EMILIO DEL PESO NAVARRO
MIGUEL ÁNGEL RAMOS GONZÁLEZ
MARGARITA DEL PESO RUIZ
MAR DEL PESO RUIZ

NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

MEDIDAS DE SEGURIDAD

DIAZ DE SANTOS

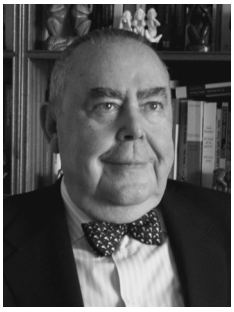
INFORMÁTICOS EUROPEOS EXPERTOS

Ediciones Díaz de Santos
E-mail: ediciones@diazdesantos.es
Internet://http:www.diazdesantos.es/ediciones

ISBN: 978:84-7978-873-5
Depósito legal: M. 22.790-2008

Diseño de cubierta: Ángel Calvete
Fotocomposición: Fernández Ciudad
Impresión: Fernández Ciudad
Encuadernación: Rústica-Hilo

Acerca de los autores



Emilio del Peso Navarro

Licenciado en Derecho por la UCM y Licenciado en Informática por la UPM, con amplia experiencia en el Derecho de las Tecnologías de la Información y las Comunicaciones, está reconocido como un experto en la interrelación de las dos materias.

Diplomado en Asesoría de Empresas, Derecho del Trabajo e Impuestos por la Escuela de Práctica Jurídica de la Facultad de Derecho de la UCM.

Socio de IEE, Informáticos Europeos Expertos.

Director del Aula de Informática Legal, ha sido profesor invitado en el Máster de Tecnologías de la Información y las Comunicaciones del Instituto de Informática Jurídica de la Facultad de Derecho (ICADE) de la UPC, en el Máster de Informática y Derecho de la UCM y en el Máster de Tecnologías de la Información y las Comunicaciones de la UCLM. Ha sido profesor externo de IBM y de IEDE, Institute for Executive Development.

Experto en Derecho de las Nuevas Tecnologías de la Información y las Comunicaciones, ha participado como conferenciante o ponente en numerosos congresos nacionales e internacionales. Ha impartido conferencias y seminarios sobre la materia en las principales instituciones del país.

Forma parte del Consejo Asesor de la revista electrónica de la Agencia de Protección de Datos de la Comunidad de Madrid *datospersonales.org*.

Ha escrito numerosos artículos sobre el tema en las principales revistas técnicas tanto nacionales como internacionales, entre ellas: *Seguridad Informática y Comunicaciones (SIC)*, *Informática y Derecho*, *En línea informática*, *Informática Jurídica Aranzadi*, *ABZ información y análisis jurídico* (Morelia,

México), *IEEE*, *Datamation*, *Security Management* y en la revista electrónica *datospersonales.org*.

Coautor de *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas*. Díaz de Santos. Madrid, 1994. 2.ª edición, 1998.

Director y coautor de la obra *Manual de Dictámenes y Peritajes Informáticos*. Díaz de Santos. Madrid, 1995. 2.ª edición, 2001.

Editor y coautor de *Auditoría informática: un enfoque práctico* (obra colectiva). RA-MA. Madrid, Bogotá y Ciudad de México, 1998. 2.ª edición, 2000.

Coautor de *LORTAD: Reglamento de Seguridad*. Díaz de Santos. Madrid, 1999. 2.ª edición, 2002.

Autor de *Ley de Protección de Datos: la nueva LORTAD*. Díaz de Santos-IEE. Madrid, 2000.

Autor de *Manual de outsourcing informático. Análisis y contratación*. Díaz de Santos-IEE. Madrid, 2000. 2.ª edición, 2003.

Coautor de *Seguridad en las bases de datos*. Fundación Dintel. Madrid, 2001.

Autor de *Servicios de la Sociedad de la Información: comercio electrónico y protección de datos*. Díaz de Santos-IEE. Madrid, 2003.

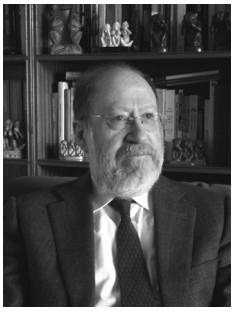
Coautor de *El Documento de Seguridad. Análisis técnico y jurídico. Modelo*. Díaz de Santos-IEE. Madrid, 2004.

Coautor de *Los datos de los ciudadanos en los ayuntamientos*. Díaz de Santos-IEE. Madrid, 2004.

Coautor de *Gobierno de las Tecnologías y los Sistemas de Información*. RA-MA. Madrid, 2007.

Editor y coautor de *Auditoría de las Tecnologías y Sistemas de Información*. RA-MA. Madrid y Ciudad de México, 2008.

Pertenece al Ilustre Colegio de Abogados de Madrid, a ISACA-España, ALI y ATI. Member of Information Systems Audit and Control Association (ISACA), ASIA (Asociación de Auditores y Auditoría y Control de los Sistemas y Tecnologías de la Información y Comunicaciones).



Miguel Ángel Ramos González

Doctor y Licenciado en Informática (tesis sobre Sistemas Expertos aplicados a la Auditoría Informática), CISA, tiene 40 años de experiencia en Informática (fue Director de S. de I. y Second Vice President de Chase Manhattan Bank) y 18 en A. I.

Socio Director de IEE, Informáticos Europeos Expertos.

Ha dirigido numerosos proyectos de auditoría informática en España, y proyectos o cursos sobre el tema en doce países, así como proyectos relacionados con datos personales.

Ha dirigido tesis sobre A. I., así como numerosos proyectos de fin de carrera sobre el tema, y es profesor de Auditoría I. y de Auditoría de S. de I. en la Universidad Carlos III.

Fue el primer presidente de ISACA en España. Fue profesor de MBAs en una escuela de negocios durante 12 años.

Coautor de *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas*. Díaz de Santos. Madrid, 1994. 2.ª edición, 1998.

Coautor de la obra *Manual de Dictámenes y Peritajes Informáticos*. Díaz de Santos. Madrid, 1995. 2.ª edición, 2001.

Coautor de *Auditoría informática: un enfoque práctico* (obra colectiva). RA-MA. Madrid, Bogotá y Ciudad de México, 1998. 2.ª edición, 2000.

Coautor de *LORTAD: Reglamento de Seguridad*. Díaz de Santos. Madrid, 1999. 2.ª edición, 2002.

Coautor de *El Documento de Seguridad. Análisis técnico y jurídico. Modelo*. Díaz de Santos-IEE. Madrid, 2004.

Coautor de *Auditoría de las Tecnologías y Sistemas de Información*. RA-MA. Madrid y Ciudad de México. 1.ª edición, 2008.

Es miembro de ISACA, ASIA, ALI, AII, ISSA…

Margarita del Peso Ruiz

Licenciada en Derecho por la Universidad Complutense de Madrid.

Licenciada en Historia con Premio Extraordinario de Licenciatura por la Universidad Complutense de Madrid. Máster en Asesoría y Consultoría en Tecnologías de la Información (comercio-e, contratación informática y protección de datos) por el Real Centro Universitario Escorial María Cristina y Davara & Davara Asesores Jurídicos.

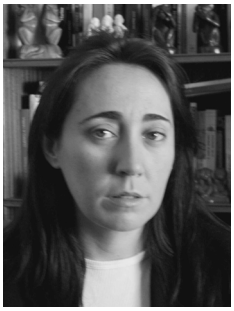
Máster en Dirección de Recursos Humanos por el CEF de Madrid.

Ha intervenido como ponente y asistente en numerosos cursos, seminarios y conferencias sobre Derecho de las Nuevas Tecnologías de la Información y las Comunicaciones.

Pertenece al Ilustre Colegio de Abogados de Madrid y es miembro de ASIA (Asociación de Auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones).

Coautora de *Los datos de los ciudadanos en los ayuntamientos*. Díaz de Santos-IEE. Madrid, 2004.

Coautora de *Auditoría de las Tecnologías y Sistemas de Información*. RA-MA. Madrid y Ciudad de México. 1.ª edición, 2008.



Mar del Peso Ruiz

Licenciada en Ciencias Económicas y Empresariales por la Universidad Autónoma de Madrid. Especialidad: Estructura Económica.

Licenciada en Derecho por la UNED.

Máster en Tributación/Asesoría Fiscal por el Centro de Estudios Financieros.

Especialista Universitario en Protección de Datos y en Comercio Electrónico por el Real Colegio Universitario Escorial María Cristina y Davara & Davara Abogados.

Directora de Formación y Consultora de IEE Informáticos Europeos Expertos, S. L.

Ha sido ponente en numerosos Seminarios, principalmente en temas relacionados con la protección de datos.

Catorce años de experiencia profesional, más de la mitad de ellos en IEE Informáticos Europeos Expertos. Ha desarrollado su trabajo también en TURBO PERSONAL COURIER, S. L., ASNEF EQUIFAX y GRANDA ASESORES, S. L. En IEE ha participado en numerosos proyectos de protección de datos, relacionados con distintos sectores de actividad.

Coautora de *El Documento de Seguridad. Análisis técnico y jurídico. Modelo*. Díaz de Santos. Madrid, 2004.

Editora y coautora de *Auditoría de las Tecnologías y Sistemas de Información*. RA-MA. Madrid y Ciudad de México. 1.ª edición, 2008.

Es miembro del Ilustre Colegio de Economistas de Madrid y del Ilustre Colegio de Abogados de Madrid, ATI, ISACA y ASIA.

Contenido

TERCERA PARTE
ANEXOS

regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo».

Este tipo de ficheros, como se puede comprobar, necesita un procedimiento distinto al régimen general y debe regularse como así se hace en el RDLOPD.

12.3. TRATAMIENTO DE DATOS RELATIVOS AL CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS FACILITADOS POR EL ACREEDOR O POR QUIEN ACTÚE POR SU CUENTA O INTERÉS

A continuación, en los artículos 38 a 44, se regula la especificidad de este tipo de ficheros.

12.3.1. Requisitos para la inclusión de los datos

Dada su especificidad, los datos referidos al cumplimiento e incumplimiento de obligaciones dinerarias, deben reunir una serie de requisitos para poder ser tratados.

«Artículo 38. Requisitos para la inclusión de los datos.

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero».

Es necesario que los datos, para poder ser tratados, cumplan los siguientes requisitos:

1. Existencia previa de una deuda cierta.
2. Que la misma haya vencido.
3. Pueda exigirse.
4. Esté impagada.
5. No se haya entablado reclamación judicial, arbitral o administrativa o reclamación en los términos del Real Decreto 303/2004, de 20 de febrero.

Es decir, una deuda cuya cuantía se halle determinada y no haya sido satisfecha a su vencimiento. Además, deberán darse las condiciones de exigibilidad de la deuda que en su caso sean aplicables y no haber sido objeto de reclamación en el marco de un procedimiento judicial, arbitral o administrativo.

«b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico».

Una vez transcurrido el plazo de seis años, los datos sobre cumplimiento o incumplimiento de obligaciones dinerarias, no podrán ser tratados, aunque cumplan los requisitos del apartado anterior.

En el caso de que se trate de vencimientos periódicos, por ejemplo el pago de un canon o una renta mensual, el periodo de seis años comenzaría a computarse desde que venza cada uno de los plazos; es decir, si hace seis años que existe una deuda de devengo periódico mensual que ha sido sistemáticamente impagada, el primer mes de los que transcurran a partir de ese momento impediría el tratamiento de los datos relativos al primer periodo impagado del conjunto de la deuda y así sucesivamente.

«c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación».

Este requisito tendrá, en caso necesario, que ser probado.

El requerimiento previo de pago está íntimamente relacionado con el principio de calidad de los datos, y en concreto con su exactitud, según criterio de la AEPD puesto de manifiesto en el Informe Jurídico 0273/2005 sobre «Requerimiento previo en ficheros de solvencia. Valor normativo de las Instrucciones de la Agencia Española de Protección de Datos[1]». Considera la AEPD que: *«La inclusión de los datos en un fichero relacionado con el cumplimiento o incumplimiento de obligaciones dinerarias resulta claramente diferenciada de la que lleve a cabo el acreedor en sus propios ficheros. De este modo, mientras que el tratamiento efectuado por el acreedor se basa en la mera relación contractual que le vincula con el deudor, no exigiéndose ningún requisito adicional a los previstos en el derecho privado, la inclusión del dato en el fichero previsto en el artículo 29.2 genera, como ha tenido ocasión de indicar esta Agencia de forma reiterada, una situación negativa para el individuo, derivada del hecho de que dichos datos no sólo serán conocidos por su acreedor, sino por la totalidad de entidades que tengan acceso al fichero, con el simple requisito de que dicho acceso tenga por objeto evaluar la solvencia del deudor.*

[1] En www.agpd.es, a fecha 27 de febrero de 2008.

También puede encontrarse una referencia al mismo en *Memoria 2005*. Agencia Española de Protección de Datos. Madrid, 2006. Pág. 128.

Esta circunstancia, y en particular, esta cesión posterior de los datos exige que se establezcan mecanismos que permitan reforzar el cumplimiento del principio de proporcionalidad, de forma que ningún dato respecto del cual puedan existir dudas en cuanto a su existencia y exactitud sea incluido en el fichero».

«2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores.

Tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero».

En caso de existir alguna duda a la hora de determinar si el dato reúne todos los requisitos precisos para que conste en un fichero de estas características, se ha optado por la prudencia evitando su tratamiento hasta que no haya seguridad de que se cumple con los requisitos exigidos.

«3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente».

La conservación de toda esta documentación suele resultar problemática y cara. Sin embargo, es una garantía frente al interesado que refuerza la obligación de los acreedores a observar una debida diligencia a la hora de comunicar este tipo de deudas, puesto que difícilmente el responsable del fichero común podrá verificar a priori, registro por registro, el cumplimiento de dichos requisitos.

12.3.2. Información previa a la inclusión

«Artículo 39. Información previa a la inclusión.

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias».

Existen dos momentos en los que el acreedor puede cumplir con este deber de información al deudor:

a) En el momento de celebración del contrato.
b) Al tiempo de efectuar el requerimiento previsto en la letra c) del apartado 1 del artículo 38.

No se trata de optar por uno u otro medio, ya que el artículo dice que en todo caso deberá hacerse en el momento de efectuar el requerimiento. Por tanto, informar en el momento de celebración del contrato puede parecer que se considera como un refuerzo a esa información que en este caso el acreedor puede elegir entre hacer o no hacer; sin embargo, el contenido del artículo establece la información como un deber en un momento «y» en otro, así que es la expresión «en todo caso» la que puede confundir.

No quedando claro cuáles son los casos en que podría obviarse la información en el momento en que se celebre el contrato, lo más adecuado parece ser informar en los dos momentos. Quizás el incluir la expresión «en todo caso» pudiera hacer referencia a que se informe todas las veces que se efectúe el requerimiento sobre una misma deuda, ya que como sabemos, éste no suele realizarse una única vez.

12.3.3. Notificación de inclusión

*«**Artículo 40. Notificación de inclusión.***

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre».

Con independencia de la información que ha de facilitar el acreedor al deudor a que se refiere el artículo 39 del RDLOPD, el responsable del fichero ha de notificar a los interesados qué datos se encuentran registrados respecto a los mismos en el plazo de treinta días.

Esta práctica, junto con la obligación de información comentada en el apartado anterior, propiciada a raíz del desarrollo de la normativa en materia de protección de datos, ha reducido notablemente el número de sorprendidos que a la hora de solicitar algún tipo de crédito, préstamo o financiación se encontraban con una negativa por motivos que a veces la entidad en cuestión ni siquiera quería desvelar.

«2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores».

La notificación se ha de hacer por cada deuda concreta y determinada, por lo que si un acreedor comunica en una misma remesa varias deudas contraídas por una misma persona no cabe el que la comunicación se haga de forma conjunta.

«3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato».

Como en otros casos, el problema puede ser la prueba, pues es preciso que, en caso necesario, se pueda demostrar que se ha efectuado la notificación pertinente.

En este sentido, el criterio mantenido por la Audiencia Nacional ha experimentado un cambio de orientación, pues en la Sentencia de 24 de enero de 2003 anuló una Resolución de la AEPD que había estimado que era suficiente para acreditar la obligación de notificación establecida en el artículo 29.2 de la LOPD que el responsable del fichero común acompañara una certificación emitida por una empresa independiente que se encargaba de enviar las notificación de inclusión en dicho fichero, y que, por consiguiente, había acordado el archivo de las correspondientes actuaciones previas de investigación. En dicha Sentencia se consideraba que:

- No quedaba acreditada la emisión, y menos aún la recepción, de la correspondiente comunicación dirigida a los interesados.
- La existencia de un contrato entre el responsable del fichero común y una tercera entidad para proceder al envío de las notificaciones acredita la existencia de una relación contractual que propicia que esta clase de notificaciones se realice por una agencia independiente del titular del fichero pero no que, en el supuesto concreto, se hubiese utilizado dicha vía ni la efectiva recepción de la notificación por el denunciante.
- La certificación se refiere al envío de las notificaciones, pero no acredita la recepción por sus destinatarios.

- Cuando el destinatario niega la recepción, recae sobre el responsable del fichero la carga de la prueba.

Esta línea doctrinal se mantuvo también en la Sentencia de la Audiencia Nacional de 9 de mayo de 2003 en la que cuestionaba el valor probatorio de la inclusión de los datos de la notificación en un fichero auxiliar de notificaciones.

En la Sentencia de 20 de enero de 2006 consideró que *«La acreditación de la comunicación podrá hacerse por cualquier medio de prueba y también a través de indicios, siendo uno de ellos indudablemente la inclusión en el fichero auxiliar de NOTIFICACIONES..., aunque por sí solo sea insuficiente para desvirtuar el valor de la denuncia...»*.

En este caso, la Audiencia Nacional consideró como indicios que apuntan la realización de la comunicación los siguientes:

- Inclusión de los datos personales del denunciante en el fichero auxiliar de notificaciones.
- El hecho de que el denunciante se dirigió al responsable del fichero común sabiendo que sus datos estaban incluidos en el mismo y quién había sido la entidad informante, sin que hubiera acreditado mínimamente que tuvo dicho conocimiento de forma distinta.
- El hecho de que al domicilio al que se dirigió la comunicación que se niega haber recibido se remitieron otras notificaciones de las que el denunciante tuvo conocimiento.

A juicio de la AEPD, *«ambas Sentencias de 24/01/2003 y de 20/01/2006 no difieren tanto, sino en la medida en que en esta última se aborda, en relación a un supuesto concreto, todos los indicios que según señalaba la Sentencia de 24/01/2003 permiten suplir "la falta de prueba documental directa y concluyente de que se notificó", pero, en modo alguno, permite considerar que, por sí mismo el "Fichero Auxiliar de Notificaciones" y el certificado expedido por la empresa externa que se encarga de enviar las notificaciones al Servicio de Correos, supongan, en todo caso, prueba suficiente de la realización de la comunicación a la que se refiere el artículo 29.2 de la LOPD, cuando el interesado niega haberla recibido»*.

Por lo tanto, la AEPD entiende que *«la doctrina de la Audiencia Nacional exige de una aplicación, caso a caso, de modo que en relación a un supuesto concreto sea posible o no entender que existen indicios de que se haya producido la comunicación al afectado*[2]*»*.

[2] Ver R/00896/2006 recaída en PS/00276/2005. En este procedimiento se imputa al responsable de un fichero común el incumplimiento del deber de notificar a los interesados respecto de los que se hayan registrado datos de carácter personal su inclusión en el fichero. La AEPD consideró que, en este caso, concurren los siguientes indicios:

12.3.4. Conservación de los datos

De conformidad con lo que se dice en el artículo 4.3 de la LOPD: *«Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado»*.

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) daba otra redacción a su artículo 4.3.

«Artículo 4. Calidad de los datos.
3. Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado».

La diferencia entre «situación real» y «situación actual» dio lugar a una gran controversia sobre si debían figurar o no en los ficheros de cumplimiento o incumplimiento de obligaciones dinerarias los deudores cuando hubiesen satisfecho su deuda, conocidos como «con saldo cero». A este tema nos hemos referido con más detalle con anterioridad.

El RDLOPD dedica su artículo 41 a la conservación de los datos.

*«**Artículo 41. Conservación de los datos.***
1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

- La notificación de la inclusión en el fichero común de los datos de la denunciante se encuentra recogida en el fichero auxiliar de notificaciones del responsable del fichero común.
- La empresa encargada de realizar las notificaciones certificó que la notificación que se remitió a la denunciante informándole de la inclusión de sus datos personales en el fichero común se generó sin que se produjese ninguna incidencia y que se presentó en el Servicio de Correos para su remisión postal entre un total de 47.279 notificaciones.
- Consta acreditado que en esa fecha se presentaron en el Servicio de Correos un total de 47.279 notificaciones de inclusión en ese fichero común para su remisión a los destinatarios de las mismas.
- No concurre, en este caso, ninguna circunstancia que haga suponer que dicha notificación fue devuelta.
- La denunciante conocía, cuando presentó la denuncia ante la AEPD, que la inclusión de sus datos en el fichero común se había producido a instancia de un acreedor determinado así como la identidad del acreedor, por lo que no cabe descartar que hubiera conocido este extremo, precisamente a través de la comunicación de inclusión practicada por el responsable del fichero común, ya que no había solicitado el acceso a sus datos personales y a las entidades consultantes del fichero no se les facilita información sobre el nombre del acreedor, de acuerdo con lo dispuesto por el Tribunal de Defensa de la Competencia en su Resolución de fecha 11 de marzo de 1999.

Por todo ello, en este caso, la AEPD estimó que concurren indicios suficientes para entender que el responsable del fichero común cumplió con su obligación de notificación prescrita en el artículo 29.2 de la LOPD, de modo que sea aplicable a este caso el principio del *in dubio pro reo*.

Texto íntegro de la resolución en www.agpd.es a fecha 27 de febrero de 2008.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma».

Como se puede ver, el RDLOPD opta por que los antiguos deudores que hayan satisfecho su deuda y, por tanto, ésta tenga saldo cero, no deben permanecer en el fichero.

«2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico».

Se prevé la cancelación de los datos en función del transcurso del tiempo fijándose en seis años el plazo para que, una vez transcurridos, sean cancelados los datos.

Por lo tanto, los datos serán cancelados por los siguientes motivos:

a) Pago de la deuda.
b) Transcurso del plazo de seis años.
c) Posible error en los datos.

12.3.5. Acceso a la información contenida en el fichero

Con independencia del derecho de acceso que tiene el afectado, en este tipo de ficheros existe la posibilidad de que terceros en los que concurran ciertas circunstancias puedan también acceder a esta clase de ficheros.

El RDLOPD dedica a este tipo de acceso el artículo 42.

«Artículo 42. Acceso a la información contenida en el fichero.

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.
b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.
c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de

forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar».

Se establecen, por tanto, los supuestos en los que se entiende que para un tercero es preciso enjuiciar la solvencia económica del afectado, ciñéndolos a supuestos en que existe o se pretende establecer determinado tipo de relaciones contractuales con el interesado. En cualquier caso, también disuade de su consulta en otros supuestos el hecho de que este tipo de servicios no son gratuitos.

Hemos de entender que el apartado 2 de este artículo se refiere al caso en el que por estar incluido en el fichero el interesado vea frustrada su intención de contratar, puesto que si fuese para advertirle de que se va a realizar la consulta al fichero no vemos por qué no debería procederse a este tipo de información en el primer supuesto.

Dicha información deberá realizarse por escrito, estableciendo una excepción en el caso de que la contratación sea telefónica, indicando que le corresponde probar el cumplimiento del deber de informar, aunque entendemos que en el caso de que la información sea escrita la carga de la prueba también recaerá sobre el tercero, por lo que quizás se pretende hacer énfasis en que sólo por el hecho de que la información se haya hecho de palabra no está exenta de la obligación de ser susceptible de prueba.

12.3.6. Responsabilidad

Se perfilan dos nuevos responsables en este tipo de ficheros:

a) El acreedor o quien actúe por su cuenta o interés.
b) El responsable del fichero común.

El acreedor o quien actúe por su cuenta o interés debe verificar que cuando se notifican los datos adversos al responsable del fichero común concurren todos los requisitos exigidos en los artículos 38 y 39 del RDLOPD:

a) Existencia previa de una deuda cierta, vencida, exigible que esté impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa.
b) No haya transcurrido el plazo de seis años desde la fecha en que hubo de procederse al pago de la deuda.
c) Haya un requerimiento previo de pago a quien corresponda el pago.
d) Información al deudor de que en caso de efectuarse el pago los datos serán comunicados al fichero común de cumplimiento o incumplimiento de obligaciones dinerarias.

*«**Artículo 43. Responsabilidad.***

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre».

En un principio, en la LORTAD sólo aparecía como posible responsable el responsable del fichero como se puede ver en numerosos artículos de la Ley, tratando con ello de evitar que, en caso de que se produjese cualquier tipo de responsabilidad, ésta se diluyese entre varios posibles responsables. Éste era el «chivo expiatorio» de la Ley y parecía que ésta, más que ser una ley de protección de datos, lo era de responsables del fichero.

En la LOPD aparece un nuevo posible responsable (art. 12.4): el encargado del tratamiento.

Aquí aparece otro posible responsable que sería el acreedor o quien actúe por su cuenta o interés respecto de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero común.

En la redacción de este artículo del RDLOPD subyace la doctrina de la Audiencia Nacional confirmada por el Tribunal Supremo en cuanto a la distinción entre responsable del fichero y responsable del tratamiento. Ya hemos comentado en capítulos anteriores que, consideramos, es la misma figura. De hecho en la literalidad del artículo no aparece la expresión «responsable del tratamiento», sino «el acreedor o quien actúe por su cuenta o interés».

Basándose en los artículos de la LOPD que definen la figura del responsable del fichero o del tratamiento y del tratamiento de datos, así como en el artículo de la directiva que define al responsable del tratamiento, la Audiencia Nacional, en su Sentencia de 16 de octubre de 2003 ha declarado que *«se define al "responsable del tratamiento" como "la persona física o jurídica, autoridad pública, servicio, o cualquier otro organismo que sólo, o conjuntamente con otros, determine los fines y los medios del tratamiento de datos personales" por lo que tal figura del responsable se conecta en la Ley con el poder de decisión sobre la finalidad, contenido y uso del tratamiento.*

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

que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento».

En este mismo sentido se pronuncia la Audiencia Nacional en su sentencia de 3 de marzo de 2004, que cita en la Sentencia de 18 de enero de 2006, al señalar que: *«el tipo sancionador previsto en el artículo 44.3.d) de la Ley Orgánica 15/1999, castiga "tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la presente Ley", como el previsto en el artículo 4.3 de la citada Ley que impone la veracidad y exactitud de los datos de carácter personal. Acorde con este principio se establecen una serie de obligaciones, tendentes a alcanzar esa veracidad y exactitud de los datos de carácter personal que se encuentran en el fichero, y cuyo incumplimiento es digno de reproche y configura una infracción administrativa por la que se impone la sanción que se recurre. Dicho de otra forma, el medio de conseguir que los principios en que se inspira esta regulación sobre la protección de datos –al amparo del artículo 18.4, más allá del contenido del artículo 18.1 de la CE, como un derecho fundamental autónomo tras la STC 292/2000– sean efectivos es mediante la acción sancionadora, es decir, tipificando las conductas que impidan el cumplimiento de los expresados principios.*

El ámbito subjetivo del ilícito administrativo descrito son los "responsables de los ficheros y los encargados de los tratamientos" , pues sólo a éstos les es aplicable el régimen sancionador que diseña la Ley Orgánica 15/1999, ex artículo 43.1 de la misma Ley. Esta delimitación subjetiva ha sido ampliada en la Ley Orgánica 15/1999, a la sazón aplicable, respecto de la prevista en la Ley Orgánica 5/1992, en cuyo artículo 42.1 sólo sometía a su régimen sancionador a los responsables de los ficheros. Ahora bien, debe tenerse en cuenta que el responsable del fichero tiene una configuración más amplia en la Ley de 1999 que en la de 1992, pues sólo así puede explicarse que cuando el artículo 43.1 alude al "responsable del fichero", esta expresión comprende ahora al responsable del tratamiento, ex artículo 3.d de la Ley Orgánica 15/1999, bajo la expresión "responsable del fichero o tratamiento", desconocida en la Ley de 1992, y si bien es cierto que las definiciones son coincidentes, antes y ahora, sin embargo se ha incluido en la vigente Ley a aquellos otros que decidiendo sobre la finalidad, contenido y uso del tratamiento, no sean propiamente responsables del fichero.

Entendemos, por tanto, por responsable del fichero o del tratamiento la persona física o jurídica, que decida sobre la finalidad contenido y uso del tratamiento; y por encargado del tratamiento quien trate datos personales por cuenta del responsable del tratamiento, según define el artículo 3, apartados d) y g) de la Ley Orgánica 15/1999».

Otro punto al establecerlos es la elección del Área Cliente para arrancar: el proyecto piloto, que puede durar varios meses, y que debe ser con un área convencida y proclive a los ANS, en la que sea fácil la implantación y el seguimiento, para no empezar con un fracaso.

Es deseable que existan unas políticas así como normas que las desarrollen: sobre calidad, sobre seguridad y sobre las relaciones entre proveedores y clientes de servicios, y así los procedimientos detallados tendrán en qué basarse.

Como se ha indicado, los usuarios finales pueden ser todos internos: empleados de la propia entidad o contratados y colaboradores, y puede haber también usuarios externos: los clientes que acceden a servicios, como puede ser el caso de los que prestan las entidades financieras a los clientes que acceden por Internet, o los que acceden esporádicamente a páginas web o servicios, que normalmente accederán de forma anónima: en casi ninguno de estos casos establecen directamente las condiciones, pero esperan un cierto nivel de servicio.

Cuando hay interlocutores claros de los usuarios, los niveles mínimos de servicio los negociarán con Sistemas de Información los responsables de Marketing o de Producto, y la misma función u otra hará el seguimiento del cumplimiento, y Control Interno o Auditoría podrá, o más bien deberá, realizar revisiones.

Los ANS están en alguna medida *relacionados con*:

- Planificación y Gestión de la Capacidad.
- Gestión de Problemas y de Incidencias: en algunas entidades los diferencian según la importancia.
- Gestión de Cambios.
- Gestión del Rendimiento.
- Gestión de los Accesos y de la Seguridad en general.
- Gestión de la Disponibilidad y de la Continuidad.

Hay aspectos adicionales respecto a los ANS, que se comentan a continuación:

- Puede haber Acuerdos de Nivel de Servicio entre las propias áreas de negocio entre sí, pero en este capítulo nos estamos centrando en el caso en que el proveedor es el Área de Sistemas de Información/Tecnologías, y el servicio tiene relación con datos automatizados. El proveedor natural será Producción/Explotación, si bien también puede haber Acuerdos referidos a aplicaciones y a servicios por parte de áreas de Desarrollo y/o Mantenimiento, que a su vez puede ser cliente de Producción/Explotación.
- Los Acuerdos que pueden existir en cuanto a Desarrollo o Mantenimiento de Aplicaciones no se comentan aquí: en ellos se trataría de cumplir con calidad los requerimientos, dentro de un plazo y de un presupuesto, y minimizando el riesgo.

- Aunque hablamos de usuarios internos, cada vez más se habla en las entidades de **clientes** internos: es un cambio cultural positivo desde la perspectiva de la calidad de servicio, aun tratándose de clientes *cautivos* que no puedan contratar servicios fuera de su proveedor interno único.
  Este cambio se percibe incluso en empresas de servicios masivos, que tradicionalmente a los clientes externos nos llamaban abonados (porque lo éramos y sin alternativa); la apertura de mercados y la competitividad ha mejorado el nivel de servicio, y ése debe ser también el enfoque tanto en el caso de servicios internos como en los servicios contratados a proveedores externos.

32.3. NECESIDAD Y VENTAJAS DE ESTABLECER ACUERDOS

Cada día la dependencia de las entidades respecto a los sistemas y tecnologías de la información es mayor, y cualquier ruptura o degradación del servicio tiene peores consecuencias, en especial cuando los servicios dependen de las comunicaciones y de procesos en tiempo real.

Generalmente, los esfuerzos por satisfacer las necesidades e incluso las expectativas de servicio de los clientes resultan rentables, e imprescindibles en mercados muy competitivos.

Mediante los Acuerdos se puede llegar a:

- Conocer y medir las necesidades de los clientes y sus expectativas: éstas pueden diferir respecto a sus necesidades, en más o en menos.
- Mejorar progresivamente la calidad, dentro de un marco de garantía de servicio.
- Alcanzar un compromiso de *cultura* de servicio.
- La racionalización y el control de los costes, mediante presupuestos y análisis coste/beneficio, especialmente cuando los acuerdos internos están relacionados con un sistema de repercusión de costes, pudiendo facilitar el cálculo de la rentabilidad.
- Mejorar la comunicación entre las partes, que se obligan a un cierto *protocolo*: canalizar la comunicación a través de personas de contacto, establecer mecanismos de medida, fijar formatos y periodicidad de informes, definir indicadores..., haciendo más fácil llegar a la claridad y transparencia en las relaciones.
- Formalizar y documentar: es necesario inventariar y describir los servicios, acordar cómo medirlos, establecer procedimientos, adoptar metodologías...
- Establecer las obligaciones y responsabilidades de las partes relacionadas: los clientes internos de los servicios se pueden involucrar en las prioridades, en la planificación y en el seguimiento de la gestión.
- Mejorar la competitividad: aunque no se trate de entidades de servicios sino de *proveedores* internos, siempre es bueno un espíritu de superación

y una cultura de servicio: el objetivo debe ser la comparación con entidades externas, y verificar que no estamos por encima en cuanto a costes ni por debajo en cuanto a calidad.

- Métricas objetivas: es fácil decir que el servicio es malo, que ha habido algunas caídas de línea, que el tiempo de respuesta se ha degradado, o que a veces no se ha podido acceder a los datos o que no han funcionado los procesos, pero suelen ser expresiones vagas que en parte dependen de la subjetividad; sin embargo, si se miden los tiempos de no disponibilidad, su distribución, el tiempo de respuesta... y se analiza su evolución mediante gráficos, entonces se tienen datos objetivos y más completos, con los que ambas partes: proveedor y cliente, han de estar de acuerdo, si han acordado previamente las métricas.
- En teoría mediante los ANS se puede también medir (y mejorar) la productividad, pero es un aspecto que dependerá de los casos, y generalmente no es el objetivo.
- Mediante los ANS y los datos que hemos de recoger es más fácil comparar los servicios internos con los que podría ofrecer un proveedor externo, y será más completo si podemos comparar también los costes, y la comparación se podría hacer también con los servicios internos de otras entidades homogéneas (*benchmarking:* puntos fuertes y débiles), preferiblemente del mismo sector, o en el caso de multinacionales con los servicios que la misma entidad ofrece en otro país: en más de un caso se ha decidido que sea desde un país concreto desde el que se preste un determinado servicio, ahora que por las comunicaciones no hay barreras, y si se salvan las barreras de idioma, si es que influyen, como el caso de *help-desk*.
- Justificar los presupuestos de inversiones y de gastos: si se requiere mejor servicio o se están estimando mayores volúmenes será necesario potenciar o sustituir los equipos, las redes, a veces las aplicaciones... Las Áreas usuarias conjuntamente con la de Sistemas de Información, tal vez formando parte de un Comité, se pueden plantear las alternativas de inversión y la repercusión en el servicio y en los costes, con proyección en los próximos años.
- Sistemas de Información como Área dispone de una base para la planificación y la gestión, para realizar estudios de capacidad y proyecciones, y puede conocer las prioridades y criticidades de procesos, y ante todo tiene «eco»: hay alguien al otro lado y puede conocer en qué medida está cumpliendo.
- La Dirección General tiene mayor garantía de que se da prioridad a los objetivos de negocio, y que la tecnología y sus usos están alineados con los planes de negocio, así como que los servicios tienen unos cauces predeterminados.
- Facilitar el seguimiento y el control interno, así como la auditoría: interna y externa, tanto de cuentas como auditoría informática/de sistemas de información.

- Es posible cierto marketing interno, desde la propia difusión de los servicios, que a veces ni se conocen en el caso de entidades medias y grandes, por lo que no se aprovechan lo suficiente, y así pueden tenerse en un catálogo, por ejemplo, formando parte de la Intranet.

32.4. CONTENIDO DE LOS ACUERDOS

Aunque dependerá del entorno y del tipo de servicios, casi cualquier ANS interno deberá o podrá contener los siguientes puntos, algunos una sola vez y otros particularizados para cada uno de los servicios:

- El objeto y el ámbito de aplicación de los Acuerdos.
- En ocasiones se incluyen los objetivos generales: mejora de la eficacia, mejor control, reducción de costes, formalización de las relaciones...
  Pueden, además, incluirse objetivos particulares y concretos, como podrían ser: que el 99 por ciento de las transacciones tengan un tiempo de respuesta inferior a 1,5 segundos, que al menos el 90 por ciento de las incidencias estén resueltas antes de dos horas...
- El lugar de prestación del servicio y desde dónde se presta, si son aplicables; en ocasiones dependerá de circunstancias, de carga… y a veces interesará saber desde qué país/es.
- Las partes: departamentos o áreas que *contratan* y las posibles personas de contacto. El proveedor será normalmente el Área de Producción (dentro de Sistemas de Información); y el cliente, un Área de *Negocio* de la entidad.
- La descripción de los servicios cubiertos y el nivel a alcanzar, y descripción de los recursos objeto del servicio. Si están recogidos en un catálogo bastaría con incluir una referencia. Su criticidad y posible prioridad frente a otros servicios o áreas cliente, incluso según fechas y circunstancias.
  La posibilidad o no de subcontratación y en qué circunstancias: periodos, cuellos de botella, volúmenes...
  Podemos distinguir entre niveles deseables (horizonte), niveles realmente alcanzables en un periodo, y niveles que pueden considerarse aceptables.
  Posibles servicios extra y condiciones: extensión de horarios, por ejemplo, y forma de preaviso, quién puede autorizar…
  La capacidad o carga que se podría soportar: volúmenes y posible distribución, tanto a lo largo del tiempo como, por ejemplo, porque se garantice un cierto balanceo de cargas, y capacidad de crecimiento proyectada, o incluso fijada para determinados periodos, como puede ser en verano, en el periodo navideño, o a principios o fines de mes, en función del sector y de las previsiones basadas en estadísticas.
  La capacidad de almacenamiento en disco, así como los soportes dispo-

nibles: cartuchos, por ejemplo, en el caso de las copias, o capacidad en general sin especificar soportes, en *terabytes*…
Licencias de software: nuevas versiones, aplicación de *service packs*, o equivalentes según fabricante, y parches.
Tipo de información en línea y tiempo máximo de disponibilidad para la que no esté en línea y sea necesario cargar. Periodicidad de refresco en el caso de Almacenes de Datos (Data Warehouse), sistemas EIS (Executive Information Systems), cotizaciones, noticias o equivalentes.
El rendimiento: número de transacciones por segundo, por ejemplo. La posibilidad de funcionamiento con un rendimiento degradado en según qué circunstancias y determinando cargas y duraciones máximas aceptables.
La disponibilidad y la fiabilidad: puede admitirse un máximo de tiempo de caída del servicio (por ejemplo, inferior a 0,5 a lo largo del año: que sería disponibilidad mayor de 99,5 %; una disponibilidad del 99,93 % puede suponer 60 segundos de caída al día de promedio), pero es importante su distribución: no es lo mismo un tiempo de no disponibilidad de dos horas a lo largo de un mes en intervalos de fin de semana (si no son momentos críticos para el servicio) que concentrado el tiempo en un día poco oportuno en medio de una hora punta.
Situaciones o supuestos que estén excluidos.

- En ocasiones se describen o se referencian los recursos relacionados con los servicios: un servidor concreto, la relación de equipos o puestos a los que se da servicio, las redes locales objeto de servicio, los servicios de impresión comprendidos... A veces se incluye el incremento de volumen máximo admitido, e incluso las acciones en caso de rebasar ese máximo: incremento de cargos económicos, necesidad de preaviso, sustitución de servidores...
- En comunicaciones, el volumen puede ser de número de terminales conectados (o de usuarios), de transacciones, de paquetes transmitidos…
- En algunos casos se especifican consumos (de UCP – Unidad Central de Proceso), de espacio reservado en disco, o velocidades de líneas, o volúmenes como se ha indicado, o descarga de ficheros... Sistemas concretos o configuraciones mínimas, o garantía de compatibilidad de sistemas.
- Procedimiento a seguir en el caso de petición de nuevos servicios.
- Las métricas usadas: para medir los servicios, la no disponibilidad, los tiempos de arranque, los volúmenes... y, en definitiva, los indicadores a utilizar, cómo calcularlos y cómo relacionarlos o cruzarlos.
- Los compromisos y las responsabilidades por ambas partes; además de algo tan obvio como cumplir lo estipulado en cuanto a formalización, plazos y medio de comunicar, cumplir las paradas previstas para mantenimientos, realizar las copias locales o remotas estipuladas, mantener la confidencialidad en función de los datos procesados.
- Formación, asistencia y soporte: disponibilidad de técnicos y nivel de conocimientos y experiencia.

- Aspectos de seguridad: confidencialidad, integridad, soluciones alternativas ante contingencias.
- Especialmente si se trata de servicios relacionados con datos personales, se puede incluir una relación de activos y su clasificación, y si se trata de bases de datos el nivel de los mismos, lo que conlleva el grado de protección y cumplimiento de determinados artículos del RDLOPD. La clasificación general de los activos puede ser atendiendo a la confidencialidad, la integridad y la disponibilidad.
- Los días y horarios de disponibilidad y las condiciones de preaviso en el caso de necesidad de extensión: fines de mes, puntas de trabajo... No está de más adjuntar algún calendario o hacer una referencia a fiestas locales, días en que la jornada puede ser reducida por este mismo motivo... para evitar problemas.
- La vigencia: generalmente se prevé una revisión de niveles anual o semestral, y la prolongación del servicio por años; en las revisiones se intentará ir mejorando el servicio, en un proceso continuo. Si se trata de entidades diferentes (proveedor y cliente) y sobre todo no son de un mismo Grupo *(outsourcing)*, la duración del contrato puede estar entre cinco y diez años.
- Posibles causas de suspensión o terminación del servicio, además de por haber alcanzado el fin del plazo.
- Tarifas: posibles costes fijos y variables; no son imprescindibles y a veces figuran aun no existiendo repercusión de costes, pero permiten calcular importes de lo que habría sido una factura o un cargo interno dentro de la misma entidad.
- Posibles supuestos de modificación o de interrupción del servicio, o de servicio degradado.
- Acciones en el caso de incumplimientos, y posibles penalizaciones o compensaciones: aunque en el caso de los internos todo «queda» dentro de la misma entidad, y sin tratarse de *multas* económicas pueden tener su utilidad al reflejarse en informes y comentarse en un Comité de Seguimiento.

  Las penalizaciones pueden ser por días en los que no se haya alcanzado el tiempo de disponibilidad o porque el número de caídas haya sido superior al estimado, o por número de transacciones con tiempo de respuesta superior al fijado, o incidencias no resueltas dentro del margen, entre otros casos. Se pueden asignar pesos fijos a los servicios, o bien fijar la importancia en función de los momentos e impacto.
- La firma de los representantes por ambas partes, y es recomendable que también firme alguien por encima de ambas personas, como puede ser un Director General en el caso de ANS internos.
- Mecanismos de seguimiento. Tipos de informes, contenido y nivel de detalle *(granularidad)* y periodicidad, así como emisor y receptores, y periodicidad de reuniones prevista, que pueden estar condicionadas a

los resultados, y mientras no haya incidencias importantes no ser necesarias.
- En algún caso en que hemos desarrollado ANS hemos aportado un Glosario de términos, a fin de que las partes interpretaran el significado de todos los términos de la misma forma.

El proveedor ha de considerar si en conjunto puede cumplir los compromisos con sus diferentes clientes, cuando en la práctica probablemente las sobrecargas coincidan en fechas y horas.

Los ANS hay que darlos a conocer, en la medida en que les afecten, a los encargados de cumplirlos, a quienes han de controlar de modo directo su cumplimiento por ambas partes y a posibles funciones de Control Interno y de Auditoría Interna. A los auditores externos, en función de las revisiones que puedan estar realizando.

32.5. TIPOS DE SERVICIOS

Pueden ser muy variados, e incluso tratarse de un servicio único. Entre los posibles pueden estar los siguientes, y con frecuencia se ofrecerá una combinación de ellos:

- Procesos en servidores.
- Almacenamiento.
- Uso de aplicaciones.
- Uso de redes de comunicaciones: muy importante la disponibilidad del servicio.
- CAU (Centro de Asistencia a Usuarios) o *Help-desk*.
- Servicios de programación/mantenimiento de aplicaciones.
- Impresión, ensobrado y distribución de formularios.
- Instalación de equipos o de software.
- Servicios relacionados con la seguridad.

32.6. LA SEGURIDAD Y LOS SERVICIOS

Pueden ser servicios en sí mismos, o compromisos relacionados con servicios de los indicados; algunos pueden ser:

- Proceso alternativo para caso de emergencia (Planes de Continuidad).
- Asistencia en la administración de seguridad lógica.
- Compromiso respecto a confidencialidad e integridad de datos, en especial los de carácter personal, y cumplimiento del Documento de Seguridad.

- Evaluación/auditoría de los riesgos en las áreas de los clientes: en cuanto a cumplimiento de aspectos jurídicos, organizativos (funciones, normas), de seguridad física y de seguridad lógica o más técnica.
- Compromiso en cuanto a integridad de software.
- Compromiso de confidencialidad (y en general de cumplimiento de la legislación vigente en especial en cuanto a datos de carácter personal).
- Cifrado de datos, si procede.
- Obtención de copias de seguridad y no difusión o uso indebido de la información. Número de copias o *generaciones*: lunes a viernes, las tres últimas... Envío a lugares diferentes y debidamente protegidos en cuanto a transporte y almacenamiento.
- Concienciación de usuarios.
- Aplicación de parches, sobre todo de seguridad.
- Ficheros/almacenamiento *espejo*.
- Tiempo de rearranque de los servicios.
- Bitácoras *(logs)* de transacciones o de accesos.
- Administración de sistemas, de cortafuegos o de filtros de correo. Simulación periódica de ataques controlados. Privacidad del correo electrónico, y medidas para intentar evitar la proliferación de correos no deseados o *spam*.
- Registro/solución de incidencias.
- Asistencia en la relación con proveedores (de dispositivos, de paquetes...) en temas relacionados con la seguridad.
- Control de virus: preventivo (antivirus y su actualización) así como eliminación y recuperación en caso de infección.
- Protección de activos, y en el caso de protección física: vigilantes, detección y extinción de incendios, control de accesos, recepción y gestión de alarmas...
- Tiempo máximo de reanudación de cada servicio, con soluciones propias u otras externas previstas.
- Cobertura de los seguros: en más de un caso hemos encontrado que había riesgos no cubiertos, porque las áreas usuarias daban por hecho que Sistemas de Información o Servicios Centrales/Generales tenían contratadas pólizas que cubrían los elementos que estaban utilizando, y Sistemas de Información pensaba que era un tema de cada Área.

Algunos de estos puntos tienen relación con varios artículos del RDLOPD.

32.7. LA MEDIDA DEL SERVICIO

El objetivo debe ser, más que medir la utilización de componentes y dispositivos, medir el grado de satisfacción de los clientes: la calidad percibida.

Puede darse también el caso de clientes satisfechos con un servicio malo, a veces por una conformidad labrada a lo largo del tiempo.

Estableciendo métricas se pueden fijar niveles y verificar hasta qué punto se alcanzan, aunque sea convirtiendo a valores numéricos respuestas de clientes acerca del servicio, y esperando que al menos nueve de cada diez estén satisfechos o muy satisfechos.

Es preferible que los indicadores se elijan pensando en los clientes y no en aspectos técnicos, pudiendo los indicadores técnicos servir para conocer desviaciones y el porqué.

Dependerá del servicio de que se trate, pero algunos indicadores pueden ser:

- Disponibilidad del servicio, que en porcentaje se calculará como:

$$\frac{\text{Tiempo convenido} - \text{Tiempo de no disponibilidad}}{\text{Tiempo convenido}} \times 100$$

- Utilización: la carga que realmente ha habido: en transacciones, en volumen de datos transmitidos, en operaciones de comercio electrónico, en consultas a una web, mensajes de correo electrónico y extensión... Preferiblemente medida en unidades que puedan entender y contrastar los clientes, como decíamos dejando los parámetros técnicos para los análisis técnicos.
- Margen real de aviso para interrupción del servicio por mantenimiento o incidencias.
- Tiempo medio entre fallos (TMEF o MTBF – Mean Time Between Failures), expresado en horas o en días.
- Tiempo de reparación máximo en el caso de fallos.
- Tiempo medio de reparación (TMDR o MTTR – Mean Time to Repair), siglas que ahora interpretamos con frecuencia como Mean Time to Restore, por no existir la reparación sino el rearranque o la normalización de la situación sin más.
- Tiempo máximo de resolución de incidencias, tiempo medio, número de ellas resueltas, y de las no resueltas: tiempo medio de espera.
- Tiempo máximo de altas de usuarios (o de variación de perfiles si se quiere diferenciar).
- Número de llamadas al Servicio de Ayuda (*Help-desk)*, duración media, tiempo máximo en atender la llamada, así como en la resolución de la incidencia, distribución, origen, concentración de incidencias por horas, por tipos, por servicios…
- En los casos en que pueda haber procesos por lotes *(batch)* número de trabajos *(JOBS)* procesados y número de terminaciones anormales *(abend)*.
- Minutos de usuario de no disponibilidad: si una caída de media hora ha afectado a cien usuarios, por ejemplo, los que estaban conectados a una red local, en total son 3.000 minutos de no disponibilidad: 50 horas.

- Número de cartuchos/soportes colocados, o directamente utilizados por los equipos.
- Instalación de componentes hardware, software y aplicaciones, o bien equipos de comunicaciones, con y sin desplazamiento.

Con el conjunto de indicadores, y asignándoles pesos, se pueden crear cuadros de mando.

Hay, además, aspectos cualitativos a considerar que deben traducirse a valores numéricos para comparar; así, la satisfacción de los clientes respecto a cada servicio se puede conocer mediante cuestionarios y comentarlos en entrevistas, que pueden ser una buena ocasión de contrastar la situación y las perspectivas.

Para cuantificar y poder comparar una variable como la satisfacción podemos recurrir a una puntuación (de 0 a 5, de 0 a 10, o empezando desde el uno para evitar el impacto psicológico del cero), o bien con opciones entre las que se debe elegir una: muy satisfecho, satisfecho, ni satisfecho ni insatisfecho, insatisfecho y muy insatisfecho.

En este último supuesto se pueden asignar valores numéricos para poder incorporar a una hoja de cálculo, y medir los que en general están satisfechos (añadiendo los muy satisfechos e incluso con mayor peso).

Será imprescindible incluir comentarios respecto a las cuestiones en que no haya satisfacción, incluso en los casos neutrales: ni satisfechos ni insatisfechos.

En muchos de los casos en los informes se pueden incluir cifras y comparación con los objetivos: cuántas de las incidencias han sido resueltas dentro del plazo acordado, así como desviación (y distribución) de las que han excedido el margen.

También se pueden comparar datos del mes anterior con el mismo mes de hace un año, de lo transcurrido del año con el mismo periodo del año anterior, calcular el total anual móvil (doce últimos meses transcurridos) e igualmente comparación con periodos similares anteriores, posible proyección, tendencias, simulaciones...

La periodicidad de los informes puede ser: semanal para los informes más técnicos, e incluso para las incidencias habidas, y mensual para los destinados a los clientes y a la Dirección, debiendo ser estos informes muy *visuales*.

No deben descartarse los informes en tiempo real, sobre incidencias y cómo evoluciona su resolución, sobre todo de las graves, o avisando de posibles problemas o cambios, para lo que puede valer el correo electrónico o incluso una llamada de teléfono anticipándolo.

32.8. CUESTIONES

32.8.0. ¿Cómo podríamos definir los ANS?
32.8.1. El posible contenido de los ANS.

32.8.2. ¿Cuáles pueden ser los beneficios de los ANS para los clientes?
32.8.3. ¿Cuáles pueden ser los beneficios para el proveedor: entidad o área interna de Sistemas de Información?
32.8.4. ¿Cuáles pueden ser para la Dirección General de la entidad que recibe el servicio?
32.8.5. ¿Cuál puede ser el papel de funciones como Control Interno y Auditoría Informática/de Sistemas de Información? ¿Y de Auditoría Financiera?
32.8.6. Relación de los ANS con la Ley Orgánica 15/99, con los contratos y con la seguridad.
32.8.7. El papel del cliente y su responsabilidad.
32.8.8. Relación entre calidad y seguridad.
32.8.9. ANS y servicios prestados por Internet.

32.9. CASO PRÁCTICO

La Entidad X, a través de su Departamento de Sistemas de Información, tiene contratados con empresas externas estos servicios:

- Atención a usuarios internos y soporte de ofimática.
- Soporte técnico y funcional de SAP R/3.
- Impresiones masivas, incluidos ensobrados y envíos.

Además, presta de forma directa servicios de proceso en servidores locales a diferentes áreas funcionales de la entidad.

En relación con ello, se pide reflexionar sobre las siguientes cuestiones:

- ¿Qué contratos y/o ANS deben suscribirse en estos casos y entre quiénes?
- ¿Qué ventajas podría tener la formalización de los ANS?
- ¿Qué dificultades se podrían presentar?
- ¿En qué puede afectar el artículo 12 de la LOPD?
- ¿Qué podría influir del RDLOPD?
- ¿Qué recursos podrían estar relacionados con cada uno de estos servicios?
- ¿Qué funciones deberían intervenir en la redacción y negociación de los ANS?
- ¿Qué funciones podrían participar en el seguimiento del cumplimiento?
- ¿Qué métricas/indicadores podrían establecerse en cada caso en relación con la calidad?
- ¿Y en relación con la seguridad?

sado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés.

   En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV
Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I
Ficheros de información sobre solvencia patrimonial y crédito

Sección 1.ª
Disposiciones generales

Artículo 37. Régimen aplicable.

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999,

de 13 de diciembre, se someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.
b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección 2.ª
Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. Requisitos para la inclusión de los datos.

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.
b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores.

Tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. Información previa a la inclusión.

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. Notificación de inclusión.

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.

2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. Conservación de los datos.

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. Acceso a la información contenida en el fichero.

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.
b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.
c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. Responsabilidad.

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión

en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.

2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.
   En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

2.ª Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al

afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II
Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. Datos susceptibles de tratamiento e información al interesado.

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.
b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. Tratamiento de datos en campañas publicitarias.

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.
b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.
c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. Depuración de datos personales.

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. Ficheros de exclusión del envío de comunicaciones comerciales.

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. Ficheros comunes de exclusión del envío de comunicaciones comerciales.

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que

resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. Derechos de acceso, rectificación y cancelación.

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. Derecho de oposición.

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja

del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento.

En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V
Obligaciones previas al tratamiento de los datos

CAPÍTULO I
Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. Disposición o Acuerdo de creación, modificación o supresión del fichero.

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. Forma de la disposición o acuerdo.

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. Contenido de la disposición o acuerdo.

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.
b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obli-

gados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.
e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.
f) Los órganos responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II

NOTIFICACIÓN E INSCRIPCIÓN DE LOS FICHEROS DE TITULARIDAD PÚBLICA O PRIVADA

Artículo 55. Notificación de ficheros.

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas