer la posición geográfica del terminal de telefonía de una persona y se refieren siempre, por tanto, a una persona física, constituyen datos personales y su tratamiento debe respetar los principios que rigen el derecho a la protección de datos.

En el supuesto analizado en el informe, la finalidad que se perseguía, con el tratamiento de los datos de localización del escolta, era garantizar la seguridad de la persona escoltada. Por ello, para una adecuada solución del problema, el informe distingue entre la utilización de dichos datos para conocer el lugar geográfico en que se encuentra el empleado en horas de servicio, de la utilización de tales datos durante el tiempo libre del empleado.

Hecha la citada distinción, el informe considera acorde con el principio de proporcionalidad la utilización de tales datos en la jornada laboral del escolta pues tal uso permite mantener una conexión continuada entre el empleado y la empresa de seguridad y ello resulta acorde con el fin que se persigue de prestar un servicio de protección a las personas. Sin embargo declara contrario al principio de proporcionalidad el tratamiento de los datos de localización fuera del horario de trabajo ya que la citada finalidad no requiere este tratamiento.

El referido informe recuerda, en cuanto al principio de proporcionalidad, que están igualmente sometidos al principio de proporcionalidad los datos de la persona escoltada, ya sean datos de localización u otro tipo de datos, y que, en consecuencia, su recogida y uso deberá limitarse al necesario para garantizar su seguridad.

Sobre este particular puede citarse, en el ámbito europeo, el Dictamen 5/2005, sobre el uso de los datos de localización, del Grupo de trabajo del artículo 29, que señala que *<<el requisito relativo a la finalidad implica que un empresario no debería recoger datos de localización en relación con un empleado fuera de su tiempo de trabajo. Por consiguiente, el Grupo recomienda que se dote a los equipos puestos a disposición de los empleados, y especialmente a los vehículos que también puedan ser utilizados con fines privados, de un sistema que les permita desactivar la función de localización>>*

- Informe 113/2009

(https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2009-0113_Visualizaci-oo-n-foto-socio-en-pantalla-T.V.-cuando-accede-a-instalaciones.pdf)

Se plantea en este caso la cuestión relativa a si es proporcional la visualización en una pantalla de TV de la fotografía de los abonados a un *spa* con la finalidad de comprobar la identidad de las personas que acceden a las instalaciones del centro.

La Agencia Española de Protección de Datos consideró, en el referido informe, que la finalidad pretendida podía lograrse, igualmente, mediante la realización de otras conductas tendentes a lograr esa identificación, sin que ello llevara aparejado el tratamiento del dato de la imagen de una persona en una pantalla de TV.

En consecuencia, se consideró que el tratamiento del dato de la imagen podía vulnerar el principio de proporcionalidad, al resultar excesivo para la finalidad de identificación del abonado.

- Informe 368/2006 (https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2006-0368_Proporcionalidad-del-tratamiento-de-la-huella-dactilar-de-alumnos-de-un-colegio.pdf)

Se planteó, en este caso, si era lícito establecer un sistema de control para gestionar las ausencias y retrasos de los alumnos de un colegio, basado en la obtención de la huella dactilar de éstos. Mediante dicha huella dactilar se pretendía controlar la entrada y salida de los alumnos en el centro escolar.

Para resolver la cuestión, el informe recuerda, en primer lugar, que los datos biométricos pueden permitir identificar al individuo, por lo que su tratamiento debe respetar los principios de protección de datos.

En segundo lugar, recoge las consideraciones que, sobre la utilización de datos biométricos en centros escolares, realizan la Autoridad de Control Francesa y la Portuguesa, contenidas en el dictamen del Grupo de Trabajo del artículo 29, de fecha 1 agosto de 2003. Así, señala que sobre esta cuestión la Autoridad de Control Francesa considera que no es proporcional el uso de huellas digitales para el acceso de los niños a un comedor escolar y que la Autoridad de Control Portuguesa se muestra desfavorable a la utilización de un sistema biométrico por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente.

Finalmente concluye el referido informe que la obtención de la huella dactilar, como medio para identificar a los alumnos de un centro, resulta excesivo y desproporcionado para el fin que se persigue, ya que no se considera justificado el tratamiento de los datos de los menores de edad para las finalidades que se pretenden.

- Informe 266/2006 (https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2006-0266_Proporcionalidad-del-tratamiento-del-dato-de-la-fotograf-ii-a-de-los-trabajadores.pdf)

Se plantea en el informe si resulta adecuado al principio de proporcionalidad la obtención de la fotografía de los trabajadores de una empresa para garantizar la identificabilidad de los trabajadores a efectos de seguridad, a fin de evitar una suplantación de los mismos por terceras personas, asegurando así la integridad de las instalaciones.

En este caso se consideró que si por motivos de seguridad y para el adecuado desarrollo de la actividad de los trabajadores, resultaba necesaria la identificación de éstos, a través de la fotografía incorporada a su tarjeta, el tratamiento del dato de la fotografía del trabajador debía considerarse proporcional a la finalidad señalada.

Recuerde:

- El tratamiento de los datos debe ser legítimo y leal
- El tratamiento de los datos personales deberá ser adecuado, pertinente y no excesivo en relación con la finalidad que se persigue.
- Para el logro de dicha finalidad, deberán elegirse los tratamientos de menor ingerencia en el derecho a la protección de datos.

3.3 Veracidad de los datos. Contenido del principio.

Lo que se persigue con el principio de veracidad es que los datos personales que se recojan y se sometan a tratamiento sean exactos y respondan, en todo momento, a la situación actual de los afectados.

Por ello, únicamente podrán tratarse aquellos datos que, siendo adecuados, pertinentes y no excesivos, supongan una información exacta, y que se encuentre puesta al día de forma que responda con veracidad a la situación actual del afectado.

Así las cosas, los responsables de los ficheros o tratamientos deben adoptar las mediadas adecuadas para el cumplimiento de esta obligación, respondiendo de su incumplimiento.

El responsable del fichero o tratamiento queda obligado a comprobar la exactitud del dato debiendo desarrollar esta obligación de forma diligente a fin de evitar, por un lado, que datos inexactos accedan a su fichero y, por otro, la existencia de inexactitudes en los datos ya registrados.

De este modo, resulta esencial que antes de registrar un dato en el fichero se compruebe la veracidad de éste y que una vez registrado el dato se mantenga actualizado, realizando las rectificaciones y cancelaciones necesarias a fin de preservar la exactitud del dato.

Esta labor de verificar la exactitud del dato resulta crucial, por ejemplo, para evitar contrataciones fraudulentas en supuestos de suplantación de la identidad del titular de los datos

Puede citarse, aquí, la experiencia de la Agencia Española de Protección de Datos en estos casos de suplantación de la identidad. Estos supuestos se producen cuando la empresa que vende el producto o presta el servicio no contrata directamente con el cliente, sino que encomienda a una tercera empresa o persona la labor de captar clientes y obtener de ellos su consentimiento para la contratación. Este tercero, en algunas ocasiones, con la finalidad de obtener su comisión, formaliza contratos, sin que el titular de los datos utilizados haya consentido la contratación, y presenta al responsable del fichero o tratamiento documentos que no han sido firmados por el verdadero titular de los datos. En definitiva este tercero recaba los datos de forma fraudulenta.

Si los datos de la persona que no contrató son registrados finalmente en el fichero de la empresa que vende el producto o presta el servicio en calidad de cliente, y se facturan servicios no contratados, se habrá producido una vulneración del principio de consentimiento y del de calidad de datos al no reflejar el fichero la situación real del titular de los datos, ya que éste no contrató. Por ello, para evitar que los datos de las personas que no han contratado accedan al fichero, la Agencia exige que se adopten las medidas necesarias tendentes a verificar la identidad del cliente, como por ejemplo exigir la presentación de una copia del documento nacional de identidad del contratante, o confirmar la contratación con el titular de los datos que obran en el contrato. Estas comprobaciones sobre la exactitud de los datos deberán realizarse de forma diligente.

3.3.1 Supuestos que vulneran el principio de veracidad

Como se ha dicho, debe evitarse el tratamiento de datos inexactos, es decir de datos erróneos.

Como ejemplo de incumplimiento del principio de veracidad puede citarse la conducta de una empresa, a la que impuso una sanción la Agencia Española de Protección de Datos que fue, posteriormente, confirmada por la Audiencia Nacional, en la Sentencia de 3 de noviembre de 2004, que incluyó en un fichero de solvencia patrimonial los datos de una persona, a pesar de que había sido exonerada, en Sentencia firme, del pago de la deuda que se le reclamaba.

Afirma la referida Sentencia, de 3 de noviembre de 2004, que el principio de calidad de datos comienza a infringirse en el momento en que se facilitan datos erróneos a un fichero que presta información a terceros sobre el incumplimiento de obligaciones dinerarias. En el caso enjuiciado la información que se registró en el fichero de solvencia patrimonial no respondía verazmente a la situación del afectado dado que hacía referencia a su condición de deudor de una deuda de la que había sido absuelto por Sentencia firme.

Recuerda, finalmente, esta Sentencia la necesidad de exigir una especial diligencia a las entidades que tratan datos personales, que deben mantener estos al día, de conformidad con el principio de calidad de datos, como obligación que debe ser cumplida con suma diligencia.

También cabe citar, en este punto, la resolución de la Agencia de Protección de Datos recaída en el "Procedimiento Nº PS/00195/2004", que sancionó a una compañía de telecomunicaciones por facilitar a un fichero de solvencia patrimonial información relativa al impago de una deuda, asociando los datos relativos a la deuda y a su cliente moroso al número de documento nacional de identidad de otro cliente que no tenía ninguna deuda pendiente.

Este segundo cliente se enteró, casualmente, que sus datos estaban registrados en un fichero de la citada naturaleza, por lo que solicitó la cancelación de los mismos. La incidencia fue cancelada, pero con posterioridad fue registrada de nuevo, conteniendo el mismo error que el ya puesto de manifiesto, es decir los datos relativos a la deuda seguían figurando asociados al número del documento nacional de identidad del cliente que no tenía deudas con la entidad.

La referida resolución fue recurrida ante la Audiencia Nacional, que en Sentencia, de 18 de julio de 2007, confirmó la sanción impuesta por la Agencia Española de Protección de Datos, aduciendo que se produjo un tratamiento de datos personales con conculcación del principio de calidad desde el momento en que el número de documento nacional de identidad del cliente de la compañía de telecomunicaciones que no tenía ninguna deuda con dicha empresa, se asoció a una deuda de otro cliente de la entidad y se comunicaron dichos datos inexactos al fichero de solvencia patrimonial, de tal modo que aquél, a través de su documento nacional de identidad, aparecía en dicho fichero conectado con una deuda que no era suya.

¿Cualquier error supone infracción del principio de calidad de datos? ¿Qué ocurre con los errores materiales?

Para que exista una inadecuada utilización de los datos de carácter personal el error ha de ser relevante y no ha de consistir en un mero error material sin transcendencia externa. No puede calificarse de infracción del principio de calidad de datos un simple error, que no ocasiona ningún perjuicio al afectado, si no comporta una falta de diligencia en el tratamiento de los datos personales, es decir si el error se corrige en cuanto se tiene conocimiento de su existencia.

Este tipo de errores, como por ejemplo consignar en un contrato o en una factura datos identificativos de otros clientes, como nombre y apellidos, o remitir dichos documentos a una dirección errónea del cliente, podrían servir como base para ejercitar el derecho de rectificación pero no deben ser considerados como una vulneración del principio de calidad de datos, siempre que el responsable del fichero o del tratamiento actúe diligentemente cuando se detecten.

Sobre este punto puede traerse a colación la doctrina sentada en España por la Audiencia Nacional, en su Sentencia de 17 de marzo de 2004, al señalar que no puede sancionarse "*un error al teclear el número de la cuenta de cargo*" pues "*(...) cualquier error de anotación, por nimio que fuese, en los movimientos de cualquier cuenta corriente constituiría una infracción grave de la Ley Orgánica 15/1999, conclusión ésta que por su misma desproporción resulta inaceptable*". Si bien la citada afirmación ha de ser matizada como señala la referida Sentencia al indicar que "*si se constatase que hubo una utilización inadecuada de datos de carácter*

personal existiría una infracción imputable a la entidad recurrente aunque la conducta se hubiese realizado por un simple error"

Los hechos sometidos a debate en dicha Sentencia tienen que ver con una compra de valores y su posterior venta efectuadas sin la autorización de los titulares de una cuenta bancaria vinculada a los movimientos de una cartera de valores en la que, por error al teclear el número de la misma, fueron consignados el cargo y abono respectivos de aquellas operaciones.

Tomando en consideración tales hechos, concluye la referida sentencia que "*no cabe afirmar que la entidad bancaria demandante utilizase los datos de carácter personal de los denunciantes con una finalidad distinta de aquélla para la que habían sido recabados, pues se trataba de una cuenta corriente vinculada a los movimientos de una cartera de valores y lo que hizo el banco no fue sino hacer con cargo a dicha cuenta una determinada operación de compra de acciones, y luego el abono de la venta"* y califica el hecho de que hubiese un error al imputar a la cuenta de los denunciantes una concreta operación que ellos no habían ordenado de "*anomalía en la mecánica bancaria".*

En definitiva, no cabe calificar de infracciones del principio de calidad de datos los supuestos en los que los datos se tratan de acuerdo con el fin que los justifica, pero se producen errores en el tratamiento que no ocasionan perjuicios para el afectado, siempre que sean corregidos inmediatamente por el responsable, cuando se detecten.

¿Qué ocurre si es el propio interesado el que facilita los datos erróneos? En este caso podría acogerse, como regla general, la ausencia de responsabilidad del que trata el dato. Puede citarse aquí la regla que recoge la legislación española en orden a que se considerarán exactos los datos facilitados por el afectado, con lo que se evita que las inexactitudes que cometa el propio afectado al facilitar sus datos personales puedan ser consideradas como infracciones del principio de calidad de datos, de las que deba responder el responsable del fichero o tratamiento.

Ahora bien, esta regla general debe ser matizada y no puede entenderse en el sentido de exonerar, en todo caso, al responsable del fichero o tratamiento de realizar las comprobaciones precisas respecto de cualquier dato que se le facilite.

Así no le exime de realizar las verificaciones necesarias para comprobar la identidad de la persona que entrega los datos, pues sólo se presumen válidos los datos recibidos del propio afectado y no los que entregue un tercero haciéndose pasar por él. Esta labor de comprobar la identidad de la persona que facilita los datos debe realizarse respecto de los datos identificativos de la persona, que se extenderá a la verificación de la exactitud del número de documento nacional de identidad que se declara, por error o por voluntad del declarante, como propio, evitando que se incorpore al fichero el documento nacional de otra persona que la identifica de forma unívoca.

Como ejemplo puede destacarse un supuesto analizado por la Agencia Española de Protección de Datos en el que un cliente facilitó al contratar un número de documento nacional de identidad erróneo, que resultó ser el de otra persona, induciendo a error a la entidad, que facilitó, ante la falta de pago, a un fichero de solvencia patrimonial los datos de su cliente asociados al número de documento nacional de identidad de la otra persona. En este caso, el error o inexactitud afectó a la esfera personal de otra persona, que no había contratado, por lo que se consideró que la entidad pudo haber evitado el error de haber efectuado las comprobaciones precisas.

Recuerde que:

- Los datos personales deben ser exactos y actuales.
- Cuando se obtiene un dato personal deberá comprobarse la veracidad de éste y una vez sometido a tratamiento deberá mantenerse actualizado.

3.4 Finalidad de los datos

El principio de finalidad supone, de un lado, que los datos de carácter personal sólo pueden utilizarse para finalidades determinadas, explícitas y legítimas y, de otro, que los datos no podrán utilizarse para finalidades distintas de aquellas para las que los datos se hubiesen recogido.

Además, en este punto, conviene recordar que sólo pueden someterse a tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido.

3.4.1. Finalidades determinadas, explícitas y legítimas.

La primera cuestión que se plantea, en relación con este asunto, es si ¿pueden recabarse datos para cualquier tipo de finalidad? La respuesta ha de ser afirmativa siempre que la finalidad a la que se destinen los datos sea determinada, explícita y legitima y el afectado haya prestado, como regla general, su consentimiento para que sus datos sean tratados con esa finalidad.

En definitiva, la finalidad a que se destinarán los datos debe reunir los siguientes requisitos:

- Ha de ser determinada, pues los datos deberán ser recabados para unas finalidades concretas que justifiquen el tratamiento, sin que sea posible la existencia de finalidades genéricas.
- Deberá ser explícita, es decir el tratamiento de los datos de carácter personal deberá estar fundamentado en una finalidad clara sin que sea lícita la existencia de tratamientos con finalidades confusas.
- La finalidad deberá ser legítima

De lo anterior se colige que el cumplimiento de este principio implica, en primer lugar, una determinación clara de los fines para los que se recogen los datos y que la finalidad del fichero esté determinada de forma explícita y sea legitima, careciendo de validez la recogida de datos con finalidades indeterminadas o tan vagas o genéricas que admitan cualquier propósito.

3.4.2. Desvío de finalidad

Según el principio de finalidad los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades distintas o incompatibles con aquellas para las que los datos hubieran sido recogidos, pues de lo contrario se estaría incurriendo en u desvío de finalidad que podría ser sancionado como incumplimiento del principio de calidad de datos. Por tanto si la recogida de datos de carácter personal se realizó con unos fines determinados, no será conforme con el principio de calidad de datos un uso o tratamiento posterior que no esté en consonancia con dichas finalidades.

Los datos no pueden ser tratados para fines distintos a los que motivaron su recogida pues esto supondría un nuevo uso que requiere el consentimiento del interesado.

Ha de tenerse en cuenta, como anteriormente se expuso, que debe existir una nítida conexión entre los datos personales que se recaban y el uso para el que se solicitan los datos.

¿Cuándo se considerara producido un desvío de finalidad?

Para facilitar la comprensión sobre cuándo ha de considerase que los datos han sido utilizados para finalidades distintas o incompatibles con las que motivaron su recogida, puede citarse como ejemplo el caso examinado por el Tribunal Constitucional español, en Sentencia de 13 de enero de 1998, que puede servir de indicador para aclarar las dudas relativas a las finalidades a las que no podrá destinarse el tratamiento.

En la citada Sentencia se analiza un supuesto en el que una empresa ante la realización de una huelga, convocada por varios sindicatos, y debido al difícil seguimiento de la misma por parte de la empresa, utilizó el dato de afiliación sindical, facilitado por los trabajadores para el cobro de la cuota sindical, para practicar en las retribuciones correspondientes al mes en que se realizó la huelga la retención correspondiente al seguimiento de aquella. Dicho descuento se

realizó de forma generalizada a las personas afiliadas a los sindicatos convocantes de la huelga, la hubieran secundado o no. Se presumió la participación en la huelga por el hecho de pertenecer a un sindicato, atentando no sólo contra el derecho fundamental a la protección de datos, al utilizar datos especialmente protegidos para una finalidad distinta a aquella para la que fueron facilitados, sino también contra el derecho a la libertad sindical.

3.4.3 Deber de informar

Resulta conveniente recordar brevemente la cuestión relativa a la obligación de informar, pues el principio de finalidad está directamente relacionado con el principio de información.

El deber de informar, también denominado principio de transparencia, requiere, con independencia de que sea preciso el consentimiento del afectado para el tratamiento de sus datos o de que los datos no sean recogidos directamente de aquél, que éste sea informado de la finalidad de la recogida de aquéllos.

Esta obligación deberá ser cumplida sea cual sea la forma en la que se recaben los datos, por ejemplo ya sea por escrito, telefónicamente o a través de un sitio web.

Así las cosas, cuando se recaban datos del propio afectado y se solicita su consentimiento para el tratamiento de dichos datos, deberá ser informado, entre otros aspectos y con carácter previo a la recogida, de la finalidad para la que se recaban sus datos personales.

Lo anterior supone que cuando el tratamiento de los datos requiera el consentimiento del afectado, la solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, de modo que si los datos se destinan a finalidades distintas será necesario el consentimiento de los afectados.

De esta manera el consentimiento queda vinculado a las finalidades determinadas, específicas y legítimas que justifican el tratamiento de los datos.

Recuerde:

- Las finalidades a las que se destinen los datos deberán ser determinadas, explícitas y legítimas.
- Los datos no pueden ser utilizados para finalidades distintas de aquellas que justificaron su recogida.
- Los interesados deberán ser informados de la finalidad para la que se recaban sus datos.

3.5 Cancelación, bloqueo y rectificación de oficio por el responsable.

3.5.1 Cancelación de oficio y bloqueo de los datos

El principio de calidad de datos implica, entre otras cosas, que los datos sean necesarios y pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Por lo tanto, la consecuencia lógica que se desprende de la citada regla es que los datos sean cancelados cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales fueron recabados o registrados, sin necesidad de solicitud previa del afectado, es decir sin necesidad de esperar a que el afectado ejercite su derecho de cancelación.

Aquí se pone de manifiesto otra vez la conexión entre los datos y las finalidades que determinaron su recogida, pues el principio de finalidad está presente durante todo el proceso al que se somete el dato, desde su recogida hasta su cancelación (C. LESMES SERRANO, 160).

Esta obligación incumbe al responsable del fichero o tratamiento que deberá proceder de oficio y con la debida diligencia a cancelar los datos que han dejado de ser necesarios para la finalidad del fichero.

A lo anterior ha de añadirse que el responsable del fichero o tratamiento debe velar por la exactitud de los datos realizando, también de oficio, las cancelaciones o rectificaciones que fueran precisas cuando los datos sean inexactos o incompletos.

En resumen, el principio de calidad de datos requiere, por lo que respecta a este tema de la cancelación de oficio, de un lado, que los datos de carácter personal sean cancelados cuando se haya cumplido o haya desaparecido la finalidad que justificaba su tratamiento y, de otro, que los datos erróneos sean cancelados o rectificados a fin de preservar el principio de veracidad o exactitud.

¿Cómo debe realizarse esta cancelación de los datos? ¿La cancelación supone el borrado físico de los datos?

Si se produjera el borrado físico de los datos cuando dejaran de ser necesarios para la finalidad que justificó su tratamiento, como sucedería en los casos en los que se hubieran extinguido las relaciones contractuales que vinculaban al responsable del fichero o tratamiento con su cliente, no podrían exigirse responsabilidades posteriores. Además algunas leyes imponen la obligación de conservar los datos durante ciertos plazos.

Si se eliminaran los datos tras el cumplimiento de tales finalidades no podrían, por ejemplo, ejercitarse las acciones judiciales, previstas en la legislación civil o mercantil, que procedieran con base en la relación jurídica que justificó el tratamiento. Tampoco podrían exigirse, por ejemplo, responsabilidades por el incumplimiento de obligaciones tributarias al no existir los datos que podrían acreditarlo.

Por ello, una solución adecuada al problema planteado podría ser la adoptada por la normativa española que determina que la cancelación deberá producirse, en un primer momento, mediante el bloqueo de los datos de carácter personal. El bloqueo deberá mantenerse durante los plazos previstos en las disposiciones legales aplicables o, en su caso, durante el tiempo en que pueda exigirse algún tipo de responsabilidad, derivada de una relación jurídica, o, en general, del tratamiento, y sólo durante el plazo de prescripción de dichas responsabilidades.

En un momento posterior, cumplidos tales plazos, se debe proceder a la supresión de los datos. Ahora bien, en estos casos, los datos podrán conservarse si tal

conservación se realiza de forma que no resulte posible identificar a los interesados, es decir si los datos se conservan de forma que sean anónimos, sin que puedan ser asociados a una persona identificada o identificable. Contrariamente si los datos permiten la identificación de los interesados deberán ser cancelados.

Ha de tenerse en cuenta que pueden, asimismo, conservarse determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con la legislación específica que les resulte aplicable, con dichas finalidades históricas, estadísticas o científicas.

La legislación española requiere, para que en estos casos pueda procederse a la conservación de los datos, que la Agencia Española de Protección de Datos declare previamente, a petición del interesado, la concurrencia en el tratamiento de datos para el que se solicita la declaración de valores históricos, científicos o estadísticos.

¿En qué consiste el bloqueo de los datos? El bloqueo se asimila a la cancelación de datos, por ello deberá realizarse de forma que los datos no puedan seguir siendo tratados. Para que sea efectivo deberá producir unos efectos similares al borrado físico de los datos. El bloqueo supone el cese en el uso de los datos, lo que puede conseguirse impidiendo que sea posible el acceso a los datos o su tratamiento por parte del personal que habitualmente realiza estas gestiones. Sólo será lícito el acceso a los datos bloqueados cuando exista un requerimiento judicial o administrativo a tal efecto, sin que, consecuentemente, los afectados puedan ejercitar los derechos de acceso, rectificación, cancelación y oposición respecto de tales datos. De este modo, quedaría asimilado el bloqueo a la supresión o eliminación de los datos.

Sobre esta cuestión puede citarse la definición de cancelación de datos que perfila el Reglamento de desarrollo de la Ley de Protección de Datos, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en cuyo artículo 5.b) recoge la siguiente declaración: "*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".

3.5.2 Rectificación de oficio

La actualización de los datos puede hacerse bien de oficio o bien mediante el ejercicio del derecho de rectificación o cancelación, a través del cual el afectado puede solicitar al responsable del fichero la rectificación o cancelación de los datos que sean inexactos o incompletos. El responsable debe velar por la veracidad de la información y procurar que la información incluida en el fichero esté permanentemente actualizada.

Así las cosas, si el responsable del fichero o tratamiento observara que los datos son inexactos o no actuales deberá realizar de oficio las rectificaciones que fueran necesarias para asegurar la calidad del dato. Además, si los datos que se rectifican o cancelan hubieran sido cedidos previamente, el responsable del fichero o tratamiento deberá notificar al cesionario la rectificación o cancelación efectuada con la finalidad de que éste proceda, respecto de los tratamientos que realiza, a la rectificación o cancelación notificada.

Como ejemplo puede citarse el supuesto de hecho del que trae causa el "Procedimiento Nº PS/00167/2004" tramitado en la Agencia Española de Protección de Datos. En este caso una persona había contratado, a través de Internet, distintos productos financieros con una determinada entidad bancaria, suscribiendo para ello un formulario electrónico en el que hizo constar su nuevo domicilio. El banco quedó comprometido a remitirle la documentación por correo postal para que fuera firmada por la interesada.

Ante el retraso en recibir la documentación que debía firmar, la interesada se puso en contacto telefónico con el banco que le informó que la documentación se había remitido a su antiguo domicilio, cuya dirección obraba ya en los ficheros del banco.

El banco remitió de nuevo la documentación, pero en esta ocasión al domicilio indicado por la interesada. Ésta cuando recibió la documentación que debía firmar

incorporó los datos relativos a su nuevo domicilio. Sin embargo, el banco volvió a remitirle a su antiguo domicilio las tarjetas de crédito que había contratado, sin proceder a rectificar el dato erróneo.

La Agencia Española de Protección de Datos sancionó a la entidad bancaria porque tras haber facilitado su cliente los datos de su domicilio actual, continuó remitiéndole documentación bancaria, incluidas las tarjetas de crédito, a un antiguo domicilio familiar, sin haber procedido a la actualización del dato.

La sanción impuesta fue posteriormente confirmada por la Audiencia Nacional, en su Sentencia de fecha 30 de noviembre de 2006, en la que se afirma que "*por lo que se sanciona es por la obligación de mantener la exactitud de los datos una vez que es el propio titular del dato quien facilita la rectificación del mismo y esa rectificación no es atendida por el banco titular del fichero*"

Recoge la citada Sentencia la obligación del responsable del fichero o tratamiento de rectificar o completar de oficio los datos de carácter personal que fueran inexactos o incompletos y señala que la responsabilidad de la entidad bancaria sancionada procede del hecho de que, conociendo la inexactitud de su base de datos en la que figuraba un domicilio que no era el actual del cliente, no procedió a la correspondiente rectificación o modificación.

Finalmente, en cuanto a la observancia del deber de diligencia, apunta que dicha diligencia faltó desde el momento en que a pesar de que el cliente aportó su nuevo domicilio, el banco siguió remitiendo documentación de interés al antiguo domicilio, sin actualizar su base de datos.

Resumen:

- Los datos de carácter personal deberán ser tratados de forma leal y lícita.
- Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
- Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
- Los datos personales serán cancelados de oficio cuando hayan dejado de ser necesarios para los fines para los cuales fueron recabados.
- La cancelación dará lugar al bloqueo de los datos, quedando los datos cancelados exclusivamente a disposición de las Administraciones públicas, Jueces y Tribunales, durante el plazo previsto en las disposiciones legales aplicables o de prescripción de las posibles responsabilidades nacidas del tratamiento.
- Cuando concurren en un determinado tratamiento de datos valores históricos, científicos o estadísticos, los datos podrán ser conservados.
- Si los datos resultaran ser inexactos o incompletos, el responsable del fichero o tratamiento deberá proceder a la rectificación de oficio de los datos.

4. LA TUTELA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS (ENFORCEMENT)

Recuerde:

El cumplimiento de la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo, es un imperativo legal emanado del marco normativo de la Unión Europea. Las previsiones y mandatos contenidos en esta normativa se encuentran bajo el control de la Agencia Española de Protección de Datos, órgano de la Administración independiente, con personalidad jurídica propia, y con potestad sancionadora.

El derecho fundamental a la protección de datos, que supone el reconocimiento al ciudadano de la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos, es un derecho fundamental que deriva directamente de la Constitución, en concreto del artículo 18.4. En desarrollo del citado artículo fue aprobada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD).

La citada Ley garantiza una serie de derechos a las personas físicas, titulares de los datos, tales como el derecho a ser informado de cuándo y por qué se tratan sus datos personales, el derecho a acceder a los datos y, en caso necesario, el derecho a la modificación o supresión de los datos o el derecho a la oposición al tratamiento de los mismos.

La normativa española en materia de protección de datos se encuentra además armonizada con la europea, en concreto a la Directiva Europea 95/46/CE de 24 de octubre, del Parlamento Europeo y del Consejo, 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. Ésta normativa exige que todos los países miembros de la Unión dispongan de una autoridad independiente que garantice y tutele tal derecho.

Como consecuencia de la transposición que de dicha normativa comunitaria se realizó a través de la Ley Orgánica 15/1999, en esta Ley se encomendó la tutela y garantía del derecho a la protección de datos a la Agencia Española de Protección de Datos.

Por tanto, la Agencia Española de Protección de Datos (en lo sucesivo AEPD) es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales, actuando para ello con plena independencia de las Administraciones Públicas.

En cuanto a la efectividad de la protección de datos, depende del correcto funcionamiento de ésta Autoridad tanto en su dimensión preventiva, como en la dirigida a restablecer el cumplimiento de la norma en caso de infracción.

Para ello, es decir, para la consecución de una mayor efectividad en la protección de datos, la característica de la independencia de la AEPD supone la garantía de su actuación sin sometimiento a ningún otro criterio que no sea la propia normativa reguladora de la materia y, por tanto, evita posibles interferencias en la defensa del citado derecho fundamental.

Por lo que respecta a las funciones de la Agencia dirigidas al restablecimiento del cumplimiento de la norma en caso de incumplimiento o infracción, la LOPD le otorga las potestades administrativas de inspección, sancionadora y de resolución de las reclamaciones de los afectados (tutela de derechos).

En cuanto a la normativa que contiene las bases para el ejercicio de estas funciones, además de la LOPD, hay que tener en cuenta su Reglamento de desarrollo aprobado mediante el Real Decreto 1720/2007, de 21 de Diciembre (en adelante RLOPD).

Por otra parte, en España junto con la AEPD, coexisten otras autoridades de control que se han ido constituyendo en el plano autonómico con competencias de actuación o de control.

Actualmente existen tres Agencias Autonómicas de Protección de Datos: la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

En síntesis, la tutela del derecho fundamental de la protección de datos se lleva a cabo desde estas Agencias en base al siguiente reparto:

- ✓ La AEPD tiene la competencia:

    1. exclusiva de control de todos los ficheros de titularidad privada.

    2. Respecto al control de ficheros de titularidad pública, la AEPD es competente respecto de los ficheros a la Administración del Estado y de los de las Administraciones autonómica y local de las CCAA que no cuenten con Agencia propia de control.

- ✓ Las Agencias autonómicas ya constituidas y citadas con anterioridad tienen competencia respecto de los ficheros de titularidad pública de las administraciones autonómica y local de sus respectivos ámbitos territoriales.

Con el objetivo de garantizar el cumplimiento del derecho de protección de datos de los ciudadanos, existen ciertos mecanismos de cooperación y coordinación entre las diferentes Agencias, Central y Autonómicas.

Recuerde: La AEPD, así como el resto de autoridades de garantía de este derecho, realizan en el ámbito de sus competencias las actuaciones necesarias dirigidas a:

- ✓ TUTELAR al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos por los responsables de los ficheros.

- ✓ GARANTIZAR el derecho a la protección de datos investigando aquellas actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la LOPD e imponer, en su caso, la correspondiente sanción.

El ejercicio de las funciones de control de todas estas autoridades, junto con otras que se desarrollan desde el plano normativo y divulgativo, determina que las autoridades de control sean en la práctica intérpretes cualificados del derecho fundamental a la protección de datos personales.

4.1 Tutela de Derechos

Los poderes de disposición y control de los ciudadanos sobre sus propios datos personales, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los mismos, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Y ese derecho a consentir el conocimiento y el tratamiento de los datos personales, supone:

- ✓ por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y,
- ✓ por otro lado, el poder rectificar o cancelar esos datos personales.
- ✓ Asimismo, el poder oponerse a esa posesión y usos.

Todo ello se concreta en el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición.

4.1.1 El ejercicio de estos derechos:

En orden a una mejor comprensión del objetivo, alcance y contenido de la actuación de la Agencia en sus funciones de tutela de derechos, resulta necesario recordar previamente al examen de dicha función lo relativo al ejercicio de los derechos objeto de tutela, por ser requisito necesario para la posterior actuación garantista de la Agencia.

Los derechos de acceso, rectificación, cancelación y oposición tienen carácter personalísimo, es decir, sólo pueden ejercerse por el titular de los mismos o por su representante legal. No obstante, podrá encomendarse su ejercicio a un representante, siempre que el mismo pueda acreditar suficientemente tal condición.

Para el ejercicio de estos derechos, que tiene carácter gratuito, el interesado tiene que dirigirse al responsable del fichero o tratamiento, aportando fotocopia del DNI o documento que acredite la identidad y sea admitido en Derecho, o en caso de representación, documento acreditativo de la misma, e indicando el domicilio a efectos de notificaciones, la fecha y firma del solicitante.

En el caso de que la solicitud no reúna los requisitos establecidos en la norma (p. ejemplo, falta DNI, documentos que acrediten la petición, etc.), el responsable del fichero deberá solicitar la subsanación.

Al objeto de posibles reclamaciones posteriores, y al objeto de servir de prueba, los interesados deben utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

El responsable del fichero o tratamiento tiene la obligación de hacer efectivo el derecho solicitado debiendo contestar de forma motivada a la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros. Asimismo, puede denegarse el derecho o derechos solicitados en los supuestos legalmente previstos (por ejemplo, no conceder el derecho de acceso por razones de seguridad pública, denegar el derecho de oposición cuando el interesado no motiva y justifica su ejercicio (en el supuesto legalmente exigible tal justificación), no cancelar cuando existe una relación jurídica que motiva el tratamiento del dato, etc.)

Asimismo y a fin de que sirva como medio de prueba ante posibles reclamaciones, la contestación que realice el responsable del fichero o tratamiento a la solicitud por la que se ejercita el derecho, ha de practicarse utilizando cualquier medio que permita acreditar el envío y la recepción de la misma.

En la página web de la Agencia se encuentran disponibles los modelos de solicitudes para ejercitar los derechos ante el responsable del fichero o del tratamiento.

4.1.1.1 Ejercicio derecho de acceso (arts. 15 de la LOPD, 27, 28, 29 y 30 RLOPD).

Mediante el ejercicio del derecho de acceso la persona puede dirigirse al responsable del fichero o encargado del tratamiento y así controlar tanto la existencia y totalidad de los datos de que dispone, su exactitud, origen, posibles destinatarios y finalidades del tratamiento. (Por ejemplo datos de solvencia en un fichero de morosos).

Esta información puede obtenerse bien mediante la mera consulta de los datos por medio de su visualización en pantalla, o bien a través de escrito, copia, telecopia o fotocopia, certificada o no, realizada en forma inteligible, sin utilizar claves o códigos que requieran para su comprensión el uso de dispositivos mecánicos específicos.

El derecho de acceso sólo podrá ejercitarse a intervalos no inferiores a doce meses, salvo que se justifique un interés legítimo que posibilite su ejercicio con anterioridad al cumplimiento de dicho período.

El responsable del fichero o tratamiento tiene que resolver la solicitud de acceso en el plazo máximo de un mes a contar desde la fecha en que haya recibido la solicitud. En caso de estimar la solicitud, el acceso debe hacerse efectivo en el plazo de los diez días siguientes a la notificación.

4.1.1.2.- Ejercicio derecho de Rectificación (arts. 16 LOPD, 31, 32 y 33 RLOPD)

Mediante el ejercicio de este derecho, se posibilita al interesado que constata que sus datos personales figuran en un fichero de forma inexacta o incompleta a dirigirse al responsable, mediante la correspondiente solicitud, para que proceda a la rectificación de sus datos que resulte pertinente. P. ej.: rectificación de dirección.

La solicitud de rectificación debe indicar el dato que se estima erróneo y la corrección que debe realizarse, debiendo acompañar la documentación justificativa de la rectificación solicitada.

El responsable del fichero o tratamiento tiene el deber de atender la solicitud de rectificación en el plazo de diez días naturales.

Si los datos rectificados hubieran sido cedidos previamente a un tercero, el responsable del fichero tiene la obligación de notificar al cesionario la rectificación practicada.

4.1.1.3.- Ejercicio del Derecho de cancelación (art. 16 LOPD, 31,32 y 33 RLOPD)

Este derecho concede al interesado la posibilidad de dirigirse al responsable solicitando la cancelación de sus datos personales que resulten inadecuados o excesivos.

En la solicitud de cancelación, el interesado debe indicar el dato o datos que desea que sean cancelados del fichero. P. ej.: cancelación de datos incluidos en un blog o página web.

Cuando sea preciso conservar los datos de los que se ha solicitado la cancelación, por resultar necesario que los mismos estén a disposición de las Administraciones Públicas, Jueces y Tribunales, la cancelación se efectuará a través del bloqueo, quedando los datos bloqueados únicamente a disposición de las instancias citadas. El bloqueo tendrá una duración equivalente al plazo de prescripción de las responsabilidades que motivan su permanencia, debiéndose proceder a la total supresión de los datos una vez cumplido dicho plazo.

El responsable del fichero o tratamiento tiene la obligación de hacer efectivo el derecho de cancelación en el plazo de diez días naturales.

Si los datos cancelados hubieran sido cedidos previamente a un tercero, el responsable del fichero deberá notificar al cesionario la cancelación efectuada.

4.1.1.4.- Ejercicio del Derecho de Oposición (arts. 6.4, 17,30 LOPD y 34, 35 y 36 del RLOPD)

Toda persona tiene la posibilidad de oponerse a que no se lleve a cabo el tratamiento de sus datos o éste cese. Este derecho se produce respecto de unos determinados supuestos que están recogidos en el artículo 34 del Reglamento de la LOPD.

Estos son:

- ✓ "cuando no sea necesario su consentimiento para el tratamiento y siempre que una Ley no disponga lo contrario". En este supuesto puede plantearse el derecho de oposición siempre que se justifique un motivo legítimo y fundado referido a su concreta situación personal.

- ✓ "cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial"

- ✓ "cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal"

El responsable del fichero o tratamiento tiene un plazo máximo de diez días a contar desde la recepción de la petición para resolver la solicitud de oposición.

4.1.2.- El procedimiento de tutela de derechos. (arts. 18 LOPD y 117,118 y 119 del RLOPD)

Recuerde:

El procedimiento de tutela tiene por finalidad garantizar el ejercicio efectivo por parte de los interesados de los derechos de acceso, rectificación, cancelación y oposición.

Si un ciudadano ejercita los derechos descritos en el apartado anterior y no recibe respuesta a su solicitud o, a su juicio, la contestación no resulta adecuada puede

dirigirse a la Agencia Española de Protección de Datos para solicitar la tutela de estos derechos, para lo cual se instruirá el correspondiente procedimiento.

Se trata de un procedimiento específicamente contemplado en la LOPD y en el RLOPD, que, para poder iniciarse, tiene como premisa previa la denegación de un derecho a un ciudadano consistente en, o bien, no dar respuesta a la solicitud realizada, o bien, no permitir el acceso a sus datos personales, negarse a modificarlos, cancelarlos o bloquearlos, según el caso. Este procedimiento especial se denomina Tutela de Derechos.

El objetivo de este procedimiento, a diferencia del procedimiento sancionador, no es castigar el posible incumplimiento de la ley por un responsable de tratamiento, sino garantizar el efectivo ejercicio de los derechos de los ciudadanos. No tiene carácter punitivo sino reparador. El procedimiento prevé una aproximación entre las partes, por medio de un intermediario, la AEPD o alguna de las Agencias autonómicas según su competencia, que tomará la decisión final.

En consecuencia, este procedimiento, a diferencia también del procedimiento sancionador, se inicia siempre a instancia de la parte interesada, a través del correspondiente escrito de reclamación o solicitud de tutela de derechos. Al ser el ejercicio del derecho personalísimo, también la interposición de la reclamación debe realizarse por el propio interesado o su representante legal o autorizado expresamente para ello por el interesado.

Por otra parte, para solicitar la tutela de derechos, el ciudadano tiene que presentar en la AEPD su escrito de reclamación, en el que, además de constar sus datos, deben expresarse con claridad el contenido de la reclamación y los preceptos de la LOPD que considere vulnerados.

Después de recibir una de estas reclamaciones, se nombra un instructor para tramitar el expediente. Su primera acción es remitir al responsable del fichero o del tratamiento la reclamación del ciudadano, instándole para que, en el plazo de quince días, presente las alegaciones que estime pertinentes.

Tras recibir la respuesta, el instructor puede remitirla al interesado para obtener sus comentarios respecto de las alegaciones del responsable y éstos pueden ser, de nuevo, enviados al responsable para que pueda realizar sus comentarios finales.

También existen otras posibilidades a disposición del instructor en caso de que estime necesario utilizarlas, incluyendo la obtención de información adicional de otras fuentes.

Tomando en consideración todos los elementos y la legislación aplicable, el instructor redacta un borrador de resolución y, tras considerar todos los elementos del caso, el Director de la AEPD adopta la resolución final motivada.

Como antes se señaló, los procedimientos de tutela de derechos no tienen carácter sancionador, y por tanto se limitan a estimar o desestimar las reclamaciones planteadas por los ciudadanos ante la AEPD. Ello con independencia de que, en algunas ocasiones, los hechos constatados en los citados procedimientos puedan dar lugar a la iniciación de procedimientos sancionadores.

En el supuesto de que en la resolución se estime la reclamación planteada, en la misma se insta al responsable para que en el plazo de diez días atienda la solicitud y conceda el derecho solicitado o bien, en los supuestos legalmente previstos, lo deniegue motivadamente.

La resolución deberá dictarse en el plazo máximo de 6 meses; transcurrido dicho plazo sin que se haya adoptado resolución expresa se entenderá estimada la reclamación como consecuencia del silencio positivo.

Las resoluciones del Director de la Agencia Española de Protección de Datos son firmes en vía administrativa por lo que, contra las mismas, sólo se podrá interponer recurso potestativo de reposición, y el recurso contencioso-administrativo ante la Audiencia Nacional.

Como consecuencia de las previsiones del artículo 116 del RLOPD, una vez dictadas las resoluciones de tutelas de derechos se publicarán; para ello, se insertan en el sitio web de la AEPD dentro del plazo de un mes contado desde su notificación a los interesados.

En la página web de la Agencia se encuentran disponibles los modelos para interponer la reclamación y, por tanto, solicitar la tutela de la AEPD.

Gráfico 1

CIFRAS COMPARATIVAS DE TUTELAS DE DERECHOS			
	2006	2007	2008
PROCEDIMIENTOS INICIADOS	630	896	1687
RESOLUCIONES	552	849	1229

Gráfico 2

DERECHOS EJERCIDOS Y SENTIDO DE LA RESOLUCIÓN RECAIDA TUTELAS EN 2008

(Nota: el apartado otros que figura con asterisco se refiere a inadmisiones, archivos y desistimientos)

	ESTIMACIÓN	DESESTIMACIÓN	EST.FORMAL O PARCIAL	OTROS *	TOTAL
CANCELACIÓN	334	338	166	21	859
ACCESO	112	69	77	19	277
RECTIFICACIÓN	11	16	11	2	40
OPOSICIÓN	10	7	4	1	22
DOS O MAS Dº	18	9	4		31
TOTAL	485	439	262	43	1229

El mayor conocimiento de la normativa de protección de datos se ha traducido en una conducta más activa en el uso de los instrumentos de autoprotección contemplados en ella, como son el ejercicio directo de sus derechos ante quienes tratan su información personal. Alguna información sobre el ejercicio de derechos de tutela durante 2008 puede resultar clarificadora.

El ejercicio de derechos se ha incrementado cuantitativamente y, también, cualitativamente poniendo de manifiesto las nuevas inquietudes de los ciudadanos. El fuerte incremento de las reclamaciones ante la Agencia en solicitudes de tutelas de derecho se consolida e incrementa cerca de un 14% (13,8%) aproximándose a las 2000 solicitudes.

Más significativo aún que este dato cuantitativo es el objeto de las reclamaciones planteadas que indican sus nuevas inquietudes. Las solicitudes de cancelación de los datos o de oposición al tratamiento de los mismos por los buscadores de Internet, aún no siendo muy numerosas en valores absolutos, se han incrementado en un 216.6%.

Lo que revela que cada vez es mayor el interés mostrado por los ciudadanos para que no aparezcan sus datos personales en los índices que ofrecen los servicios de búsqueda en Internet a partir de los datos identificativos de una persona.

Los ciudadanos se preguntan ¿tengo que soportar estar expuesto en Internet? La respuesta es NO.

De los casos planteados ante la AEPD, relacionados con la publicación de sus datos en ediciones digitales de diarios oficiales o medios de comunicación, destacan los siguientes:

- Publicación de sanciones administrativas ya cumplidas.
- Publicación por edictos de deudas vencidas.
- Sanciones disciplinarias a funcionarios de prisiones que afectan a su seguridad.

- Publicación de datos de una mujer y sus hijos menores, victimas de violencia doméstica que facilitan su localización para el cónyuge.

- Publicación en una página web que replica la edición electrónica de boletines oficiales de ayudas de exclusión social y desempleo.

- Publicación de indultos.

En esta materia, las resoluciones dictadas por la AEPD van en la línea de resolver que se adopten las medidas necesarias para evitar la indexación de los datos de carácter personal. También ha habido que tener en cuenta las posibles acciones que los webmasters pudiesen adoptar encaminadas a hacer efectivo el derecho solicitado por el particular.

En 2009 destaca también el aumento de las reclamaciones relacionadas con la inclusión de los datos por motivos de morosidad en ficheros de información sobre solvencia patrimonial y crédito.

Al margen de estas cuestiones las principales preocupaciones de los ciudadanos siguen siendo: ¿Quién tiene mis datos?, ¿Cómo los cancelo?

Así resulta del importante incremento de las resoluciones relacionadas con la tutela de los derechos de acceso (Δ 59%) y de cancelación (Δ 40,8%) sumando sólo estas últimas un total de 1.366 resoluciones, cifra superior al total de las dictadas en el año anterior.

Es también novedoso el fuerte crecimiento de las resoluciones sobre el derecho de oposición (Δ 470%) que, en años anteriores, ocupaban el último lugar.

En el caso de los derechos de acceso y oposición la mayor parte de las resoluciones fueron estimatorias de los derechos de los ciudadanos, sucediendo lo contrario respecto de los derechos de cancelación y rectificación.

Para entender el elevado número de desestimaciones del derecho de cancelación, hay que tener en cuenta que en muchos de los casos se refieren a la cancelación de datos en los ficheros de solvencia patrimonial y de crédito en los que, al quedar confirmada la deuda por el acreedor, los responsables de dichos ficheros han actuado conforme a la normativa de protección de datos.

Asimismo, cuando se ha pedido la cancelación de datos a determinados organismos administrativos que se rigen por sus procedimientos específicos, se desestiman las solicitudes.

Las principales solicitudes de cancelación son las siguientes:

- Cancelación de anotaciones en informes técnicos realizados por profesionales en el ejercicio de sus funciones.
- Supresión de los datos una vez concluida la prestación de los servicios contratados; especialmente con operadores de telecomunicaciones.
- Supresión de antecedentes policiales, penales y penitenciarios de las administraciones públicas competentes.
- Cancelación de datos en foros de Internet.
- Datos que figuren en historial clínico.
- Supresión de datos o documentos que figuren en papel dentro de expedientes.

Respecto del derecho de acceso las cuestiones más relevantes son:

- Valoración de solvencia económica realizada por entidades financieras.
- Historial clínico de familiar fallecido.
- Historia clínica que se considera se ha suministrado de manera incompleta.

Sobre el derecho de rectificación destacan:

- Rectificar las bases de cotización contenida en ficheros de la Seguridad Social.

- Datos bancarios disponibles por otra empresa.

Y, en cuanto al derecho de oposición cabe reseñar los siguientes:

- Reflejar en los acuses de recibo el DNI del personal del Servicio de Correos y Telégrafos que realiza la entrega del correo.

- Recepción de publicidad de una empresa con la que se tiene contrato.

4.2 Inspección

La potestad de inspección de la AEPD se configura como un requisito imprescindible para el ejercicio de sus funciones de garantía del derecho a la protección de datos.

Desde un punto de vista formal, el hecho de que esta potestad esté conferida por nuestro derecho a la AEPD viene motivada por la transposición de la directiva 95/46/CE, ya que en ésta se dispone que a la Autoridad de Control independiente se le atribuyan poderes de investigación, de intervención y sancionadores.

En el ejercicio de las potestades de inspección y sanción, la AEPD sigue las normas contenidas tanto en la LOPD como en su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007.

Dentro de la AEPD, es la Subdirección General de Inspección de Datos el órgano administrativo al cual competen las funciones inherentes al ejercicio de la potestad de inspección, bajo la dirección y superior autoridad del Director.

Para el correcto desempeño de estas funciones inspectoras, el responsable del fichero está obligado a permitir el acceso a los locales en los que éstos se encuentren y los equipos informáticos, previa exhibición por el inspector de la autorización expedida por el Director de la AEPD. La obstrucción al ejercicio de esta función inspectora está tipificada por la LOPD como infracción grave.

Las autoridades de control :

- ✓ podrán inspeccionar los ficheros a que hace referencia la LOPD, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.
- ✓ tendrán la consideración de autoridad pública en el desempeño de sus cometidos.
- ✓ estarán obligados a guardar secreto sobre las informaciones que conozcan
- ✓ en la realización de sus funciones pueden
    1. solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados,
    2. inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados

4.2.1.- Los poderes de inspección del cumplimiento de la normativa de protección de datos.

El ejercicio de los poderes de inspección del cumplimiento de la normativa de protección de datos puede materializarse en una actuación "preventiva" (que conlleva las campañas o planes de auditoria, denominados planes sectoriales) o reactiva (como consecuencia del conocimiento de infracciones).

En el primer caso, esto es, la actuación "preventiva", es llevada a cabo por iniciativa propia de la AEPD.

En el segundo caso, el ejercicio de inspección para comprobación del cumplimiento de la normativa de protección de datos se puede iniciar bien tras la recepción en la AEPD de una denuncia formulada por un ciudadano, asociación o grupo de ciudadanos, o bien, en algunos casos, tras conocerse por la Agencia la posible existencia de problemas relativos a la protección de datos a través de los medios de comunicación social.

La Inspección de Datos podrá efectuar inspecciones, periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualquier fichero, de titularidad pública o privada, en los locales en los que se hallen y los equipos informáticos correspondientes.

El responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen y los equipos informáticos previa exhibición por el funcionario actuante de la autorización expedida por el Director de la Agencia.

4.2.1.1.- La actuación de inspección "preventiva"

La actuación de inspección "preventiva" del cumplimiento de la normativa de protección de datos se produce cuando el Director de la APD, normalmente tras consultar con la Inspección de Datos, decide que ciertos sectores deberán ser auditados a lo largo de un periodo de tiempo, con el objetivo de incrementar el conocimiento de sus actividades, detectar posibles deficiencias y proporcionar directrices sobre como mejorar el nivel de cumplimiento de las reglas sobre protección de datos a las empresas e instituciones públicas implicadas.

La decisión se toma teniendo en cuenta ciertos parámetros, como son los sectores que desarrollan una intensa actividad de tratamiento de datos personales para llevar a cabo sus intereses de negocio, el tratamiento habitual de datos

especialmente protegidos, las condiciones especiales sobre los tratamientos que pueden aparecer debido a excepciones de la legislación o a la presencia de regulaciones sectoriales o, incluso, por el elevado número de denuncias individuales recibidas en la AEPD en relación con un sector de actividad específico.

Una vez que el sector que va a ser objeto de inspección se ha definido, se nombra a un inspector como encargado de la auditoría.

El inspector comienza el estudio analizando las notificaciones realizadas a la AEPD por las entidades del sector en cuestión, lee los informes anuales de las asociaciones más importantes del sector y estudia su regulación legal. Todas estas tareas permiten escoger una muestra de compañías de tal manera que se pueda asegurar que los resultados obtenidos tras la inspección representan, con un buen grado de aproximación, las deficiencias o problemas prácticos encontrados en las operaciones del día a día de la mayoría de las empresas.

Tras decidir las compañías que serán inspeccionadas, se redacta un plan de auditoria y, en la mayor parte de los casos, se les remite por adelantado un cuestionario para obtener un mejor conocimiento sobre como se implantan en el sector los principios y derechos derivados de la legislación de protección de datos.

Las respuestas ayudan tanto al inspector como a la empresa auditada a ahorrar tiempo y esfuerzos y a enfocar la auditoria en los aspectos más importantes y relevantes, ya que algunos de ellos dependen muchísimo del sector auditado.

Después, se llevan a cabo las inspecciones *in situ* previstas. El número y extensión de las mismas difiere de una auditoria a otra.

Una vez finalizados todos estos trabajos, el inspector encargado de la auditoria redacta un informe final, describiendo el proceso seguido, los hechos más relevantes puestos de manifiesto, las conclusiones generales y una propuesta de recomendaciones para el sector estudiado.

Basándose en el informe, el Director de la AEPD, decide sobre el contenido final de las recomendaciones que se dirigirán al sector. Éstas son enviadas a las compañías auditadas y a las asociaciones más representativas del sector para su difusión entre sus afiliados.

Así en 2009 se ha realizado investigaciones preventivas en materias como videovigilancia a través de Internet o geolocalización.

4.2.1.2.- La actuación de inspección reactiva ante posibles infracciones.

El segundo supuesto antes planteado, esto es, el ejercicio de verificación o de inspección reactiva surge cuando la AEPD tiene noticia de una presunta infracción a la LOPD.

Principalmente el conocimiento de la presunta infracción se produce mediante la recepción en la AEPD de una denuncia, aunque existen también otras posibilidades como son las noticias a través de los medios de comunicación.

En los casos de actuación por denuncia, que es el supuesto general, examinado que el hecho denunciado pudiera constituir una infracción a la normativa de protección de datos y, en su caso, habiendo solicitado al reclamante cualquier dato que se estime pertinente para complementar la denuncia recibida, la forma de actuación para la inspección es la siguiente:

En primer lugar, se nombra un inspector para tramitar el caso y llevar a cabo todas las investigaciones preliminares centradas en averiguar si existen o no indicios suficientes para iniciar un procedimiento sancionador. El inspector puede usar una variedad de medios para obtener información sobre los hechos, incluyendo la realización de inspecciones presenciales. De esta forma los inspectores:

- ✓ podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos pudiendo requerir el envío de los documentos y datos que resulten necesarios y pertinentes.
- ✓ podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros. En este caso:

- los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.
- las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.
- el acta se emite por duplicado y se firma por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.
- en caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma.
- se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.
- El acta no contiene ninguna evaluación jurídica del caso.

Cuándo se considera que todos los hechos que han sido obtenidos por el inspector son relevantes, el caso es elevado al Director de la AEPD quien decide el inicio de un procedimiento sancionador o no; en este último caso el expediente se archiva.

Todas estas actuaciones de investigación previas al inicio de un procedimiento sancionador, deberán llevarse a cabo en el plazo máximo de doce meses a contar desde la fecha en la que la denuncia tuviera entrada en la AEPD, o en caso de no existir denuncia, desde que el Director de la Agencia acordase la realización de las actuaciones de inspección. Transcurrido dicho plazo sin haberse notificado acuerdo de inicio del procedimiento sancionador se produce la caducidad de dichas actuaciones.

CIFRAS COMPARATIVAS DE ACTUACIONES DE INSPECCIÓN

(Nota: las cifras incluyen procedimientos de admisión a trámite, solicitudes de mejora de la solicitud o no subsanada, acuerdos de no inicio de procedimientos sancionadores y actuaciones de inspección incoadas)

AÑO 2006	AÑO 2007	AÑO 2008
1519	1624	2362

4.2.2. El procedimiento sancionador en materia de protección de datos.

Compete a la Subdirección General de Inspección de Datos de la AEPD, dentro de su ámbito competencial de actuación, el ejercicio de los actos de instrucción relativos a los expedientes sancionadores. Estos se inician cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD

Como en todo procedimiento sancionador, han de tomarse todo tipo de garantías y salvaguardias para evitar la indefensión del responsable o responsables imputados.

Así, el procedimiento se desarrolla a través de pasos precisos y bien definidos:

- ✓ Es obligatorio informar al responsable, desde el mismo momento de la iniciación del procedimiento, de las presuntas infracciones que se le imputan y sus posibles consecuencias jurídicas.
- ✓ es obligatorio nombrar formalmente un instructor que puede ser recusado por el responsable imputado.
- ✓ existe una división entre el órgano que tramita el procedimiento (el instructor) y el órgano que toma la decisión final (el Director de la APD)
- ✓ el responsable tiene derecho a presentar sus alegaciones y pedir la práctica de pruebas adicionales
- ✓ en el momento procesal adecuado, al responsable se le pone de manifiesto el expediente completo y puede hacer alegaciones adicionales y presentar nuevos documentos

Atendiendo a estas premisas, el procedimiento sancionador se produce siempre de oficio mediante el acuerdo de inicio firmado por el Director de la Agencia, que deberá contener:

- ✓ Identificación de la persona o personas presuntamente responsables
- ✓ Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder
- ✓ Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos
- ✓ Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.
- ✓ Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos
- ✓ Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes
- ✓ Medidas de carácter provisional que pudieran acordarse.

Durante un plazo de quince días los interesados podrán aportar las alegaciones, documentos o informaciones que estimen pertinentes; así mismo podrán proponer pruebas concretando los medios de que pretenda valerse

Por otra parte, el instructor realizará de oficio cuantas actuaciones resulten necesarias para el examen de los hechos, recabando los datos e informaciones que sean relevantes para determinar, en su caso, la existencia de responsabilidades susceptibles de sanción. Así mismo podrá acordarse por el instructor la práctica de prueba.

Una vez se han completado todos los pasos del procedimiento, el instructor redacta una propuesta de resolución en la que:

- ✓ se fijarán de forma motivada los hechos, especificándose los que se consideren probados y su exacta calificación jurídica,
- ✓ se determinará la infracción
- ✓ se determinará la persona o personas que resulten responsables,

- ✓ se especificará la sanción que propone que se imponga o bien se propondrá la declaración de no existencia de infracción o responsabilidad.

Dicha propuesta de resolución se remite al responsable para que haga sus alegaciones finales en el plazo de quince días y, tras recibirlas o transcurrido el plazo, el expediente es elevado al Director. Éste puede confirmar la propuesta de resolución o, en caso contrario, puede ordenar actuaciones adicionales o, redactar una resolución apartándose del criterio del instructor. En estos últimos casos, estos hechos son comunicados al responsable para darle una nueva oportunidad de alegar, ya que las circunstancias han cambiado respecto de aquellas en que se produjeron sus últimos comentarios.

Es importante destacar la posibilidad legal de adoptar medidas cautelares. Esta posibilidad se produce en el caso de que exista una presunta infracción muy grave a la Ley y que puedan verse afectados los derechos y libertades fundamentales de los ciudadanos. En este supuesto el Director puede adoptar estas medidas para bloquear los datos e impedir la continuación de su tratamiento, como por ejemplo, la inmovilización de ficheros, regulada en el artículo 121 del RD 1720/2007. Por supuesto, esta decisión se toma sólo en circunstancias muy especiales y puede recurrirse ante los tribunales.

Finalmente, el Director firma una resolución motivada que debe finalizar con un pronunciamiento sobre el archivo del caso o sobre la existencia de una infracción a la Ley cometida por el responsable o responsables del tratamiento y, en este caso, la sanción económica que la misma lleva aparejada.

En el caso de instituciones públicas, la multa se sustituye por la comunicación al infractor, su superior jerárquico y al Defensor del Pueblo de la resolución en la que se declara la existencia de la infracción y, en su caso, la solicitud de inicio de actuaciones disciplinarias contra el funcionario o funcionarios responsables de la infracción.

La resolución debe ser notificada a todos los interesados en el procedimiento, teniendo en cuenta que el plazo para dictar y notificar la resolución es de seis meses a partir de su entrada en la Agencia. Transcurrido dicho plazo sin haber recaído resolución expresa se producirá la caducidad del procedimiento y el archivo de las actuaciones.

Notificada la resolución a los intervinientes en el procedimiento, y dentro del mes siguiente a la citada notificación, la resolución es publicada de forma anonimizada en la página web de la AEPD

Las resoluciones del Director de la Agencia Española de Protección de Datos son firmes en vía administrativa por lo que, contra las mismas, sólo se podrá interponer recurso potestativo de reposición, y el recurso contencioso-administrativo ante la Audiencia Nacional.

Gráfico 3

CIFRAS RELATIVAS A PROCEDIMIENTOS RELATIVOS AL EJERCICIO DE LA POTESTAD SANCIONADORA				
	AÑO 2006	AÑO 2007	AÑO 2008	AÑO 2009
Nº PROC. SANCI	1070	1246	2419	3.905.
SANCIONES	24.422.292,48 €	19.674.480,03 €	22.625.839,38 €	27.072.991,44 €

Los principales sectores objeto de investigación en 2009 han sido telecomunicaciones, entidades financieras y videovigilancia resaltando en este último ámbito un incremento en las denuncias de casi u 230% respecto a 2008

Junto a ello las principales infracciones declaradas a las Administraciones Públicas han sido:

- Infracciones al Deber de Secreto.
- Falta de medidas de seguridad, incluidos los hallazgos de documentación accesibles en la vía publica o en la basura.
- Tratamiento de datos con conculcación del principio de calidad de datos.
- Omisión del deber de información.
- Creación de ficheros sin disposición general habilitante y no inscripción en el Registro General de Protección de Datos.
- Cesión ilícita de datos

Finalmente, cabe destacar investigaciones de oficio que han derivado en la apertura de procedimientos sancionadores iniciados sin previa denuncia. Entre ellos:

- Documentos con datos de carácter personal hallados en contenedores de basura en la vía pública procedentes de una agencia de seguros y un bingo.
- Documentos abandonados en los locales de antigua comisaría de policía.
- Cámaras de videovigilancia instaladas por los vecinos en un barrio.
- Documentos al alcance de los ciudadanos en el Registro Civil.
- Almacenamiento de diversa documentación clínica en áreas no restringidas al público de un hospital psiquiátrico.
- Portales de contactos personales que facilitan la votación de la imagen física de los usuarios, en particular cuando son menores de 14 años.
- Portal de contactos personales con usuarios de todo el mundo, clasificados según país (en particular, España) y centro educativo. (El sitio web está registrado en Argentina y posiblemente alojado en un servidor estadounidense)
- Hallazgo por la Inspección de Datos en la red *eMule* de un fichero conteniendo datos de más de 3.000 clientes de una clínica.

4.3 Tutela Jurisdiccional.

El capítulo III de la Directiva 95/46/CE, 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, está dedicado a los recursos judiciales, responsabilidad y sanciones.

Más concretamente el artículo 22.de la citada directiva esta referido a los Recursos, y en él se dispone que:

> *"Sin perjuicio del recurso administrativo que pueda interponerse en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate."*

Pues bien, en nuestro derecho la previsión establecida en dicho artículo de la directiva se garantiza mediante la posibilidad de que, finalizado un procedimiento tanto de tutela de derechos como sancionador, y con independencia de que opcionalmente pueda interponerse el recurso de reposición ante la propia AEPD, el interesado pueda interponer el recurso contencioso-administrativo ante la Audiencia Nacional –sin perjuicio de la tutela de su derecho por las vías procesales ordinarias en atención, entre otras normas, a la LO 1/1982 de 5 de mayo, de Protección Civil del Derecho al Honor, a la integridad personal y familiar y a la propia imagen.

Dicho recurso judicial debe ser planteado conforme lo indicado en la Ley 29/1998, reguladora de la Jurisdicción Contencioso-Administrativa, y, en concreto, conforme al artículo 46 se presentará en el plazo de dos meses desde la notificación de la resolución administrativa.

Bibliografía del módulo

- "REVISTA ESPAÑOLA DE PROTECCIÓN DE DATOS 1"

Editorial Thomson Civitas - Año 2006

- Estudio práctico sobre el principio de consentimiento en el marco de la normativa sobre protección de datos de carácter personal: el caso RACC (2006) Miguel Acosta Ramírez.

- "REVISTA ESPAÑOLA DE PROTECCIÓN DE DATOS 2"

Editorial Thomson Civitas - Año 2007

- El principio del consentimiento en los Estados miembros de la Unión Europea. Montea Arenas.

- "LA LEY DE PROTECCIÓN DE DATOS. ANÁLISIS Y COMENTARIO DE SU JURISPRUDENCIA" 2007. Varios autores (coordinador: Carlos Lesmes Serrano)