

<http://idp.uoc.edu>

ARTÍCULO

El fin de la situación de transitoriedad: la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ya tiene desarrollo reglamentario

 Mònica Vilasau Solana

Fecha de presentación: mayo de 2008

Fecha de aceptación: junio de 2008

Fecha de publicación: septiembre de 2008

Resumen

El 19 de abril del 2008 entró en vigor el Reglamento 1720/2007, de 21 de diciembre que desarrolla la LOPD. Este texto había sido muy esperado por los aplicadores del derecho, por las empresas de consultoría y de seguridad, por sectores del marketing y publicidad, por empresas dedicadas a la solvencia patrimonial y crédito y, en menor medida, por los consumidores y usuarios. La norma responde a la necesidad de dotar la Ley orgánica sobre la materia del correspondiente desarrollo reglamentario y dar respuesta a las nuevas necesidades de la sociedad de la información constantemente en evolución. En el RLOPD se regula el otorgamiento del consentimiento por silencio positivo, el otorgamiento del consentimiento del menor, se sistematiza el ejercicio de los derechos por parte del afectado, se regulan detalladamente los ficheros de marketing y publicidad, los de solvencia patrimonial y crédito, se dota a la figura del encargado de un estatus jurídico, se proporciona todo un nuevo marco a las medidas de seguridad y se sistematizan los procedimientos tramitados por la Agencia española de protección de datos. El texto aprobado evidentemente no complacerá a todo el mundo, la existencia de múltiples instancias involucradas (estatales y autonómicas) y de múltiples agentes con diferentes perspectivas hace que las soluciones proporcionadas no se ajusten a los ideales de todos los implicados. Sin embargo el nuevo Reglamento es un paso adelante en la consolidación del derecho a la protección de datos de carácter personal, aporta mayor seguridad jurídica y flexibilización y tiene que verse como una oportunidad de crear una nueva cultura de protección de datos integrada en el tratamiento de la información de una forma global.

Palabras clave

protección de datos, medidas de seguridad, responsable del tratamiento, encargado de tratamiento, consentimiento, cesión de datos, menor de edad, publicidad y marketing, ficheros de solvencia patrimonial y crédito, derecho de acceso, derecho de rectificación, derecho de cancelación, derecho de oposición, inscripción de ficheros, fuentes accesibles al público, datos relativos al empresario individual, deber de secreto, subcontratación, documento de seguridad, niveles de seguridad, tratamientos automatizados, tratamientos no automatizados

Tema

Protección de datos y tratamiento de la información

The end of the transitory situation: the development of the Organic Law 15/1999, of 13 December 1999, on personal data protection, is now regulated

Abstract

The Royal Decree of 1720/2007, 21 December 2007, came into effect on 19 April 2008 to regulate the development of the Organic Law on Personal Data Protection (LOPD). This has been long awaited by those who apply the law, consulting and security companies, by marketing and advertising sectors of companies dedicated to financial and credit solvency, and, to a lesser extent by consumers and users. It gives the corresponding regulated development to the Organic Law on personal data protection, and responds to the new needs of the constantly evolving information society. The RLOPD (Reglamento governing the LOPD) regulates giving consent for positive administrative silence, giving of consent by minors, introduces systematic exercising of rights by those affected, exhaustively regulates marketing and advertising databases and those of financial solvency and credit, gives the processor a legal status, supplies a whole new framework for security measures, and systemises the procedures passed on by the Spanish Agency for Data Protection. The approved text obviously is not to the satisfaction of all: the many authorities involved (state and automatic) and many agents with different perspectives mean that the solutions offered are not those which all those involved consider ideal. However, the new regulations are a step forward in the consolidation of rights for personal data protection, bring better legal security and flexibility, and must be seen as an opportunity to create a new culture for data protection integrated in processing information on a global scale.

Keywords

data protection, security measures, controller, processor, consent, cession of data, minors, marketing and advertising, files, solvency and credit, right to access, right to rectification, right to cancellation, right to block, registering files, sources accessible to the public, data regarding the individual contractor, respecting confidentiality, subcontracting, security document, levels of security, automatic processing, non-automatic processing

Topic

Data protection and information processing

Introducción

La situación de transitoriedad ha durado ocho años. La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal¹ (LOPD en lo sucesivo) dejó subsistentes los RD 1332/1994, de 20 de junio y RD 994/1999, de 11 de junio que desarrollaron la antigua y primera

Ley dedicada al tratamiento de datos de carácter personal,² la LORTAD,³ derogada por la LOPD.

Los mencionados Reales Decretos hacían referencia a los procedimientos a seguir en el ejercicio de los derechos reconocidos al afectado, al ejercicio de la potestad sancionadora por parte de la Agencia Española de Protección de Datos (AEPD) y a las medidas de seguridad en el trata-

1. BOE n.º 298, de 14 de diciembre de 1999.

2. Véase Disposición transitoria 3 de la LOPD.

3. LO 5/1992, de 29 de octubre, de regulación del tratamiento automático de datos de carácter personal.

miento de datos de carácter personal (DCP). Todos estos aspectos han sido objeto de regulación específica y detallada por el RD 1720/2007 de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD en lo sucesivo).⁴ Esta nueva norma también desarrolla reglamentariamente las competencias que en materia sancionadora la LSSI⁵ y la LGT⁶ han atribuido a la AEPD.⁷

Los primeros borradores de Reglamento de desarrollo de la LOPD se pusieron sobre la mesa hace más de tres años. El hecho de que se haya tardado tanto tiempo en aprobar el texto que desarrolla la LOPD nos indica que se trata de una norma compleja y que tiene múltiples implicaciones, entre las cuales cabe destacar:

I. El tratamiento de DCP afecta gran parte de las esferas jurídicas relacionadas con la persona y por ello podemos decir que es una materia transversal. Hay todo un entramado de normas que bien de forma directa bien de forma indirecta hacen referencia al tratamiento de DCP (pensemos en aspectos como los datos ideológicos, los relativos a la salud, los biométricos, los que revelan perfil psicológico del sujeto, los de violencia de género...)

II. Los sectores implicados también son múltiples: empresas de software, de telecomunicaciones, de prestación de servicios, de marketing y publicidad, de información sobre la solvencia patrimonial y crédito, asociaciones de consumidores y usuarios y de internautas, la propia administración. Además los datos de carácter personal (DCP) tienen cada vez más un componente comercial, se trata de un bien cada vez más codiciado por determinados agentes económicos.

III. Nos encontramos ante una materia que no está reservada a la competencia exclusiva del Estado y algunos

Estatutos de Autonomía han reconocido una competencia al respecto.⁸ Si bien la LOPD tiene naturaleza de Ley orgánica, no todo su contenido tiene esta característica. Además, aparte de la creación de la Agencia Española de Protección de Datos (AEPD), en el marco que reconoce la LOPD, han sido creadas algunas agencias autonómicas (la de la Comunidad de Madrid, Cataluña y País Vasco) que desarrollan las funciones de velar y controlar el cumplimiento respecto de este derecho en los respectivos territorios.

IV. El derecho a la protección de datos personales está cada vez más en tensión con la seguridad, aunque es discutible que podamos hablar de un derecho a la seguridad, podemos hablar de un derecho a la vida, a la libertad, a la integridad física... pero no está reconocido en nuestra Constitución un derecho a la seguridad. También es necesario encontrar un equilibrio entre el derecho a la protección de datos y las libertades de expresión e información. Por otra parte en algunos casos nos encontraremos en conflicto con el derecho a acceder a los registros públicos y a pedir información de las administraciones.

V. La evolución y transformación tecnológica es constante, lo que comporta que el legislador deba tener una gran capacidad previsora con el fin de poder dar una respuesta a la realidad tecnológica.

Durante el proceso de elaboración del RLOPD, y vistas las implicaciones de la norma, se argumentó por algunos sectores que en realidad habría hecho falta una reforma de la propia Ley Orgánica. También se advirtió del peligro de que el RLOPD constituyera una cristalización de la doctrina de la AEPD, pero se alega que habría sido un desacierto no partir y prescindir totalmente de la interpretación de la agencia estatal. Por otra parte, además de la impronta de la Agencia Española, el Gobierno ha marcado su propia dirección en la elaboración de la

4. BOE n.º 17 de 19 de enero 2008.

5. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE n.º 166, de 12 de julio).

6. Ley 32/2003, de 3 de noviembre, general de telecomunicaciones.

7. Véase el apartado III de la exposición de motivos del RLOPD. La única materia que no se incorpora al texto aprobado es el Estatuto de la AEPD, regulado por el RD 428/1993, de 26 de marzo.

8. En el caso de la CA de Cataluña, su Estatuto de autonomía reconoce en el art. 31 el derecho a la protección de datos personales y el art. 156 establece las competencias de la Generalitat en materia de protección de datos de carácter personal. Véase Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de autonomía de Cataluña, publicado por el Decreto 306/2006, de 20 de julio, por el cual se da publicidad a la Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de autonomía de Cataluña. (DOG de 20 de julio de 2006, n.º 4680).

norma reglamentaria y ha establecido los criterios de redacción.⁹

Visto el punto de partida del RLOPD, a continuación analizaremos los principales aspectos tratados por el texto aprobado.

1. Ámbito de aplicación de la normativa sobre protección de datos

El art. 2.1 RLOPD, siguiendo lo que establece la LOPD, prevé que la norma aprobada se aplica a los datos de carácter personal registrados en un soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de los datos.

Para poder hablar de un dato de carácter personal (de ahora en adelante, DCP) hace falta que exista un dato, la vinculación a una persona identificada o identificable, y que esta vinculación lo sea por medios relativamente sencillos.

Veamos ahora cuáles son los principales interrogantes planteados y las soluciones que proporciona el RLOPD.

1.1. El término dato

Partiendo del art. 3.a) LOPD que considera por DCP «cualquier información concerniente a personas físicas identificadas o identificables», el art. 5.1.f) RLOPD especifica que dentro del término dato se incluye «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables». El concepto de DCP comprende pues, entre muchos otros datos la imagen, la voz,

las huellas dactilares, los datos biométricos, la información genética. Por otra parte la LOPD resulta aplicable a cualquier dato, con independencia de su relevancia, incluso si no incide en la esfera de la intimidad, ya que mediante datos irrelevantes se puede obtener información íntima y trazar perfiles de los sujetos. Sin embargo no todos los datos tienen la misma importancia, los que revelan la ideología, afiliación sindical, religión o creencias, los relativos a la salud, raza o vida sexual disfrutan de una protección especial (art. 7 LOPD).

1.2. El término personal

La información tiene que ser relativa a *personas físicas identificadas o identificables* [art. 3.a) LOPD]. Hace falta que la información se pueda vincular a una determinada persona física y mediante métodos que no sean complejos.¹⁰ ¿Qué comprende el término personal?

1.2.1. Los datos relativos a una persona muerta

En sentido riguroso no podemos hablar de datos relativos a una persona muerta (la muerte extingue la personalidad, art. 32 CC), pero el art. 2.4 RLOPD permite que las personas vinculadas al difunto por razones familiares o análogas puedan dirigirse a los responsables de los ficheros o tratamientos que contengan DCP relativos al finado con el fin de notificar y acreditar la muerte y solicitar la cancelación de los datos.

1.2.2. Los datos relativos a las personas jurídicas

La jurisprudencia constitucional ha reconocido a las personas jurídicas la titularidad de algunos derechos fundamentales (inviolabilidad del domicilio, tutela judicial efectiva, secreto de las comunicaciones, libertad de expresión e información)¹¹ si bien es bastante dudoso que puedan ser titulares del derecho a la intimidad.¹²

9. R. MARTÍNEZ MARTÍNEZ, «El Reglamento de desarrollo...», pág. 74.

10. «La identificación del titular del vehículo no exige esfuerzos o plazos desproporcionados, por lo que el tratamiento de la matrícula tiene que considerarse un tratamiento de un DCP», Informe de la AEPD 425/2006.

11. Para todos véase DÍEZ-PICAZO GIMÉNEZ, *Sistema de Derechos Fundamentales*. El autor critica la solución dada por alguna STC reconociendo el derecho al honor de una persona jurídica ya que el autor considera que el honor es una característica profundamente humana, pág. 133-136.

12. DÍEZ-PICAZO GIMÉNEZ considera que no se puede predicar el derecho a la intimidad ya que no tienen vida personal ni familiar y es muy dudoso que les corresponda el derecho a la protección de DCP sobre la base del art. 3 LOPD que solo hace referencia a las personas físicas. (*Sistema de Derechos Fundamentales*, pág. 288 a 312).

Con respecto a la protección de datos, diferentes textos normativos excluyen de la tutela del derecho a la protección de datos a las personas jurídicas: el art. 18.4 CE hace referencia a los ciudadanos en cuanto a sujetos protegidos; los arts. 1.1 y 2.a) Directiva hacen referencia a la protección de las personas físicas¹³ y la misma referencia se hace en el art. 1, 3.a) y 3.e) LOPD. El art. 2.2 RLOPD lo ha dejado todavía más claro ya que establece que el reglamento en cuestión no será aplicable a los tratamientos de datos referidos a personas jurídicas.¹⁴

Sin embargo, aunque se excluyen del concepto de dato personal y del ámbito de protección de la LOPD los datos referidos a las personas jurídicas, éstas no quedan desprotegidas frente al uso indebido de sus datos ya que pueden recorrer a la tutela del art. 1902 CC, a la tutela penal si es necesario y también les resulta aplicable la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas,¹⁵ la LSSI y la LGT.

1.2.3. Los datos relativos al empresario individual

En la interpretación de la LOPD se planteaba si la norma era aplicable a los datos relativos a un sujeto que ejerce una actividad empresarial o profesional ya que en ocasiones determinados datos como el domicilio o el teléfono pueden hacer referencia tanto a la esfera profesional como a la privada.

A partir de la aprobación y entrada en vigor del RLOPD se clarifican un poco estos interrogantes.

Por un lado la normativa analizada no será aplicable a los datos de las personas de contacto ni al directorio interno que se puede utilizar en una empresa u organización,

siempre y cuando la información tratada se limite exclusivamente al nombre y apellidos, las funciones realizadas, la dirección postal o electrónica, el teléfono y número de fax profesionales (art. 2.2. RLOPD). Se excluyen únicamente los datos expresamente mencionados en el precepto, como afirmó la AEPD en la primera sesión abierta sobre la problemática, interpretación y aplicación del RLOPD.¹⁶

Por otra parte tampoco resulta aplicable la normativa a los datos de los empresarios individuales cuando se haga referencia a estos sujetos en su condición de comerciantes, industriales o navieros (art. 2.3 RLOPD).

Según la AEPD, a fin de que operen las excepciones del art. 2.2 y 2.3 del RLOPD hace falta que se cumplan dos requisitos:¹⁷ a) Con respecto a los datos, tendrán que limitarse en el caso de personas de contacto a las enumeradas en el art. 2.2 y en el caso de comerciantes (art. 2.3) a los datos vinculados exclusivamente con la actividad empresarial (la excepción no opera si los datos se refieren tanto a la esfera personal como la empresarial). b) Con respecto a la finalidad, el tratamiento tiene que tener como destinatario a la empresa, nunca la persona física. Con respecto a si dentro del término *empresario individual* y la excepción del art. 2.3 RLOPD quedan incluidos profesionales como arquitectos, médicos o abogados, la AEPD consideró que a fin de que se excluya la aplicación de la LOPD los datos tienen que ser relativos a un profesional que tenga organizada su actividad en forma de empresa. Si el profesional actúa por cuenta ajena o no está organizado en forma de empresa no se considerarán incluidos en el art. 2.3 RLOPD¹⁸ y por lo tanto resultará aplicable la legislación sobre protección de datos.

13. El considerando 24 de la Directiva 95/46/CE determina que: «Las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernen no son objeto de la presente Directiva».

14. En este sentido consultad el Informe de la AEPD 0234/2008, pág. 2.

15. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (DOCE L 201 de 31.7.2002). En concreto véase el considerando 12 y el art. 13.5.

16. «1.ª Sesión abierta de la AEPD. El nuevo Reglamento de desarrollo de la Ley Orgánica de protección de datos: problemática, interpretación y aplicación». Pueden encontrarse las ponencias y las FAQ en la página web de la AEPD (<https://www.agpd.es/index.php>), sección «Jornadas de la Agencia».

17. Respuesta 3, pág. 5, 1.ª sesión.

18. Respuesta 6, pág. 8, 1.ª sesión. En el mismo sentido, puede consultarse el Informe del gabinete jurídico de la AEPD 0234/2008.

1.3. Constancia de los datos

La LOPD, a diferencia de la LORTAD,¹⁹ resulta aplicable tanto a los tratamientos automatizados como a los no automatizados.²⁰ El art. 5.1.n) RLOPD define qué hay que entender por fichero no automatizado: «Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica».

Los tratamientos no automatizados de datos se hallaban sometidos a un régimen transitorio que duraría 12 años desde la aprobación de la LOPD y a lo largo del cual tenían que adecuarse al texto aprobado (art. 32.2 Directiva 95/46/CE y DA 1.2 LOPD). Transcurrido este plazo, que finalizó el 24 de octubre de 2007, la LOPD resultó plenamente aplicable a los tratamientos no automatizados si bien el RLOPD establece un régimen transitorio con respecto a la aplicación de las disposiciones relativas a las medidas de seguridad correspondientes tanto a los ficheros automatizados como a los que no lo son que ya existían en el momento de la entrada en vigor del Reglamento (Disposición transitoria 2.ª RLOPD).

1.4. Tratamientos regulados por la LOPD

La LOPD determina su ámbito de aplicación y excluye los ficheros mantenidos por personas físicas en el ejercicio de sus actividades personales o domésticas, los sometidos a normativa sobre protección de materias clasificadas y los archivos establecidos para la investigación del terrorismo y de la delincuencia organizada (art. 2.2 LOPD y art. 4 RLOPD).

Respecto de los ficheros de carácter doméstico, no siempre es fácil delimitar cuándo estamos en una esfera y cuándo se traspasa. Un ejemplo de esta dificultad lo

encontramos en el supuesto que dio lugar a la SAN 15 de junio de 2006, en la que una promoción militar para celebrar las bodas de plata recopiló los datos de los compañeros y los entregó a una agencia de viajes que se encargó de la gestión del acontecimiento. Denunciada la comisión de fiestas delante de la AEPD por cesión de datos sin consentimiento, los sancionados invocaron la excepción del art. 2.2.a) LOPD mientras que la AEPD sostenía que una vez los DCP habían salido de las agendas personales para integrarlos en un conjunto de DCP para la promoción de un acontecimiento, resultaba aplicable la LOPD.

Sin embargo la AN declaró que lo que hay que tener en cuenta es si el tratamiento en cuestión se ha realizado en un ámbito o finalidad que sea *exclusivamente doméstico* y considera que en el caso expuesto la finalidad del tratamiento no excedía el ámbito familiar ya que:

«[...] tiene por objeto mantener los lazos de amistad y compañerismo creados durante el período formativo mediante la celebración de un acto puntual de confraternización de todos los miembros de una determinada promoción con ocasión del veinticinco aniversario de su jura de bandera. No se pretende pues una finalidad profesional, aunque todos los partícipes de la celebración pertenezcan a una misma corporación profesional como es la militar.» (FD 3.º)

2. Obligaciones previas al inicio del tratamiento

Tanto en un sentido cronológico como sobre la base de lo que prevé la normativa,²¹ antes de proceder al tratamiento de cualquier dato de carácter personal hay que cumplir unas determinadas obligaciones entre las que en primer lugar destaca la creación de los correspondientes ficheros.

19. El art. 2.1 LORTAD hacía referencia al hecho que la Ley era aplicable a los datos de carácter personal que figuraran en ficheros automatizados.

20. El art. 2.1 LOPD dispone simplemente que la norma es de aplicación a los datos de carácter personal registrados en soporte físico.

21. Véase art. 26.1 LOPD que prescribe que toda persona que proceda a la creación de ficheros de datos de carácter personal lo notificará *previamente* a la AEPD, y el art. 52.2 RLOPD, según el cual la disposición o acuerdo que establezca la creación, modificación o supresión de un fichero de titularidad pública, tendrá que dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

La LOPD hace referencia a este aspecto en el Título IV²² *Disposiciones sectoriales* (regulando aspectos muy diversos) y el RLOPD dedica el Título V exclusivamente a las obligaciones previas al tratamiento de los datos y se centra en la creación, modificación, supresión, notificación e inscripción de los ficheros.

Debe subrayarse que la LOPD, tanto respecto a la creación de ficheros como respecto al régimen sancionador aplicable a los tratamientos –y a diferencia de la Directiva 95/46/CE– distingue entre ficheros de titularidad pública y de titularidad privada, otorgando a los primeros un tratamiento ciertamente privilegiado.

Sin embargo, la LOPD no proporciona una definición de ambos tipos de ficheros, cosa que sí que hace el RLOPD en el art. 5.2.l) y 5.2.m). Hay que tener claro que las definiciones proporcionadas no son en absoluto neutras, sino que tienen consecuencias importantes respecto de la creación de los ficheros y del ejercicio de la potestad sancionadora. El criterio adoptado en el RLOPD hace prevalecer la forma adoptada por el ente responsable del fichero por encima de la finalidad a la que se destine el fichero, consolidando de este modo el criterio utilizado por la AEPD. En cambio la APDCAT, con el fin de distinguir entre ficheros de titularidad pública y privada, adoptó un criterio material según el cual eran públicos los ficheros necesarios para el ejercicio de las funciones públicas, con independencia de la forma adoptada por el ente que las ejercitara y los ficheros de carácter público quedaban sometidos al ámbito de actuación de la Agencia catalana.

Sin embargo, como señala Farré, la equiparación entre fichero público / ámbito de actuación de la Agencia Catalana se empezó a romper con el art. 156 EAC que sometió al control de la APDCAT determinados ficheros de naturaleza privada. Esta no identificación se ve acentuada con el RLOPD ya que determinadas entidades gestoras de servicios públicos creadas por las administraciones públicas pero de naturaleza privada, sólo podrán ser titulares de

ficheros de titularidad privada. Como ya se ha indicado, este régimen establecido por el RLOPD tiene importantes consecuencias respecto el ejercicio de la potestad sancionadora y la creación de los ficheros e, indirectamente, el RLOPD ha modificado el régimen sancionador aplicable a determinadas entidades sometidas a la competencia de la APDCAT.²³

2.1. Disposiciones comunes a ambos tipos de ficheros

A pesar de la división establecida por la LOPD entre los ficheros de naturaleza pública y los de naturaleza privada, el capítulo II, título IV RLOPD establece una serie de disposiciones que son comunes a ambos tipos de ficheros entre las que hay que destacar:

La coordinación entre los Registros de protección de datos existentes, de manera que haya una sola notificación y si es necesario una doble inscripción (Registro estatal y autonómico, según prevé el art. 55.3 RLOD).²⁴

En caso de creación de un fichero por parte de varias personas o entidades de forma simultánea, cada una de ellas tiene que notificar la creación (art. 57 RLOPD).

La inscripción de un fichero tiene que estar siempre actualizada y hay que notificar previamente cualquier modificación que afecte al contenido de la inscripción (art. 58.1 RLOPD).

La inscripción de un fichero en el RGPD no exime al responsable cumplimiento del resto de las obligaciones previstas en la LOPD (art. 60.3 RLOPD).

Se permite la actuación de oficio por parte del Director de la AEPD en determinados supuestos: cancelación (art. 61.2), rectificación de errores (art. 62) e inscripción de ficheros de titularidad pública en circunstancias excepcionales (art. 63).

22. Hace falta tener en cuenta, según lo que establece la DF 2.^a LOPD, que este título tiene carácter de Ley ordinaria.

23. Véase S. FARRÉ TOUS, «Novetats del RLOPD...», pág. 2-4.

24. FARRÉ hace referencia a la situación existente antes de la entrada en vigor del RLOPD sobre la base de cuya normativa a veces se producían dos notificaciones (a las Autoridades estatales y autonómicas) y a veces sólo una. Aunque la colaboración entre las Agencias había permitido solucionar parte de los problemas planteados, la APDCAT puso especial énfasis en la fase de elaboración del Reglamento en la notificación única y si fuera necesario, la doble inscripción. («Novetats del RLOPD...», pág. 6-8).

Finalmente el art. 64 RLOP prevé la colaboración entre las autoridades de control de las CCAA y la AEPD con el fin de garantizar la inscripción en el RGPD de los ficheros sometidos a la competencia de las autoridades autonómicas.

2.2. Ficheros de titularidad pública

La creación, modificación y supresión de ficheros de titularidad pública sólo se podrá realizar por medio de disposición general publicada, con carácter previo, en el BOE o en el diario oficial correspondiente (art. 20.1 LOPD y 52 RLOPD). El art. 53 RLOPD regula la forma de la disposición o acuerdo de creación, modificación o supresión. Las disposiciones de creación/modificación tendrán que indicar lo que prevé el artículo 20.2. LOPD y 54 RLOPD. Con respecto a la supresión de los ficheros, en las disposiciones que se dicten al respecto habrá que establecer el destino o, si es necesario, las previsiones que se adopten para su destrucción (art. 20.3 LOPD y 54.3 RLOPD).

También es preciso tener en cuenta que todo fichero de DCP de titularidad pública deberá notificarse a la AEPD 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 30 días desde la publicación de la norma o acuerdo de creación en el diario oficial correspondiente (art. 55.1. RLOPD).

Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una CA que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos (art. 55.3 RLOPD).

2.3. Ficheros de titularidad privada

Podrán crearse ficheros de titularidad privada que contengan DCP cuando sean necesarios para la consecución de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que establece la LOPD (art. 25 LOPD). Cuando se proceda a la creación de estos ficheros habrá que notificarlo *previamente* a la AEPD proporcionando la información establecida en el artículo 26.2 LOPD y desarrollada por el art. 55.2 RLOPD. Cuando la obligación de notificar afecte a ficheros sujetos a la compe-

tencia de la autoridad de control de una CA que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente que dará traslado de la inscripción al RGPD (art. 55.3 RLOPD).

3. Mecanismos que legitiman el tratamiento de los DCP

El art. 10 RLOPD sistematiza los mecanismos (ya previstos en la LOPD) que permiten el tratamiento de los DCP estableciendo que aparte del supuesto en que el propio interesado haya otorgado su consentimiento, los datos también podrán tratarse, aunque no exista el mencionado consentimiento, en los siguientes casos:

- Cuando los datos consten en fuentes accesibles al público.
- Cuando concurren determinados supuestos (ejercicio de las funciones de las administraciones públicas, existencia de una relación contractual o administrativa, protección de un interés vital del afectado).
- En determinados casos, cuando los datos se obtengan a través de un sujeto diferente del interesado (cesión de datos).
- Cuando la Ley lo autorice o lo establezca expresamente y con el fin de satisfacer un interés legítimo del responsable del tratamiento o con el fin de cumplir un deber impuesto por una norma.

3.1. El consentimiento del interesado

Cuando se obtengan los datos del propio interesado, éste tendrá que ser informado de modo expreso, preciso e inequívoco entre otros aspectos de la existencia del tratamiento y de la finalidad de la recogida de los datos [art. 5.1.a) LOPD]. Según establece el art. 18 RLOPD, el deber de información tendrá que llevarse a cabo de forma que permita acreditar su cumplimiento y el responsable del tratamiento tendrá que conservar el soporte donde conste el cumplimiento de este deber si bien puede procederse al escaneado de la documentación en soporte papel.

Con respecto a la regulación de la obtención del consentimiento en el Reglamento, podemos destacar dos novedades importantes: las consecuencias del silencio y la obtención del consentimiento de los menores.

3.1.1. Las consecuencias del silencio

Tanto la LOPD como el Reglamento parten de la regla general de que el consentimiento tiene que ser inequívoco²⁵ si bien en los casos que se traten datos que se consideran sensibles se establece un mecanismo reforzado de prestación del consentimiento.²⁶ Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado (art. 12.3. RLOPD), consentimiento que es revocable cuando haya una causa justificada y no se le atribuya efectos retroactivos (art. 6.3 LOPD y art. 17 RLOPD).

El término inequívoco planteaba una serie de interrogantes, en concreto las consecuencias que debían atribuirse al silencio.²⁷ La RLOPD regula expresamente esta cuestión en el art. 14 RLOPD si bien sólo resultará aplicable en los casos en que no haga falta un consentimiento expreso para el tratamiento de DCP. Este precepto permite al responsable del tratamiento dirigirse al afectado, cumpliendo los deberes de información previstos en el art. 5 LOPD y 12 RLOPD y concederle un plazo de 30 días a fin de que manifieste su negativa al tratamiento, advirtiéndole de que en caso de no manifestarse al respecto se entenderá que consiente el tratamiento (art. 14.2 RLOPD). Por lo tanto, se establece una regla de silencio positivo, si no se dice nada en un determinado tiempo, se entiende que se consiente.

A fin de que entre en juego esta regla es necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa,

caso en el cual no podrá proceder al tratamiento de los DCP referidos al interesado (art. 14.3 RLOPD). Además deberá facilitarse al interesado un medio sencillo y gratuito que le permita manifestar su negativa al tratamiento de los DCP (art. 14.4 RLOPD).

Una vez que el responsable haya utilizado este procedimiento con el fin de obtener el consentimiento del interesado, no será posible solicitar de nuevo el consentimiento para los mismos tratamientos y para las mismas finalidades hasta pasado un año desde la fecha de la anterior solicitud (art. 14.5 RLOPD).

Este precepto ha generado cierta polémica ya que la regulación proporcionada no se adecua plenamente a la jurisprudencia de la sala 1.^a del TS relativa al valor del silencio.²⁸ Entre la doctrina civilista cabe destacar autores como CAVANILLAS que no es favorable a la solución proporcionada y fundamenta su opinión en lo que él califica de nuevo derecho emergente del consumidor en el s. XXI: el *derecho a no ser molestado*. Este derecho hallaría su fundamento último en el derecho a la intimidad en el sentido que la jurisprudencia del TEDH atribuye a la inviolabilidad domiciliaria en casos de inmisiones (ruidos, olores) y que defendería la tranquilidad del sujeto (no ser importunado).²⁹

GRIMALT está de acuerdo con las observaciones de CAVANILLAS y señala que el art. 14 RLOPD parece que consagra un derecho a molestar. Sin embargo, a pesar de lamentarlo, reconoce que la solución proporcionada -otorgar valor positivo al silencio en los términos expues-

25. El art. 6.1. LOPD anuncia la regla general para el tratamiento de los DCP según la cual es necesario el consentimiento inequívoco del afectado, a no ser que la Ley disponga otra cosa. En el mismo sentido art. 10.1 y 12.1 RLOPD. Según el art. 3h) LOPD, se entiende por consentimiento del interesado: «Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen» [en el mismo sentido, art. 5.1.d) RLOPD].
26. El legislador ha considerado que determinados DCP deben tener un mayor nivel de protección ya que se consideran especialmente sensibles y se establecen unos requisitos más estrictos con el fin de obtener el consentimiento del afectado. Se establece un nivel más intenso de protección: consentimiento expreso y por escrito (art. 7.2 LOPD) y un nivel menos intenso de protección: consentimiento expreso o previsión legal (art. 7.3 LOPD). En determinados casos resultan aplicables excepciones a las exigencias previstas (art. 7.6 LOPD).
27. El silencio se puede considerar como una declaración en todos aquellos casos en que la buena fe impone un deber positivo de manifestar una repulsa. (Para todos, DÍEZ-PICAZO Y PONCE DE LEÓN, pág. 150-151).
28. Véase DÍEZ-PICAZO Y PONCE DE LEÓN, pág. 150-151 y GRIMALT, «El consentimiento y el tratamiento...», pág. 7, nota n.º 15, donde hace referencia a la jurisprudencia del TS al respecto.
29. Véase CAVANILLAS, «Dos derechos emergentes del consumidor...», pág. 211 y 216. Las reflexiones citadas fueron realizadas en el marco del Proyecto de Reglamento y la redacción definitiva suaviza un poco la posibilidad de enviar publicidad de forma ininterrumpida. En concreto la previsión del art. 14.5 fue introducida a raíz de las observaciones del propio CAVANILLAS. (Véase sobre este último aspecto R. MARTÍNEZ, «Principis i aspectes clau del nou Reglament», pág. 20, nota n.º 33).

tos- se puede defender en el marco de la LOPD sobre la base de los antecedentes parlamentarios de la Ley Orgánica que admitieron el consentimiento por falta de oposición expresa del afectado.³⁰

Si sobre la base de las argumentaciones de Grimalt entendemos que la solución proporcionada por el art. 14 RLOPD es admisible en nuestro ordenamiento, un problema que plantea el precepto es que se atribuyen consecuencias diferentes a la inactividad por parte del destinatario de una comunicación.

En caso de envío de una oferta contractual en que se indique que de la falta de respuesta por parte del receptor se deducirá que está interesado en el producto y que además se podrá proceder al tratamiento de los datos personales del receptor de la comunicación, las consecuencias del silencio del destinatario según la legislación de defensa de los consumidores y según el RLOPD son diferentes en uno y otro caso. El legislador está pues enviando dos mensajes diferentes al ciudadano. En un caso le está diciendo que no tiene que preocuparse de hacer nada, puede permanecer en la inactividad y de ella no se deducirá ninguna consecuencia, mientras que en el otro caso le indica que tiene que estar alerta. Este doble mensaje puede generar cierta confusión y si en un caso el ciudadano queda protegido, en el segundo tiene que mantener siempre una actitud vigilante.

3.1.2. El consentimiento para el tratamiento de los datos de los menores

El tratamiento de los DCP de los menores no es un tema que se aborde de forma específica en la LOPD y para dar una respuesta a los interrogantes que se planteaban antes de la entrada en vigor del RLOPD debía acudir al marco normativo general: LO 1/1982, LO 1/1996 de protección jurídica al menor, Código Civil o legislación civil de las respectivas comunidades autónomas según correspondiera.

El RLOPD regula expresamente esta cuestión en el art. 13 RLOPD.

Según este precepto, podrán tratarse los DCP de los menores que sean mayores de 14 años con su consentimiento, excepto aquellos supuestos en que la Ley exija para su otorgamiento la asistencia de los titulares de la patria potestad o tutela. Respecto de los menores de catorce años, hará falta el consentimiento de los padres o tutores (art. 13.1 RLOPD).

El RLOPD quiere impedir y evitar que se utilice al menor para obtener datos de su entorno familiar (actividad profesional, información económica o datos sociológicos de los progenitores) y el art. 13.2 expresamente establece que en ningún caso se podrá recoger este tipo de datos sin el consentimiento de sus titulares.³¹ No obstante, podrán recogerse determinados datos de los titulares de la potestad o tutela (identidad y dirección) con la única finalidad de obtener la autorización prevista en el Reglamento con respecto a los menores de más de 14 años.

Cuándo se traten DCP de menores de edad, la información que se les dirija deberá ser clara y fácilmente comprensible por ellos, con expresa indicación de todo lo que prevé el precepto (art. 13.3 RLOPD).

Finalmente, corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento otorgado, en su caso, por los padres, tutores o representantes legales (art. 13.4 RLOPD). Respecto de este último apartado, lo que hay que acreditar es que se han establecido determinados controles con el fin de limitar y evitar que un menor de la edad establecida pueda acceder a una determinada página y proporcionar datos personales (por ejemplo tests de madurez, adjunción de determinada documentación digitalizada, envío a posteriori de docu-

30. GRIMALT hace este planteamiento sobre la base de las discusiones que tuvieron lugar en el Senado y en concreto basándose en el hecho que el Senado expresamente rechazara las enmiendas que pretendían excluir la posibilidad de que se pudiera considerar otorgado el consentimiento por silencio del afectado. Véase GRIMALT, «El consentimiento y el tratamiento...», pág. 6 y 7 y especialmente nota a pie n.º 15.

31. Desde un punto de vista práctico, la mejor manera de asegurarse el cumplimiento del precepto es no pedir este tipo de datos, ya que si se piden y se obtienen deberá acreditarse que si el menor los ha proporcionado ha sido con el consentimiento del titular de los mencionados datos y no será fácil esta prueba.

mentación acreditativa de la edad). Fijémonos que el precepto hace referencia a *articular procedimientos que garanticen*, no establece *garantizar en cualquier caso*. Por lo tanto no cumpliría con las exigencias legales una página que permitiera el acceso y recogida de datos de un menor sin ningún tipo de control.³²

El art. 13 también ha sido un precepto que ha generado cierta discusión en la medida en que hay quien considera que no corresponde a un Reglamento regular este aspecto y más teniendo en cuenta que se contradice en algunos casos con normas de rango superior como la LO 1/1982 o la LO 1/1996.³³

Sin embargo, si bien son acertadas parte de las críticas que se formulan al art. 13 RLOPD, también es cierto que el problema que se plantea es cómo proteger a los menores que navegan por la red ya que constantemente se está produciendo un flujo de sus datos. Por lo tanto, aunque posiblemente la solución proporcionada no es desde un punto de vista dogmático la más correcta, sí que trata de proteger a los menores de forma un poco más eficaz.³⁴

3.2. La constancia de los DCP en fuentes accesibles al público

El art. 7 RLOPD, siguiendo lo que prevé el art. 3.j) LOPD,³⁵ delimita qué se entiende por fuentes accesibles al público (FAP) introduciendo alguna precisión al respecto. La característica esencial de las FAP es que los datos que

constan pueden tratarse sin que haga falta el consentimiento del afectado.

El art. 7.1.a) RLOPD se limita a mencionar el censo promocional como una FAP sin especificar nada más; a pesar de la previsión expresa del art. 31 LOPD, el mencionado censo no ha sido todavía elaborado.

Si bien el art. 3.j) LOPD hace referencia a los repertorios telefónicos, remitiéndose a lo que establezca la normativa específica, el RLOPD opta por un término más amplio, el de guías de servicios de comunicaciones electrónicas [art. 7.1.b) LOPD]. Actualmente la remisión tiene que entenderse efectuada a la LGT, cuyo art. 22.b) establece la necesidad de poner a disposición de los abonados una guía general de números de abonados y un servicio de información general sobre los números que consten y el art. 38.6 prevé el derecho a no constar en dichas guías. Estos requisitos han sido desarrollados por el RD 424/2005, de 15 de abril,³⁶ que regula el uso que puede hacerse de los datos que constan en los mencionados listados así como la forma de oponerse a constar en ellos.

Para que los listados profesionales tengan la consideración de fuentes accesibles al público deben contener únicamente los datos relativos a nombre, título, profesión, actividad, grado académico, dirección e indicación de la pertenencia en el grupo. Para añadir cualquier dato será preciso el consentimiento del interesado que podrá ser revocado en cualquier momento (art. 28.1 LOPD). El RLOPD recoge los requisitos establecidos por el art. 3.j) LOPD si bien realiza una pequeña

32. Véase R. MARTÍNEZ, que hace referencia a posibles mecanismos de control de la edad del menor cuando accede a una página web y también señala que el responsable que no tiene por objeto tratar datos de menores tendría que fijar estrategias con el fin de impedirles el acceso al entorno virtual. («Principis i aspectes clau del nou Reglament», pág. 18).

33. En este sentido véase GRIMALT, «El consentimiento...», pág. 17 y 18. El autor señala que no considera adecuado regular este aspecto por RD en la medida que estaría sujeto a Ley Orgánica. Además considera que la edad fijada por el legislador sería en todo caso meramente orientadora ya que el ordenamiento utiliza muy a menudo otro criterio, el de *condiciones de madurez*. Según GRIMALT es este último parámetro mencionado el que debería determinar la capacidad del menor para otorgar consentimiento válido para el tratamiento de sus datos, véase «El consentimiento...», pág. 20.

34. En este sentido véase R. MARTÍNEZ, que hace referencia a diferentes informes de la AEPD al respecto y que señala que la edad de los 14 años es meramente orientadora y utilizada en derecho comparado, como por ejemplo en la *Children's Online Privacy Protection Act norteamericana*. («Principis i aspectes clau del nou Reglament», pág. 15 a 19).

35. Según el artículo 3.j) son fuentes accesibles al público: «Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.»

36. BOE n.º 102 de 29 de abril 2005, pág. 14545 y ss.

puntualización al hacer referencia a la dirección *profesional* ya que establece que esta «podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica». Además prevé que en el caso de colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional» [art. 7.1.c) RLOPD].

Por otra parte el interesado podrá solicitar que se haga constar que sus datos no se pueden utilizar para finalidades de prospección comercial o de publicidad y tiene derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional (art. 28.2 LOPD).

El art. 7.1.d) y e) RLOPD hace referencia a que los diarios y boletines oficiales tienen el carácter de FAP sin hacer ningún tipo de acotación. La información que se publica es muy diversa y puede incluir, por ejemplo, datos relativos a determinadas infracciones o nombramientos (que incluyen el DNI de los interesados). Por este motivo por parte de la APDCAT se ha indicado que sería conveniente una cierta cautela a la hora de publicar datos personales en los boletines y diarios oficiales DCP.³⁷

En relación con los medios de comunicación, debe ponerse de relieve que la AEPD considera que internet no es un medio de comunicación, por lo que no tendrá el carácter de FAP. Según la Agencia Española, «podrán considerarse incluidos en fuentes accesibles al público los datos que hayan sido objeto de difusión a través de prensa, radio y televisión (convencional o digital). Las revistas puramente científicas no deberían considerarse fuente accesible al público a efectos de la aplicación de la LOPD. Internet no es, a efectos de protección de datos un *medio de comunicación social*, sino un *canal de comunicación*, por lo que no es una FAP».³⁸

3.3. La existencia de un interés legítimo y el cumplimiento de una obligación legal

El RD 1720/2007 establece que a pesar de la regla general según la cual no podrán tratarse los DCP sin el consentimiento del interesado, en aquellos casos en que lo

autorice una norma con rango de Ley o una norma de derecho comunitario, podrán tratarse los datos si se dan los supuestos siguientes [art. 10.2.a) RLOPD]:

- El tratamiento o la cesión tenga por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por las normas y siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados ex art. 1 LOPD.
- El tratamiento o la cesión de los datos sean necesarios a fin de que el responsable del tratamiento cumpla un deber que le imponga una norma

Este precepto transpone al ordenamiento español el art. 7.f) de la Directiva 95/46 que no había sido transpuesto.

3.4. La obtención a través de un sujeto diferente del interesado

Otra manera de acceder a los DCP es porque un sujeto diferente del interesado los ha comunicado. Dentro de esta excepción hallamos dos supuestos diferentes, aquellos que se consideran cesión de datos y los que no se incluyen dentro de esta categoría.

3.4.1. Accesos que se consideran cesión de datos

La LOPD regula la comunicación o cesión de datos y establece en el art. 11.1 LOPD los requisitos a fin de que la comunicación sea legítima, exigiendo entre otros aspectos el previo consentimiento del interesado (art. 11.1. LOPD y art. 12.2. RLOPD). Por otra parte, según prevé el art. 11.3 LOPD, será nulo el consentimiento para la comunicación de datos cuando la información que se proporciona al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza o bien el tipo de actividad de aquél a quien se pretenden comunicar.³⁹

A pesar del principio del consentimiento, la legislación también prevé una serie de excepciones a la necesidad del consentimiento (art. 11.2 LOPD y art. 10.4 RLOPD), con-

37. Véase, al respecto, la interesante Recomendación 1/2008 de la Agencia Catalana de Protección de Datos sobre la difusión de información que contenga datos de carácter personal a través de Internet y en concreto su capítulo III dedicado a la publicación en diarios oficiales y boletines oficiales electrónicos.

38. Véase «1.ª Sesión abierta de la AEPD...» Respuesta a la pregunta 8, pág. 10 de las FAQ.

sentimiento que también es revocable (art. 6.3 LOPD y art. 17 RLOPD).

La comunicación de datos entre administraciones públicas se encuentra regulada en el artículo 21 LOPD, precepto que fue declarado parcialmente inconstitucional. La cesión de datos en caso de ficheros de titularidad privada se regula en el artículo 27 LOPD. Un supuesto concreto que tiene un marco específico es el caso de cesión de datos relativos a información sobre solvencia patrimonial y crédito (art. 29 LOPD) y que analizaremos más adelante.

Como dispone el art. 19 RLOPD, cuando se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, u otras operaciones de reestructuración societaria de naturaleza análoga contemplada por la legislación mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento de lo que establece el art. 5 LOPD.

Finalmente hay que recordar que el derecho de información que garantiza la LOPD prevé, entre otros aspectos, el derecho a solicitar y obtener información gratuita sobre las comunicaciones de datos realizadas o que se pretendan llevar a cabo (art. 15.1 LOPD).

3.4.2. Accesos que no se consideran cesión de datos

Según el artículo 12.1 LOPD no se considera comunicación de datos el acceso de un tercero a los datos cuando el mencionado acceso sea necesario para la prestación de un servicio al responsable del tratamiento. (La consecuencia es que en este caso se excluirá el requisito del consentimiento previo del interesado que de lo contrario sería preciso ex art. 11.1 LOPD).⁴⁰

Cuando un tercero tenga que intervenir en el tratamiento de los datos, según la previsión del artículo 12.2 LOPD, deberá formalizarse un contrato entre el responsable del tratamiento y el tercero. Este contrato tendrá que constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido. En este contrato tendrá que constar entre otros aspectos: el tratamiento de los datos conforme a las instrucciones del responsable del tratamiento, la no aplicación de los datos a finalidades diferentes de la prevista en el contrato o bien la no comunicación, ni siquiera para su conservación, a otras personas. Se establecerán asimismo las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

4. Tratamientos específicos: ficheros sobre solvencia patrimonial y crédito

4.1. Los ficheros de solvencia patrimonial y crédito

El artículo 29 LOPD regula los ficheros que contienen datos relativos a solvencia patrimonial y crédito, aspecto al que la AEPD dedicó la Instrucción 1/1995, de 1 de marzo y que se regula con detalle en los arts. 37 a 44, capítulo I, título IV del RLOPD. La existencia de estos ficheros constituye una excepción al consentimiento del afectado motivada por razones de interés público concretadas en la protección del tráfico económico.⁴¹

El art. 29 LOPD contempla dos supuestos diferentes. El primero es aquél en que la información sobre solvencia patrimonial y crédito objeto de tratamiento se ha obtenido de un registro o de una FAP establecida al efecto o bien ha sido facilitada por el propio interesado o con su

39. En el mismo sentido se pronuncia el art. 12.2 del RD 1720/2007 que ha enfatizado todavía más la necesidad de que quede clara la finalidad a la que se destinarán los datos objeto de la cesión.

40. A menudo no es fácil distinguir entre cesión y acceso sobre la base de la previsión del art. 12 LOPD. Al respecto E. CHAVELI DONNET, señala que el elemento clave a fin de que resulte aplicable el art. 12 LOPD es el hecho de prestar un servicio al responsable del tratamiento. («El Estatuto del Encargado del Tratamiento...», pág. 4).

41. Sobre la existencia y regulación de estos ficheros, véase PALOMAR que advierte del peligro de que en la sociedad informatizada los deudores se conviertan en unos «muertos civiles», si bien el autor considera que la regulación proporcionada por el RLOPD es más garantista y equilibrada y facilita el ejercicio de los derechos. («Un apunte sobre los ficheros de solvencia», pág. 17-18).

consentimiento (art. 29.1 LOPD). En este caso, con respecto al ejercicio de los derechos del afectado hay que tener en cuenta el art. 37.2 RLOPD.

El segundo supuesto es aquél en que la información relativa al cumplimiento o incumplimiento de obligaciones dinerarias la ha facilitado el acreedor (art. 29.2. LOPD). Dada la existencia de una determinada obligación dineraria que no se ha satisfecho, el acreedor, sobre la base de la excepción prevista, comunica el dato del no pago a otra persona que realiza un tratamiento sobre insolvencia patrimonial. En este fichero se añaden otros datos suministrados por muchos otros acreedores. La información contenida en estos tipos de ficheros es consultada por terceros que actúan en el tráfico jurídico y para quienes es relevante conocer la solvencia de las personas con quienes quieren contratar.

A fin de que se puedan comunicar datos a estos tipos de ficheros hace falta que se den una serie de requisitos:

- i. Existencia previa de una deuda cierta, vencida y exigible que haya sido impagada y respecto de la que no se haya interpuesto una reclamación [art. 38.1.a) RLOPD].
- ii. Que no haya transcurrido 6 años desde la fecha en que tenía que pagarse la deuda o del vencimiento de la obligación o el plazo concreto [art. 38.1.b) RLOPD].
- iii. Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación [art. 38.1.c) RLOPD].
- iv. No podrán incluirse en los ficheros de esta naturaleza datos personales respecto de los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores.
- v. Proporcionar al deudor determinada información previa a la inclusión en los mencionados ficheros (art. 39 RLOPD).
- vi. La información destinada a los ficheros de solvencia patrimonial y crédito debe facilitarla el propio acreedor o bien quien actúe por su cuenta e interés.

vii. Debe notificarse al interesado (el deudor) en el plazo de 30 días desde la inclusión en el registro, una referencia de los datos relativos a su persona (deudor) que se hayan incluido y del derecho a pedir información (art. 29.2 LOPD).

viii. Cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos así como las evaluaciones y apreciaciones que hayan sido comunicadas a terceros (art. 29.3 LOPD y art. 44.2.1.ª RLOPD).

El art. 44 RLOPD regula el ejercicio de los derechos del afectado en estos tratamientos y distingue en función de frente a qué persona se ejerciten: frente quien ha facilitado los datos (cedente), el responsable del fichero común, el cesionario de la información o bien cualquier otra entidad participando en el sistema.

4.2. Los ficheros de publicidad y prospección comercial

El tratamiento de datos con finalidad de publicidad y prospección comercial se regula en el art. 30 LOPD y en los arts. 45 a 51 RLOPD. Los DCP únicamente podrán tratarse para las finalidades de marketing, publicidad, venta a distancia, prospección comercial u otras actividades análogas en determinados supuestos. En primer lugar si los datos han sido facilitados por el propio interesado o bien obtenidos con su consentimiento [art. 30. 1 LOPD y art. 45.1.b) RLOPD]. En segundo lugar si los DCP figuran en FAP y no consta la oposición o negativa del interesado a recibir comunicaciones comerciales [art. 6.2. y 30.1 LOPD y art. 45.1.a) RLOPD].⁴²

En el tratamiento de DCP para las finalidades que ahora analizamos a menudo participan todo un entramado de personas. Con el fin de identificar cada sujeto y su responsabilidad, el RLOPD tiene en cuenta cómo se organiza la campaña publicitaria y establece que será responsable del tratamiento aquél que efectivamente realice la *selección de destinatarios* (determinación de los parámetros identificativos), según prevé el art. 46 RLOPD.⁴³

42. Hay que tener en cuenta el deber de información que establece el art. 30.2 LOPD y el art. 45.2 RLOPD cuando se realicen comunicaciones comerciales y los datos se hayan obtenido de FAP.

Una importante novedad del RLOPD es que se regulan las llamadas *listas Robinson*, es decir la posibilidad de crear ficheros comunes de carácter general o sectorial cuyo objetivo es el tratamiento de DCP que sean necesarios para evitar el envío de comunicaciones comerciales a personas que han manifestado su negativa o bien oposición a recibir publicidad. A tales efectos los mencionados ficheros podrán tener los DCP imprescindibles para identificar al afectado (art. 49 RLOPD).

Los arts. 50 y 51 RLOPD regulan el ejercicio de los derechos, haciendo especial referencia a los supuestos en que en las campañas de marketing intervienen diferentes sujetos, uno encargando una campaña y otro delimitando los parámetros.

El art. 30 LOPD y los correspondientes del RLOPD hacen referencia a las fuentes de donde se obtienen los datos. Pero para realizar una actividad publicitaria y efectuar envíos comerciales en algunas ocasiones no es suficiente con estar en posesión de los datos (aunque sea de forma legal). Hay que poner en relación la normativa sobre protección de datos con la LSSI ya que esta última regula las comunicaciones comerciales por vía electrónica (art. 19-22 LSSI).

El artículo 21.1 LSSI⁴⁴ establece de entrada la regla del *opt-in* de modo que el envío de publicidad por correo electrónico o cualquier otro medio de comunicación electrónica equivalente está condicionado al consentimiento del destinatario -éste tiene que solicitarlo previamente o autorizarlo expresamente-, tal como establece el art. 13.1 Directiva 2002/58. A continuación el art. 21.2 LSSI recoge la excepción prevista en el artículo 13.2 Directiva 2002/58 de manera que se podrá enviar publicidad en aquellos casos en que haya una relación contractual previa, si el remitente ha obtenido los datos de forma lícita y se utilizan para enviar publicidad relativa a productos/servicios similares a los contratados inicialmente. Asi-

mismo debe ofrecerse al destinatario la posibilidad de oponerse al tratamiento en el momento de la recogida de los datos y en cualquier comunicación ulterior con el destinatario. El consentimiento podrá revocarse en cualquier momento (art. 22.1 LSSI).

En definitiva, para las comunicaciones publicitarias o promocionales por vía electrónica, a pesar de estar en posesión de una serie de datos, con el fin de poder llevar a cabo una campaña de marketing deberá tenerse en cuenta las previsiones de la LSSI para determinar si efectivamente pueden enviarse comunicaciones comerciales.

Si se trata de comunicaciones no electrónicas, no resulta aplicable la LSSI y la normativa de referencia será la LOPD y la relativa a publicidad.

5. El tratamiento de los datos, especial referencia a las medidas de seguridad

Si el responsable del tratamiento es la persona que decide sobre la finalidad, contenido y uso del tratamiento [art. 3.d) LOPD], el encargado del tratamiento es quien trata datos personales por cuenta del responsable del tratamiento [art. 3.g) LOPD]. A fin de que un tercero pueda intervenir en el tratamiento de datos para dar un servicio al responsable, hace falta que entre el responsable y el sujeto que se califica de encargado se celebre un contrato en los términos previstos por el art. 12 LOPD.^{45 46}

En este contrato, formalizado por escrito o en alguna otra forma que permita acreditar su celebración y contenido, tendrán que constar entre otros aspectos las instrucciones del responsable para el tratamiento de los datos, la prohibición de aplicar los datos a finalidades diferentes de las pre-

43. A menudo sucede que la persona que encarga una determinada campaña y quien realiza efectivamente la selección de destinatarios -determinación de los parámetros identificativos- no coinciden.

44. La disposición final primera de la LGT modificó los artículos 21, 22, 38.3 b), 38.4 de) y 43.1 redacción original de la LSSI con el fin de adaptarlos a la Directiva 2002/58.

45. Véase el art. 5.1.i) RLOPD que recogiendo la definición de encargado que proporciona la LOPD añade que la actuación del encargado es consecuencia de la existencia de una relación jurídica entre responsable y encargado que delimita el ámbito de actuación.

46. El acceso por un tercero a los datos sin que se haya celebrado el contrato previsto en la LOPD y que no constituya una cesión de datos legalmente admitida podría constituir una infracción muy grave de la LOPD [art. 44.4.b) LOPD].

vistas, la prohibición de comunicación y las medidas de seguridad que el encargado tenga que implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal tendrán que destruirse o devolverse al responsable del tratamiento (art. 12.3 LOPD). En el caso de incumplimiento por parte del encargado del tratamiento, éste se considerará responsable del tratamiento, respondiendo de las infracciones en que haya incurrido personalmente (12.4 LOPD).

El RLOPD regula lo que se ha calificado como *el estatuto del encargado del tratamiento*,⁴⁷ contenido en el art. 20 a 22 del capítulo III, título II del RLOPD. Respecto a la relación entre el responsable y el encargado, el primero tiene que velar a fin de que la persona que ha contratado como encargado reúna garantías suficientes de que cumplirá las obligaciones establecidas por la Ley (art. 20.2 RLOPD). Un aspecto novedoso es que se permite la subcontratación de los servicios por parte del encargado del tratamiento (art. 21 RLOPD).

De entrada el art. 21.1 RLOPD establece que el encargado sólo puede subcontratar a un tercero si se ha obtenido autorización del responsable para hacerlo, caso en el que la contratación se efectuará en nombre y por cuenta del responsable del tratamiento.⁴⁸ Sin embargo el art. 22.2 RLOPD también prevé que sea posible la subcontratación sin necesidad de autorización del responsable del tratamiento si se cumplen los requisitos previstos en el propio precepto. Finalmente el RLOPD también trata de la conservación de los datos por parte del encargado y el supuesto de intervención sucesiva de encargados y la transmisión de datos del primero al sustituto (art. 20.3 y 22 RLOPD).

Un aspecto primordial en el tratamiento de los datos es el deber impuesto al responsable del fichero y al encargado de garantizar la seguridad de los datos tratados y evitar

su alteración, pérdida, tratamiento o acceso no autorizado (art. 9 LOPD). Este deber comporta la necesidad de adoptar medidas de seguridad adecuadas que no se dejan totalmente al libre criterio del responsable sino que se fijan por el legislador en relación a unos parámetros concretos: el estado de la tecnología, el tipo de tratamiento a realizar y los riesgos a que estén expuestos los datos. El RLOPD⁴⁹ constituye el instrumento normativo básico en materia de seguridad de ficheros y representa y comporta entre otras obligaciones la necesidad de plasmar la política de seguridad definida en la organización en un documento de seguridad. El RLOPD resulta aplicable tanto a los tratamientos automatizados como a los no automatizados.⁵⁰

El Reglamento establece tres niveles de seguridad: básico, medio y alto y el art. 81 RLOPD determina cuándo corresponde aplicar cada uno de ellos. El nivel básico es exigible para todos los ficheros o tratamientos de datos y el nivel superior incluye todas las medidas del nivel inferior. Estos niveles tienen la condición de mínimo exigible, por lo tanto, no hay ningún obstáculo en optar por un nivel de seguridad superior (art. 81.7 RLOPD).

En relación con los niveles de seguridad, y respecto de la regulación anterior, algunos ficheros cambian de nivel, como por ejemplo los ficheros propios de la seguridad social y de mutuas de accidentes que se incorporan al nivel medio (art. 81.2 RLOPD).

En el caso de las operadoras de servicios de comunicaciones electrónicas y con respecto a los tratamientos de los datos de tráfico y de localización, se establece un nivel de protección medio con el añadido que deberá cumplirse con el deber de seguridad de nivel alto establecido en el art. 103 RLOPD (contar con registros de acceso). A los ficheros que contengan datos relativos a la violencia de género les resultarán aplicables las medidas de nivel alto [art. 81.3.c) RLOPD].

47. Véase el apartado III de la exposición de motivos del RD 1720/2007.

48. Respecto de la posibilidad de la subcontratación, véase CHAVELI, «El Estatuto del Encargado del Tratamiento...», pág. 5-7.

49. El RLOPD deroga el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. (Disposición derogatoria única RLOPD).

50. Sobre la aplicación del RLOPD a los tratamientos que ya existían a la entrada en vigor del mismo, véase R. MIRALLES LÓPEZ, «Mesures de seguretat: adequació dels tractaments preexistents al nou Reglament». El autor hace referencia a los ejes básicos que hay que tener en cuenta con el fin de adaptarse a la normativa: I. hace falta una revisión de los *niveles de seguridad*, II. una revisión de las *medidas de seguridad*, III. hace falta una revisión del *documento de seguridad*.

No debe identificarse datos sensibles con nivel más elevado de protección; el legislador parte de otros criterios con el fin de definir la protección que considera relevante como son la finalidad del tratamiento, la obligatoriedad de realizarlo y el contenido informativo objetivo.⁵¹ Sobre la base de estos criterios, será suficiente el nivel básico respecto determinados tratamientos de datos relativos a la ideología⁵² y determinados tratamientos de datos de salud.⁵³

La política de seguridad de un sistema de información tiene que quedar reflejada en el documento de seguridad, cuyo contenido se regula en el art. 88 RLOPD y tiene que mantenerse siempre actualizado. Este precepto regula el contenido mínimo del documento de seguridad y tendrá que registrar toda la información relevante respecto a cómo se efectúa el tratamiento de los datos. El RLOPD permite el nombramiento de más de un responsable de seguridad e incluso delegar la redacción del documento de seguridad a un encargado.⁵⁴

Con respecto a las medidas de seguridad concretas que integran cada nivel, el RLOPD distingue entre los tratamientos automatizados (arts. 89-104) y los no automatizados (art. 105-114). Con el fin de determinar en qué caso es exigible cada nivel de seguridad también debe tenerse en cuenta las disposiciones transitorias del Reglamento. La DT 2 RLOPD prevé los plazos de implantación de las medidas de seguridad relativas a los tratamientos que ya existían cuando entró en vigor el mencionado Reglamento (distinguiendo de nuevo entre tratamientos automatizados y no automatizados). Respecto de los ficheros creados con posterioridad a la entrada en vigor del RD 1720/2007 (tanto automatizados como no automatizados), deberá implementarse la totalidad de las medidas de seguridad pre-

vistas en el RLOPD a partir del momento de su creación (DT 2.3.a).⁵⁵

Finalmente debe ponerse de relieve la DA única del RLOPD según la cual los productos de software destinados al tratamiento automatizado de datos personales tendrán que incluir en su descripción técnica el nivel de seguridad (básico, medio o alto) que permitan alcanzar de acuerdo con lo que establece el propio RLOPD.

Además del cumplimiento de las medidas de seguridad, el responsable del fichero y todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los datos que traten. Estas obligaciones subsistirán incluso después de finalizada la relación con el titular o responsable del fichero (art. 10 LOPD).⁵⁶

6. El ejercicio de los derechos ARCO

El título III LOPD se dedica a los derechos de las personas, que se concretan en los derechos de acceso, rectificación, cancelación y oposición (identificados con las siglas ARCO) que, según palabras del Tribunal Constitucional en la sentencia 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

El artículo 17 LOPD realiza una remisión reglamentaria al establecimiento de un procedimiento para ejercitar los dere-

51. MARTÍNEZ hace referencia a una nueva percepción del regulador, «Principis i aspectes clau del nou Reglament», pág. 32.

52. En concreto cuando el tratamiento tenga por finalidad realizar una transferencia dineraria a las entidades a las que los afectados estén asociados o bien en caso de tratamientos no automatizados si los datos han sido recogidos de forma incidental (art. 81.5 RLOPD).

53. 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 el fin de cumplir con determinados deberes públicos (art. 81.6 RLOPD).

54. Respecto de la figura del encargado del tratamiento y las medidas de seguridad: CHAVELI, «El Estatuto del Encargado del Tratamiento...», pág. 13-15.

55. Según lo que prevé el art. 44.3.h) LOPD el incumplimiento de las medidas de seguridad puede constituir una infracción grave.

56. El incumplimiento del deber de secreto puede constituir una infracción leve, grave o muy grave en función de los datos afectados, art. 44.2.e); 44.3.g) y 44.4.g) LOPD.

chos de oposición, acceso, rectificación y cancelación. Este precepto subraya por otra parte que el ejercicio de estos derechos será gratuito. Una vez derogado el RD 1332/1994 por el RD 1720/2007, el procedimiento a seguir es el regulado por el título III y título IX, capítulo II RLOPD.

Los derechos ARCO tienen la naturaleza de personalísimos y se configuran como independientes, de modo que no puede entenderse que el ejercicio de alguno de ellos sea requisito para ejercitar el otro (art. 24 RLOPD). En el ejercicio de estos derechos respecto de los ficheros de las fuerzas y cuerpos de seguridad, se establecen una serie de restricciones previstas en el art. 23 LOPD. Este precepto prevé que el afectado a quien se deniegue total o parcialmente el ejercicio de sus derechos podrá ponerlo en conocimiento de la AEPD o del organismo correspondiente de la CA según corresponda y las autoridades de control tendrán que asegurarse de la procedencia o improcedencia de la denegación.

Cuando se trate de datos de carácter personal registrados en ficheros de titularidad privada, únicamente se denegará el acceso cuando la solicitud se formule por una persona diferente de la afectada (art. 23.3 RLOPD).

6.1. Disposiciones generales

El Título III del RD 1720/2007 establece de entrada unas previsiones de carácter general, aplicables al ejercicio de cualquier derecho (y predicables tanto respecto de los ficheros públicos como respecto de los privados).

A pesar del carácter personalísimo de estos derechos (art. 23.1. RLOPD), en determinados casos podrán ser ejercitados por el representante legal o voluntario expresamente designado (art. 23.2 RLOPD).⁵⁷ Deberá establecerse un medio sencillo y gratuito para el ejercicio de los derechos ARCO que en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento (art. 24.2 y 3 RLOPD).

El responsable del fichero o tratamiento tendrá que atender la solicitud de ejercicio de los derechos aunque el procedimiento utilizado no sea aquél establecido específicamente, siempre que el interesado haya utilizado un medio que permita acreditar el envío y recepción de la solicitud y que contenga todos los elementos exigidos por el RLOPD (art. 24.5 RLOPD).

El art. 25 RLOPD establece el contenido de la solicitud y la documentación a adjuntar y la obligación del responsable del tratamiento de contestar aunque no trate datos relativos al interesado. En caso de que los afectados ejerzan sus derechos delante del encargado del tratamiento en vez de hacerlo delante del responsable, el primero tiene que trasladar la solicitud al responsable a fin de que la resuelva excepto que se hubiera previsto en la relación responsable-encargado que este último contestaría las solicitudes de ejercicio de derechos por cuenta del responsable (art. 26 RLOPD).

6.2. Consulta y acceso a los datos

El derecho de consulta permite a cualquier persona conocer de forma gratuita, pidiendo la información al Registro General de Protección de Datos, la existencia de un tratamiento de DCP determinado, las finalidades y la identidad del responsable (art. 14 LOPD). El ejercicio del derecho de acceso permite al interesado obtener información sobre si los datos que hacen referencia a su persona están siendo objeto de tratamiento, la finalidad del tratamiento, la información disponible sobre el origen de los mencionados datos y las comunicaciones realizadas o previstas realizar (art. 15 LOPD y 27.1 RLOPD).

Desarrollando lo que establece el art. 15.2 LOPD, el art. 28 y 29 RLOPD especifican cómo se materializa el derecho de acceso y se establece como puede recibir el afectado la información que tiene que ser en todo caso legible e inteligible. Los sistemas de consulta del fichero se modularán en función de la configuración o implantación mate-

57. Es interesante la reflexión que hace C. SAN JOSÉ AMAT en el sentido de que el art. 23.2.b) RLOPD no ha incluido, al menos de forma clara, la posibilidad de que actúe el menor por sí mismo, tal como en cambio se ha hecho respecto del consentimiento en el art. 13 RLOPD cuando se permite que los menores consientan el tratamiento de sus datos, por lo que señala que se permitiría la autodeterminación informativa con respecto al consentimiento del tratamiento pero en cambio no respecto del ejercicio de los derechos ARCO. Quizás lo más lógico sería, siguiendo este comentario, que si pueden consentir también pudieran ejercer los derechos sin necesidad de representante. (Véase «Les garanties del ciutadà: tutela de drets ARCO i règim sancionador», pág. 3).

rial del fichero y de la naturaleza del tratamiento. El responsable del fichero tiene que resolver en el plazo máximo de un mes. El derecho de acceso únicamente podrá ejercitarse a intervalos no inferiores de doce meses si bien si se acredita un interés legítimo se podrá hacer antes (art. 15.3 LOPD y art. 30.1 RLOPD).

6.3. Rectificación, cancelación y oposición

Como consecuencia del principio de calidad de los datos (art. 4 LOPD), el art. 16 LOPD regula el derecho de rectificación y cancelación según el cual se rectificarán o cancelarán los datos de carácter personal cuyo tratamiento no se ajuste a lo que dispone la normativa y cuando los datos resulten inexactos o incompletos (art. 16.2. LOPD y art. 31.1. RLOPD).

Sin embargo la cancelación no comporta borrar los datos, sino que se mantendrán bloqueados conservándolos a disposición de las administraciones públicas y de los tribunales a efectos de determinar posibles responsabilidades (art. 16.3 LOPD y 31.2 RLOPD). El art. 32.1 RLOPD especifica el contenido de la solicitud de rectificación y la documentación a adjuntar. Tal como prevé el art. 16.1 LOPD, el responsable del tratamiento tendrá que hacer efectivo el derecho de rectificación o cancelación en el plazo de diez días.

Si los datos rectificadas o cancelados han sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario a fin de que éste proceda también a rectificarlos o cancelarlos (art. 16.4 LOPD y art. 32.3. RLOPD). Sin embargo, en determinados casos la cancelación no procederá (art. 16.5 LOPD y art. 33 RLOPD).

6.4. El derecho de oposición

Mediante el ejercicio del derecho de oposición⁵⁸ el afectado puede solicitar que no se realice o que se cese en el tratamiento de datos relativos a su persona (art. 34 RLOPD). Este derecho podrá ejercerse en los siguientes supuestos:

En caso de que no sea necesario el consentimiento del afectado para el tratamiento de los datos y la Ley no establezca lo contrario, según prevé el art. 6.4 LOPD, el afectado podrá oponerse al tratamiento si existen motivos fundamentados y legítimos relativos a una concreta situación personal [cfr. también art. 34a) RLOPD] que tendrá que hacerse constar al ejercer el derecho (art. 35.1 RLOPD). Esta justificación no será precisa en los supuestos de ficheros de publicidad y prospección comercial [art. 30.4 LOPD, 34b) y 51 RLOPD].

Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de los datos relativos al interesado [art. 13 LOPD y art. 34c) RLOPD]. No obstante, el art. 36.2 RLOPD permite que los afectados se vean sometidos a las decisiones mencionadas si esta posibilidad se ha establecido contractualmente a petición del interesado o bien está autorizada por una norma con rango de Ley.

Cuando se ejercite el derecho de oposición, el responsable del tratamiento deberá resolver en el plazo de diez días a contar desde la recepción de la solicitud bien excluyendo del tratamiento los datos relativos al afectado bien denegando motivadamente la solicitud presentada (art. 35.3 RLOPD).

6.5. Resultado infructuoso del ejercicio de los derechos

En aquellos casos en que el ejercicio de los derechos hasta ahora mencionados haya dado un resultado infructuoso por la oposición y reticencias del responsable del fichero o del encargado del tratamiento (denegación total o parcial) y tal como establece el art. 18.2 LOPD, el interesado podrá ponerlo en conocimiento de la AEPD o, en su caso, del organismo competente de cada CA, que tendrá que asegurarse de la procedencia o improcedencia de la denegación.⁵⁹

En estos casos la LOPD prevé un procedimiento de tutela (la AEPD deberá dictar resolución expresa en el plazo de

58. Se encuentra regulado en los arts. 34 a 36 RLOPD.

59. En este sentido, y respecto del ejercicio de cada derecho, véase art. 29.1 RLOPD -derecho de acceso-; art. 32.2 RLOPD -derechos de rectificación y cancelación- y art. 35.2 RLOPD -derecho de oposición.

6 meses ex art. 18.3 RLOPD) y se remite al desarrollo reglamentario. Se trata de los arts. 117 a 119 RLOPD ubicados en el capítulo II (procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición), del título IX (Procedimientos tramitados por la AEPD).

Contra la resolución definitiva de la AEPD procede recurso Contencioso-Administrativo (art. 18.4 LOPD), en concreto se puede recurrir en única instancia delante de la Sala Contenciosa Administrativa de la Audiencia Nacional (DA 4.ª, 5 LRJCA).

Conclusiones

Hemos realizado un recorrido por las principales novedades que presenta el RLOPD, tomando como hilo conductor el texto de la Ley orgánica. A menudo la normativa sobre protección de datos se ve como una losa, como una carrera de obstáculos que hay que salvar con el fin de evitar la imposición de sanciones. Incluso es utilizada en alguna ocasión de forma abusiva para causar un daño a otro. En ocasiones puede suceder que con el fin de perjudicar la competencia, como venganza frente a un antiguo empleador o ante la impotencia experimentada frente a un incumplimiento contractual, -y como consecuencia de la insuficiencia o lentitud de otros mecanismos- se recurra a la normativa de protección de datos para denunciar a los supuestos infractores, aunque el motivo no sea la preocupación por la privacidad sino causar un perjuicio al infractor.⁶⁰

Esta aproximación, pese a ser comprensible, no deja de estar desenfocada. No debe perderse de vista que el tra-

tamiento de los DCP va estrechamente ligado a la gestión de la información de una empresa, entidad u organización y es preciso realizar un enfoque global de la gestión de uno de los principales activos de toda organización (la información). Por lo tanto, hay que planificar la gestión de la información teniendo en cuenta la normativa sobre protección de datos. Esta planificación afecta tanto a la esfera interna como a la externa. Hace falta una política adecuada de gestión de la información que tenga en cuenta los diferentes momentos de la vida de una organización, desde que se establece la estructura de los sistemas de información, durante el funcionamiento diario, en el momento de la recogida de información o bien cuando es necesario encargar la creación de programas o aplicaciones informáticas.

En defecto de una planificación con perspectiva de todos los flujos informativos y de los datos que se generan constantemente, el tratamiento de los DCP acaba constituyendo realmente un problema y el afán es exclusivamente el de poner remiendos en las estructuras ya existentes con el fin de adecuarse, al menos superficialmente, a la normativa.

La clave es pues generar una nueva cultura del tratamiento de la información y de los datos personales. Este cambio en el enfoque beneficia la propia organización y también a los implicados en el tratamiento ya que permite racionalizar procesos y ordenar estructuras. La entrada en vigor del RD 1720/2007 puede representar una oportunidad de repensar la estructura de la información en cualquier empresa u organización.

Bibliografía

AEPD (2008). «El nuevo Reglamento de desarrollo de la Ley Orgánica de protección de datos: problemática, interpretación y aplicación». En: *1.ª Sesión abierta de la AEPD*. (2008: Madrid) [en línea]. <https://www.agpd.es/portalweb/jornadas/1_sesion_abierta/index-ides-idphp.php>

CAVANILLAS MÚGICA, Santiago (2007). «Dos derechos emergentes del consumidor». En: *Liber Amicorum Guido Alpa. Private Law Beyond the National Systems*. Londres: British Institute of International and Comparative Law. Pág. 206-214.

60. Así lo pone de relieve R. MARTÍNEZ MARTÍNEZ, «El Reglamento de desarrollo de la Ley Orgánica ... », pág.71.

- CHAVELI DONET, Eduard (2008). «El Estatuto del Encargado del Tratamiento en el nuevo reglamento de desarrollo de la LOPD». En: *Jornada sobre el Nou Reglament de Desenvolupament de la LOPD*. Ponencia. Barcelona, 3 de abril de 2008 (pendiente de publicación).
- DÍEZ-PICAZO GIMÉNEZ, Luis María (2005). *Sistema de Derechos Fundamentales*. Madrid: Civitas. 2.ª ed.
- DÍEZ-PICAZO Y PONCE DE LEÓN, Luis (1993). *Fundamentos del Derecho civil patrimonial. I Introducción. Teoría del contrato*. Madrid: Civitas. 4.ª ed. y 6.ª ed., 2007.
- FARRÉ TOUS, Santiago (2003). «Novetats del RLOPD per a les Administracions Públiques». En: *Jornada sobre el Nou Reglament de Desenvolupament de la LOPD*. Ponencia. Barcelona, 3 de abril de 2008 (pendiente de publicación).
- GRIMALT SERVERA, Pere (2008). «El consentimiento y el tratamiento con fines publicitarios y prospección comercial». En: *Jornada sobre el Nou Reglament de Desenvolupament de la LOPD*. Ponencia. Barcelona, 3 de abril de 2008 (pendiente de publicación).
- MARTÍNEZ MARTÍNEZ, Ricard (2007). «El Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Consideraciones generales». *Revista Española de Protección de Datos*. N.º 2, pág. 63-94.
- MARTÍNEZ MARTÍNEZ, Ricard (2008). «Principis i aspectes clau del nou reglament». En: *Jornada sobre el Nou Reglament de Desenvolupament de la LOPD*. Ponencia. Barcelona, 3 de abril de 2008 (pendiente de publicación).
- MIRALLES I LÓPEZ, Ramon (2008). «Mesures de seguretat: adequació dels tractaments preexistents al nou reglament». En: *Jornada sobre el Nou Reglament de Desenvolupament de la LOPD*. Ponencia. Barcelona, 3 de abril de 2008 (pendiente de publicación).
- PALOMAR OLMEDA, Alberto (2008). «Un apunte sobre los ficheros de solvencia». En: *Jornada sobre el Nou Reglament de Desenvolupament de la LOPD*. Ponencia. Barcelona, 3 de abril de 2008 (pendiente de publicación).
- SAN JOSÉ AMAT, Carles (2008). «Les garanties del ciutadà: tutela de drets ARCO i règim sancionador». En: *Jornada sobre el Nou Reglament de Desenvolupament de la LOPD*. Ponencia. Barcelona, 3 de abril de 2008 (pendiente de publicación).

Cita recomendada

VILASAU, Mònica (2008). «El fin de la situación de transitoriedad: la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ya tiene desarrollo reglamentario» [artículo en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 7. UOC. [Fecha de consulta: dd/mm/aa].

<http://www.uoc.edu/idp/7/dt/esp/vilasau_1.pdf>

ISSN 1699-8154



Esta obra está bajo la licencia Reconocimiento-NoComercial-SinObraDerivada 2.5 España de Creative Commons. Así pues, se permite la copia, distribución y comunicación pública siempre y cuando se cite el autor de esta obra y la fuente (*IDP. Revista de Internet, Derecho y Política*) y el uso concreto no tenga finalidad comercial. No se pueden hacer usos comerciales ni obras derivadas. La licencia completa se puede consultar en: <<http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.es>>

Sobre la autora

Mònica Vilasau Solana

mvilasau@uoc.edu

Profesora de Derecho Civil en la UOC. Ha publicado diversos trabajos sobre la responsabilidad en la construcción. En la actualidad su línea de investigación es la protección del derecho a la intimidad en relación con el uso de las tecnologías de la información y comunicación. Participa en el proyecto I+D, del Ministerio de Ciencia y Tecnología, «Las transformaciones del derecho en la sociedad de la información y el conocimiento» y es miembro del Grupo de Investigación INTERDRET reconocido por el IN3.