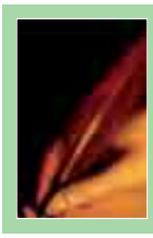

Doctrina

La adaptación de la Ley Orgánica de protección de datos en un despacho de abogados

LA LEY 3139/2012

La adaptación de la Ley Orgánica de protección de datos en un despacho de abogados

Eloisa María FEBLES YANES
Abogada del Ilustre Colegio de Abogados de Santa Cruz de Tenerife

En la actualidad, nuestra LOPD es una de las más exigentes del mundo. En este artículo se aborda lo que supone esta Ley en el campo de la abogacía y, por supuesto, se analizan los puntos fundamentales de la normativa: ¿Quién es «responsable»? ¿Quién es «encargado»?, el registro general de la protección de datos, las sanciones, etc. También se incluye el análisis de un hecho real, así como otras curiosidades relacionadas con el tema de estudio.

I. VENTAJAS DE LA ADAPTACIÓN DE LA LOPD EN UN DESPACHO DE ABOGADOS

Como he señalado anteriormente, la LOPD es una de las más exigentes del mundo y las sanciones aplicables por su incumplimiento son muy elevadas. Por ello, y como abogada en ejercicio, considero que hay una serie de ventajas, implícitas y explícitas, si cumplimos con lo dispuesto en dicha Ley.

Estas ventajas son:

1.º Cumplir con la legalidad establecida por la LOPD y evitar de este modo las sanciones.

2.º El cumplimiento de ese primer punto provoca que debamos llevar una organización de los datos y archivos con los que trabajamos en el despacho.

3.º Tendremos un mayor control de los datos.

4.º De ello se deriva una valoración de los datos con los que tratamos, lo cual se traduce en el activo comercial.

5.º También provocará una adaptación a las normas de calidad.

6.º Todo unido, genera una mayor seguridad y es un valor añadido para los clientes.

II. ¿CÓMO PODEMOS ADAPTARNOS LOS ABOGADOS A LOS REQUISITOS EXIGIDOS POR LA LOPD?

La adaptación se consigue a través de tres factores: análisis, implantación y control.

a) ANÁLISIS.- En primer lugar, hay que proceder a un estudio de qué tipo de bufete se trata (pequeño, mediano, gran empresa...) y de cuál es el tipo de ámbito de actuación que abarca.

b) IMPLANTACIÓN.- Este paso se consigue a través de programas informáticos (generales o específicos). La Ley también habla de tratamiento de datos no informatizados, pero es evidente que en los tiempos que corren en los cuales las nuevas tecnologías ocupan un lugar primordial, y en donde la sociedad es tan competitiva, no contar con las ventajas que suponen las nuevas tecnologías supone estar fuera del mercado en poco tiempo.

c) *CONTROL.*- A través de un responsable tecnológico, por medio de una/s persona/s que se encargue del tratamiento de los datos y que sea responsable de la seguridad. También se debe de tener, al menos, un mínimo conocimiento de la materia y contar con la información necesaria y actualizada (estudio de la normativa).

III. ¿QUIÉN ES «RESPONSABLE»?

Es RESPONSABLE de un fichero o tratamiento la entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.

Sobre el responsable del fichero recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización. El responsable debe:

a) Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.

b) Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.

c) Garantizar el cumplimiento de los deberes de secreto y seguridad.

d) Informar a los titulares de los datos personales de la recogida de éstos.

e) Obtener el consentimiento para el tratamiento de los datos personales.

f) Facilitar y garantizar el ejercicio de los derechos de oposición tratamiento, acceso, rectificación y cancelación.

g) Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto por la LOPD.

h) Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación.

IV. ¿QUIÉN ES EL «ENCARGADO»?

El ENCARGADO del tratamiento es la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta de responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Asociada a la figura del RESPONSABLE, está la figura del ENCARGADO, que es la persona o entidad, autoridad pública, servicio o cualquier otro organismo que, sólo o con otros, trate datos por cuenta del responsable del fichero.

La realización de un tratamiento por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero.

Ambos, encargado y responsable del tratamiento, pueden ser sancionados de acuerdo con la LOPD si incumplen sus obligaciones.

V. ¿CUÁNDO SE TRATAN LOS DATOS PERSONALES?

Los datos personales permiten identificar a una persona. Si se recogen y tratan el nombre, los apellidos, la fecha de nacimiento, el número de D.N.I., se están usando datos que identifican a una persona, ya sea directa o indirectamente. Con todas esas actuaciones se están tratando datos personales y se deben cumplir las obligaciones impuestas por la LOPD, salvo que sea en el ámbito del ejercicio de actividades exclusivamente personales o domésticas.

Es frecuente que prácticamente para cualquier actividad sea necesario que los datos personales se recojan y utilicen en la vida cotidiana. La LOPD regula el tratamiento de cualquier tipo de dato personal con independencia de que éste pertenezca o no a la vida privada del titular. La LOPD se aplica a los tratamientos de datos personales públicos y privados.

No obstante, existen excepciones a las obligaciones fijadas por la LOPD. Según su art. 2.2. La LOPD no será de aplicación:

• «A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas».

• «A los ficheros sometidos a la normativa sobre protección de materias clasificadas».

• «A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la AEPD».

Por otra parte, según lo dispuesto por el art. 2.3. LOPD determinados tratamientos se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la LOPD. Se trata de «ficheros 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».

VI. ÁMBITO DE APLICACIÓN DE LA LOPD

VII. FICHEROS AUTOMATIZADOS Y NO AUTOMATIZADOS

La LOPD define el FICHERO como «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso». Art. 3.b) LOPD.

A partir de esta definición dada por la propia Ley, vemos que el contenido y los requisitos de la misma, no sólo son exigibles respecto de los ficheros automatizados, sino que también comprende a aquellos ficheros no automatizados.

Y es el RDLOPD, en su art. 5.1.n), el que completa esta definición, y por tanto FICHERO NO AUTOMATIZADO es «todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica».

VIII. LA NOTIFICACIÓN DE LOS FICHEROS

1. El deber de notificar

La creación de ficheros se debe notificar para su inscripción en el Registro General de Protección de Datos (RGPD) de la AEPD.

2. ¿Quién debe efectuar la notificación?

La notificación la debe efectuar el responsable del fichero, y esta notificación debe efectuarla:

— Con anterioridad al uso del fichero.

— Cuando de producen cambios respecto a la inscripción inicial.

— Cuando cesa el uso del fichero.

La notificación supone el compromiso por parte del responsable de que el fichero declarado para su inscripción cumple con todas las exigencias legales. Esta notificación no tiene ningún tipo de coste, y permite que los titulares de los datos puedan conocer quiénes son los responsables de los ficheros ante los que ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición.

El no proceder a la notificación de la existencia de un fichero supone una infracción leve o grave, tal y como prevé el art. 44 LOPD, quedando sujeto al régimen sancionador previsto por esta Ley.

IX. EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

El Registro General de Protección de Datos es el órgano al que le corresponde velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal, con la intención de hacer posible el ejercicio de los derechos de acceso, rectificación, oposición y cancelación, regulados en los arts. 14 a 16 LOPD. Por todo ello, es el órgano encargado de la gestión de las inscripciones. El acceso al Registro es público y gratuito.

De acuerdo con lo establecido en el art. 39 de la LOPD, serán objeto de inscripción en el Registro:

a) Los ficheros de los que sean titulares las Administraciones Públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones de transferencias internacionales.

d) Los códigos tipo.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

X. ¿CÓMO ACTUAR AL RECOGER Y TRATAR LOS DATOS?

Siempre hay que informar a los afectados, los cuales deben conocer:

a) Para qué se utilizan sus datos.

b) La existencia de un fichero o un tratamiento de sus datos.

c) Debe indicársele quién es el responsable del fichero y su dirección o la de su representante.

Cualquier persona tiene el derecho a saber si sus datos personales van a ser incluidos en un fichero, y los tratamientos que se van a realizar con esos datos.

Los responsables tienen la obligación de informar al ciudadano cuando recojan datos personales que le afecten. Este derecho de información es básico, porque garantiza que el consentimiento que se preste sea previo, específico e informado y es necesario para permitir el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El art. 5 de la LOPD recoge la obligación que tienen los responsables de los ficheros o tratamientos de informar a los ciudadanos de la incorporación de sus datos a un fichero, de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Sin embargo, la Ley exime del deber de informar sobre alguno de estos aspectos cuando se deduzcan inequívocamente de la naturaleza de los propios datos personales y de las circunstancias en las que se produce la recogida de esos datos.

Esta información debe estar incluida en los cuestionarios o impresos de recogida de datos. En el caso de utilizar Internet como medio de recogida de datos, también existe la obligación de dar esta información a los usuarios que registran sus datos y debe hacerse de tal forma que la información sea siempre previa al tratamiento. Además, el texto informativo debe ser claro y legible. En caso de los menores de edad, el RDLOPD exige que la información se exprese en un lenguaje que sea fácilmente comprensible.

Si los datos se recogen directamente de los afectados, la información debe facilitarse con carácter previo a la recogida de los datos personales.

En el supuesto de que los datos de carácter personal no hubieran sido recabados del interesado, el responsable del fichero o su representante deben informarle de esa recogida en el plazo de los 3 meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad.

El incumplimiento del deber de información se encuentra tipificado como falta leve en el art. 44.2.d) LOPD.

XI. LA IMPORTANCIA DEL CONSENTIMIENTO

Hay que pedir el consentimiento siempre, pues sólo así se podrán tratar los datos del interesado.

OPINIÓN

No hace mucho tiempo, en España no existían normas legales que protegieran de forma expresa los datos personales. En cambio, hoy en día, nuestra Ley Orgánica de Protección de Datos es una de las más exigentes del mundo.

Con este artículo, he realizado un breve estudio por la evolución normativa en esta materia (tanto en nuestro derecho interno como de la normativa procedente de la Unión Europea), e intento acercar el tema de la protección de datos, no sólo de una forma general sino, sobre todo, desde la perspectiva de un abogado en ejercicio: aclarar el ámbito de aplicación de la Ley; aclarar los conceptos innovadores que la misma incorpora; las consecuencias que su vulneración lleva aparejada; cómo evitar infringir la normativa; cómo adaptarnos los abogados a los requisitos exigidos por la LOPD y las ventajas que todo ello conlleva. Y, por supuesto, no olvidar el papel fundamental que para el cumplimiento de la normativa lleva a cabo la Agencia Española de Protección de Datos.

También he intentado completar este trabajo recogiendo algunas curiosidades relacionadas con la protección de datos, y los problemas que se han derivado de la aplicación de las nuevas tecnologías (en concreto, con la utilización de Internet y con ciertos buscadores). De hecho, pocas semanas después de concluir la redacción de este trabajo, Bruselas presentó una reforma legal que llega a establecer sanciones de hasta un millón de euros para las grandes compañías de Internet que no borren los datos de un/os ciudadano/os que haya/n decidido darse de baja (el derecho al «olvido digital»). Y es que, es un tema de tal importancia y actualidad, que a más del 70% de los europeos les preocupa seriamente que sus datos puedan llegar a ser usados para asuntos que desconocen.

El art. 3 h) de la LOPD define el consentimiento como «toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen». Así, para que el consentimiento pueda ser considerado conforme a derecho deben darse esos requisitos: Manifestación de voluntad, libre, inequívoca, específica e informada.

El consentimiento podrá ser tácito en el tratamiento de datos que no sean especialmente protegidos. En este caso será preciso otorgar al afectado un plazo de 30 días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente al tratamiento de sus datos de carácter personal. El responsable del tratamiento debe conocer si la comunicación ha sido objeto de devolución por cualquier causa. Si realmente ha sido devuelta no podrá proceder al tratamiento de los datos referidos a ese interesado.

El afectado debe disponer de un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. Una vez planteada, este tipo de solicitud de consentimiento no será nuevamente posible respecto de los mismos tratamientos y para las mismas finalidades en el plazo de 1 año a contar desde la fecha de la solicitud.

En el caso de los menores de edad hay que distinguir entre los mayores de 14 años, que pueden prestarlo salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela; y los menores de 14 años, supuesto en los que se requerirá el consentimiento de los padres o tutores.

Una manifestación específica del consentimiento se da en los casos del envío de comunicaciones comerciales realizadas a través del correo electrónico o medios de comunicación electrónica equivalentes y regulados por la Ley de Servicios de la Sociedad de Información y del Comercio Electrónico (1). Este tipo de comunicaciones sólo podrá realizarse cuando hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas (opt-in). También pueden realizarse cuando exista una relación contractual previa, siempre que se hubieran obtenido de forma lícita los datos de contacto del destinatario y se emplearan para el envío de comunicaciones comerciales referentes a productos o servicios de la propia empresa que sean similares a los que inicialmente fueron objeto de contratación por el cliente (opt-out). En cualquier caso, el prestador debe ofrecer al destinatario la posibilidad de oponerse a su envío mediante un procedimiento sencillo y gratuito.

El tratamiento de datos sin consentimiento previo del afectado en los supuestos que no estén exceptuados legalmente, puede ser motivo de infracción grave de acuerdo con el art. 44.3.c) LOPD.

Por su parte, la Ley de Servicios de la Sociedad de Información del Comercio Electrónico considera infracción leve el envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos de la Ley y no constituyan infracción grave.

No obstante, no será necesario el consentimiento:

• Si el tratamiento tiene por objeto la satisfacción de un interés legítimo del responsable y lo autoriza una norma con rango de ley o una norma de derecho siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el art. 1 LOPD o cuando sea necesario para que el responsable de su tratamiento cumpla un deber que le imponga una de las citadas normas.

• Si el tratamiento es necesario para el mantenimiento o cumplimiento de un contrato o precontrato de una relación negocial, laboral o administrativa y los datos se refieren a las partes.

• Si el tratamiento es necesario para proteger un interés vital del interesado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento y el tratamiento de los datos es necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos siempre que dicho tratamiento de datos se realice por un profesional sanitario.

• Si el tratamiento es necesario para cumplir las funciones de las Administraciones Públicas en el ámbito de sus competencias.

• Cuando una Ley habilite el tratamiento sin requerir el consentimiento inequívoco de su titular.

• Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo del responsable del fichero o de un tercero a quien se comuniquen los datos.

XII. REVOLUCIÓN EN LA NORMATIVA DE LA PROTECCIÓN DE DATOS

Ahora mismo, la posibilidad del uso de datos personales sin el consentimiento del afectado tiene su origen en un recurso contencioso-administrativo (2) planteado en el 2008 por la Federación de Comercio Electrónico y Marketing Directo ante el Tribunal Supremo en el cual se cuestionaban varios preceptos del RLOPD (3).

Pero, para poder dictar sentencia sobre el problema planteado, el Tribunal Supremo se encontró ante la necesidad de plantear una cuestión prejudicial (4) ante el Tribunal de Justicia de las Comunidades Europeas (TJCE) para que se pronunciara sobre si la normativa española de protección de datos se ajustaba o no a la legislación europea. Por ello, el 24 de noviembre de 2011, el TJCE publica la Sentencia que resolvió las cuestiones prejudiciales planteadas por nuestro Tribunal Supremo.

El art. 7 f) de la Directiva 95/46/CE (5) 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 establece que los Estados miembros dispondrán que el tratamiento de los datos personales sólo podrán efectuarse, entre otros supuestos, si «es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del art. 1 de la presente Directiva»; en concreto, los derechos a la intimidad y a la protección de datos personales, recogidos ahora en los arts. 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

La Sentencia del TJCE señala que el citado art. 7 f) tiene un efecto directo, y que no es admisible que las normativas de los estados miembros en los casos de ausencia del consentimiento del interesado exijan para permitir el tratamiento de datos de carácter personal sea «necesario para la satisfacción de un interés legítimo» y que esos datos se encuentren siempre en fuentes accesibles al público.

No obstante, no hay que entender que sólo la mera invocación de un interés legítimo será motivo suficiente para legitimar el tratamiento de los datos de carácter personal sin el consentimiento del afectado. De hecho, en los propios Fundamentos de Derecho de la Sentencia, el TJCE sostiene la necesidad

de realizar, caso a caso, una ponderación entre el interés legítimo de quien va a realizar el tratamiento de los datos y los derechos fundamentales de los ciudadanos afectados, para poder de esta forma determinar qué interés debe prevalecer atendiendo a las circunstancias concretas. Y también deja claro que «la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado».

Y entre los criterios de ponderación, dicha Sentencia se refiere al hecho de que los datos no se encuentren en fuentes accesibles al público, recordando al respecto que «a diferencia de los tratamientos de datos que figuran en fuentes accesibles al público, los tratamientos de datos que figuran en fuentes no accesibles al público implican necesariamente que el responsable del tratamiento y, en su caso, el tercero/s a quienes se comuniquen los datos dispondrán en lo sucesivo de ciertas informaciones sobre la vida privada del interesado. Esta lesión, más grave, de los derechos del interesado consagrados en los arts. 7 y 8 de la Carta debe ser apreciada en su justo valor, contrapesándola con el interés legítimo perseguido por el responsable del tratamiento o por el tercero/s a los que se comuniquen los datos».

Los efectos derivados de esta Sentencia fueron contemplados por el Tribunal Supremo para pronunciarse sobre el recurso interpuesto contra el Reglamento de la LOPD.

Así, la Sentencia del Tribunal Supremo de 8 de febrero de 2012 gira en torno a si el art. 10.2.b) del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de la LOPD excedía o no de lo previsto en el art. 7 de la Directiva 95/46/CE. Y es que, éste art. 7 de la Directiva establece aquellos supuestos que los Estados miembros tienen que tomar en consideración para autorizar el tratamiento de datos personales, y en concreto en relación a aquel en que el tratamiento es necesario para la satisfacción del interés legítimo perseguido por los responsables del tratamiento o por tercero/s a quienes se comuniquen esos datos, sin otra condición que la prevalencia del interés o de los derechos y libertades fundamentales del interesado que requieren protección. Por el contrario, el art. 10.2.b) del Reglamento de la LOPD, lo que contempla es la necesidad del consentimiento previo del interesado para el tratamiento o cesión de los datos de carácter personal, que los datos figuren en fuentes accesibles al público y que el responsable del fichero, o el

tercero a quien s comuniquen los datos, tengan un interés legítimo para su tratamiento o conocimiento, y siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El fallo de dicha Sentencia es que se anula el art. 10.2.b) del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de la LOPD, por exceder de lo previsto en el art. 7 de la Directiva 95/46/CE, y con ello se «autoriza» a las empresas para que puedan utilizar datos personales sin el consentimiento de sus titulares cuando haya un interés legítimo para ello.

De esta forma, el Tribunal Supremo ha dado un paso innovador y revolucionario en la normativa relativa a la protección de datos de carácter personal, pues se permite hacer un uso de los mismos sin el consentimiento de sus titulares cuando es para un «fin legítimo» y sin la necesidad de que el origen de esos datos sea una fuente de acceso público.

XIII. UN HECHO REAL

1. Supuesto de hecho

El 23 de abril de 1997 Telefónica y Fabregas-Oriola Advocats-Associats suscribieron un contrato de gestión de cobros, a través del cual Telefónica encomendaba al citado Despacho de abogados la gestión del cobro de deudas no pagadas por los titulares del servicio telefónico cuyo domicilio radicara en la zona de Barcelona. A través de ese contrato de gestión de cobros, los abogados del Despacho podían realizar no sólo gestiones extrajudiciales, sino también iniciar el ejercicio de acciones judiciales en nombre de Telefónica (en reclamación de las deudas).

Don Pascual fue un cliente de Telefónica, siendo titular de una línea de teléfono desde el 11 de octubre de 1995 hasta el 30 de noviembre de 2000, dejando una deuda de 38.98 euros (según Telefónica).

El 3 de agosto de 2001, Telefónica comunica al Despacho de Abogados la deuda pendiente de pago de Don Pascual.

El 27 de mayo de 2004 se produjo cese y nombramiento de cargos, traslado de domicilio y cambio de denominaciones sociales del Bufete Fabregas-Oriola, S.L. a Oriola Advocats Associats, S.L.

Oriola Advocats remitió dos escritos a Don Pascual (en agosto de 2004 y en septiembre de 2005), en los que en nombre y representación de Telefónica, le reclamaba el pago de la deuda de 38.98 euros; y en el texto de los dos escritos aparecían dos números de contacto (de teléfono y otro de fax), así como un número de cuenta corriente del Banco Popular para que procediera a la realización de su ingreso.

Telefónica y Oriola Advocats suscribieron el 1 de enero de 2006 un contrato de arrendamiento de servicios profesionales, acordando someter las estipulaciones de dicho contrato a los asuntos en trámite encomendados con anterioridad por telefónica.

La dirección a la que enviaron las dos notificaciones a Don Pascual no eran válidas, y por ello Oriola Advocats contrató los servicios de una empresa de detectives para localizar el domicilio real de Don Pascual. Dicha empresa de detectives cumplió con su trabajo y les facilitó una dirección.

Con la dirección facilitada por los detectives, el Despacho de abogados se pone de nuevo en contacto con Don Pascual, y le dicen que tienen en su poder una serie de datos facilitados por Telefónica y que entienden que pudieran estar incompletos, por lo cual le solicitan que se ponga en contacto con el despacho para poder aclarar algunos aspectos sobre la información que poseen, y así no causarle ninguna otra molestia. Al pie de la carta (y como en los dos supuestos anteriores) se informa que los datos que obran en poder de Oriola Advocats han sido proporcionados por Telefónica, responsable del fichero en el que obran los mismos y respecto al que Oriola Advocats actúa como encargada del tratamiento.

Cuando Don Pascual recibe esta comunicación formula una denuncia ante la AEPD, el 31 de mayo de 2006, por tratamiento inadecuado de sus datos, alegando que no mantiene relación contractual con Telefónica, que concluyó en el año 2000 y que mientras esa relación duró su domicilio era otro.

La AEPD abre un procedimiento sancionador contra Oriola Advocats, S.L (PS/00152/2008) y después de estudiar el caso en cuestión, le impone una multa de 60.101,21 euros.

2. Comentario

Los puntos principales del procedimiento sancionador contra el Despacho de abogados, en mi opinión, son:

a) El haber conseguido el nuevo domicilio a través de una agencia de detectives, no está amparado por el contrato de prestación de servicios que tiene suscrito con Telefónica, vulnerando así lo establecido por el art. 6 en cuanto al consentimiento del afectado. El Despacho tenía que haber tenido el consentimiento expreso de Don Pascual para someterlo a tratamiento, o bien probar que concurrían algunas de las excepciones previstas por el art. 6.2 de la LOPD. La Ley exige el consentimiento expreso e inequívoco por parte del afectado, salvo que la Ley disponga otra cosa, y es evidente que en este caso Don Pascual no pudo dar su consentimiento. Pero sí que entiendo que se da una de las circunstancias especiales del art. 6.2. puesto que se puede prescindir de dicho consentimiento cuando los datos se refieran a las partes de un contrato o precontrato y sean necesarios para su mantenimiento y/o cumplimiento. Aquí es obvio que la relación con Telefónica existía con anterioridad y que había dejado una deuda que debía pagar.

b) La infracción por la que se sanciona a Oriola Advocats se tipifica en el art. 44.3.d) LOPD, en relación con el art. 6 del mismo cuerpo legal. Y que supone el tratamiento de datos de carácter personal con vulneración del principio de consentimiento (que es uno de los pilares básicos de la normativa de protección de datos).

c) Por otra parte, también puede considerarse que ha habido un acceso a los datos por cuenta de terceros, vulnerando así lo establecido por el art. 12 LOPD. Sin embargo, debido a los contratos de gestión de cobro y de servicios realizados entre el Despacho y Telefónica puede considerase que los abogados han quedado como encargados del tratamiento, con lo cual no se habría vulnerado dicho art. 12.

Obviamente, el Despacho recurre la sanción de la AEPD, y la Sentencia de la Audiencia Nacional de 21 de enero de 2010 declara en su Fundamento de Derecho quinto párrafo cuarto: «... la deuda cuya gestión de cobro fue encomendada a la actora por Telefónica deriva de la relación contractual mantenida por dicha operadora con el señor Pascual para la que facilitó el dato de su domicilio. Denunciante que se convirtió en moroso de Telefónica, por lo que la entidad recurrente en virtud del contrato suscrito con la operadora realizó dos gestiones de cobro en el domicilio por ella facilitado, y como quiera que dicho señor Pascual cambió de domicilio la recurrente encomendó a una empresa de detectives su localización facilitándole uno nuevo al que se remitió la comunicación de mayo de 2006, siendo necesario el tratamiento del dato del domicilio para el cumplimiento o ejecución del citado contrato. Por todo lo cual... cabe concluir que no se ha producido infracción del principio del consentimiento por lo que procede estimar el recurso y anular la resolución recurrida».

XIV. MEDIDAS DE SEGURIDAD

Se deben adoptar las medidas de índole técnica que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

El art. 9 de la LOPD condiciona estas medidas al 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.

a) La aplicación de las medidas de seguridad se ordena a garantizar la confidencialidad, integridad, y disponibilidad de los datos. La seguridad constituye un instrumento esencial para garantizar el derecho fundamental a la protección de datos.

b) Las medidas de seguridad se aplican tanto por el responsable del fichero, como por el encargado del tratamiento.

c) Deben aplicarse medidas de seguridad a ficheros y tratamientos en soportes no automatizados.

De conformidad con lo dispuesto en el art. 44.3 h) de la LOPD, constituye infracción grave «mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen».

XV. ¿CUÁLES SON LOS NIVELES DE SEGURIDAD?

El Reglamento de desarrollo de la LOPD fija tres niveles de seguridad, atendiendo a la naturaleza de la información.

Los niveles de seguridad son acumulativos de modo que, por ejemplo, un fichero de nivel alto deberá aplicar también las medidas previstas en el nivel básico y medio.

→ **NIVEL BÁSICO** = Abarca todos los ficheros que contengan datos de carácter personal. En el caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual será suficiente la implantación de las medidas de seguridad de nivel básico cuando:

a) 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.

b) Se trate de ficheros de tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

c) Se trate de ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

→ **NIVEL MEDIO** = Este nivel abarca aquellos ficheros o tratamientos relativos a:

a) La comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el art. 29 de la LOPD.

c) Aquellos de los que sean responsables las Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias, y aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquellos 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 de localización. Estos ficheros aplicarán además de previsto en el art. 103 RDLOPD respecto del registro de acceso.

g) Aquellos 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.

→ **NIVEL ALTO** = Se aplicará en aquellos ficheros o tratamientos que:

a) Se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales son consentimiento de las personas afectadas.

c) Los que contengan datos derivados de actos de violencia de género.

XVI. EL DEBER DE GUARDAR SILENCIO

Existe una obligación de guardar secreto profesional sobre los datos de carácter personal a los que se tenga acceso, y ello implica a todos aquellos/as que intervengan en cualquier fase del tratamiento; y este deber de guardar silencio, subsiste incluso después de finalizar su relación con el responsable del fichero. Art. 10 de la LOPD.

El incumplimiento del deber de secreto puede ser constitutivo de una infracción leve, en los términos del art. 44.2.e); o de una infracción grave de acuerdo con lo previsto en el art. 44.3.g) LOPD.

La vulneración del deber de guardar secreto sobre los datos de carácter personal especialmente protegidos a los que hacen referencia el art. 7 en sus apartados 2 y 3 de la LOPD, así como aquellos que hayan sido recabados para fines policiales sin el consentimiento de las personas afectadas, pueden ser constitutivos de una infracción muy grave en los términos del art. 44.4.g) LOPD.

XVII. LAS SANCIONES

Las sanciones se establecen en el art. 45 LOPD. Sobre las mismas, se especifica que la cuantía se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos afectados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora. Además, existe un régimen específico en el caso de los ficheros de titularidad pública.

En ningún caso puede imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

Soplan vientos de cambio en la normativa de protección de datos. El domingo 6 de marzo de 2011 entró en vigor la modificación del régimen sancionador de la LOPD, una reforma que se ha «colado» dentro de la Ley de Economía Sostenible (6). Esta reforma supone la mayor novedad en la normativa de protección de datos desde que en el año 2007 se aprobó el Reglamento de desarrollo de la LOPD.

El nuevo texto crea la figura del *apercibimiento*, que permitirá a la AEPD solicitar acciones correctoras en lugar de abrir directamente un expediente sancionador a las empresas que cometan una infracción.

El texto también modifica la tipificación de las infracciones que contempla la LOPD, y que se clasifican en leves, graves y muy graves (modificando el grado —hacia arriba o hacia abajo— de ciertas infracciones), y establece nuevos criterios de atenuación de las sanciones (los que permiten a la AEPD fijar la cuantía de la sanción aplicando la escala relativa a las sanciones que precedan en gravedad a la del caso de que se trate).

Y eso no es todo, pues también ha modificado ligeramente el importe de las sanciones. Así, podemos encontrarnos:

→ INFRACCIONES LEVES = De 900 a 40.000 euros

→ INFRACCIONES GRAVES = De 40.001 a 300.000 euros

→ INFRACCIONES MUY GRAVE = De 300.001 a 600.000 euros

XVIII. EL «DÍA DE LA PROTECCIÓN DE DATOS»

El día 28 de enero se celebra el «Día de la Protección de Datos». Es una jornada impulsada por la Comisión Europea, el Consejo de Europa y las autoridades de protección de datos de los Estados miembros de la Unión Europea, con el objetivo de impulsar el conocimiento entre los ciudadanos acerca de cuáles son sus derechos y responsabilidades en materia de protección de datos.

La elección del 28 de enero como fecha para la celebración de este día no es casual. Fue el 28 de enero de hace 30 años cuando se firmó el Convenio 108 del Consejo de Europa, piedra angular de la protección de datos en Europa para garantizar en el territorio de cada Estado a cualquier persona física el derecho a su vida privada con respecto al tratamiento de los datos de carácter personal.

Como celebración conjunta, el Consejo de Europa y la Comisión Europea celebraron el pasado 28 de enero, en Bruselas, una jornada bajo el nombre de *«Data protection 30 years later: from European to internacional Standard»*. Este encuentro marcó, además, el inicio de una consulta pública abierta a los ciudadanos, estados, empresas e instituciones, en el contexto del proceso de modernización del Convenio 108.

Además, algunos organismos de cada uno de los Estados miembros ha aprovechado esta celebración para organizar sus propios actos.

XIX. ESPAÑA, A LA CABEZA DE LA UE EN VULNERACIÓN DE DATOS PERSONALES EN INTERNET

España y Bulgaria están en la cima de los países de la Unión Europea en cuanto a fallos en la protección de datos personales en Internet, según un informe de la oficina comunitaria de estadística, Eurostat. En ambos países, un 7% de los usuarios denunciaron haber visto en los últimos doce meses en la Red información personal sin que previamente se les haya pedido su consentimiento para su manejo *online*.

A nivel europeo, la media de denuncias sobre abusos de este tipo se situó en un 4%. Detrás de España y Bulgaria, los países que acumulan más abusos son Italia y Holanda, con un 6% de denuncias; seguidas de Francia, Portugal, Rumanía y Letonia, con un 5% de casos.

XX. LA AUDIENCIA NACIONAL CONSULTA AL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA QUÉ HACE CON GOOGLE

¿Se puede entender la localización de páginas web y su indexación en un buscador de Internet como tratamiento de datos? Ésta es una de las cuestiones que ha planteado la AEPD a la Audiencia Nacional. El investigado es nada menos que Google, el líder en búsquedas a través de la red, al que denunciaron 80 particulares que consideraron que su intimidad fue vulnerada porque sus datos personales se recogieron en sus resultados de búsquedas. Piden que se ejecuten acciones para garantizar su «derecho al olvido», es decir, que se borre de los índices del buscador información personal que quieren que desaparezca de Internet.

El caso podría llegar al Tribunal de Justicia de la Unión Europea, en Luxemburgo, porque son numerosas las dudas que plantea a la Audiencia Nacional, que se enfrenta también a cuestiones interpretativas sobre derecho europeo. Por ello, ha abierto un plazo de 15 días para que las partes presenten sus alegaciones ante la posibilidad de que el caso llegue al Tribunal Europeo.

Las versiones de las partes son diametralmente opuestas. Por un lado, Google alega que ni la AEPD ni los tribunales españoles tienen competencia para sancionarlo porque el almacenamiento de páginas web y su enlace es una actividad que se realiza en Estados Unidos. Asimismo, cree que la responsabilidad sobre la información y datos que publican las webs recae en los editores de las mismas y apela a la libertad de expresión: exigir a un motor de búsqueda que censure el material publicado por terceros atentaría contra este derecho fundamental.

Sin embargo, la AEPD cree que ningún ciudadano que no sea un personaje público de relevancia debe resignarse a que sus datos personales circulen por la red, por lo que insiste en defender el derecho de quienes solicitan la cancelación de referencias privadas en foros, blogs, redes y otros soportes de Internet que vulneren su dignidad personal.

Luxemburgo tendrá la última palabra para determinar si Google realiza un tratamiento de datos a la hora de indexar páginas web y si los responsables de borrar esa información son las webs o el gigante mundial de los buscadores online. El caso va para largo.

XXI. LA UE QUIERE GARANTIZAR POR LEY EL «DERECHO AL OLVIDO» EN INTERNET

El *«derecho al olvido»*, es decir, la posibilidad de que los datos personales de un usuario que se da de baja de una red social desaparezcan de Internet, se incorporará en la reforma de las normas de protección de datos que impulsará la Unión Europea, una iniciativa que busca adaptar la legislación actual de los países miembros a los cambios provocados en los últimos años por el uso generalizado de las nuevas tecnologías.

La vicepresidenta de la Comisión Europea, Viviane Reding, ha anunciado que antes del verano presentará una propuesta legislativa con varias novedades. Entre ellas están las garantías *«por defecto»* para la protección de información personal en internet, que exigirá el consentimiento expreso de los usuarios de redes sociales como Facebook para el tratamiento de sus datos con fines que no hayan sido especificados inicialmente.

Pero eso no es todo. También se exigirá a las redes sociales que cumplan con el deber de informar a los internautas sobre los datos que recogerán, los fines de su recogida, el uso que se dará por parte de terceros y los riesgos que supone subir información personal en Internet. La nueva legislación se aplicará también a empresas situadas fuera de la UE pero que su actividad implique el tratamiento de datos de ciudadanos comunitarios, como es el caso de Google. Además, la nueva normativa otorgará mayores competencias a los organismos estatales encargados de velar por la seguridad de los datos personales, como la AEPD.

XXII. LAS SUGERENCIAS DE LA AEPD PARA REFORMAR LAS NORMAS DE PROTECCIÓN DE DATOS DE LA UE

La AEPD envió sus sugerencias a la Comisión Europea para que las tome en consideración de cara a la próxima revisión de la Directiva 95/46/CE, relativa a la protección de datos de las personas físicas. Alguno de los puntos más destacados de esta propuesta son:

⇔ **COLABORACIÓN** = Mayor cooperación entre las autoridades nacionales de protección de datos, abriendo la posibilidad de que estos organismos participen en actividades de investigación y auditorías realizadas en otros estados miembros de la Unión Europea cuando los hechos que investiguen afecten a individuos bajo su tutela.

⇔ ***«DERECHO AL OLVIDO»* EN INTERNET** = La Agencia propuso que el marco legal comunitario establezca medidas de obligado cumplimiento para los responsables del tratamiento que permitan el *«borrar de la red»* los datos de aquellos usuarios que así lo deseen. Entre estas medidas, se ha propuesto la adopción de tecnologías que impidan la indexación de datos de carácter personal por motores de búsqueda y su aplicación efectiva en plazos perentorios.

⇔ **DEFINICIÓN DE DATO PERSONAL** = La AEPD quiere que el concepto de *«dato personal»* incluya en su definición las técnicas para el tratamiento de la información que permitan singularizar a una persona o usuario. La idea es que abarque aquellas situaciones en las que se desconoce el nombre del sujeto, pero se tiene un perfil completo de él.

⇔ **SEÑALES INFORMATIVAS** = Otra de las interesantes propuestas consiste en acuñar símbolos o iconos informativos sobre el tratamiento de protección de datos, que permitan a los usuarios reconocer fácilmente las características de los tratamientos que se están llevando a cabo sobre su información personal. Se trata de una medida pensada especialmente para los menores de edad que introducen sus datos personales en Internet.

XXIII. BIBLIOGRAFÍA

DÍAZ-AMBRONA BARDAJÍ, María Dolores; HERNÁNDEZ DÍAZ-AMBRONA,

María Dolores; POUS DE LA FLOR, M. P.; TEJEDOR MUÑOZ, L. *Derecho Civil de la Unión Europea*. Cuarta edición. Editorial Colex. 2010.

MARTÍNEZ, R. *Resumen técnico: ámbito de aplicación de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal*. Tirant lo Blanch. Valencia 2010.

TRONCOSO REIGADA, A. *Comentario a la Ley de Protección de Datos*. Editorial Civitas. Madrid 2010.

VIZCAÍNO CALDERÓN, M. *Comentarios a la Ley Orgánica de Protección de Datos de carácter personal*. Editorial Civitas. Madrid 2011.

XIV. LEGISLACIÓN

— Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 d diciembre, de Protección de Datos de Carácter Personal.

— Ley 2/2011, de 4 de marzo, de Economía Sostenible.

— Reglamento n.º 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

— Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

— Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

XV. INTERNET

www.aepd.es

www.tirantonline.com

www.laleydigital.es

www.boe.es ■

NOTAS

(1) BOE número 166 de 12 de julio de 2002.

(2) Recurso contencioso-administrativo número 25/08.

(3) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE número 17 de 19 de enero de 2008.

(4) Asunto C-468/10 y C-469/10

(5) Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

(6) BOE número 55 de 5 de marzo de 2011.

rincón DELECTURA

LA LEY 107/2012

Esquemas procesales civiles, penales y concursales (3.ª edición)

AUTOR: Redacción La Ley

EDICIÓN: LA LEY, 2012, 292 páginas

En un entorno jurídico cuya complejidad crece día a día, esquematizar al máximo los pasos a dar en los procesos judiciales, sin que suponga una merma en el caudal informativo, constituye un importante desafío que hemos querido afrontar con esta publicación.

LA LEY recoge en esta obra un riguroso y exhaustivo compendio de esquemas procesales CIVILES, PENALES y CONCURSALES, que constituyen una extraordinaria herramienta de trabajo para profesionales del derecho: abogados, jueces, fiscales y procuradores, porque les ayudará a acercarse con éxito a los Tribunales, conociendo con soltura cuál es la vía procesal adecuada. También es útil para los estudiantes de derecho y sus profesores: a los primeros les supondrá contar con un esquema de sus libros de texto, y a los segundos les apoyará en la difícil tarea de explicar en sus clases el entramado de fases procesales. Un manual de consulta y referencia absolutamente imprescindible en cualquier biblioteca jurídica.

En esta nueva edición incorporamos las reformas y novedades de la Ley 37/2011, de 10 de octubre, de medidas de AGILIZACIÓN PROCESAL y de la Ley 38/2011, de 10 de octubre, de reforma de la LEY CONCURSAL.

CONTENIDO

Procesos Civiles

Juicio ordinario; Juicio verbal; Juicio verbal de desahucio por falta de pago; Juicio monitorio; Juicio cambiario; Procesos sobre la capacidad de las personas; Procesos sobre filiación, paternidad y maternidad; Procesos matrimoniales; Procesos de adopción; Procesos sobre determinados aspectos de la protección de menores; Procesos de división de la herencia; Procesos de liquidación del régimen económico matrimonial; Procesos de cuenta de procurador y abogado, y Fases comunes (acumulación, medidas cautelares, recursos, ejecución y revisión de sentencias).

Procesos Penales

Procedimiento ordinario; Procedimiento abreviado; Procedimiento ante el Tribunal del Jurado; Juicios rápidos; Juicios de faltas; Procedimiento para exigir la responsabilidad penal de los menores; Procedimientos especiales; Medidas cautelares; Recursos; Ejecución de sentencias.

Procesos Concursales

Esquema general; Declaración de concurso; Administración concursal; Fase común; El convenio y su cumplimiento; Liquidación; Calificación concursal; Conclusión y reapertura; Incidente concursal; Procedimiento abreviado; Derecho internacional privado, y Refinanciación. ■