EL REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE, POR EL QUE SE APRUEBA EL REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. ASPECTOS CLAVE[1]

Ricard Martínez Martínez

Coordinador del Área de estudios de la Agencia Española de Protección de Datos
Profesor de Derecho Constitucional de la UOC

En este artículo el autor examina los elementos a su juicio más relevantes del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. El Reglamento es una norma particularmente compleja que se erige en la práctica en un completo código de la protección de datos. En este trabajo se destacan aquellos elementos que, por su proyección, su dificultad o su trascendencia práctica destacan en la nueva regulación.

1. Este artículo se corresponde parcialmente con la conferencia impartida el 3 de abril de 2008 en la «Jornada sobre el Nou Reglament de Protecció de Dades: Anàlisi de les Principals Novetats», organizada por la Agència Catalana de Protección de Datos y los Estudios de Derecho de la Universitat Oberta de Catalunya y que ha dado lugar a un trabajo sobre la materia que verá la luz en un futuro número de la Revista de Internet Derecho y Política. Disponible en <http://www.uoc.edu/idp/6/esp/numeros.html>.

SUMARIO

1. CONSIDERACIÓN PRELIMINAR.
2. DIFICULTADES PREVIAS: UNA REALIDAD MATERIAL Y NORMATIVA COMPLEJA.
3. ELEMENTOS CLAVE DE LA REGULACIÓN.
   - 3.1. La exclusión de empresarios individuales y personas de contacto.
   - 3.2. El principio de calidad de los datos.
   - 3.3. El consentimiento.
     - 3.3.1. Los datos de los menores.
     - 3.3.2. El consentimiento tácito.
     - 3.3.3. El consentimiento para finalidad diferente.
     - 3.3.4. La revocación del consentimiento.
   - 3.4. El deber de información en la recogida de datos.
   - 3.5. El ejercicio de los derechos.
   - 3.6. El Estatuto del encargado del tratamiento.
   - 3.7. Ficheros específicos.
     - 3.7.1. Solvencia.
     - 3.7.2. Publicidad.
   - 3.8. Medidas de seguridad.
4. BREVE CONCLUSIÓN.

1. CONSIDERACIÓN PRELIMINAR

El texto de este artículo constituye expresión de un conjunto de conferencias y sesiones de trabajo desarrollados durante el periodo 2006-2008. Durante esta etapa tuve la oportunidad única de compartir tareas con un colectivo amplio de personas, tanto en el Ministerio de Justicia como en la Agencia Española de Protección de Datos. Todas ellas se implicaron con intensidad en el desarrollo de los trabajos que dieron lugar a este Reglamento y trabajaron duramente en la confección de una norma ciertamente compleja y al mismo tiempo muy relevante para el quehacer cotidiano de las organizaciones públicas y privadas españolas.

A lo largo de un bienio la futura norma ha sido sometida a escrutinio y crítica de todos los sectores implicados. Autoridades Autonómicas de Protección de Datos, Administraciones Públicas, organizaciones empresariales y sindicatos, profesionales del sector de la protección de datos o universidades han manifestado su opinión, crítica o sugerencia respecto de la futura norma.

Sin duda, los éxitos del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RDLOPD) se deben a este carácter de norma públicamente discutida hasta la saciedad y de las aportaciones que en esta fase de debate la han ido enriqueciendo.

Este interés público deriva, indudablemente, del carácter horizontal que poseen las normas sobre protección de datos personales. Es evidente que en la sociedad de la información las decisiones basadas en tecnologías de la información y del conocimiento poseen un valor estratégico [(2)]. Gran parte de esa información se refiere a personas físicas, afecta a su vida privada, a su derecho fundamental

---

2. CASTELLS, Manuel: *La Galaxia Internet,* Areté, Barcelona, 2001. Asimismo puede consultarse el excelente trabajo desarrollado por este investigador en *Projecte Internet Catalunya del IN3*, disponible a <http://www.uoc.edu/in3/pic/esp/>.

a la protección de datos. Por tanto, el desarrollo normativo de este derecho se proyecta sobre todas las ramas del Derecho y sobre todos los sectores de actividad.

Esa horizontalidad singulariza el bien jurídico protegido por el derecho a la protección de datos y se proyecta sobre los aspectos esenciales de la identidad y la vida de las personas. En la medida en que atribuye a los sujetos las facultades necesarias por ejercer un control material sobre la propia información personal se proyecta sobre todas los ámbitos vitales del individuo. Por todo ello la realidad que pretende regular el RDLOPD se proyecta sobre el conjunto del Ordenamiento.

En efecto en la sociedad de la información y el conocimiento el ser humano, aquello que un antropólogo identificaría como *homo sapiens,* adquiere nuevos perfiles y ya no solo es el hombre autoconsciente, ni el hombre económico o productor, sino que hablamos de un hombre digital (3). Se trata de un hombre cuyo ámbito vital supera las tradicionales barreras del espacio físico y desarrolla un conjunto de relaciones basadas en el uso de las tecnologías de la información que requieren de una aproximación cualitativa.

La protección de la información de este nuevo sujeto digital traspasa las barreras de la concepción tradicional de la vida privada (4) entendida como espacio físico y social reservado y protegido por la esfera física de la propiedad, o delimitada por la distinción público/privado. Ahora se trata de proteger algo más cualitativo definible prácticamente en términos informáticos como bite. Cada sujeto aporta información personal en cada momento y con cada una de sus acciones. En la sociedad de las tecnologías de la información lo fundamental no solo es el volumen unitario de información que incorpora un determinado dato sino la información que nos aporte un concreto tratamiento. De ahí que en las últimas décadas a la categoría del derecho a la intimidad se le hayan debido sumar conceptos como el de *«informational privacy»* (5), autodeterminación informativa (6), o derecho a la protección de datos.

---

3. TERCEIRO José B.: *Sociedad digital*, Madrid, Alianza ed., 1996.

4. WARREN, Samuel D. y BRANDEIS, Louis D.: «The right to privacy», en *Harvard Law Review*, vol. IV, núm. 5, diciembre de 1890.

5. MARTÍNEZ MARTÍNEZ, Ricard: *Una aproximación crítica a la autodeterminación informativa*,Madrid, APDCM-Thomson-Civitas, 2004.

6. Véanse los ya clásicos LUCAS MURILLO DE LA CUEVA, Pablo: *El derecho a la autodeterminación informativa,* Madrid, Tecnos, Temas clave,1990 y PÉREZ LUÑO, A.E.: «La protección de la intimidad frente a la

Por otro lado, durante el último año se están produciendo en el mundo de la red fenómenos que pueden afectar de manera particular al derecho a la protección de datos. Así, la potencia lesiva de la capacidad de almacenamiento de los motores de búsqueda, como Google, que además de indexar vínculos a páginas con información personal de un sujeto determinado (7) la pueden incorporar al contenido de su memoria caché haciendo del derecho al olvido una pura ilusión (8). Además, espacios de comunidad como FaceBook, servidores dirigidos a *«colgar»* información como YouTube, o programas para intercambiar información y archivos (9) se han manifestado como herramientas particularmente invasivas para la privacidad, sea por decisión de sus responsables o por acciones de los propios usuarios (10).

---

informática en la Constitución Española de 1978», *Revista de Estudios Políticos*, nueva época, núm. 9, mayo-junio de 1979. PÉREZ LUÑO, A.E.: «Informática y libertad. Comentario al artículo 18.4 de la Constitución Española», en *Revista de Estudios Políticos,* núm. 24 (nueva época), noviembre-diciembre de 1981.

Asimismo, LUCAS MURILLO DE LA CUEVA, Pablo: «La construcción del derecho a la autodeterminación informativa», en *Revista de Estudios Políticos*, nueva época, núm. 104, abril-junio de 1999.

7. AEPD: «Declaración sobre buscadores de internet. 1 de diciembre de 2007». Disponible en <https://212.170.242.196/portalweb/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores.pdf>. Véase también el documento del Grupo de Trabajo del artículo 29 de la Directiva.

WP: «Opinion on data protection issues related to search engines». WP 148/2008 de 04/04/2008. Disponible en <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf>.

8. Véase la tutela de derechos núm. TD/00463/2007 disponible en <https://212.170.242.196/portalweb/resoluciones/tutela_derechos/tutela_derechos_2007/common/pdfs/TD-00463-2007_Resolucion-de-fecha-20-11-2007_Articulo-17-LOPD_Recurrida.pdf>

9. El primer caso en el que se pudo constatar con claridad los problemas para el derecho fundamental a la protección de datos vinculados al uso de programas *peer to peer* puede examinarse en la PSS/00233/2005. Disponible en <https://212.170.242.196/portalweb/resoluciones/procedimientos_sancionadores/ps_2006/common/pdfs/PS-00233-2005_Resolucion-de-fecha-08-09-2006_Articulo-9-y-10-LOPD.pdf>.

10. Aunque un ejemplo de potencial uso lesivo es el buscador de personas disponible en <http://www.dateas.com/>, el responsable declara cumplir la legislación en la materia:

> *«3. Estamos comprometidos con la protección de su privacidad. Exclusivamente usaremos la información que recogemos de Ud. de conformidad con la Ley de Protección de Datos de 1998».*
>
> *«Dateas respeta los máximos estándares internacionales en protección de datos personales, encontrándose inscripta ante la Oficina del Comisionado de Información».*

Obsérvese la descripción de sus servicios:

> *«Dateas es el primer servicio internacional de Búsqueda e Información sobre Personas y Empresas, Investigación Genealógica y Localización de Paraderos. Es líder en calidad porque los Informes Personales se sustentan en un concepto revolucionario de búsqueda inteligente en múltiples bases en constante expansión.*
>
> *A través de Dateas Ud. ahora puede acceder a bases de datos y padrones con millones de registros. Averigüe teléfonos, domicilios, información comercial, antecedentes judiciales y mucho más, de acuerdo al país vinculado a su investigación».*

Con estas pinceladas, y teniendo en cuenta los discursos al uso, parecería lógico afrontar todo aquello que se acaba de describir desde el punto de vista del pesimismo normativo. En esta línea de pensamiento podría afirmarse que la RDLOPD es una norma que nace anticuada, que la tecnología la desborda y podríamos seguir con todo un alud de afirmaciones negativas y seguramente poco atinadas.

Debe afirmarse justo lo contrario. El RDLOPD fija un conjunto de principios que deberán ser fundamentales para concretar la regulación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y aplicarla a la realidad.

El nuevo Reglamento ofrece herramientas que de algún modo obligan a cambiar con este discurso que consiste en afirmar que nunca pueden aplicarse las normas sobre protección de datos porque el regulador va por detrás de la realidad [11]. En estos momentos comienza a abrirse camino la idea del Privacy

---

Curiosamente, afirma Marcelo BAUZÁ: *«En Uruguay no existe, por lo menos no existe aún hoy, a principios del mes de julio de año 2003, una ley de protección de datos personales. Tampoco existen regulaciones jurídicas sectoriales afines al tema, si se exceptúan algunas pocas a las que luego referiré».*

Véase BAUZA REILLY, Marcelo: «La protección jurídica de los datos personales en Uruguay», *Primer Seminario Internacional e Interdisciplinario sobre la Protección de los Datos Personales*, Buenos Aires, Argentina, 2003. Disponible en <http://www.frcu.utn.edu.ar/deptos/depto_3/32JAIIO/sid/SID_18.pdf>.

11. En este sentido, pensar que una norma jurídica debe adaptarse a todas y cada una de las realidades tecnológicas individuales y concretas, o decir que una norma no sirve porque la evolución de la técnica la convierte en obsoleta, o aquello tan antiguo de «*no se pueden poner puertas al campo*» (TRIAS SAGNIER, Jorge: «Informática y privacidad. ¿Se pueden poner puertas al campo?», en *Cuenta y razón del pensamiento actual*, núm. 63, 1992, pp. 98-101). Podría decirse que se trata de una inversión de los principios morales que deben inspirar la tarea de los juristas.

El Derecho regula relaciones humanas, positiva los principios rectores que regulan la convivencia social. Algunas normas, dada la compleja realidad social y técnica, pueden descender a regular los componentes técnicos de una máquina. Pero en el caso del RDLOPD no se trata de la homologación técnica de componentes o materiales, tarea que recaería en el Ministerio de Industria. Estamos hablando del derecho a la protección de datos y en este terreno aquellos que desarrollan la tecnología, diseñan espacios web y servicios a Internet, o los responsables de los ficheros deben llevar a cabo su tarea teniendo en cuenta los principios básicos y las directrices de la LOPD y el RDLOPD. La aplicación de estas normas no puede ser menospreciada por los protagonistas de la sociedad de la información, sino que lo deben tener en cuenta desde el primer momento.

Como ha señalado, Artemi RALLO, actual Director de la AEPD:

> *«Desde una posición meramente reactiva, las Autoridades de Protección de Datos nos enfrentamos en este punto a una paradoja: la ilustrada por el ilustre filósofo griego presocrático Zenón en su fábula sobre "la carrera de Aquiles y la Tortuga". Al vertiginoso ritmo marcado por la Ley de Moore, la garantía reactiva de la privacidad frente a cada nueva tecnología emergente siempre llegará tarde. Como Aquiles, al terminar de recorrer la mitad del camino, la tortuga ya no estará allí. Siempre habrá una nueva tecnología,*

Impact Assessment [12]. En su formulación más básica supone la necesidad de que al adoptar un modelo de gestión basado en el tratamiento de datos personales o desarrollar un software que los trate debe realizarse un análisis previo para determinar la incidencia de estos sobre el derecho fundamental a la protección de datos. Pues bien, gran parte de los elementos necesarios como criterio guía se encuentran en el RDLOPD, ya que es una norma muy detallada en múltiples aspectos fijando principios muy específicos en cuanto a calidad y conservación de los datos, información previa al titular o afectado, formas de acceso, normas de seguridad, etc.

En este sentido, aunque la idea de realizar un análisis de impacto en la privacidad no cuente con una formulación ni teórica, ni normativa, expresa, en el contexto español de una aplicación inteligente del Reglamento se derivarían consecuencias semejantes Por ejemplo, desde el punto de vista de las medidas de seguridad, no se puede hacer un cambio sustancial sin haber hecho una auditoría previa. Por otro lado la disposición adicional del RDLOPD obliga a documentar el nivel de seguridad de que proporciona un software [13]. En cualquier caso, se echa en falta un corpus sistemático que obligue a las or-

---

siempre nos quedará la mitad del camino por recorrer y así hasta el infinito. ¡Siempre llegaremos tarde si sólo buscamos reaccionar frente a los riesgos ya consolidados!

Sin embargo, permítanme una pregunta: ¿Acaso quienes diseñan e implantan las nuevas tecnologías desconocen los principios de protección de datos personales? ¿No son conscientes de los estándares de seguridad necesarios? ¿Agreden nuestra privacidad de modo consciente?

Queridos amigos;

Con el tiempo, los matemáticos demostraron que la aporía de Zenón era un sofisma. Que bastaba con cambiar de paradigma para demostrar su falsedad. Seguramente, la cuestión no es qué capacidad tenemos para regular una nueva tecnología sino qué criterios jurídicos deben regir el diseño de tecnologías invasivas de la privacidad».

RALLO LOMBARTE, Artemi: «What Do Citizens Know And Feel? What Are Citizens Fear On New Technologies?», *Conferencia de primavera*, Roma, 2008. Disponible en <https://www.agpd.es/portalweb/internacional/Europa/conferencias/common/speech_roma_es.pdf>.

12. El PIA no solo se proyecta sobre el cumplimiento de la legalidad, afecta a aspectos como el análisis de riesgos, la calidad, prestigio y reputación empresarial, o a los propios costes de la actividad. Véase INFORMATION COMISSION OFFICER: *PIA Handbook,* Disponible en <http://www.ico.gov.uk/upload/documents/pia_handbook_html/ html/1-intro.html>.

13. *«Disposición adicional única. Productos de software.*

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento».

ganizaciones a incorporar las cuestiones relativas a la protección de datos en la fase de diseño inicial de sus acciones y decisiones.

2. DIFICULTADES PREVIAS: UNA REALIDAD MATERIAL Y NORMATIVA COMPLEJA

El reglamento nace en un contexto normativo peculiar. En primer lugar, la LOPD nace como proyecto de reforma de la Ley Orgánica 5/1992, la conocida LORTAD; pero acaba su periplo parlamentario como norma que deroga la Ley Orgánica. Nace, probablemente por ello, sin Exposición de Motivos y con cierta polémica parlamentaria [(14)]. El legislador tan sólo encuentra un modo de salvar un problema inmediato que causaba la derogación de la LORTAD. El régimen jurídico de la protección de datos personales es muy complejo y requiere de herramientas reglamentarias que concreten las previsiones legislativas. Por ello, la LOPD dispuso en su Disposición transitoria tercera:

---

14. LUCAS MURILLO ha apuntado en esta línea subrayando lo extraño del proceso de tramitación de la Ley Orgánica, el hecho previo de la renuncia al recurso de inconstitucionalidad que en su día presentó el Partido Popular así como la escasa fundamentación de las innovaciones incluidas en la regulación de los ficheros privados con la finalidad de facilitar actividades como el marketing comercial o el cálculo de riesgos a la compañías aseguradoras.

LUCAS MURILLO DE LA CUEVA, Pablo: «Las vicisitudes del Derecho de la protección de datos personales», en *Revista Vasca de Administración Pública*, núm. 58, septiembre-diciembre de 2000, pp. 217 y ss.

En efecto, la sesión plenaria del Congreso de 25 de noviembre de 1999, en la que se discutieron las enmiendas del Senado al proyecto de Ley Orgánica de Protección de Datos, cabe citar las intervenciones de los diputados López Garrido y Navarrete Merino. El primero afirmó con rotundidad:

> *«Si hoy aprobáramos la ley —que probablemente se va a producir— se dejaría sin objeto jurídico real ese recurso de inconstitucionalidad ante el Tribunal Constitucional, por lo que habrá que reproducirlo. Ya tenemos un primer ejemplo de un fraude, querido o no querido, consciente o inconsciente, a una acción ante el Tribunal Constitucional. El Tribunal Constitucional decidirá el año que viene sobre el recurso de una ley que ya habrá sido derogada por este proyecto de ley, aunque éste reproduce los mismos artículos considerados inconstitucionales por el Defensor del Pueblo y por el Grupo Popular».*

En idéntico sentido el segundo afirmó:

> *«No nos gusta el título de la ley ni su disposición derogatoria. Creemos que es una operación fraudulenta contra las competencias jurisdiccionales del Tribunal Constitucional».*

CORTES GENERALES: *Diario de Sesiones del Congreso de los Diputados. Pleno y Diputación Permanente,* VI Legislatura, año 1999, núm. 277.

«Disposición transitoria tercera. Subsistencia de normas preexistentes.

Hasta tanto se lleven a efecto las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1983, de 26 de marzo, 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley».

El Gobierno, habilitado por la citada disposición final para el desarrollo reglamentario, se enfrentaba además a una necesidad de adaptación puesta de manifiesto por la propia LOPD:

«Disposición adicional primera. Ficheros preexistentes.

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior, deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados».

Por tanto, de un lado había un complejo y disperso corpus normativo integrado no sólo por los reglamentos expresamente citados por la LOPD, sino también por distintas Instrucciones de la Agencia Española de Protección de Datos. De otro, octubre de 2007 se erigía en una frontera a partir de la cual los operadores necesitaban criterios claros aplicables a los ficheros no automatizados o manuales.

Todo ello en un entorno material muy complejo ya que puede afirmarse que, desde una perspectiva sectorial, existe protección de datos en la salud, protección de datos en la publicidad, protección de datos en todos y cada uno de

los sectores de actividad. Por lo tanto, había una necesidad de ofrecer respuestas a multitud de problemas que afectaban a sectores muy diferentes y que necesitaban algún tipo de respuesta, en unas ocasiones general, en otras particular. Además la protección de datos se da en un contexto altamente técnico que ha exigido la redacción de un apartado de definiciones. Los operadores necesitaban referentes y respuestas.

En este sentido, las decisiones normativas del regulador han tratado de responder a dos objetivos claros. El primero de ellos ha sido la voluntad de dar claridad y seguridad jurídica al sistema ofreciendo conceptos y una guía normativa que permita el cumplimiento de la normativa de protección de datos (15). Por otro lado, el regulador ha procurado dotar de una cierta flexibilidad que permita una aplicación eficaz de las normas por parte del responsable del fichero.

3. ELEMENTOS CLAVE DE LA REGULACIÓN

La naturaleza de este artículo obliga a un doble esfuerzo intelectual. En primer lugar, debe abordarse el conjunto del RDLOPD, casi sobrevolarlo, tratando de ofrecer una visión unitaria de su contenido y objetivos. Por otra parte, deben ofrecerse al lector distintas pinceladas que subrayen aquellos elementos que, a juicio del autor, resultan estratégicos. Por tanto, ello obliga a usar una pincelada con cierto trazo grueso y a abrir caminos, a explorar posibilidades, más que a cerrar de modo definitivo los temas. Por ello, la elección será puramente subjetiva, aunque se espera que útil (16).

---

15. En este sentido, el reglamento es tributario de la experiencia acumulada por la Agencia Española de Protección de Datos, en sus informes y resoluciones, y la jurisprudencia dictada en la materia.

Al respecto véase LESMES SERRANO, Carlos: *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008.

16. Hay elementos que podrían parecer menores, y por ello no se van a abordar, y sin embargo no carecen de importancia. Así por ejemplo, el nuevo sistema de cómputo de plazos no parece tener entidad suficiente para ser tratado como un epígrafe y sin embargo resuelve una diferencia de tratamiento particularmente injusta en lo concerniente a la satisfacción de las obligaciones por parte del responsable del fichero. En virtud de un informe de la AEPD se aplicaban a las Administraciones Públicas los criterios propios de las leyes administrativas. En consecuencia allá donde los plazos se expresaban en días estos se entendían hábiles. En cambio, en cuanto a los ficheros de titularidad privada los días eran contados como naturales. Con el artículo 6 del RDLOPD el criterio será homogéneo y en los supuestos en que el Reglamento señale un plazo por días se computarán únicamente los hábiles y, cuando el plazo sea por meses, se computarán de fecha a fecha.

3.1. LA EXCLUSIÓN DE EMPRESARIOS INDIVIDUALES Y PERSONAS DE CONTACTO

El regulador, con la intención de delimitar el ámbito de aplicación del RDLOPD, añadió en el último momento de la tramitación dos párrafos en el artículo segundo dirigido a excluir de su aplicación a personas de contacto y empresarios individuales:

> *«Artículo 2. Ámbito objetivo de aplicación.*
>
> *2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.*
>
> *3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o*

Véase el Informe 534/2003, «Cómputo del plazo para la satisfacción de los derechos de rectificación y cancelación». Disponible en <https://212.170.242.196/portalweb/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2003-0534_Computo-del-plazo-para-la-satisfaccion-de-los-derechos-de-rectificacion-y-cancelacion.pdf>.

En otro orden de cosas el artículo 2 del RDLOPD contiene una previsión específica en lo concerniente al caso de haberse producido una defunción que permite a las personas vinculadas al fallecido, por razones familiares o análogas, *«dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos»*. Con ello se consigue el doble objetivo de facilitar al responsable el cumplimiento del principio de calidad y resolver problemas y situaciones dolorosas.

Véase Informe 61/2008. Aplicación de las normas de protección de datos a los datos de personas fallecidas. Disponible en <https://212.170.242.196/portalweb/canaldocumentacion/informes_juridicos/reglamento_lopd/common/ pdfs/2008-0061_Aplicacion-de-las-normas-de-proteccion-de-datos-a-datos-de-fallecidos.pdf>.

La bibliografía en la materia es muy extensa. Véase, entre otros, CLAVERÍA GOSALBES, Luis Humberto: «Reflexiones sobre los derechos de la personalidad a la luz de la Ley Orgánica 1/1982, de 5 de mayo», en *Anuario de Derecho Civil*, vol. XXXVI, fasc. 4, 1983. ROMERO COLOMA, M.ª Aurelia: *Los bienes y derechos de la personalidad*, Trivium, Madrid, 1985. BUSTOS PUECHE, José Enrique: *Manual sobre bienes y derechos de la personalidad,* Dykinson, Madrid, 1997. REBOLLO DELGADO, Lucrecio: «Derechos de la personalidad y datos personales», en *Revista de Derecho Político*, núm. 44, 1998 , pp. 143-206. VIDAL MARTÍNEZ, Jaime: «Algunos datos y observaciones acerca de la construcción civil de los derechos de la personalidad (derechos y libertades inherentes a la persona) en la actual etapa de desarrollo tecnológico», en CABANILLAS SÁNCHEZ, Antonio (coord.): *Estudios jurídicos en homenaje al profesor Luis Díez-Picazo,* vol. 1, Civitas, Madrid, 2002.

navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal».

Eso ha obligado a delimitar cuándo opera la exclusión y cuándo nos encontramos ante la aplicación de la normativa en materia de protección de datos personales, apostando por una interpretación estricta de la norma.

En este sentido, cabe plantearse hasta qué punto este precepto innova el Ordenamiento y resuelve problemas preexistentes. Podría afirmarse que, en referencia a los empresarios individuales, en realidad no hace ni lo uno ni lo otro. La cuestión de la aplicabilidad de las normas sobre protección de datos personales se habían planteado ya en distintos informes de la Agencia Española de Protección de Datos. La Agencia, partiendo de estos informes y de distintas resoluciones jurisprudenciales, interpreta el nuevo precepto en su Informe 42/2008 sobre «Novedades del Reglamento: Empresarios individuales» [17]:

«A la vista de lo que se ha venido indicando cabe considerar que los datos referidos a los empresarios individuales y que aparecen exclusivamente ligados a su actividad comercial o mercantil, o que identifican, aún con su nombre y apellidos, un determinado establecimiento o la marca de un determinado producto o servicio, como consecuencia de la existencia de una libre decisión empresarial adoptada en este sentido, no se encuentran sometidos a la protección conferida por la Ley Orgánica 15/1999. Este es el criterio recogido por el artículo 2.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999.

Al propio tiempo, el tratamiento ha de llevarse a cabo en el ámbito empresarial. Quiere ello decir que a los efectos del tratamiento de los datos, la finalidad perseguida por quien trata el dato es la de recabar y mantener información sobre la empresa y no sobre el comerciante que la ha constituido.

Así, el tratamiento de los datos del empresario individual, con las limitaciones que se han venido señalando, para mantener una relación comer-

17. Disponible en <https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/index-ides-idphp.php>.

cial con el mismo, podría encontrarse amparado por el artículo 2.3 del Reglamento, en conexión con las normas de la Ley Orgánica 15/1999 que se han venido indicando.

Sin embargo, no podrá considerarse amparado por el precepto, y en consecuencia excluido de la aplicación de la Ley Orgánica 15/1999, el tratamiento de los datos del comerciante llevado a cabo no con la finalidad de mantener una relación empresarial con el establecimiento u organización que el mismo hubiera creado, sino para conocer la información del propio sujeto organizado en forma de empresa, siendo el destinatario del tratamiento no la empresa sino el propio empresario en tanto, por ejemplo, que consumidor individual».

En el mismo informe, se aborda la problemática de las personas de contacto, señalándose:

«Como se ha indicado, el fundamento de la exclusión efectuada por el inciso segundo del precepto tiene una fundamentación similar a la que se acaba de indicar en relación con el artículo 2.3, limitándose a considerar excluidos de la aplicación de la Ley Orgánica 15/1999 los ficheros en los que la inclusión de los datos identificativos de una determinada persona física es meramente accidental en relación con el contenido y finalidad del tratamiento, teniendo en cuenta lo que ha venido señalándose al respecto en diversas resoluciones de esta Agencia [18]*.*

(…)

En consecuencia, la Agencia ha venido señalando que en los supuestos en que el tratamiento del dato de la persona de contacto es meramente ac-

---

18. *«En resolución de 20 de julio de 2005 se acuerda el archivo de actuaciones al constatarse que el fichero objeto de investigación únicamente contiene los datos de sociedades, incorporando en uno de sus apartados el nombre de la persona de contacto habitual, entiendo que "el tratamiento de dichos datos de apoderados de empresas no se encuentra, en el presente caso, dentro del ámbito de aplicación de la LOPD".*

Las resoluciones de 24 de agosto de 2005 y 9 de mayo de 2006 se refieren al tratamiento de direcciones de correo electrónico en que figuran algunos nombres de personas de la empresa con la que el responsable del tratamiento mantuvo relación comercial, considerando la segunda de las resoluciones citadas que «se trata de direcciones institucionales de empresa que, por lo tanto, no tienen la consideración de dato personal, por lo que procede acordar el archivo de las presentes actuaciones previas de investigación"».

cidental en relación con la finalidad del tratamiento, referida realmente a las personas jurídicas en las que el sujeto presta sus servicios, no resulta de aplicación lo dispuesto en la Ley Orgánica 15/1999, viniendo el Reglamento a plasmar este principio.

No obstante, nuevamente, es necesario que el tratamiento del dato de la persona de contacto sea accesorio en relación con la finalidad perseguida. Ello se materializará mediante el cumplimiento de dos requisitos:

El primero, que aparece expresamente recogido en el Reglamento será el de que los datos tratados se limiten efectivamente a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta sus servicios. Por este motivo, el Reglamento impone que el tratamiento se limite a los datos de nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales.

(…)

El segundo de los límites se encuentra, como en el supuesto contemplado en el artículo 2.3, en la finalidad que justifica el tratamiento. Como se ha venido indicando reiteradamente, la inclusión de los datos de la persona de contacto debe ser meramente accidental o incidental respecto de la verdadera finalidad perseguida por el tratamiento, que ha de residenciarse no en el sujeto, sino en la entidad en la que el mismo desarrolla su actividad o a la que aquél representa en sus relaciones con quienes tratan los datos.

De este modo, la finalidad del tratamiento debe perseguir una relación directa entre quienes traten el dato y la entidad y no entre aquéllos y quien ostente una determinada posición en la empresa. De este modo, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto únicamente el medio para lograr esa finalidad».

En resumen, los aplicadores de la norma deben ser capaces, si quieren excluir la aplicación del bloque normativo de la protección de datos personales, de ceñirse a las previsiones del RDLOPD limitándose a tratar exclusivamente los datos que en él se describen y para una finalidad empresarial. Ello exige, indudablemente, que la decisión se base en un análisis previo del riesgo en

que se incurre, ya que una simple desviación de la finalidad podría conducir a la aplicación de las normas sobre protección de datos, y por tanto derivar en la comisión de distintas infracciones en cascada —información en la recogida, consentimiento, inscripción, documento de seguridad…—, y, por otra parte, a mantener un rigor adecuado en la gestión de ese concreto tratamiento.

3.2. EL PRINCIPIO DE CALIDAD DE LOS DATOS

Hay dos cuestiones que procede destacar en esta materia. En primer lugar, hay que subrayar la aparición y la clarificación del mecanismo de funcionamiento de la cancelación de los datos ya sea a instancia de parte, ya sea de oficio. En ambos casos cancelar dará siempre lugar al bloqueo. En este sentido el Reglamento es muy claro desde la propia definición de cancelación del artículo 5, que incorpora la del bloqueo:

> «b) *Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos».*

En la praxis se trataba de subsanar una omisión de la LOPD puesto que, mientras que el artículo 16.3 dice expresamente que la cancelación da lugar al bloqueo, en cambio no se contiene una previsión idéntica en el artículo 4. De ahí que el RDLOPD sea más claro:

> *«Artículo 8. Principios relativos a la calidad de los datos.*
>
> (…)
>
> 6. *Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento».

Como la finalidad no es otra que conservar los datos a los efectos de determinar eventuales responsabilidades de todo tipo, el criterio material aplicable es el mismo en todos los casos. Por otro lado era necesario, como en todos los procedimientos, el traslado al cesionario de estas cancelaciones:

«Artículo 8. Principios relativos a la calidad de los datos.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento».

3.3. EL CONSENTIMIENTO

El consentimiento ha sido objeto de una regulación muy específica y completa en el RDLOPD. Esta regulación ha tratado de tener en cuenta en primer lugar la necesidad de adaptar el régimen jurídico vigente en España a las exigencias de la Directiva 95/46/CE haciendo la regulación más coherente y armonizada. En este sentido se ha trasladado la doctrina del interés legítimo de la Directiva con todas las consecuencias e implicaciones que ello pueda comportar [19].

Sin embargo, aparte de este objetivo existían otras cuestiones a las que hacer frente.

3.3.1. Los datos de los menores

El consentimiento de los menores ha sido regulado por un artículo particularmente denso, el artículo 13 del RDLOPD, que fija criterios y normas de procedimiento ordenadas a captar el consentimiento de los menores.

> *«Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.*
>
> *1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.*
>
> *2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los ti-*

19. Éste es el objetivo del artículo 10 del RDLOPD.

tulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. *Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.*
4. *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 prestado, en su caso, por los padres, tutores o representantes legales».*

Este artículo ha sido objeto de críticas diversas desde una perspectiva dogmática. En principio, dos son los aspectos susceptibles de crítica. En primer lugar, el hecho de que la propia naturaleza reglamentaria de la norma pueda resultar la menos conveniente tratándose de un esfuerzo normativo de tanta trascendencia. Quizá hubiese sido más apropiado jurídica y políticamente acudir a una norma con rango de ley. Sin embargo, y a pesar de que la legislación sobre menores se refiere a la intimidad y la propia imagen de los menores [(20)],

---

20. El artículo 4 de la Ley Orgánica 1/1996 dispone:

«1. Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

2. La difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados.

3. Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales.

4. Sin perjuicio de las acciones de las que sean titulares los representantes legales del menor, corresponde en todo caso al Ministerio Fiscal su ejercicio, que podrá actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física, jurídica o entidad pública.

5. Los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques de terceros».

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

el legislador no ha regulado nunca este ámbito en lo que a la protección de datos se refiere.

La segunda cuestión afecta a la opción del regulador al fijar la frontera del consentimiento en los 14 años [21]. En concreto, en el artículo se fijan tres reglas. En primer lugar, podrán consentir los menores de 18 años y mayores de 14. Esta regla queda modulada por una segunda que obliga a contar con el consentimiento concurrente de padre, madre o tutor legal cuando el negocio jurídico afecte a un mayor de 14 años y se requiera para su perfección también el de aquellos. Por último, será necesaria siempre autorización parental cuando el menor lo sea de menos de 14 años. En este sentido hay que admitir que, a pesar de que el parámetro que fija el Reglamento se puede deducir del Código Civil, también es cierto que en ésta y en otras normas se utilizan criterios como el del mayor de 12 años y del mayor maduro [22]. En cualquier caso, el problema de los derechos de la personalidad del menor y la protección de datos de carácter personal provocarán sin duda un amplio debate doctrinal [23].

Desde el punto de vista de los objetivos del regulador se trataba de proteger los derechos de los menores y del entorno familiar inmediato. Los menores son objeto de tratamientos de datos o de captaciones de datos por ellos mismos y como fuente de información de su inmediato entorno familiar. En este

---

21. El precedente de este criterio se encuentra en el Informe de la AEPD sobre consentimiento prestado por menores de edad. Disponible en <https://212.170.242.196/portalweb/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf>.

22. Respecto del consentimiento informado establece, por ejemplo, la Ley 41/2002:

«Artículo 9. Límites del consentimiento informado y consentimiento por representación.

3. Se otorgará el consentimiento por representación en los siguientes supuestos:

(…)

c) Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor después de haber escuchado su opinión si tiene doce años cumplidos. Cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, no cabe prestar el consentimiento por representación. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente».

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

23. DE LAMA AYMÁ, Alejandra: *La protección de los derechos de la personalidad del menor de edad*. Tirant lo Blanch, Valencia, 2006.

último caso el menor era relevante porque puede ser instrumentalmente utilizado para revelar datos parentales como el tipo de trabajo de los padres, los ingresos, posesiones, preferencias de la familia etc. De ahí que el RDLOPD haya establecido una prohibición de uso instrumental del menor para captar datos del entorno familiar, salvo que se trate de los datos estrictamente necesarios para poder obtener la autorización parental.

En segundo lugar, se han fijado las condiciones de cumplimiento del artículo 5 de la LOPD en el caso de los menores. El derecho de información en la recogida de los datos constituye el presupuesto de la capacidad de autodeterminación en protección de datos y, en cuanto a los menores, la satisfacción del derecho no tendría sentido si la información no resulta clara y comprensible (24).

Por último, probablemente la cuestión más compleja sea la fijación de procedimientos de verificación de la edad del menor. Se trata de una decisión de política normativa del regulador y es preciso ser conscientes de que es una cuestión probablemente complicada que plantea dificultades. En cualquier caso no parece que se trate de obligar al responsable del fichero a una prueba imposible. Más bien, supone una obligación de diligencia para el responsable del fichero a la hora de establecer mecanismos ordenados a conseguir este objetivo. Si un menor altera de cualquier manera su identidad no se debería considerar la existencia de infracción alguna, o cuando menos la concurrencia de negligencia o culpa, por parte del responsable del fichero cuando este haya sido diligente.

A partir de estos elementos debe contemplarse la cuestión desde una doble perspectiva. En primer lugar, el responsable que no tenga por objeto tratar datos de menores debería fijar estrategias ordenadas a impedirles el acceso a su entorno. Aunque es cierto que este objetivo resulta limitadamente sencillo en el mundo físico puede plantear problemas en los entornos *on-line* (25). En, principio si no requiere registro y no hay un tratamiento de datos el riesgo afecta más al tipo de contenido que estrictamente hablando a la protección de da-

---

24. AEPD: «Derechos de niños y niñas. Deberes de padres y madres: Guía de recomendaciones 2008». Disponible en <https://212.170.242.196/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf>.

25. Véase la resolución núm. PS/00269/2007 relativa al envío a un menor de un producto financiero. Disponible en <https://212.170.242.196/portalweb/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00269-2007_Resolucion-de-fecha-28-01-2008_Articulo-6.1-LOPD.pdf>.

tos. No obstante, debe recordarse el potencial de los tratamientos invisibles como las cookies y el uso instrumental de hiperenlaces, banners, etc. Por tanto, parece que un mínimo razonable sería el de indicar de algún modo la necesaria concurrencia de cierta edad para navegar por los contenidos. Si hay un registro del usuario y una recogida de datos personales deberían adoptarse estrategias adicionales limitar el campo de fecha de nacimiento haciendo imposible incluir un año posterior al actual restados 18. Los riesgos, al menos desde un punto de vista formal, se reducen y van a depender no del concreto responsable del fichero sino de la educación del menor.

Otra propuesta adicional para ambos casos tendría que ver con el que debería ser obligatorio uso de etiquetas, tags, que puedan ser leídas por el navegador cuando los padres hayan activado políticas de control parental o de control de contenidos.

Por otro lado, cuando el responsable tenga por objeto tratar específicamente datos de menores deberá aplicar el artículo 13 del RDLOPD. Aquí la mayor dificultad reside en la prueba de la edad del mayor de 14 años en Internet. En principio cuando el DNI electrónico se implante —acompañado de la necesaria infraestructura doméstica como los lectores del chip que el ingenio incorpora—, la prueba de edad, identidad y capacidad será una cuestión puramente técnica. Mientras, el responsable deberá emplear criterios como solicitar datos relativos a documentos propios de un mayor de 14 años —DNI, permiso para conducir ciclomotor o cualesquiera otros—, utilizar tests o cuestionarios que sirvan para determinar su edad, solicitar que se acompañen en formato físico o digitalizado documentos que prueben la edad —partida de nacimiento, libro de familia…— y en último extremo diferir la confirmación del consentimiento a una confirmación mediante los tradicionales medios escritos en soporte papel. En cualquier caso se trata de objetivos en los que el regulador español no difiere necesariamente del de otros países [(26)].

Por último conviene subrayar un elemento no estrictamente jurídico que se da en esta materia. Cuando el responsable del fichero o tratamiento decide tratar datos de menores, de modo lícito, leal y legítimo, como objeto o finalidad

---

26. Véase la *Children's Online Privacy Protection Act of 1998* y la sección sobre la forma de cumplir sus prescripciones en <http://www.ftc.gov/ogc/coppa1.htm> y la página informativa <http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.shtm>.

de su negocio debe soportar las cargas que ello comporta. Por tanto, el responsable debe incorporar a su estructura de costes y al análisis de riesgos el necesario cumplimiento de la legalidad vigente en esta materia, ya que desarrolla su actividad en una sociedad que ha atribuido a la protección de datos personales la naturaleza de un derecho fundamental y que predica como valor fundamental en el ámbito constitucional, legislativo y reglamentario la protección de la juventud y de la infancia.

3.3.2. El consentimiento tácito

El RDLOPD consolida una praxis admitida y consistente al informar de la realización de un determinado tratamiento haciendo saber al titular de los datos que, transcurridos 30 días sin respuesta negativa, se entenderá que consiente el mencionado tratamiento [(27)].

«Artículo 14. Forma de recabar el consentimiento.

1. *El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.*

2. *El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.*

   En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma

27. AEPD: «Informe sobre Caracteres del consentimiento definido por la LOPD». Disponible en <https://212.170. 242.196/portalweb/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Caracteres-del-consentimiento-definido-por-la-LOPD.pdf>.

conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

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

4. *Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.*

5. *Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud».*

De esta norma debe subrayarse cómo el regulador ha sido particularmente riguroso en lo concerniente a la exigencia de una información conveniente y sobre la comprobación de la no devolución de la comunicación para la que se pide el consentimiento. Además, y eso es común al conjunto del Reglamento, se impone al responsable el facilitar un medio sencillo y gratuito para oponer su negativa al tratamiento. Por último resulta necesario destacar la rápida reacción del regulador ante críticas doctrinales relativas a la necesidad de enmarcar esta práctica dentro de límites razonables que evitasen, teniendo en cuenta la redacción de borradores previos del RDLOPD, reiterar una petición idéntica hasta conseguir no ya un consentimiento tácito sino un consentimiento *«por agotamiento».*

3.3.3. El consentimiento para finalidad diferente

Otra cuestión muy importante en esta materia es la regulación en el artículo 15 del RDLOPD del consentimiento para finalidades no relacionadas con la re-

lación contractual. Y en concreto en lo concerniente a la captación del consentimiento mediante la utilización de condiciones generales de la contratación [28]. En este sentido, el objetivo de la norma no es otro que impedir prácticas consistentes en utilizar un supuesto en el que se dan las condiciones de los artículos 6.2 o 11.2.c) de la LOPD para a continuación incluir un conjunto de cláusulas generales que conducen a tratar datos para finalidades diferentes de las de la propia contratación.

Es necesario destacar dos aspectos en esta materia. En primer lugar, el regulador ha utilizado una formulación negativa. No se trata de obtener el consentimiento para el tratamiento de datos para finalidad diferente, sino de permitir al afectado *«que manifieste expresamente su negativa al tratamiento o comunicación de datos».* Por lo tanto, y a pesar de los aspectos positivos de la medida, nos encontramos ante la necesidad de que el titular se niegue, con todas las connotaciones que tiene esta opción en el marco de una relación en la que en ocasiones va a ser el eslabón más débil. Sin embargo el regulador ha introducido un factor de corrección:

> *«En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento».*

En la praxis ello obligará al titular de los datos a prestar mucha atención a los procesos de captación de datos aunque deja una pregunta en el aire: En la medida en la que en los procesos de captación de datos personales *on-line* han existido siempre prácticas poco elegantes consistentes en editar la información del artículo 5 en *«combos»* o tablas de lectura casi imposible, si ahora, además, incluyen la cláusula negativa a la que se refiere el artículo y ésta pasa inadvertida al titular de los datos, ¿qué valor tendrá este consentimiento?

---

28. PANIZA FULLANA, Antonia: *Contratación a distancia y defensa de los consumidores: su regulación tras la reforma de la Ley de Ordenación de Comercio Minorista y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico,* Comares, Granada, 2003.

3.3.4. La revocación del consentimiento

Por último, el artículo 17 del RDLOPD viene a resolver una vieja confusión diferenciando la cancelación, que presupone el ejercicio de un derecho con ciertos requisitos —como el de aportar las razones o documentos que la justifiquen—, y la simple revocación de un consentimiento libremente prestado. Por lo tanto en el caso en el que se ha consentido libremente se puede revocar el consentimiento del mismo modo. Por ello, en ningún caso el responsable podrá reconducir una revocación a la técnica de la cancelación y debe respetar ciertas obligaciones. En primer lugar, la revocación debe ser gratuita y no puede suponer ningún ingreso. Además deberá cesar en el tratamiento, para lo que dispone de un plazo de 10 días, debiendo además notificárselo al afectado cuando éste lo solicite. En cualquiera caso, este cese en el tratamiento dará lugar al bloqueo de los datos.

3.4. EL DEBER DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Este deber es presupuesto esencial para el derecho fundamental a la protección de datos y el regulador ha tratado de garantizar que se preste de manera conveniente. Se pueden subrayar algunos aspectos fundamentales en esta materia. En primer lugar, y como es lógico, prevé el artículo 18 del RDLOPD que recaerá en el responsable del fichero la acreditación y prueba del cumplimiento de su deber de informar. Esto será particularmente relevante en los procesos de captación de datos *on-line,* donde será conveniente tener en cuenta aspectos como la certificación de los websites o la realización de backup del sistema que prueben el momento a partir del que la información se encontraba disponible. Por otro lado, dado que el artículo 5 de la LOPD únicamente prevé la existencia de información escrita cuando se utilicen impresos o formularios, se plantea la duda de la prueba de la existencia de información en los casos en los que en ausencia de tales documentos se capten datos verbalmente.

En consecuencia, tanto en los entornos de Internet como en el mundo físico, no parece descabellado recomendar políticas informativas complementarias. En el primer caso puede ser conveniente disponer de políticas de privacidad, así como generar recibos y confirmaciones mediante envíos de mensajes de

correo electrónico que incorporen la información del artículo 5 de la LOPD. Por otro lado, en el mundo físico no se deberían descartar recursos como los carteles, los recibos y facturas, incluso el uso de sellos y tampones con la información de la LOPD, por ejemplo en registros de entrada de documentos.

En segundo lugar, el artículo 19 del RDLOPD aclara las políticas a seguir en los casos en los que con motivo de la sucesión del responsable, en procesos empresariales como las fusiones y absorciones, el nuevo responsable se subroga en la posición del anterior y debe informar a los titulares de los datos [29].

3.5. EL EJERCICIO DE LOS DERECHOS

En lo concerniente al ejercicio de los derechos, desde el punto de vista de este trabajo, resulta necesario destacar dos elementos que se consideran centrales. En primer lugar, hay que subrayar el énfasis del regulador en la gratuidad. Dice el artículo 24.3 del RDLOPD:

> *«3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.*
>
> *No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o 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».*

Por lo tanto, esto obliga al responsable a tener un cierto cuidado y no establecer formas de ejercicio de los derechos que puedan suponer cargas para

---

29. Véase la Resolución núm. E/00659/2004. Disponible en <https://212.170.242.196/portalweb/resoluciones/ archivo_actuaciones/archivo_actuaciones_2004/common/pdfs/E-00659-2004_Resolucion-de-fecha-29-12-2004_Articulo-6-y-12-LOPD.pdf>.

el titular y, por encima de todo, la de evitar la tentación de utilizar estos medios como fórmula para disuadirlo de su ejercicio.

La segunda palabra que define las opciones del regulador en esta materia es *«flexibilidad».* En efecto, los párrafos cuarto y quinto del mismo precepto disponen:

> *«4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.*
>
> *5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aun cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente».*

Es evidente que los servicios de atención, en la mayor parte de los casos, disponen de un protocolo previo de identificación del sujeto. Cuando el servicio sea *on-line,* con independencia de la aplicación del artículo 2 de la LISI [30],

---

30. Este precepto indica:

«Artículo 2. Obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica.

1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio de interlocución telemática que, mediante el uso de certificados reconocidos de firma electrónica, les permita la realización de, al menos, los siguientes trámites:

(…)

la identificación se suele realizar mediante la atribución de un usuario y un pin o contraseña. Normalmente, cuando el proceso de contratación es riguroso la atribución de usuario y clave de acceso se hace previa identificación física del titular en condiciones que permiten considerar como firma electrónica simple estos identificadores [31]. Por la misma razón, una identificación telefónica mediante la solicitud de datos de contraste proporcionadas en procesos previos de contratación también identifica a un sujeto. Por lo tanto, el acceso al ejercicio de los derechos se producirá porque el titular se ha identificado plenamente y se dan todas las condiciones de ejercicio personalísimo del derecho.

Por otro lado, del párrafo quinto se deriva una libertad formal y procedimental que, si por una parte evita prácticas dilatorias o disuasorias por parte de los responsables, de otra los obliga a poner mucha atención en los diferentes canales de entrada de potenciales ejercicios de derechos y a estar atentos a facilitar la respuesta adecuada en tiempo y forma.

Por último, hay que citar la necesidad de insertar una cláusula de estilo que debe utilizar el responsable cuando deniegue el ejercicio de un derecho. En efecto, dice por ejemplo el artículo 30.3 del RDLOPD respecto del derecho de acceso:

> *«3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre».*

---

d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal».

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

31. En efecto conforme al artículo 3.1 de la Ley 59/2003:

«Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante».

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Esta cláusula puede tener un efecto pedagógico muy importante. Será en efecto pedagógico en lo concerniente al responsable, en la medida en la que al contestar una petición de ejercicio de derechos para denegarla no actuará de manera arbitraria ante la posibilidad del ejercicio de una eventual tutela. En lo concerniente al ciudadano que recibe esa información, le ayudará a descubrir la existencia de autoridades de protección de datos (32).

3.6. EL ESTATUTO DEL ENCARGADO DEL TRATAMIENTO

Uno de los elementos destacados del Reglamento es lo que se ha denominado por distintos autores y conferenciantes como *«Estatuto del encargado del tratamiento»* (33). El encargado es una figura muy relevante en la medida en la que la contratación y subcontratación de servicios que comportan tratamientos de datos es muy común a casi todos los sectores productivos —y a la Administración Pública (34)—, y por lo tanto tiene mucha trascendencia.

---

32. Las respuestas a las preguntas 7 a 23 del Barómetro del CIS de febrero de 2008 son particularmente significativas en lo que respecta a la sensibilidad social respecto del tratamiento de datos personales, que viene acompañada de un cierto desconocimiento de los medios de tutela. Disponible en <http://www.cis.es/cis/opencms/Archivos/Marginales/2740_2759/2754/e275400.html>.

33. Feliz definición que en principio debería atribuirse a D. Jesús Rubí Navarrete, adjunto al Director de la Agencia Española de Protección de Datos.

34. Indica la nueva Ley de Contratos:

«Disposición adicional trigésimo primera. Protección de datos de carácter personal.

1. *Los contratos regulados en la presente Ley que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo.*
2. *Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento.*

   En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán de constar por escrito.

   Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que ésta hubiese designado.

   El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.
3. *En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:*

En este ámbito es oportuno subrayar algunos aspectos, sin perjuicio de un análisis de más profundidad en trabajos específicos. En primer lugar, se pide al responsable que actúe con un cierto cuidado, que sea diligente al escoger al encargado:

> *«Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.*
>
> (…)
>
> *2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento».*

Esta previsión posee una enorme trascendencia, ya que traslada el deber al responsable de tener un conocimiento efectivo y supervisar de algún modo las tareas del encargado y simultáneamente traslada a los encargados la necesidad de ser diligentes en el cumplimiento de la LOPD si desean concurrir en el mercado. En cualquiera caso, no se debería entender este deber de diligencia como una obligación de control material y efectivo de cada una de las actuaciones del encargado. En el momento de la contratación, este deber como mínimo debería traducirse en que el responsable exija al encargado la exhibición de ciertos documentos como la inscripción de los ficheros propios del encargado, la presentación del último informe de auditoría, o la prueba de disponer de documento de seguridad. En este último caso también sería aconsejable plantearle una batería de cuestiones que determinen si está en condiciones de

---

a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.

b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.

c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento».

Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.

garantizar la seguridad. Otro elemento a considerar es que el encargado pueda aportar certificaciones de calidad como «SGSI» (35). En cualquier caso, es importante subrayar que el control material que el responsable pueda tener respecto de la actuación del encargado deberá ser respetuoso con las obligaciones que este encargado pueda tener, a su vez, con otros responsables.

El siguiente elemento relevante es la regulación del régimen de la subcontratación. Al respecto el artículo 21 fija un complejo régimen jurídico, el resumen del cual podría consistir en afirmar que en todo momento el responsable del fichero debe mantener un control efectivo sobre la prestación de cualquier encargado del tratamiento (36).

Por otro lado resulta fundamental la clarificación del hecho de que el encargado bajo ciertas condiciones pueda, o deba, conservar datos, así como las fórmulas de devolución de los mismos.

«Artículo 22. Conservación de los datos por el encargado del tratamiento.

1. *Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*

   No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. *El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento».*

---

35. Véase la Norma UNE-ISO/IEC 27001:2007: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información.

36. Informe AEPD núm. 513/2004. Subcontratación de servicios por el encargado del tratamiento. Disponible en <https://212.170.242.196/portalweb/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2004-0513_Subcontratacion-por-un-encargado-del-tratamiento.pdf>.

Es importante que se haya regulado el momento de la finalización de la relación contractual con el encargado cuando ésta realmente no se producía en un contexto en el que el encargado devolviese los datos al responsable, sino que las pasaba a otro encargado. Y, por lo tanto, la posibilidad de cumplir con la extinción de la relación mediante el traspaso de los datos al nuevo encargado. Por otro lado, la posibilidad de conservar los datos bloqueados para garantizar una eventual responsabilidad del encargado resultará fundamental en sectores, como el del asesoramiento fiscal y laboral, en los que la tarea del encargado tiene trascendencia más allá del propio tratamiento de los datos.

Por último, y como más adelante se subraya, el estatuto del encargado debe completarse con las previsiones que en materia de seguridad existen en el Título VIII.

3.7. FICHEROS ESPECÍFICOS

El Título IV del RDLOPD regula en dos capítulos diferenciados los ficheros de información sobre solvencia patrimonial y crédito y los tratamientos para actividades de publicidad y prospección comercial. Se trata de ficheros particularmente sensibles desde dos puntos de vista.

En primer lugar, desde la perspectiva de su complejidad estructural tanto en lo concerniente a las fuentes origen de los datos —siempre o casi siempre se trata de terceros ajenos al titular de los datos— como por lo que se refiere a los agentes en juego con un conglomerado de responsables del fichero, responsables del tratamiento y encargados. Eso obliga a un rigor particular en lo concerniente al principio de calidad y a garantizar el ejercicio de los derechos.

Por otro lado son ficheros con una importante proyección social. Desde el punto de vista del sistema económico juegan un papel estratégico y, en lo concerniente a la percepción de las personas, pueden considerarse como recursos o bien muy útiles, o bien extremadamente molestos [37]. En este sen-

37. En este sentido, los responsables políticos del Ministerio de Justicia han subrayado en distintas declaraciones públicas la importancia de esta regulación. Véase <http://canarias24horas.com/index.php/2008022845941/tecnologia/el-secretario-de-estado-de-justicia-defiende-la-perfeccion-en-la-proteccion-de-datos.html>.

tido, se trata de ficheros que dan lugar a mucha conflictividad y cuyo uso provoca con cierta frecuencia la interposición de reclamaciones y la exigencia de indemnizaciones por daños [38].

3.7.1. Solvencia

La regulación en esta materia ha respondido a objetivos muy claros. Primero trata de garantizar a toda costa el principio de calidad de los datos. Y lo hace precisando un concepto que probablemente será muy discutido, el de deuda, al fijar como requisito el que dicha deuda no haya sido objeto de contradicción alguna, ni haya sido discutida o reclamada procesal o arbitralmente.

> *«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».*

Por lo tanto, la deuda además de ser cierta, vencida y exigible, si es objeto de discusión no podrá ser incluida en el fichero. A continuación se incide en los deberes del acreedor, fijando el propio artículo 38 del RDLOPD un conjunto de obligaciones relativas a la conservación de la documentación, a las condiciones en las que el responsable debe facilitar la información al titular de los datos y por último a la conservación de la información en los ficheros.

---

38. GRIMALT SERVERA, Pedro: *La responsabilidad civil en el tratamiento automatizado de datos personales*, Comares, Granada, 1999.

Por último se diseña todo un circuito para el ejercicio de los derechos que tiene como objeto principal que el titular de los datos, con independencia de por dónde acceda al sistema, acabe pudiendo obtener información. Y si no es información directa respeto de sus datos sí respecto de quien los trata, consulta o proporciona.

3.7.2. Publicidad

En el ámbito de la publicidad se ha tratado de delimitar con precisión la compleja trama de relaciones que se dan cuando se encarga una campaña publicitaria. Para ello era necesario establecer criterios que permitan determinar quién tiene la condición de responsable del fichero, la de responsable del tratamiento y la de encargado [39]. Ahí será determinante el concepto de parámetros de identificación:

> *«Artículo 46. Tratamiento de datos en campañas publicitarias.*
>
> (…)
>
> *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 responsables del tratamiento.*
>
> *c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.*

---

39. Sobre la diferencia entre responsable del fichero y del tratamiento véase la STS de 5 de junio de 2004. Disponible en <https://212.170.242.196/portalweb/canaldocumentacion/sentencias/tribunal_supremo/common/pdfs/Sentencia-del-Tribunal-Supremo-05-06-2004.pdf>.

(…)

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».*

Por otro lado, se regulan también en el artículo 47 del RDLOPD los cruces de datos tratando de corregir conductas tendentes a cruzar indiscriminadamente, y sin conocimiento del titular, datos contenidos en ficheros de diferentes responsables. Postreramente el Reglamento alumbra el nacimiento, jurídicamente hablando, de los ficheros de exclusión, o ficheros Robinsón, que serán propios de la organización, sectoriales o generales [40].

3.8. MEDIDAS DE SEGURIDAD

Para finalizar, la última cuestión destacable del Reglamento es la regulación en el Título VIII de las medidas de seguridad. En esta materia, y de manera muy resumida, procede destacar algunas de las opciones del regulador.

En primer lugar, en lo concerniente a la determinación de los niveles de seguridad se incorporan nuevos ficheros. Así, según el artículo 81 se incorporan al nivel medio ficheros propios de la Seguridad Social y de mutuas de accidentes profesionales. Se trata de ficheros respecto de los que, como antes ocurriera con los de Hacienda, se piensa que pueden aportar información personal valiosa merecedora de protección. Por otro lado, se incorporan también, con el añadido de contar con un registro de usuarios de nivel alto, los ficheros de las operadoras de comunicaciones en lo concerniente a la conservación de datos de tráfico en las comunicaciones. La razón de ello se debe a que con la trasposición de la Directiva sobre conservación de datos

40. Informe 514/2006. Creación de listas de exclusión. Disponible en <https://212.170.242.196/portalweb/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2006-0514_Creacion-de-listas-de-exclusion.pdf>.

de tráfico en las comunicaciones estos datos poseen un valor relevante para la seguridad pública [41].

Por otro lado se considerará de nivel alto todo fichero que contenga datos de violencia de género, cuestión lógica dado el valor íntimo de esta información y de su proyección sobre la seguridad de las personas.

Un elemento determinante en la fijación del nivel de seguridad viene dado por una nueva percepción del regulador. Ya no es relevante, o al menos no de manera exclusiva, la naturaleza objetiva del dato. De esta manera, deberá decaer la habitual confusión entre el concepto de dato especialmente protegido del artículo 7 de la LOPD, categoría a la que comenté se denomina como dato sensible y sobre todo como dato de nivel alto, en una evidente confusión de planos normativos. En estos momentos debe tenerse en cuenta la finalidad del tratamiento, la obligatoriedad para el responsable del mismo y el contenido informativo objetivo de los datos. De ahí que se regulen excepciones en el artículo 81 que permiten aplicar el nivel básico:

«5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

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

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la sim-

41. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

ple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos» [42].

La segunda característica del RDLOPD en esta materia parte de la flexibilidad organizativa. Para ello se prevé la delegación de funciones, el nombramiento de múltiples responsables de seguridad, una cierta libertad en la confección del documento de seguridad e incluso en la posible delegación de su llevanza en el encargado.

Por otro lado, el regulador ha tratado de precisar aspectos que tienen que ver con las necesidades emergentes de las organizaciones en materia de seguridad. Ahí se ahonda en la regulación de las relaciones con los encargados, se tienen en cuenta los riesgos para la seguridad de tareas que si bien no suponen acceso a datos pueden comportar riesgos físicos, y se contemplan las medidas de seguridad para dispositivos portátiles y redes inalámbricas.

Finalmente, se regulan las medidas de seguridad para ficheros no automatizados ofreciéndose un conjunto de criterios, realmente muy básicos, que deberían constituir el mínimo exigible a las organizaciones.

4. BREVE CONCLUSIÓN

La redacción del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RDLOPD) ha sido todo un reto de casi tres años para el regulador. Afronta una realidad compleja que se proyecta sobre casi todos los sectores del Ordenamiento. Ciertamente, como toda obra humana, contendrá errores y omisiones que el tiempo y su aplicación irán ajustando y corrigiendo. En cualquier caso era una norma muy necesaria que dará seguridad jurídica y estabilidad a todo el sistema.

---

42. Para una aplicación precisa de las excepciones consúltese la documentación de la I Sesión Anual Abierta de la AEPD. Disponible en <https://212.170.242.196/portalweb/jornadas/1_sesion_abierta/index-ides-idphp.php>.