MANUAL SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL PARA ABOGADOS

Manual elaborado para el Ilustre Colegio de Abogados de Sevilla con la colaboración de la Comisión de Nuevas Tecnologías del ICAS, y la Asociación de Abogados Especialistas en Nuevas Tecnologías de Andalucía, cuyo objetivo es ayudar a los abogados a cumplir la normativa de protección de datos personales en su actividad profesional.

Pedro Rodríguez López de Lemus
Junio de 2008

Prólogo

Los avances tecnológicos impregnan hoy día todos los aspectos de nuestras vidas, en nuestra esfera privada, en las relaciones con las Administraciones, y sobre todo, en el desarrollo de nuestra labor profesional. Tanto es así, que es difícil encontrar algún compañero letrado que no necesite de estas nuevas tecnologías para desarrollar su ejercicio profesional, ya sea mediante el uso equipos informáticos y procesadores de texto, correos electrónicos y páginas web, o incluso de bases de datos y dispositivos móviles.

Estos avances nos proporcionan nuevas herramientas para desarrollar nuestro trabajo de una manera más eficiente, pero también implican nuevas obligaciones. Una de estas obligaciones, aunque quizás no tan reciente, pues la primera normativa que la regula data del año 1992, es el cumplimiento de la normativa en protección de datos de carácter personal, un derecho fundamental autónomo según indica nuestro Tribunal Constitucional.

Como es sabido, los abogados en nuestro desempeño diario manejamos constantemente datos de carácter personal, de ahí la importancia de cumplir escrupulosamente la normativa que regula su uso.

Así, para ayudar a este cumplimiento, ha surgido la idea de este *Manual sobre protección de datos de carácter personal para Abogados*, cuyo objetivo no es otro que acercar de manera sencilla el conocimiento de esta materia a los abogados del Ilustre Colegio de Abogados de Sevilla, con el deseo de que sea útil a todos aquellos que lo precisen.

JOSÉ JOAQUÍN GALLARDO RODRÍGUEZ
Decano del Ilustre Colegio de Abogados de Sevilla

Índice

0. INTRODUCCIÓN

A los abogados les afecta la protección de datos personales desde una doble perspectiva, como sujeto activo deben impulsar su cumplimiento entre sus clientes, y como sujeto pasivo tienen la obligación de cumplirla respecto a los tratamientos de datos personales que realizan en su actividad profesional.

Por ello, el objetivo de este manual es ayudar a los abogados a cumplir la normativa de protección de datos personales en su actividad profesional. Para ello analizamos el contenido principal de esta normativa, añadiendo la documentación necesaria para su efectiva aplicación.

Una vez declaradas nuestras intenciones, pasamos a dicho análisis. Lo primero es saber sobre que estamos hablando realmente, ¿qué es la protección de datos personales?

1. ¿QUÉ ES LA PROTECCIÓN DE DATOS PERSONALES?

Definiremos la protección de datos personales como el derecho que tienen los ciudadanos a que sus datos personales no sean utilizados por terceros sin la autorización debida.

El objeto de la normativa en protección de datos personales no es otro que garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor e intimidad personal y familiar.

1.1. DERECHO FUNDAMENTAL

En efecto, el derecho a la protección de datos personales es un derecho fundamental, con todo lo que esto conlleva respecto a su tratamiento legislativo y su especial protección en los Tribunales.

En nuestra Constitución de 1978 el artículo 18.4, dice literalmente “La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.” No se refiere este artículo a la protección de datos propiamente dicha, sino a su fundamento primigenio.

Es el Tribunal Constitucional quien en su Sentencia 292/2000 consagra el derecho a la protección de datos como un derecho fundamental autónomo y distinto del derecho a la intimidad, pues es más amplio, ya que abarca a aspectos que no podrían considerarse como íntimos propiamente y que, sin embargo, son protegidos igualmente.

1.2. LEGISLACIÓN

A partir del mandato Constitucional de garantizar el honor y la intimidad personal y familiar frente al uso de la informática el Legislador dio a luz en el año 1992 la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal, conocida como la LORTAD. Fue ésta la primera regulación en nuestro país en esta materia, que fue seguida por distintos Reglamentos de desarrollo.

En el año 1995 se aprobó la Directiva Europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos.

En diciembre de 1999 se publicó la Ley Orgánica de Protección de Datos de Carácter Personal, en adelante LOPD, actualmente en vigor.

Con bastante posterioridad a la aparición de la LOPD se publica el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el primer Reglamento de desarrollo de la LOPD, ya que los anteriores Reglamentos desarrollaban la LORTAD. El día 19 de abril de 2008 entró en vigor el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en adelante RDLOPD, que deroga el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en este Real Decreto.

1.3. CÓDIGOS TIPO

Los códigos tipo son códigos deontológicos o de buena praxis profesional. Estamos hablando de acuerdos voluntarios de empresas o profesionales, o convenios administrativos, así como de las organizaciones en que éstos se agrupen. Estos códigos deben ser depositados o inscritos en el Registro General de Protección de Datos.

Este manual que nos ocupa no es un código tipo que añada un plus de cumplimiento para los abogados en esta materia, sino una descripción práctica de la normativa en protección de datos personales.

2. ÁMBITO DE APLICACIÓN

2.1. ÁMBITO OBJETIVO

Según la LOPD, “será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.”

Ante todo hay que saber que es un dato de carácter personal. Es cualquier información concerniente a personas físicas identificadas o identificables. Ello nos lleva a definir persona identificable como toda aquella cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

Además de que haya un dato personal, es necesario que esté registrado en un soporte físico que lo haga susceptible de tratamiento. Los soportes más habituales son el informático y el papel. Respecto a que sea susceptible de tratamiento, quiere decir que esté en un fichero. Un fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso, responda tanto a una estructura como a una finalidad común.

Los tratamientos de datos son 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. Por tanto, casi todo lo que podamos imaginar que se puede hacer con un dato es un tratamiento.

Es importante señalar que el tratamiento no es sólo informático, sino que también puede ser manual.

No será de aplicación esta normativa a los siguientes ficheros:

- Los mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

- Los sometidos a la normativa sobre protección de materias clasificadas.

- Los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Se regirán por sus disposiciones específicas los siguientes ficheros:

- Los regulados por la legislación de régimen electoral.

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

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

- Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

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

- Los sometidos a la normativa sobre protección de materias clasificadas.

- Los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto.

Pasamos ahora a exponer algunos casos donde es y no es aplicable esta normativa:

- No se aplica esta Normativa a datos de personas fallecidas.

- Tampoco se aplica a ficheros personales de uso doméstico, respecto a las actividades que se inscriban en el marco de la vida privada o familiar de los particulares.

- No es aplicable a datos de personas jurídicas ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

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

- Caso más complejo es el de los correos electrónicos, que serán datos personales si identifican a su titular. Por ejemplo vivayo@hotmail.com difícilmente puede identificar a alguien, pero javiergarciadelreal@hotmail.com si nos permitirá identificar a su titular, por lo que sí será un dato personal.

Es evidente que los abogados, como cualquier otro profesional, tratan ficheros con datos de carácter personal. Ejemplo de ello son los ficheros de clientes, de procuradores, de contrarios, de expedientes, del personal de su despacho, etcétera.

2.2. ÁMBITO TERRITORIAL

Se regirá por esta normativa todo tratamiento de datos personales siempre que se dé alguna de las siguientes circunstancias:

- Cuando sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. Caso habitual del tratamiento por parte de los abogados.

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

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

3. SUJETOS

Los sujetos que de algún modo intervienen en la materia de protección de datos personales son:

- El responsable del fichero.
- El afectado.
- El encargado del tratamiento por cuenta de tercero.
- La Agencia de Protección de Datos

3.1. EL RESPONSABLE DEL FICHERO

El responsable del fichero dice la ley que es “la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decide sobre la finalidad, contenido y uso del tratamiento”. Es responsable del fichero aquél que decide sobre la finalidad del fichero, es decir, para qué se van a utilizar los datos personales que contiene el fichero.

Si el ejercicio de la abogacía se realiza a través de una sociedad con personalidad jurídica, será ésta la responsable de los ficheros, pero si se realiza como un profesional autónomo, será el propio abogado el responsable del fichero.

3.2. EL AFECTADO

El afectado o interesado es la persona física titular de los datos que sean objeto del tratamiento. Es el titular de los datos, la persona a la que hacen referencia los mismos. Es el auténtico propietario de la información sobre la que versan los ficheros.

Como hemos indicado anteriormente, los afectados serán fundamentalmente los clientes, contrarios y personal del despacho.

3.3. AGENCIA DE PROTECCIÓN DE DATOS

Veremos en este punto un nuevo sujeto, la Agencia de Protección de Datos, aunque en realidad debemos decir las Agencias de Protección de Datos, pues hay una estatal y varias autonómicas.

3.3.1. Agencia Española de Protección de Datos

La A.E.P.D., es un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada. Actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Su principal función es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Al frente de esta Agencia está el Director de la misma. Forman también parte de la estructura de la A.E.P.D. un Consejo Consultivo, el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General de la Agencia.

3.3.2. Agencias de Protección de Datos Autonómicas

Además de la Agencia Estatal todas las Comunidades Autónomas tienen la posibilidad de crear su propia Agencia de Protección de Datos, con un ámbito de actuación territorial autonómico, y solamente respecto a los ficheros de titularidad de la Administración Autonómica, las Administraciones Locales de esa Comunidad y de todos los Organismos dependientes de ambas.

Comunidades Autónomas como Madrid, Cataluña y País Vasco ya tienen su propia Agencia.

3.3.3. Agencia de Protección de Datos de Andalucía

En Andalucía no hay aún Agencia de Protección de Datos. En el año 2003, impulsada por la Asociación Andaluza de Comercio Electrónico, se elaboró la proposición de Ley 6-03/PPL-0 00008, de creación de la Agencia Andaluza de Protección de Datos, pero no salió adelante.

No obstante, la propuesta de reforma del Estatuto de Autonomía de Andalucía hace referencia a ésta en tres ocasiones.

4. OBLIGACIONES DEL RESPONSABLE

A continuación vamos a explicar cuáles son las principales obligaciones del responsable del fichero.

Entre estas obligaciones se encuentran los principios generales de la protección de datos, que son los principios básicos que han de ser respetados en toda fase del tratamiento de los datos, cuando resulten aplicables.

Estos principios son:

- Calidad de datos.
- Derecho de información en la recogida de datos.
- Consentimiento del afectado.
- Datos especialmente protegidos.
- Datos relativos a la salud.
- Seguridad de los datos.
- Deber de secreto.
- Comunicación de datos.
- Acceso a los datos por cuenta de terceros.

4.1 INSCRIPCIÓN DE FICHEROS

Se puede crear un fichero de titularidad privada que contengan datos personales, siempre que resulte necesario para el logro de la actividad u objeto legítimos de abogado o empresa, y se respeten las garantías que la normativa recoge.

En el caso de los ficheros de titularidad privada, es obligatorio proceder a la notificación ante el Registro General de Protección de Datos, mediante la cumplimentación de un formulario oficial. Igualmente hay que comunicar los cambios que se produzcan en la finalidad del fichero, en su responsable o en la dirección de su ubicación.

La realización de esta inscripción se puede llevar a efecto a través de los siguientes formatos:

- Telemático
- En soporte informático
- En formato papel

Lo que aquí se notifica no son los datos que contienen los ficheros, sino algunas características del mismo.

Este Registro General, inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que se hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Por tanto, un abogado antes de iniciar su actividad y tratar datos personales, debe notificar e inscribir los correspondientes ficheros ante el Registro General de Protección de Datos.

Junto a este manual se incluye como Anexo III el formulario electrónico NOTA para la notificación de ficheros.

4.2. CALIDAD DE LOS DATOS

Hay total libertad para crear un fichero, pero se deben cumplir algunos requisitos. Uno de ellos es el que se refiere a la calidad de los datos.

Así, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Dice la actual normativa que los datos “no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”.

Los datos deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

Algo más complejo es la obligación de que los datos deberán ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Una vez que haya desaparecido la finalidad para la que fueron tratados los datos, éstos han de eliminarse.

Al decir cancelarse, nos referimos a eliminarlos definitivamente, de cualquier manera que nadie pueda acceder a ellos en el futuro. Solo en el caso de que estos datos puedan ser requeridos por un tercero legítimamente debemos mantenerlos aunque haya desaparecido su finalidad. No obstante, dentro de lo posible se guardarán bloqueados, es decir, no accesibles. En el caso concreto de datos personales registrados con fines policiales, se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

En cuanto a la forma de recogida de datos, hemos de señalar que se prohíbe expresamente la recogida de datos por medios fraudulentos, desleales o ilícitos.

Para los abogados es complejo cumplir con este requisito de calidad, ya que en protección de nuestros clientes solemos almacenar información indefinidamente. No obstante, se ha de cumplir este requisito de calidad como debe hacerlo cualquier otro profesional o empresa, ya sea mediante la eliminación real de la información cuando sea necesario, o al mediante la restricción de acceso a la misma, algo relativamente más sencillo de cumplir.

4.3. DERECHO DE INFORMACIÓN

4.3.1. Regla general

Como regla general, a quienes se les soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Lo dicho hasta ahora en este punto no será de aplicación a la recogida de datos cuando ésta afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.

Junto a este manual se incluye en el *Anexo I* un modelo de cláusula de información.

4.3.2. Excepciones

No obstante, este deber no es absoluto, sino que tiene sus excepciones. Así, no será necesario cumplir con este deber de información cuando:

- Una Ley así lo prevea.

- Se trate de datos para fines históricos, estadísticos o científicos según marca su normativa.

- Resulte imposible o exija esfuerzos desproporcionados el llevarlo a cabo, siempre bajo criterio de la Agencia Española de Protección de Datos.

- Los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial.

En este último caso, en cada comunicación que se dirija al afectado se le informará del origen de los datos, de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

Siempre que un abogado tome los datos de un cliente debe informarle de lo dicho en este punto, y a ser posible quedando constancia de ello, para así evitar problemas de prueba en caso de necesidad. Por ello, el deber de información ha de llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado, pudiéndose utilizar soportes informáticos o telemáticos para ello, como el escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

4.3.3. Fuentes accesibles al público

A los efectos de la LOPD, se consideran fuentes accesibles al público “aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.”

Tienen la consideración de fuentes de acceso público, exclusivamente, las siguientes:

- El censo promocional.

- Los repertorios telefónicos en los términos previstos por su normativa específica.

- Las listas de personas pertenecientes a grupos de profesionales, que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, indicación de su pertenencia al grupo, y dirección profesional, que podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, como es un colegio de abogados, podrá indicarse el número de colegiado, fecha de incorporación y situación de ejercicio profesional.

- Los Diarios y Boletines oficiales

- Los medios de comunicación social.

4.4. EL CONSENTIMIENTO

Toda la normativa de protección de datos gira en torno al consentimiento. Casi todo puede hacerse con los datos personales de alguien siempre que se cuente con su consentimiento. Pero a su vez podemos decir que siempre que se vaya a realizar un tratamiento de datos es necesario que previamente todos los titulares de los mismos hayan prestado su consentimiento para ello.

4.4.1. Regla general

Como norma general, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

Por consentimiento debemos entender toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

En la solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma, el responsable del tratamiento deberá permitir al afectado que manifieste su negativa al tratamiento de datos.

4.4.2. Excepciones

Las excepciones a la regla general de necesidad de consentimiento son las siguientes:

- Cuando así lo autorice una norma con rango de Ley o una norma de derecho comunitario.

- Éste no será necesario para los ficheros con datos personales cuya finalidad sean las funciones propias de las Administraciones Públicas en el ámbito de sus competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

- Tampoco será necesario entre las partes de un contrato o precontrato de una relación negocial, laboral o administrativa cuando sean necesarios para su mantenimiento o cumplimiento.

- Cuando se trate de proteger un interés vital del interesado.

- Por último, cuando los datos provengan de las denominadas fuentes accesibles al público.

En estos casos en los que no es necesario el consentimiento del afectado para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

4.4.3. Tipos de consentimiento

En la LOPD se exigen tres tipos de consentimiento según el tipo de datos personales de que se trate. Para el tratamiento de cualquier dato personal de un titular hace falta su consentimiento tácito, es decir que se entienda por sus acciones u omisiones que se presta, sin que deba quedar constancia de ello. Aunque es muy importante dejar constancia de que el titular ha prestado su consentimiento, ya que si por cualquier motivo éste manifestara que nunca lo prestó, será el responsable del fichero quien tenga que demostrar que efectivamente se contó con el consentimiento del titular para tratar sus datos personales, puesto que corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Este tipo de consentimiento puede recabarse dirigiéndose al afectado, y concediéndole un plazo de treinta días hábiles para manifestar su negativa al tratamiento mediante un método sencillo y gratuito, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

El segundo tipo de consentimiento es el expreso, es decir que no basta con que a través de sus actos se intuya que se presta el mismo, sino que tiene que declarar expresamente que se da ese consentimiento. Este tipo es necesario para datos relacionados con la salud, el origen racial y la vida sexual. Cabe decir aquí lo mismo respecto a la necesidad de disponer de alguna prueba respecto a la existencia del mismo.

El consentimiento expreso y por escrito es el tercer y último tipo. Se requiere para tratar datos de ideología, religión, creencias y afiliación sindical.

Se exceptúan de la necesidad de este consentimiento los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

4.4.4. Datos especialmente protegidos

Están prohibidos los ficheros cuya única finalidad sea la de almacenar datos personales especialmente protegidos. Éstos son aquellos que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de datos especialmente protegidos podrán realizarse en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.

Por último, se ha de indicar que los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

4.4.5. Datos de salud

Entre estos datos especialmente protegidos, debemos destacar por su relevancia los datos de salud, el RDLOPD define dato de carácter personal relacionado con la salud como "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética."

4.4.6. Datos de los trabajadores

Los datos personales de los trabajadores, deben ser adecuados, pertinentes y no excesivos para las finalidades para las cuales fueron recabados.

La conservación de estos datos debe ir aparejada a la vigencia del contrato que los origina.

4.4.7. Videovigilancia

La videovigilancia está en auge, cada vez son más las cámaras que nos observan y nos vigilan. Las podemos ver en las empresas, en los comercios y bancos a los que acudimos, en nuestros lugares de ocio, e incluso en algunos despachos de abogados. Están en casi todos los sitios a los que acudimos y desarrollamos nuestra vida profesional o privada.

Este aumento de instalación de dispositivos de videovigilancia se debe a los avances técnicos en este campo, que han llevado al consiguiente abaratamiento de los mismos. Está claro que estos sistemas son eficaces para la seguridad, pero también pueden ser usados con otros fines, por ello la pregunta que debemos hacernos es la siguiente, ¿son legales estas actuaciones de videovigilancia a las que nos vemos sometidos?

La respuesta, aunque con muchos matices, es sí. La A.E.P.D. ha publicado una Instrucción que aclara las dudas que han generado la proliferación de sistemas de cámaras y videocámaras, y cuya intención es adecuar los tratamientos de imágenes con fines de vigilancia a los principios de la LOPD, y garantizar los derechos de las personas cuyas imágenes son tratadas por estos sistemas, ya que una imagen es un dato de carácter personal, y por tanto amparado por la protección de este derecho fundamental.

Así, sólo se es admisible la instalación de estas cámaras cuando la finalidad de videovigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal. Pero, ¿cuándo es una medida proporcionada el uso de un sistema de cámaras con fines de vigilancia? Se considera proporcionada cuando este uso sea susceptible de conseguir el objetivo presupuesto; además tiene que ser necesario, en el sentido que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia; y por último, ha de ser ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Debemos señalar también que se debe colocar en las zonas videovigiladas, al menos un distintivo informativo ubicado en un lugar suficientemente visible, y tener a disposición de los interesados impresos donde se detalle la información necesaria sobre ese tratamiento de datos.

4.4.8. Tratamiento por Abogados y Procuradores de los datos de las partes en un proceso

Se ha consultado a la A.E.P.D. si los abogados y procuradores habrán de recabar el consentimiento de sus clientes y de la contraparte de los mismos en procesos en que aquéllos les confieran su representación o defensa.

Ésta ha respondido que como regla general, la inclusión de los datos de los clientes y sus oponentes en un fichero supondrá un tratamiento de datos de carácter personal, que requeriría, en principio, el consentimiento del afectado, con el deber de informar al mismo de los extremos contenidos en el artículo 5.1 o, en caso de no recabarse los datos del propio afectado, la obligación de informar a éste de dicha inclusión en el plazo de tres meses, tal y como dispone el artículo 5.4, ambos de la LOPD.

En lo referente al tratamiento de los datos de los clientes, podrá efectuarse el mismo sin consentimiento del afectado, a tenor de lo establecido en el artículo 6.2 de la Ley Orgánica 15/199, que excluye del consentimiento los supuestos en que los datos “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”.

Sin embargo, el problema se plantea en el supuesto de que los datos se refieran a los oponentes de los clientes del abogado o procurador, dado que en ese caso el tratamiento resulta absolutamente imprescindible para la asistencia letrada al cliente, si bien ese tratamiento pudiera chocar con el derecho a la protección de datos de la persona cuyos datos son objeto de tratamiento.

En este caso surgiría una colisión entre dos derechos fundamentales: el derecho a la protección de datos de carácter personal, derivado del artículo 18 de la Constitución y consagrado como derecho autónomo e informador del texto constitucional por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, por un lado; y el derecho a la asistencia letrada, como manifestación del derecho de los ciudadanos a obtener la tutela judicial efectiva de los jueces y tribunales, contenido en el artículo 24.2 de la Constitución.

Para resolver esta cuestión, debe indicarse que, en primer lugar, que la propia LOPD permite establecer los límites para la exigencia del consentimiento, dado que su artículo 6.1 exige, como regla general, el consentimiento para el tratamiento de los datos “salvo que la Ley disponga otra cosa”.

A la vista de este precepto, el legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio legislador haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En este caso, el tratamiento por los abogados y procuradores de los datos referidos a la contraparte de sus clientes en los litigios en que aquéllos ejerzan la postulación procesal trae su causa, directamente, del derecho de todos los ciudadanos a la asistencia letrada, consagrado por el artículo 24.2 del Texto Constitucional.

En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de los medios de prueba pertinentes para su defensa, vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Por todo ello, si bien ninguna disposición con rango de Ley establece expresamente la posibilidad del tratamiento por abogados y procuradores de los datos referidos al oponente de su cliente en el seno de un determinado proceso judicial, es evidente que dicha posibilidad trae causa directa de una norma de rango constitucional, reguladora además de uno de los derechos fundamentales y libertades públicas consagrados por la Constitución, y desarrollado por las leyes reguladoras de cada uno de los Órdenes Jurisdiccionales, en los preceptos referidos a la representación y defensa de las partes, por lo que existirá, desde el punto de vista de la Agencia, una habilitación legal para el tratamiento de los datos, que trae su cobertura del propio artículo 24 de la Constitución y sus normas de desarrollo.

Dicho esto, deberá analizarse si el abogado o procurador se encuentra obligado, por imperativo del artículo 5.4 de la Ley Orgánica, a informar a los oponentes de su cliente de la existencia de un fichero o tratamiento, su responsable, su finalidad, la posibilidad que los afectados ejerciten los derechos que la Ley les atribuye y los destinatarios de los datos, dada la concurrencia entre el derecho del cliente a obtener la adecuada asistencia de letrado y, en definitiva, a ver satisfecha la tutela judicial efectiva, consagrada por el artículo 24 de la Constitución, y del oponente a la protección de sus datos de carácter personal, lo que supondrá el cumplimiento del citado deber de información.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional “el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho”.

Pues bien, aplicando la doctrina antedicha al supuesto concreto, y sin perjuicio de lo que, en su caso, manifestare en el futuro el Tribunal Constitucional, procederá ponderar en qué caso la limitación del ejercicio de uno de los derechos en conflicto puede producir una mayor merma de los derechos de la otra parte o, en su caso, las medidas que permitirán mitigar ese potencial perjuicio.

Siguiendo esta premisa, debería darse una prevalencia al derecho consagrado por el artículo 24 de la Constitución, garantizando a su vez las medidas que evitarán un mayor perjuicio a los afectados (en este caso, los oponentes de los clientes cuyos datos son objeto de tratamiento).

Ello se funda en que la comunicación a los afectados de las informaciones de que los abogados o procuradores puedan disponer, procedentes de sus clientes, podrían perjudicar, como ya se indicó, el adecuado ejercicio por el propio interesado de las facultades vinculadas con su derecho a obtener la tutela efectiva de los Jueces y Tribunales (al quedar en conocimiento de la otra parte los datos que pudieran ser aportados a juicio en defensa de su derecho).

4.5. CESIÓN DE DATOS

Existe la obligación general por parte del responsable del fichero de no ceder los datos personales incorporados en sus ficheros. Éstos solo podrán ser cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. Debemos entender por cesión de datos todo tratamiento de datos que supone su revelación a una persona distinta del interesado.

Cuando se obtiene el consentimiento del titular, por parte del responsable del fichero para tratar sus datos personales, sólo el responsable puede tratarlos.

4.5.1. Regla general

Como regla general, para poder ceder cualquier dato es necesario contar antes con el consentimiento del afectado, lo que implica tener que informarle previamente de ello.

Sin embargo, sí es válido informar y pedir el consentimiento para poder ceder los datos a cualquier tercero.

También es posible recabar el consentimiento con posterioridad a cuando se recabaron en un primer momento. Bastaría con que el responsable informara y pidiera el consentimiento.

Todo esto hace muy difícil, por no decir imposible, muchos tratamientos que son vitales para cualquier abogado o empresa.

Junto a este manual se incluye en el *Anexo I* un modelo de cláusula para comunicación de datos.

4.5.2. Excepciones

Por ello, para evitar esta imposibilidad de cumplimiento, pasamos a ver las excepciones a la regla general de la necesidad del consentimiento del titular de los datos para poder ceder los mismos:

- Si una norma con rango de ley o una norma de derecho comunitario autoriza la cesión.

- Cuando los datos sean obtenidos de fuentes accesibles al público.

- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

- Cuando la comunicación tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

- Cuando se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, o cuando los datos hayan sido recogidos o elaborados por una Administración Pública con destino a otra, o cuando la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

- Cuando la cesión de datos sobre salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

- Por último, respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Es importante para los abogados tener en cuenta que cada profesional autónomo es responsable de sus ficheros, y que cualquier acceso por un tercero a los datos de los mismos,

aunque sea este otro abogado, puede ser considerado una cesión de datos, salvo que se trate de un tratamiento por cuenta de terceros, que explicamos a continuación.

Aun con estas excepciones, hay muchos tratamientos de datos que siguen siendo imposibles para el responsable del fichero. Por ello, con el fin de adaptar la norma a las necesidades de la actividad profesional y empresarial, la LOPD creó una figura que no existía en la normativa en protección de datos personales que le precedió, la LORTAD, surgiendo así el tratamiento por cuenta de terceros.

4.5.3. Tratamiento por cuenta de tercero

El tratamiento por cuenta de terceros es una novedad de la LOPD. Es una excepción genérica a la exigencia de consentimiento para poder realizar una cesión de datos. Así no se considerará cesión de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

Se exige que para la efectiva realización de un tratamiento por cuenta de terceros, que no sea considerada una cesión ilegal de datos en su caso, deberán de cumplirse los siguientes requisitos:

- Dicho tratamiento deberá estar regulado en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

- Debe establecerse expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

- Que el encargado del tratamiento no aplicará o utilizará los datos con un fin distinto al que figure en el citado contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

- En el contrato habrán de estipularse las medidas de seguridad que el encargado del tratamiento estará obligado a implementar.

- Debe de incluirse en el contrato el compromiso de que, una vez cumplida la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. No obstante, el encargado de tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

4.5.4. El encargado del tratamiento

El encargado del tratamiento por cuenta de un tercero es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

El hecho de que se realice un trabajo para un tercero, no convierte automáticamente en un encargado del tratamiento.

El responsable del tratamiento debe velar por que el encargado del tratamiento reúna las garantías necesarias que marca la normativa en protección de datos de carácter personal. El encargado del tratamiento está sujeto, junto con el responsable del fichero al régimen de sanciones previsto en la LOPD.

Por último, indicar que el encargado del tratamiento no subcontratará con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello, bien mediante autorización previa individual o estipulándolo en el contrato entre el responsable y el encargado. En cualquier caso la contratación se hará en nombre y por cuenta del responsable del tratamiento.

Junto a este manual se incluye en el *Anexo I* un modelo de cláusula de tratamiento por cuenta de terceros.

4.5.5. Deber de información en la cesión

El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario, salvo en los casos siguientes:

- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.

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

- Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

- Cuando la cesión venga impuesta por Ley.

4.6. MEDIDAS DE SEGURIDAD

4.6.1. El documento de seguridad

La obligación más conocida es la de adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Esto se traduce fundamentalmente en tener un documento de seguridad en protección de datos personales. Este documento es una “política de seguridad” que contiene estas medidas técnicas y organizativas cuyo fin es garantizar la integridad y seguridad de los datos personales tratados. En el caso de que los datos sean tratados por un tercero, éste tiene igualmente la obligación de disponer de su propio documento de seguridad, si es que el tratamiento se produce fuera de los locales del responsable del fichero.

Este documento de seguridad debe seguir las normas establecidas en el RDLOPD, en su Título VIII, de las medidas de seguridad en el tratamiento de datos de carácter personal. El documento de seguridad podrá ser único y comprensivo de todos los ficheros y tratamientos o bien individualizado para cada uno de ellos.

Adentrémonos brevemente en el contenido de este documento de seguridad. Lo primero que debemos saber es que los ficheros se clasifican en tres niveles. Cada uno de ellos requiere unas determinadas medidas de seguridad.

Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico, que veremos más adelante.

Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, como son muchos de los que disponen los abogados, aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias, aquellos de los que sean responsables entidades financieras para finalidades relacionadas con la prestación de servicios financieros, y aquellos de los que sean responsables Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar algunas de las medidas de nivel medio.

Los ficheros más sensibles, los que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas, o aquellos que contengan datos derivados de actos de violencia de género deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

En el caso de ficheros o tratamiento de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de mas medidas de seguridad de nivel básico cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros, y cuando se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. También se podrán aplicar las medidas de nivel básico cuando contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple consideración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

4.6.2. Medidas de seguridad

Veamos esquemáticamente en qué consisten estas medidas.

Nivel Básico:

- Ámbito de aplicación con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad.
- Control de acceso y relación actualizada de usuarios.
- Identificación y autenticación de los usuarios.
- Funciones y obligaciones del personal en relación con el tratamiento de los ficheros.
- Estructura de los ficheros y descripción de los sistemas de información que lo tratan.
- Procedimientos de notificación, gestión y respuestas ante las incidencias.

- Procedimientos de copias de respaldo y recuperación de datos en los ficheros automatizados.

- Gestión de soportes y documentos.

- Las medidas a adoptar en el transporte, reutilización y destrucción de soportes y documentos.

Nivel Medio:

- La identificación de uno o varios responsables de seguridad.

- Los controles periódicos que se deben realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

- Auditoría interna o externa bienal de las medidas de seguridad.

- Una gestión de soportes y documentos más detallada que la del nivel anterior.

- Control de acceso físico a los lugares donde estén los equipos físicos que den soporte a los sistemas de información.

- Un registro de incidencias más detallado que el de nivel anterior.

Nivel Alto:

- Una gestión y distribución de soportes más detallada que la del nivel anterior.

- Proceder al cifrado en la distribución de soportes, en la transmisión de datos por redes públicas o inalámbricas, y en el uso de portátiles.

- Establecer un sistema que permita la trazabilidad de accesos.

- Tener el *backup* en lugar distinto al del sistema de información.

- Cifrar los datos en las telecomunicaciones.

Junto a este manual se incluye como Anexo IV una guía de seguridad de la A.E.P.D. con las distintas medidas de seguridad y un modelo de documento de seguridad.

4.6.3. Plazos de implantación

La implantación de las medidas de seguridad deberá producirse con arreglo a las siguientes reglas:

Respecto de los ficheros automatizados que existieran el 19 de abril de 2008:

- Antes del día 19 de abril de 2009, deberán tenerse implantadas las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

    - Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

- Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

- Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del anterior Reglamento de Medidas de seguridad.

- Antes del día 19 de abril de 2009 deberán tenerse implantadas las medidas de seguridad de nivel medio y antes del 19 de octubre de 2009, las de nivel alto exigibles a los siguientes ficheros:

  - Aquéllos que contengan datos derivados de actos de violencia de género.

  - Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

- En los demás supuestos, cuando se exija la implantación de una medida adicional, no prevista en el anterior Reglamento de Medidas de seguridad, dicha medida deberá implantarse antes del 19 de abril de 2009.

Respecto de los ficheros no automatizados que existieran el 19 de abril de 2008:

- Las medidas de seguridad de nivel básico deberán implantarse antes del día 19 de abril de 2009.

- Las medidas de seguridad de nivel medio deberán implantarse antes del día 19 de octubre de 2009.

- Las medidas de seguridad de nivel alto deberán implantarse antes del día 19 de abril de 2010.

Los ficheros, tanto automatizados como no automatizados, creados con posterioridad al día 19 de abril de 2008 deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Por último, hay que señalar respecto a este documento, que no basta con que un abogado o empresa lo tenga para cumplir la normativa, sino que lo realmente importante es tener efectivamente implantadas las medidas que éste contiene. No obstante, queda prohibido registrar datos personales en ficheros que no reúnan las condiciones determinadas con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

4.7. DEBER DE SECRETO

Poco que explicar a los abogados sobre el deber de secreto que ya no sepan, no obstante insistiremos en que existe la obligación del secreto profesional respecto de los datos tratados. Es una obligación que corresponde al responsable del fichero y a cuantos intervengan en cualquier fase del tratamiento de los datos. Ésta perdurará incluso finalizada la relación que

permitía el acceso al fichero. Por ello, todas las empresas o abogados deben informar a todos sus trabajadores de este deber.

Junto a este manual se incluye en el *Anexo I* un modelo de cláusula de deber de secreto.

4.8. TRANSFERENCIAS INTERNACIONALES

Existe la obligación de no realizar transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable a la LOPD, salvo que, se obtenga autorización previa del Director de la A.E.P.D., que sólo podrá otorgarla si se obtienen garantías adecuadas.

Por transferencia internacional de datos hemos de entender el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

Para llevar a cabo una transferencia internacional de datos se requiere previamente una autorización especial de la A.E.P.D., por lo que hay que notificarlo oficialmente a la misma.

Ésta es la norma general, que como siempre tiene sus excepciones, las cuales vemos a continuación:

- Cuando resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- Cuando sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- Cuando sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración las solicitadas por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

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

5. RESPONSABILIDADES DEL RESPONSABLE

La principal responsabilidad del responsable del fichero, ya sea abogado autónomo o sociedad, es que, junto con el encargado del tratamiento, son los únicos sujetos al régimen de sanciones que regula la LOPD.

Otra responsabilidad importante es que ante él se ejercitan los derechos de los afectados

5.1. DERECHOS DE LOS AFECTADOS

Una vez vistas las obligaciones del responsable del fichero, y en su caso del responsable del tratamiento, situémonos ahora al otro lado de la barrera. Vamos a describir los principales derechos de los afectados. Recordemos primero que el afectado es la persona física a la que hacen referencia los datos. Él es el único titular con capacidad para prestar consentimiento al tratamiento de sus datos, y por tanto la LOPD le reconoce una serie de derechos mediante los cuales pueden hacer valer ante el responsable del fichero, su condición de auténtico propietario de la información sobre el recogida en los ficheros.

Los más importantes de todos estos derechos del afectado son los de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales. Estos derechos son independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

Todos estos derechos son personalísimos. Por lo que su ejercicio se limita al afectado. No obstante, también podrá ejercitarse por el representante legal, acreditando dicha condición, cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos. También podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho.

El medio para ejercitar los mismos debe dejar constancia de que la persona que lo realiza es realmente el afectado, ya que, si fuera otra distinta y se le proporcionaran los datos del afectado, nos encontraríamos ante una cesión ilegal de datos. Con el objeto de poder acreditar el ejercicio del derecho se recomienda dejar constancia tanto del envío de la solicitud de ejercicio del derecho y de su remitente, como de la recepción de la misma por parte del responsable del fichero.

Además, el ejercicio de estos derechos deberá ser gratuito, y el procedimiento a seguir para ello sencillo. La comunicación dirigida al responsable del fichero para ejercer estos derechos deberá contener el nombre y apellidos del interesado, fotocopia de su DNI o equivalente, o en su caso firma electrónica identificativa del afectado.

El responsable del tratamiento deberá contestar siempre las solicitudes que le dirijan, independientemente de que figuren datos del afectado en sus ficheros, y le corresponderá la prueba de este deber.

Junto a este manual se incluye como *Anexo II* distintos modelos, facilitados por la A.E.P.D., de ejercicio de estos derechos.

Pasemos a ver el primero de estos derechos.

5.1.1. El derecho de acceso

El derecho de acceso es el derecho del titular de los datos a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.

El responsable del fichero resolverá la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Si la solicitud fuera estimada, y el responsable no acompañase la información a su comunicación, el acceso se hará efectivo durante los diez días hábiles siguientes. Si la petición del afectado no es atendida adecuadamente, podrá dirigirse a la A.E.P.D. para que ésta se dirija al responsable del fichero con el objetivo de hacer efectivo el ejercicio de ese derecho.

Este derecho no puede ser ejercitado en intervalos inferiores a 12 meses, salvo que se acredite un interés legítimo para ello.

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

Respecto a los ficheros de las fuerzas y cuerpos de seguridad del Estado, cuando la finalidad no sea simplemente administrativa, se podrá denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Igualmente, los responsables de los ficheros de la Hacienda Pública podrán denegar el ejercicio de estos derechos cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Sin embargo, el afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la A.E.P.D o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

5.1.2. El derecho de cancelación

Cuando el titular de los datos tuviera conocimiento de que sus datos personales en un fichero son inexactos o incompletos, inadecuados o excesivos, podrá solicitar del responsable del fichero la cancelación de los mismos o su rectificación. Este derecho está limitado por el deber de conservación de los datos durante los plazos previstos en las disposiciones aplicables o durante las relaciones contractuales con la persona o entidad responsable del tratamiento, sin perjuicio de la posible rectificación de los mismos.

Si en el plazo de 10 días no recibe contestación o ésta es insatisfactoria, puede reclamar ante la A.E.P.D., acompañando la documentación acreditativa de haber solicitado la cancelación de datos ante la entidad de que se trate.

Como ya vimos en el punto 4.2 los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados o registrados, y no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Igualmente señala la LOPD que serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en dicha Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

Por lo tanto, si existe una normativa que impida que se puedan cancelar los datos o que permite u obliga a conservarlos, puede denegarse la cancelación de los mismos, haciéndoselo saber al reclamante.

5.1.3. El derecho de rectificación

El derecho de rectificación supone el derecho del afectado a que los datos almacenados en los ficheros del responsable sean veraces y exactos. Asimismo, expresa la obligación del responsable de mantener la veracidad y exactitud de sus ficheros.

Los medios y plazos para el ejercicio del derecho de rectificación son idénticos a los establecidos para el derecho de cancelación.

5.1.4. El derecho de oposición

El derecho de oposición puede ejercitarse en los casos en los que no es necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal. Siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado. Igualmente que los anteriores derechos, el plazo máximo de resolución es de diez días hábiles.

También puede ejercerse este derecho cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, y cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en el tratamiento automatizado de sus datos.

En el caso de los listados de los Colegios profesionales, los afectados tienen derecho a que la entidad responsable del mantenimiento de los mismos, indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial. La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

5.1.5. Comunicaciones electrónicas

Por último respecto a los derechos de los afectados, enunciaremos brevemente algunos de los derechos de los destinatarios de servicios de comunicaciones electrónicas:

- Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable. En el comienzo del mensaje se deberá incluir la palabra “publicidad” o su abreviatura “publi”.

- Prohibición de envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas (*SPAM*). A excepción de cuando exista una relación contractual previa, siempre que se hubieran obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

- Posibilidad de oponerse a su tratamiento mediante un procedimiento sencillo y gratuito.

- Que los destinatarios sean informados de manera clara y completa sobre su utilización y finalidad de las *cookies* en sus accesos a las páginas *web*.

5.2. INFRACCIONES

Los responsables de los ficheros y los encargados de los tratamientos están sujetos al régimen sancionador establecido en la LOPD.

Las infracciones se dividen en tres tipos según la sanción económica que acarrea. Éstas son las siguientes:

- Leves: Sanción de 601,01 € a 60.101,21 €.

- Graves: Sanción de 60.101,21 € a 300.506,05 €.

- Muy Graves: Sanción de 300.506,05 € a 601.012,10 €.

Veamos a continuación ejemplos de estas infracciones.

5.2.1. Infracciones leves

Son infracciones leves:

- No atender solicitud de rectificación y cancelación de datos del interesado.

- No proporcionar información a la A.E.P.D. en aspectos no sustantivos.
- No inscribir ficheros en registro cuando no es infracción grave.
- Proceder a la recogida de datos sin informar a los afectados.
- Incumplir el deber de secreto.

5.2.2. Infracciones graves

Son infracciones graves:

- Crear ficheros sin autorización publicada en el B.O.E.
- Crear o recoger ficheros de titularidad privada con fines distintos al objeto de la empresa.
- Recabar datos sin consentimiento expreso, cuando se precise.
- Incumplir los principios y garantías legales en el tratamiento o uso, cuando no constituya infracción muy grave.
- Impedir ejercer derechos de acceso y oposición o no facilitar información solicitada.
- Mantener datos inexactos o no rectificarlos cuando afecten a los derechos de las personas.
- Vulnerar el deber de guardar secreto en ficheros que contengan datos administrativos, penales, Hacienda pública, servicios financieros, solvencia patrimonial y crédito.
- No otorgar las debidas condiciones de seguridad.
- No remitir las notificaciones requeridas a la A.E.P.D.
- No permitir acceso a la función inspectora.
- Incumplir el deber de información cuando los datos se recaban de persona distinta del afectado.

5.2.3. Infracciones muy graves

Son infracciones muy graves:

- Recabar datos de forma engañosa y fraudulenta.
- Comunicar y ceder datos fuera de los casos permitidos.
- Tratar y crear datos de los especialmente protegidos sin mediar consentimiento expreso.
- No cesar en el uso ilegítimo cuando sea requerido por la A.E.P.D.
- Transferir a países extranjeros sin nivel de protección y sin autorización del Director de la A.E.P.D.

- Tratar los datos de forma ilegítima.
- Vulnerar el deber de guardar secreto de los datos especialmente protegidos.
- No atender u obstaculizar derechos de los afectados.
- No atender sistemáticamente la notificación de inclusión de datos en un fichero.

5.2.4. Administraciones Públicas

Cuando las infracciones fueran respecto de ficheros de los que sean responsables las Administraciones Públicas, no habrá sanción económica, sino que el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que proceda adoptar para que cesen o se corrijan los efectos de la infracción.

5.2.5. Prescripción

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años, y las impuestas por faltas leves al año. El plazo de prescripción de las sanciones, comenzará a contarse desde el día siguiente a aquél en que adquiera firmeza la resolución por la que se impone la sanción.

6. PROTECCIÓN DE DATOS Y ABOGADOS

Como hemos visto, todos los entes con personalidad jurídica tienen la obligación de cumplir la normativa en protección de datos personales. Por tanto, los abogados también tienen esta obligación. Por tanto, es fundamental la concienciación respecto al cumplimiento de la LOPD.

Una vez adquiridos esta concienciación y conocimiento, ha de pasarse a adaptar la actividad laboral a las exigencias de la LOPD.

Lo primero que debe hacerse es localizar todos los ficheros con datos personales que posea el profesional, tanto de los que sea responsable como aquellos otros que trate y sean responsabilidad de otros. Una vez localizados, han de notificarse e inscribirse en el Registro General de Protección de Datos. Tras ello, han de analizar el tratamiento que realizan de estos datos. Han de comprobar si cumplen todas las obligaciones que aquí hemos descrito. Si no fuera así, se han de implantar las medidas necesarias para su cumplimiento. También debe preverse el cumplimiento de los derechos de los afectados.

Tras ello, debe de redactarse un documento de seguridad adaptado a las circunstancias específicas de cada profesional. Y lo que es más importante: deben implantarse efectivamente esas medidas en el proceso de trabajo habitual. Una vez realizado esto, se estará evitando un riesgo muy importante, e incluso será un signo de calidad del trabajo desarrollado.