ARTÍCULOS

EL NUEVO REGLAMENTO DE DESARROLLO DE LA LOPD

CECILIA ÁLVAREZ RIGAUDIAS (*)
(*) Abogado

El 19 de enero de 2008 se publicó en el BOE el Reglamento 1720/2007, de 21 de diciembre de 2007, que desarrolla la Ley Orgánica de Datos de Carácter Personal (el «Reglamento» y la «LOPD»).

El Reglamento, que entró en vigor el 19 de abril de 2008, pretende (i) desarrollar la LOPD de forma completa, adaptando la regulación reglamentaria parcial existente (que es anterior a su entrada en vigor) y (ii) plasmar ciertos criterios interpretativos de los tribunales y de la Agencia Española de Protección de Datos (la «AEPD»).

Se resumen a continuación las principales novedades o precisiones que introduce el Reglamento y se sugieren determinadas acciones a adoptar a la luz de éstas.

1 · ÁMBITO OBJETIVO DE APLICACIÓN

El Reglamento excluye de su ámbito de aplicación objetiva a ciertos ficheros de datos de contacto de las personas jurídicas así como a los ficheros relativos a la actividad de comerciante del empresario individual.

Respecto de los primeros, el artículo 2.2 del Reglamento establece que:

> *«Este Reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, 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».*

Para que esta excepción sea de aplicación, es necesario que se cumplan dos condiciones: (i) que los datos tratados se limiten a los listados en el Reglamento (por ello, no se encontrarían excluidos los ficheros en los que, por ejemplo, constara el DNI); y (ii) la finalidad del tratamiento debe corresponderse con el contacto con la persona jurídica, siendo el dato del afectado únicamente el medio para lograr esa finalidad.

Por otra parte, respecto de los datos del empresario individual, el Reglamento excluye de su ámbito de aplicación, en su artículo 2.3, a los datos del comerciante que hagan únicamente referencia a su actividad empresarial (a su condición de comerciante, industrial o naviero). De nuevo, el uso de los datos deberá quedar limitado a las actividades empresariales tal y como expresa la AEPD:

> *«El sujeto respecto del que pretende llevarse a cabo el tratamiento es la empresa constituida por el comerciante industrial o naviero y no el empresario mismo que la hubiese constituido. Si la utilización de dichos datos se produjera en relación con un ámbito distinto quedaría plenamente sometida a las disposiciones de la Ley Orgánica.»* [1]

(*) Del Area de Derecho Mercantil de Uría Menéndez (Madrid). Especialista en protección de datos.

1 Informe de la AEPD 2008/0078.

2 · LEGITIMIDAD DEL TRATAMIENTO

El Reglamento regula de manera sistemática las causas que determinan la legitimidad del tratamiento, destacando, en particular, la regulación del interés legítimo, las previsiones específicas relativas al consentimiento tácito y la información que ha facilitarse para la validez del consentimiento para la cesión.

2.1 · Interés legítimo

Es conocida la —aparente— dificultad que ha expresado en ocasiones la AEPD respecto del reconocimiento del «interés legítimo del responsable» como causa legitimadora del tratamiento, por causa de la incorrecta transposición en la LOPD de la 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 (la «Directiva 95/46/CE»).

El interés legítimo del responsable se expresa como sigue en el artículo 7 de la Directiva 95/46/CE:

> *«Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:* [...]
>
> *f) 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 artículo 1 de la presente Directiva.»*

A este respecto, de acuerdo con el *principio de «interpretación conforme»* desarrollado por la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, la norma nacional de transposición, y el Derecho nacional en su conjunto, han de interpretarse y aplicarse a la luz del texto y la finalidad de la Directiva comunitaria (*vid.* TJCE, sentencia de 10 de abril de 1984, Von Colson y Kamann, asunto 14/83; sentencia de 13.11.1990, Marleasing, asunto C-106/89; TJCE, sentencia de 16.12.1993, Wagner Miret, asunto C-334/92; sentencia de 11.7.2002, Marks & Spencer, asunto C-62/00).

En palabras de nuestro Tribunal Supremo:

> «*Las normas del ordenamiento jurídico interno deben ser interpretadas por todos los tribunales en el sentido más conforme al Derecho Comunitario, con independencia de que la norma sea anterior o posterior a una Directiva, y que ésta haya sido o no transpuesta mediante Ley interna.*» (Sentencia núm. 428/2007, de 16 abril de 2007).

De conformidad con esta doctrina, al aplicar el Derecho interno, el órgano jurisdiccional nacional está obligado a hacer todo lo posible, a la luz de la letra y de la finalidad de la Directiva, para, al efectuar dicha interpretación, alcanzar el resultado que persigue la Directiva y de esta forma atenerse al artículo 189.3 del Tratado CE (actualmente artículo 249 TCE, párrafo tercero). De hecho, si dicha interpretación conforme no es posible, el órgano jurisdiccional nacional debe aplicar íntegramente el Derecho comunitario y proteger los derechos que éste concede a los particulares, así como abstenerse de aplicar, en su caso, cualquier disposición en la medida en que tal aplicación conduzca, en las circunstancias del litigio, a un resultado contrario al Derecho comunitario.

Por tanto, el «interés legítimo» debe entenderse incorporado a nuestro ordenamiento por el principio de interpretación conforme desarrollado por la jurisprudencia del TJCE, en este caso, del artículo 6.2 de la LOPD con el artículo 7.1 de la Directiva que (a diferencia del Reglamento), como hemos visto, prevé este supuesto como una causa legitimadora autónoma del tratamiento, *distinta de otras* tales como el consentimiento del afectado, la habilitación legal o el desarrollo del contrato con el afectado. Por ello, a nuestro juicio, es incorrecto subsumir el «interés legítimo» en las otras causas que legitiman el tratamiento como hace el Reglamento (el amparo en una norma con rango de ley, el desarrollo del contrato entre el responsable y el afectado, etc.), sin haberlo tratado como una categoría propia.

2.2 · Consentimiento tácito

Para la validez del consentimiento tácito, se establecen las siguientes condiciones:

(i) otorgamiento de un plazo de treinta días para que el afectado manifieste su oposición, en su caso;

(ii) información precisa al afectado de que su silencio será considerado como consentimiento al tratamiento de sus datos personales;

(iii) puesta a disposición de un medio sencillo y gratuito para que el afectado manifieste su oposición (el Reglamento cita expresamente a estos efectos, con carácter ejemplificativo, los envíos prefranqueados o los números telefónicos gratuitos o a los servicios de atención al público);

(iv) que no se haya solicitado el consentimiento para los mismos tratamientos y finalidades sin que haya transcurrido al menos un año; y

(v) constancia de que el afectado ha recibido la solicitud.

Respecto de la prueba de este último requisito, la AEPD se ha mostrado particularmente estricta en casos similares [2]:

«— La mera contratación de un medio independiente para la notificación no acredita más que la existencia del contrato, pero no que se ha hecho el envío.

— La prueba del envío de una notificación no acredita por sí misma su recepción por el afectado.

— Si el destinatario niega la recepción, la carga de la prueba del envío recae sobre el responsable del tratamiento.

— El que se hayan efectuado otras notificaciones al afectado no es suficiente para probar la notificación del «documento» respecto del cual se niega la recepción.»

Si la remisión de la solicitud del consentimiento es encargada a un tercero, el responsable debe asegurarse que en el contrato de prestación de servicios se garantice este extremo (además del contenido obligatorio del artículo 12.2 de la LOPD).

A estos efectos, basándonos en algunos precedentes valorados positivamente por la AEPD, sería adecuado que en el contrato se prevea expresamente que el prestador de servicios certifique el proceso de generación e impresión de las comunicaciones (fecha, número de cartas identificadas e incidencias) y la puesta a disposición del servicio de correos para su posterior distribución por parte de dicho servicio (fecha y número de cartas identificadas e incidencias) y proporcione copia de la nota de entrega en Correos y Telégrafos (número de cartas y fecha) a nombre del responsable y albarán de entrega. El consentimiento no se podrá entender prestado por aquéllos que consten en las listas de devoluciones o respecto de los cuales haya habido incidencias en el proceso de generación e impresión de las comunicaciones o de su puesta a disposición al servicio de correos.

2.3 · Cesión

Respecto de la información que ha facilitarse para la validez del consentimiento para la cesión, el Reglamento (artículo 12.2.) se refiere de forma cumulativa (a diferencia del artículo 11.3 de la LOPD) a la finalidad concreta y el tipo de actividad del cesionario:

«Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.»

3 · ENCARGADO DE TRATAMIENTO

El Reglamento establece un estatuto propio del encargado de tratamiento. Destacan, en particular, los siguientes extremos: la diligencia *in eligendo* que ha de desplegar el responsable, la subcontratación, la conservación de los datos una vez finalizada la prestación, las medidas de seguridad cuando el tratamiento se efectúa en los locales del responsable o el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) ante el encargado.

3.1 · Diligencia *in eligendo*

Conforme al artículo 20 del Reglamento, cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales conforme al artículo 12.1 de la LOPD deberá velar por que el encargado reúna las garantías para el cumplimiento de sus obligaciones de conformidad con el Reglamento.

3.2 · Subcontratación

Los problemas que plantea la subcontratación surgen desde el momento en que el encargado tiene prohibido comunicar los datos a cualquier tercero, conforme al artículo 12.2 de la LOPD, que dispone que:

«*El encargado del tratamiento* [...] *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*».

Recogiendo la doctrina de la AEPD [3] sobre la subcontratación, el artículo 21 del Reglamento establece dos posibles escenarios:

2 Informe de al AEPD 0111/2005.

3 Recomendaciones de la AEPD referentes al plan de inspección de oficio a las empresas participantes en la elaboración de los censos de población y viviendas del año 2001, de fecha 17 de julio de 2003, así como el informe de la AEPD 513/2004.

(i) que el responsable contrate con el subcontratista (que será un «subencargado»), apoderando al efecto al encargado; o

(ii) que el responsable autorice al encargado cada subcontratación, a cuyos efectos (a) el responsable deberá conocer la identidad del subcontratista y los servicios objeto de subcontratación; (b) el tratamiento de los datos personales por el subcontratista deberá ajustarse a las instrucciones del responsable; y (c) el encargado y el subcontratista deberán suscribir el contrato del artículo 12 de la LOPD.

El artículo 21 del Reglamento no limita su aplicación a los encargados de tratamiento sitos en el Espacio Económico Europeo u otros países (territorios o sistemas) cuyo nivel de protección haya sido considerado «adecuado», y la definición de «exportador» de datos del Reglamento (artículo 5.1j) [4]) ya no se circunscribe al responsable [5], por lo que no debería de plantear dificultades insalvables trasladar el escenario (ii) al encargado de tratamiento «internacional», sustituyendo el contrato del artículo 12 de la LOPD por las cláusulas contractuales tipo de la Comisión Europea.

3.3 · Delimitación de responsabilidades: conservación de los datos, medidas de seguridad y derechos ARCO

El Reglamento establece determinados criterios que permiten delimitar la responsabilidad de encargado y responsable respecto de los conservación de los datos, medidas de seguridad y los derechos ARCO:

(i) Conservación (artículo 22 del Reglamento)

Tal y como establece el artículo 12.3 de la LOPD, el encargado debe destruir o devolver al responsable los datos personales una vez terminada la prestación de servicios que legitimaba su tratamiento. Sin embargo, el cumplimiento de esta obligación había venido planteando no pocas dudas respecto de las eventuales obligaciones legales de conservación de datos que pudieran pesar sobre el encargado o simplemente de la capacidad del encargado de poder probar la corrección de la prestación realizada y de sus eventuales obligaciones de bloqueo conforme al artículo 16.3 de la LOPD.

El Reglamento opta por dar respuesta a estas cuestiones de la siguiente forma:

— no procederá la destrucción de los datos cuando exista un deber legal de conservación; sin embargo para cumplirlo el encargado dependerá del responsable ya que deberá devolver los datos al responsable, sobre quien pesará la obligación de garantizar esta conservación; y

— el encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable, separándose de esta forma de los criterios establecidos en el informe de la AEPD 283/2004 [6].

(ii) Medidas de seguridad (artículos 82 y 88 del Reglamento)

Respecto de las medidas seguridad, es el lugar de prestación de los servicios el que determinará el alcance de las obligaciones del encargado. Si la

---

4 «Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.»

5 Informe de la AEPD 582/2004 (Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección. Necesidad de intervención del responsable): «De este modo, para que la transferencia a la que se refiera la consulta pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, a fin de obtener la preceptiva autorización del Director de la Agencia Española de Protección de Datos, sería necesario que en las cláusulas contractuales que se firmasen el responsable del tratamiento tuviese, en todo caso, la condición de exportador, a los efectos previstos en la Decisión 2002/16/CE.
En consecuencia, el modelo al que se refiere la solicitud de informe no resulta admisible dentro de lo establecido en la Ley Orgánica 15/1999, en conexión con la Decisión 2002/16/CE, dado que la misma únicamente resulta aplicable a los supuestos en que el exportador sea responsable del tratamiento, no existiendo ningún modelo contractual que permita la autorización del Director de la Agencia a la transferencia internacional de datos con destino a estados que no ofrezcan un nivel adecuado de protección en que tanto la parte importadora como la exportadora tengan la condición de encargadas del tratamiento.»

6 «[...] *debe concluirse que si bien no es posible la aplicación al encargado del tratamiento de la previsión contenida en el artículo 16.3, que permite la conservación de los datos previo bloqueo de los mismos a disposición de los órganos judiciales o administrativos que sean competentes para depurar las responsabilidades que se derivasen del tratamiento, cabría que en el propio instrumento contractual en que se fundase la relación existente entre el responsable y el encargado del tratamiento se hiciese constar expresamente que las partes no considerarán cumplida la prestación, a los efectos previstos en el artículo 12.3 de la Ley Orgánica 15/1999 sino hasta el momento en que el responsable del tratamiento manifieste expresamente su conformidad con la actividad desarrollada por el encargado del tratamiento, para lo que se concederá un plazo máximo, de suerte que sólo en ese momento el encargado deberá proceder conforme a lo dispuesto en el mencionado artículo 12.3.*»

prestación tiene lugar en los locales del responsable (o el acceso a éstos se produce de forma remota), el encargado ha de cumplir las medidas de seguridad que haya implantado el responsable (y reflejado en su documento de seguridad).

Por el contrario, si la prestación tiene lugar en los locales del encargado, éste será quien debe implementar las medidas de seguridad y reflejarlas en su documento de seguridad (sin perjuicio de que el responsable deberá anotar esta circunstancia en su propio documento de seguridad). Cuando esta circunstancia afectara a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la LOPD, con especificación de los ficheros o tratamientos afectados.

(iii) Derechos ARCO (artículo 26 del Reglamento)

Salvo previsión específica en contrario en el contrato de encargo de tratamiento, si los afectados ejercitaran sus derechos ARCO ante un encargado, el encargado deberá dar traslado de la solicitud de que se trate al responsable, para que éste sea quien proceda a darle respuesta.

4 · TRANSFERENCIAS INTERNACIONALES

El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros —que puede comportar el período de información pública que la AEPD venía otorgando desde mayo 2007— tendrá una duración máxima 3 meses.

El exportador solicitante debe consignar, entre otras cuestiones, documentación que no sólo incorpore las garantías exigibles para la obtención de la autorización, sino también «*el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso*» (artículo 137.2.c) del Reglamento).

Ahora bien, una adecuada aplicación de esta previsión debe tener en cuenta la opinión de la Audiencia Nacional, en su sentencia de 15 de marzo de 2002 (ratificada por la sentencia del Tribunal Supremo de 25 de septiembre de 2006), al analizar la adecuación a la LOPD de determinados apartados de la Instrucción 1/2000 de la AEPD:

> «[…] *la transferencia internacional de datos —esté o no sujeta a autorización previa— no excluye que sean de aplicación el conjunto de disposiciones de la Ley Orgánica 15/1999, ni impide o menoscaba el ejercicio de las competencias (inspectoras, sancionadoras,...) que la legislación atribuye a la Agencia de Protección de Datos;* […] *Pero no resulta aceptable que estas potestades de comprobación o incluso de inspección encaminadas a asegurar el cumplimiento de la Ley las ejerza la Agencia precisamente al tener conocimiento de que pretende realizarse una transferencia de datos para la que no es necesaria su autorización; y menos aun cabe aceptar que a los requerimientos realizados en esa ocasión se les atribuya la virtualidad de, si no son atendidos dentro del plazo señalado, impedir la inscripción y con ello la propia viabilidad de la transferencia.*» [F.D. 7]

Por otra parte, se recoge expresamente la posibilidad de solicitar la autorización sobre la base de reglas corporativas vinculantes, concebidas para grupos internacionales de estructura compleja (artículo 70.4 del Reglamento):

> «*En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.*
>
> *En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.*»

5 · DERECHOS ARCO

Se recoge una regulación completa sobre los derechos ARCO, debiendo el responsable conservar la acreditación del cumplimiento de su deber de respuesta a la solicitud de ejercicio de estos derechos.

Destacan, en particular, las siguientes previsiones sobre el derecho de oposición:

(i) se incluye el derecho de impugnación de valoraciones del artículo 13 de la LOPD[7] dentro

7 El artículo 13 de la LOPD no se refiere sin embargo propiamente al derecho de oposición del afectado sino el derecho a conocer la lógica de un tratamiento (i.e., los criterios de valoración y el programa utilizados) completamente automatizado (de acuerdo con la interpretación «conforme» al artículo 15 de la Directiva 95/46/CE) que ofrezca una definición de sus características o personalidad e implique una valoración de su comportamiento, a los efectos de impugnar, en su caso, la decisión basada en tal valoración adoptada únicamente por una máquina, esto es, «deshumanizadamente».

de los supuestos en que procede el derecho de oposición (artículo 34.c) del Reglamento);

(ii) el responsable debe responder la solicitud de oposición en el plazo máximo de los 10 días a su recepción (artículo 35 del Reglamento) [8];

(iii) si se solicita el consentimiento durante el proceso de formación de un contrato para finalidades sin relación directa con la relación contractual, debe permitirse al afectado que manifieste expresamente su negativa, p. ej., marcación de casilla claramente visible y no premarcada en el documento que se le entregue para la celebración del contrato (artículo 15 del Reglamento); y

(iv) si se pretende —en el marco de la celebración/ejecución de un contrato— adoptar decisiones sobre la base únicamente de procedimientos automatizados destinados a evaluar el rendimiento laboral, crédito, fiabilidad o conducta del afectado u otras manifestaciones de su personalidad (p. ej., *scoring*), éste debe ser informado previamente de que se adoptarán este tipo de decisiones, de que cancelarán los datos si no llega a celebrarse finalmente el contrato y de que puede alegar lo que estime pertinente para defender su derecho o interés (artículo 36 del Reglamento).

6 · TRATAMIENTOS DE DATOS DE MENORES DE EDAD

Conforme al artículo 13 del Reglamento, no pueden recabarse los datos de menores de 14 años salvo con el consentimiento de los padres o tutores y sujeto a determinados requisitos (salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela):

(i) no se pueden solicitar datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre sus características, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos, salvo de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización; y

(ii) la información dirigida a los menores deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en el artículo 13 del Reglamento.

El Reglamento impone que se articulen procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por los representantes legales [9].

7 · TRATAMIENTOS CON FINALIDADES DE PUBLICIDAD O PROSPECCIÓN COMERCIAL

Sin perjuicio de las implicaciones del derecho de oposición para este tipo de tratamientos, destacan las siguientes previsiones:

8 Se modifica por tanto el criterio establecido hasta la fecha por la AEPD que entendió aplicable el plazo de un mes para atender las solicitudes de ejercicio del derecho de oposición (vid., resolución de la AEPD R/00153/2006 (TD/00530/2005), de 23 de marzo de 2006):
«El artículo 17.1 de la LOPD, señala que "*Los procedimientos para ejercitar el derecho de oposición, acceso así como los de rectificación y cancelación serán establecidos reglamentariamente*."
Atendiendo al tenor de la LOPD respecto al derecho de oposición y a la normativa preexistente, declarada en vigor por la disposición transitoria tercera de la LOPD, cabe concluir que el ejercicio del derecho de oposición puede integrarse en el desarrollo reglamentario que la Ley Orgánica declara subsistente.
El artículo 17 de la LOPD, que remite al desarrollo reglamentario el ejercicio de los derechos, distingue entre los relacionados con los derechos de acceso y oposición y los de rectificación y cancelación como se desprende de la expresión "[...] *así como*" que viene a diferenciar dos bloques distintos entre unos y otros, excepto en lo que sean de aplicación las normas comunes a todos ellos. En esta línea, parece que el plazo para atender el derecho de oposición deberá ser el de un mes, que coincide con el previsto para el derecho de acceso previsto en el artículo 12.3 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor en virtud de lo previsto en la disposición transitoria tercera de la LOPD, y se diferencia del plazo para hacer efectivo los derechos de rectificación y cancelación.»

9 En virtud de la resolución de la AEPD R/00284/2008, de14 de marzo de 2008 (PS/00281/2007), se sanciona a la entidad que captó los datos de un menor y los transfirió a una entidad bancaria sin consentimiento paterno, con dos multas de 60.000 euros —por recabar los datos sin consentimiento— y 150.000 euros —por cederlos sin consentimiento— y a la entidad bancaria con una de 60.000 euros —por tratarlos sin consentimiento-. Parece ser que la captación de datos se realizaba on line en un formulario donde se solicitada el año de nacimiento, el usuario introdujo «1995» y, a pesar de ello, el usuario pudo continuar con el proceso sin el permiso de sus padres y acabó recibiendo publicidad de una tarjeta de crédito.
Esta resolución refleja que la diligencia en la verificación de la edad y existencia de los permisos parentales es exigible no sólo del que recaba los datos, sino también de su cliente que se beneficia de la campaña de publicidad que ejecuta.

(i) la dirección profesional de algunas «fuentes accesibles al público» (listas de personas pertenecientes a grupos de profesionales) incluye el número de fax y la dirección electrónica (artículo 7 del Reglamento) [10];

(ii) el consentimiento requiere informar a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad (artículo 45.1.*b)* del Reglamento);

(iii) será considerado responsable quien fije los parámetros identificativos de los destinatarios de la campaña; en cualquier caso, quien encargue la realización de la campaña publicitaria a un tercero debe asegurarse de que éste ha recabado los datos cumpliendo las exigencias establecidas en la LOPD (artículo 46 del Reglamento);

(iv) el tratamiento cruzado, con fines de promoción o comercialización, de ficheros de los que son responsables entidades distintas para identificar quiénes ostentan la condición de clientes de una u otra o de varias de ellas requiere el consentimiento de los afectados (artículo 47 del Reglamento);

(v) se requiere la consulta previa de los ficheros comunes de listas «Robinson» que pudieran afectar al tratamiento previsto (artículos 48 y 49 del Reglamento); y

(vi) cuando el responsable disponga de servicios para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, debe conceder la posibilidad de ejercer su derecho de oposición a través de dichos servicios (artículo 51.3 del Reglamento).

8 · FICHEROS DE «MOROSOS»

Sin perjuicio de las obligaciones del responsable del fichero común, el acreedor (o quien actúe por su cuenta o interés) debe asegurarse, al notificar los datos adversos al responsable del fichero común, que concurren los siguientes requisitos:

(i) que no se ha entablado reclamación judicial, arbitral o administrativa respecto de la deuda (que ha de ser cierta, vencida, exigible, impagada, y no deben de haber transcurrido más de 6 años desde su vencimiento); y

(ii) que el acreedor haya informado al deudor, en el momento de la celebración del contrato y, en todo caso, al tiempo de efectuar el obligatorio requerimiento previo de pago a quien debía cumplir la obligación que, en caso de no producirse el pago en el plazo previsto y de cumplirse los requisitos previstos, los datos relativos al impago pueden ser comunicados a este tipo de ficheros.

9 · MEDIDAS DE SEGURIDAD

Entre las novedades del Reglamento en materia de medidas de seguridad, destacan las siguientes:

(i) se regulan las medidas de seguridad específicas para ficheros no automatizados (FNA);

(ii) se reclasifican las medidas para ciertas categorías nuevas de datos (p. ej., datos de tráfico y localización o datos relativos a la violencia de género); y

(iii) se dota de una cierta flexibilidad para responsables con una infraestructura poco compleja y ficheros con ciertos datos sensibles para el mero cumplimiento de obligaciones legales [11].

Asimismo, se establecen unos períodos transitorios de adaptación a las medidas de seguridad exigidas

10 Resolución R/00300/2008 de la AEPD (PS/00355/2007), de 24 de marzo de 2008 «[...] *aunque los datos del destinatario de los faxes con contenido comercial hubieran sido obtenidos de la guías telefónicas editadas en papel, este hecho no exime de la obligación de obtener el consentimiento del destinatario de aquéllos para la remisión de envíos publicitarios vía fax, por cuanto las mismas no constituyen fuentes de acceso público para la remisión de faxes, de acuerdo con la LSSI y la LGT. Dichas guías sí son fuentes de acceso público para un tratamiento de datos de acuerdo con la LOPD, pero para la remisión de escritos por correo ordinario*.»

11 «*Artículo 81. Aplicación de los niveles de seguridad*. [...]
5. *En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará 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 o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
6. *También podrán implantarse las medidas de seguridad de nivel básico en los 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*.»

por el Reglamento para ficheros existentes en la entrada en vigor del Reglamento (i.e., el 19 de abril de 2007), que se resumen a continuación:

	Ficheros automatizados	FNA
1 año	1. Nivel medio de ficheros (i) de los que son responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social (y se relacionen con el ejercicio de sus competencias); las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; y 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 localización); y (ii) que contengan datos derivados de actos de violencia de género 2. Cualquier medida no prevista en el Real Decreto 994/1999	Básico
18 meses	Nivel alto de ficheros (i) de los que son 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 localización); y (ii) que contengan datos derivados de actos de violencia de género	Medio
2 años		Alto

Los productos de *software* destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar.

10 · SECTOR PÚBLICO

Sin perjuicio de que se le aplique la mayor parte de las disposiciones del Reglamento, destacan por su novedad:

(i) la definición de ficheros de titularidad pública:

«Artículo 5.1.m) «Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.»

(ii) las facultades de verificación de datos que obren en poder de las Administraciones públicas:

Artículo 11 «Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos.»

(iii) las cesiones de datos personales sobre la salud al Sistema para atención sanitaria:

Artículo 10.5 —2º párrafo: «En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.»

11 · PROCEDIMIENTOS

Se regulan específicamente los procedimientos tramitados por la AEPD:

(i) tutela de los derechos ARCO,

(ii) ejercicio de la potestad sancionadora,

(iii) inscripción o cancelación de ficheros,

(iv) transferencias internacionales,

(v) inscripción de códigos tipo,

(vi) exención del deber de información al interesado; y

(vii) conservación de datos para fines históricos, estadísticos o científicos.

12 · ACCIONES A ADOPTAR

(i) Revisión de la *información facilitada a los afectados y de la conservación de prueba del cumplimiento de este deber*, en particular, respecto de *tratamientos ajenos a la relación contractual* (p.ej., publicidad), *procesos de scoring, comunicación de datos de impago o consultas a ficheros de morosos y cesiones a terceros.*

(ii) Revisión de los *procedimientos ARCO*, en particular, respecto del derecho de oposición para fines publicitarios, las listas *Robinson*, los servicios de atención al cliente y la conservación de la acreditación de las respuestas al ejercicio de estos derechos.

(iii) *Revisión de las medidas de seguridad de los ficheros automatizados e incorporación* de las medidas de seguridad para los *ficheros en papel*.

(iv) Revisión de los *contratos de encargo de tratamiento*, en particular, respecto de las medidas de seguridad y las subcontrataciones.

(v) Revisión de procedimientos de encargo a terceros de realización de *campañas publicitarias* de marketing directo.

(vi) *Revisión de las declaraciones de ficheros* realizadas ante la AEPD (ficheros excluidos, ficheros en papel, modificación de medidas de seguridad, etc.).